

Lokale Netze

Die Technik für das 21. Jahrhundert

Andreas Zenk

Lokale Netze

Die Technik für das 21. Jahrhundert

Technologien, Konzepte, Praxis
6., revidierte und erweiterte Auflage



An imprint of Pearson Education

München • Bosten • San Francisco • Harlow, England
Don Mills, Ontario • Sydney • Mexico City
Madrid • Amsterdam

Die Deutsche Bibliothek - CIP-Einheitsaufnahme

Zenk, Andreas

Lokale Netze : Technologien, Konzepte, Einsatz ; Ethernet und
Gigabit Ethernet, NetWare 5 und Windows 2000 / Andreas Zenk. - 6.,
erw. und verb. Aufl. - München : Addison-Wesley-Longman, 1999
(Net.com)
ISBN 3-8273-1592-1
Buch. - 2000

Die Informationen in diesem Produkt werden ohne Rücksicht auf einen eventuellen Patentschutz veröffentlicht. Warennamen werden ohne Gewährleistung der freien Verwendbarkeit benutzt. Bei der Zusammenstellung von Texten und Abbildungen wurde mit größter Sorgfalt vorgegangen. Trotzdem können Fehler nicht vollständig ausgeschlossen werden. Verlag, Herausgeber und Autoren können für fehlerhafte Angaben und deren Folgen weder eine juristische Verantwortung noch irgendeine Haftung übernehmen. Für Verbesserungsvorschläge und Hinweise auf Fehler sind Verlag und Herausgeber dankbar.

Alle Rechte vorbehalten, auch die der fotomechanischen Wiedergabe und der Speicherung in elektronischen Medien. Die gewerbliche Nutzung der in diesem Produkt gezeigten Modelle und Arbeiten ist nicht zulässig.

Falls alle Hardware- und Softwarebezeichnungen, die in diesem Buch erwähnt werden, sind gleichzeitig auch eingetragene Warenzeichen oder sollten als solche betrachtet werden.

Umwelthinweis:

Dieses Buch wurde auf chlorfrei gebleichtem Papier gedruckt.

Die Einschrumpffolie – zum Schutz vor Verschmutzung – ist aus umweltfreundlichem und recyclingfähigem PE-Material.

10 9 8 7 6 5 4 3 2 1

03 02 01 00

ISBN 3-8273-1592-1

© 2000 Addison Wesley Longman Verlag,
ein Imprint der Pearson Education Deutschland GmbH
Martin-Kollar-Straße 10–12, D-81829 München/Germany
Alle Rechte vorbehalten
Einbandgestaltung: atelier für gestaltung, niesner & huber, Wuppertal
Lektorat: Rolf Pakendorf, rpakendorf@pearson.de
Korrektorat: Margret Neuhoﬀ, München
Herstellung: Anja Zygalakis; azygalakis@pearson.de
Satz: Reemers EDV-Satz, Krefeld
Druck und Verarbeitung: Bercker Graphischer Betrieb, Kevelaer
Printed in Germany

*Meinem Sohn Kai Georg, der zwar noch nicht weiß,
was Netzwerke sind, aber bereits bei einigen
Passagen zusehen durfte – früh übt sich.*

Inhaltsverzeichnis

Vorwort	19
Einleitung	23
1 Geschichtlicher Überblick	31
2 Definitionsgrundlagen des Lokalen Netzwerks	37
3 Kenndaten Lokaler Netzwerke	59
3.1 Topologische Strukturen Lokaler Netze	59
3.1.1 Sterntopologie	60
3.1.2 Bustopologie	63
3.1.3 Ringtopologie	64
3.2 Übertragungsmedien	67
3.3 Übertragungstechnologie (Basisband versus Breitband)	72
3.4 Zugriffsverfahren in Lokalen Netzen	74
3.4.1 CSMA/CD-Zugriffsverfahren (IEEE 802.3)	75
3.4.2 Token-Passing-Zugriffsverfahren (IEEE 802.5)	78
3.4.3 Token-Bus-Zugriffsverfahren (Token-Ring auf Bussystemen – IEEE 802.4)	83
4 Netzwerkaufbau und Netzwerktopologien	87
4.1 Ethernet-LANs	90
4.1.1 Thick-Ethernet	92
4.1.2 Thin-Ethernet	101
4.1.3 Twisted-Pair-Ethernet	103
4.2 Token-Ring-LANs	110
4.2.1 IBM-Token-Ring-Netzwerk	111
4.3 Fast Ethernet LANs	131
4.3.1 Die Technologie hinter Fast Ethernet	134
4.3.2 Base-T-Regeln zum Topologieaufbau	138
4.4 FDDI-LANs	140
4.5 100VG-AnyLAN von HP	150
4.6 ATM – Asynchronous Transfer Mode	159
4.6.1 ATM-Zellen – Aufbau und Funktion	161
4.6.2 ATM-Netzwerke	162
4.6.3 ATM im Referenzmodell	163
4.6.4 ATM-LAN-Emulation	167
4.7 Gigabit Ethernet	169
4.7.1 Ethernet – die dominierende LAN-Technik	170
4.7.2 Ziele und Gründe für Gigabit Ethernet	171

Inhaltsverzeichnis

4.7.3	Technologische Aspekte	173
4.7.4	Einsatzbereich für Gigabit Ethernet	182
4.7.5	Gigabit-Ethernet-Migration	185
4.8	High-Speed-Token-Ring (HSTR)	186
4.8.1	Switching und Workgroup-Segmentierung	189
4.8.2	TokenPipe und Multi-Link	191
4.8.3	Standards und Status (HSTR)	193
5	Netzwerkkonzeption	199
5.1	Funktion und Aufbau von Hubs	215
5.2	Verkabelung der Zukunft und Vorschriften	218
5.2.1	Physikalische Grundlagen der heute verwendeten Datenkabel	218
5.2.2	Prüfbedingungen	220
5.2.3	Übertragungseigenschaften	221
5.2.4	Elektromagnetische Verträglichkeit	221
5.2.5	Level-5-Kabel versus Kategorie-5-Kabel	222
5.2.6	Aktuelle Normen und deren Aussage	224
5.2.7	Zukunftssichere Verkabelung	230
5.3	Strukturierte Verkabelung – das ist zu beachten	231
5.3.1	Mögliche Fehlerquellen bei der Verlegung	232
5.3.2	Typische Probleme einer strukturierten Verkabelung	235
5.4	Was ist dran an den neuen Kategorien?	238
6	Netzwerkmanagement	243
6.1	Anforderungen an das Netzwerkmanagement	248
6.1.1	Fault-Management	249
6.1.2	Configuration-Management	250
6.1.3	Performance-Management	251
6.1.4	Accounting-Management	253
6.1.5	Security-Management	254
6.2	Aufbau von Netzwerkmanagement-Systemen	255
6.3	SNMP-Netzwerkmanagement	257
6.3.1	SNMP-Management-Information-Base	258
6.3.2	Remote Network Monitoring (RMON)	260
6.4	ManageWise	260
6.4.1	Netzwerkmanagement	265
6.4.2	Management von Workstations	278
6.5	Snap-in-Module anderer Hersteller	284
7	Aufgaben Lokaler Netzwerke	287
7.1	Nachrichtenaustausch	288
7.2	Zugriff auf zentrale Betriebsmittel	288

Inhaltsverzeichnis

7.3	Zugriff auf die Verarbeitungskapazität anderer Rechner	289
7.4	Zugriff auf zentrale Datenbestände	289
8	Kommunikationsgrundlagen	293
8.1	Synchronisationsverfahren	294
8.1.1	Asynchrone Datenübertragung	295
8.1.2	Synchrone Datenübertragung	296
8.2	Verbindungslose und verbindungsorientierte Kommunikation	298
8.2.1	Verbindungslose Kommunikation	299
8.2.2	Verbindungsorientierte Kommunikation	299
8.3	Kommunikationsprotokolle	301
9	Das ISO-Schichtenmodell der offenen Kommunikation	303
9.1	Prinzip des Schichtenmodells	303
9.2	Die Schichten des ISO-OSI-Modells	306
9.2.1	Physical Layer (Bitübertragungsschicht, physikalische Schicht)	311
9.2.2	Link Layer (Sicherungsschicht, Verbindungsschicht)	312
9.2.3	Network Layer (Netzwerkschicht)	313
9.2.4	Transport Layer (Transportschicht)	315
9.2.5	Session Layer (Sitzungsschicht)	316
9.2.6	Presentation Layer (Präsentationsschicht)	316
9.2.7	Application Layer (Anwendungsschicht)	317
9.3	TCP/IP – ein universelles Protokoll	321
10	Internetworking	329
10.1	Repeater	330
10.2	Bridge	331
10.3	Router	338
10.4	Gateway	343
10.5	Layer-2-Switch	348
10.6	Layer-3-Switch	351
11	Rechnernetze – Basis der Kommunikation	355
11.1	Die Einteilung von Rechnernetzen	356
11.2	Öffentliche Datenkommunikationseinrichtungen	357
11.2.1	Netze der Telekom	358
11.2.2	Die Dienste der Telekom	361
11.2.3	Der Weg zum ISDN-Netz	385
11.3	Metropolitan Area Network	409
11.3.1	Der DQDB-Standard	412
11.4	Die Zukunft der Breitbandkommunikation	419
11.4.1	IDN Plus – die Netzinfrastruktur von morgen	419

Inhaltsverzeichnis

11.4.2	Datex-M	422
11.4.3	ATM und Breitband-ISDN	426
11.5	Arcor – Was wird angeboten?	429
11.5.1	Frame-Relay-Service	430
11.5.2	X.25-Service	430
11.5.3	LAN-Connect-Service	431
11.5.4	Internet-Access-Service	432
12	Lokale Netzwerke im PC-Bereich	435
12.1	Auswahlkriterien für LANs	436
12.1.1	Die Erstellung eines Kriterienkataloges	436
12.1.2	Entwicklung eines Leistungsmeßverfahrens	446
12.1.3	Bestimmung der Datentransferrate für LANs	448
12.2	Konzeption und Realisierung eines LAN	449
12.3	Komponenten eines PC-Netzwerks	452
12.3.1	Das Transportsystem	452
12.3.2	Der Server	454
12.3.3	Die Peripherie am Server bzw. direkt im Netzwerk	455
12.3.4	Das Gateway	460
12.3.5	Bridge und Router	461
12.3.6	Arbeitsplatzrechner	461
12.3.7	Netzwerkdrucker	464
12.3.8	Streamer	466
12.3.9	FireWall-System	468
12.4	Die Phasen der Netzwerkinstallation	468
12.5	Gegenüberstellung von LAN und MDT	474
12.5.1	Der Einsatz des PC als Arbeitsplatzrechner	478
12.5.2	Verteilte und zentrale Datenverarbeitung	481
12.5.3	Die Anwendungssoftware	483
12.5.4	Integration von LANs in die Minicomputer- und Mainframe-Welt	484
12.5.5	Ausdehnung des PC zum multifunktionalen Arbeitsplatz	485
13	Die Entwicklungsgeschichte von Novell	489
13.1	Die wichtigsten Entwicklungsphasen von Novell	492
13.2	Ein strategischer Überblick	500
13.2.1	Der LAN-Markt	501
13.2.2	Die fünf Meilensteine von Novell	505
13.3	Die Server-Plattform für NetWare	507
13.4	Global-Network-Strategie	511
13.5	Internet Services	519
13.6	Open Solutions Architecture	521

Inhaltsverzeichnis

14	Netzwerkbetriebssysteme	529
14.1	Betriebssystemarchitektur	529
14.2	Die wichtigsten Anforderungen an Netzwerkbetriebssysteme	532
14.2.1	Leistungsfähigkeit	533
14.2.2	Zuverlässigkeit	533
14.2.3	Sicherheit	534
14.2.4	Workstation-Unterstützung	534
14.2.5	Standards	535
14.3	Das Client-Server-Prinzip	539
14.3.1	Lokale Netze mit Single-User-Anwendungen	539
14.3.2	File-Sharing: Lokale Netze mit netzwerkfähiger Software	540
14.3.3	Processor-Sharing: Lokale Netze mit Einsatz von netzwerkfähiger Software und Unterstützung des Client- Server-Modells	540
14.4	Die Server-Strategie von Novell	544
14.5	Multiprozessorfähigkeit	546
15	Novell NetWare 3.2	549
15.1	Allgemeiner Überblick über Novell NetWare 3.2	552
15.2	Übertragungseinrichtungen von Novell NetWare 3.2	553
15.3	NetWare 3.2 – eine offene Systemarchitektur	557
15.4	Leistungskomponenten von Novell NetWare 3.2	561
15.4.1	Grundlegende Eigenschaften	562
15.4.2	Mögliche Engpässe bezüglich Geschwindigkeit und Leistung innerhalb eines LAN	562
15.5	Der Betriebssystemkern (Nukleus)	563
15.5.1	Ablauf der Kommunikation zwischen File-Server und Workstation	564
15.5.2	Die Funktionsweise der Shell	565
15.6	Hauptspeichervoraussetzung	567
15.7	Dynamische Speicherkonfiguration	569
15.7.1	Nonreturnable Memory	570
15.7.2	Returnable Memory	571
15.8	Unterstützung der Netzwerkkarten	572
15.9	Verbesserte Plattenkanalausnutzung	574
15.10	Festplatten- und Volume-Verwaltung	575
15.10.1	NetWare Partitions	576
15.10.2	Volumes unter NetWare 3.2	576
15.10.3	Disk-I/O	577
15.10.4	Disk Allocation Blocks	579
15.10.5	File Allocation Tables (FATs)	580

Inhaltsverzeichnis

15.10.6	Turbo File Allocation Table (Turbo FAT)	581
15.10.7	Theoretische Hauptspeicher- und Plattenkapazität	583
15.10.8	Directory-Hashing in Kombination mit Directory-Caching	584
15.10.9	File-Caching unter NetWare 3.2	586
15.10.10	Optimierung der Plattenzugriffe durch Elevator-Seeking	587
15.10.11	Einsatz von mehreren Plattenkanälen	589
15.11	Dateien und Directories unter NetWare 3.2	589
15.11.1	Directory-Tabellen	589
15.11.2	Multiple Name Space Support	590
15.12	Sparse Files	592
15.13	Salvageable Dateien (wiederherstellbare Dateien)	593
15.14	Datensicherheit unter Novell NetWare 3.2	595
15.14.1	Die Bindery – zentrale Sicherheitseinrichtung	596
15.14.2	Sicherheitsgruppen und Äquivalenzdefinitionen	601
15.15	Die Accounting-Dienste von NetWare 3.2	603
15.15.1	Property ACCOUNT_SERVERS	604
15.15.2	Property ACCOUNT_BALANCE	604
15.15.3	Property ACCOUNT_HOLDS	604
15.16	Die Login-Sicherheit	606
15.16.1	Benutzername	606
15.17	Die Rechtesicherheit	612
15.18	File-Server-Sicherheit	618
15.19	Das Open Data-Link Interface	619
15.19.1	Paketübertragung	621
15.19.2	MLID Layer	622
15.19.3	Link Support Layer (LSL)	622
15.19.4	Protocol-ID-Information	623
15.19.5	NetWare 3.2 Streams Interface	625
15.20	NetWare Loadable Modules (NLMs)	629
15.21	Neuerungen von NetWare 3.2	630
16	Novell NetWare, das fehlertolerante System	639
16.1	SFT Level I	640
16.1.1	Das Kontrolllesen	640
16.1.2	Der Hot-Fix-Mechanismus	640
16.1.3	Redundante Dateisystemkomponenten	641
16.1.4	UPS-Monitoring	641
16.2	SFT Level II	642
16.2.1	Disk-Mirroring	642
16.2.2	Disk-Duplexing	643
16.2.3	Raid-Technologien	644
16.2.4	Hot Fix II	646
16.2.5	Split Seeks beim Lesen	646

Inhaltsverzeichnis

16.2.6	Das TTS-System	647
16.3	Das UPS-Monitoring	650
16.4	SFT Level III	651
17	Benutzeroberfläche von NetWare 3.2	653
17.1	Commandline-Utilities	653
17.2	Supervisor-Utilities	657
17.3	Menü-Utilities	658
17.3.1	Das Session-Menü	659
17.3.2	Das Filer-Menü	659
17.3.3	Das Dspace-Menü	660
17.3.4	Das Salvage-Menü	661
17.3.5	Das Volinfo-Menü	661
17.3.6	Das Syscon-Menü	661
17.3.7	Das Pconsole-Menü	663
17.3.8	Das Printcon-Menü	664
17.3.9	Das Printdef-Menü	665
17.3.10	Das Fconsole-Menü	666
17.3.11	Das Colorpal-Menü	666
17.3.12	Das NetWare-Menüprogramm	666
17.4	Consolen-Befehle	668
17.5	Das grafische SYSCON	676
18	Novell NetWare SFT III	679
18.1	Produktübersicht	682
18.1.1	Komponenten von SFT III	684
18.1.2	Server-Kommunikation	686
18.1.3	Dual-Prozessor-Unterstützung (Asymmetrisches Multiprocessing)	688
18.2	System Management	689
19	Novell NetWare 4.2	693
19.1	Heterogener Workstation-Support	695
19.2	Performance und Kapazität	696
19.3	Zuverlässigkeit und Sicherheit	696
19.4	Management	698
19.5	Connectivity	698
19.6	Memory Protection und Memory Management	700
19.7	Verbessertes Dateisystem	702
19.8	Verbessertes Sicherheitssystem und Auditing	705
19.9	Erweiterte Client-Dienste	708
19.9.1	Verbesserte DOS-Client-Software	708
19.9.2	NetWare Client 32	712
19.9.3	Windows- und OS/2-Unterstützung	714
19.9.4	Erweiterte Utilities	716

Inhaltsverzeichnis

19.10	Network Auditing	717
19.11	Verbesserte Druckdienste	718
19.12	National Language Support	719
19.13	Dokumentation	720
19.14	Novell Directory Services	721
19.15	Verwaltung der Novell-Directory-Services-Datenbank	734
19.16	Directory-Services-Sicherheit	743
19.17	Security Management	749
19.18	Connectivity	750
19.19	Skalierbarkeit	756
19.20	Print-Services	757
19.21	Sonstige Neuerungen für das Netzwerk- betriebsystem	757
19.21.1	Installation	763
19.21.2	Graphical User Interface	764
19.22	Produktvoraussetzungen	766
19.23	Workstation-Befehle	767
19.24	Neue und geänderte Menüsystem-Befehle	770
19.25	Workstation-Unterstützung	771
19.26	Neue Konsolen-Befehle	772
19.27	Neue NLMs	773
19.28	Änderungen im Rechtesystem	773
19.29	intraNetWare for Small Business 4.11	776
20	NetWare 5	781
20.1	Betriebsystem	781
20.1.1	NetWare 5 Kernel	782
20.1.2	Speicherschutz	785
20.1.3	Virtueller Speicher	789
20.1.4	Logische Speicheradressierung	790
20.1.5	ConsoleOne	791
20.1.6	Jahr-2000-Fähigkeit	793
20.1.7	Merced-Prozessor-Unterstützung	793
20.1.8	Hot Plug PCI	793
20.1.9	I2O	794
20.2	Novell Directory Services (NDS)	794
20.2.1	Transitive Synchronisation	794
20.2.2	Management gezielt verteilen	795
20.2.3	Catalog Services	795
20.2.4	LDAP	796
20.2.5	NDS Manager	796
20.2.6	WAN Traffic Manager (WTM)	797
20.2.7	DSDIAG (DS Diagnostics)	797
20.3	Netzwerkdienste	798
20.3.1	Native IP	798

Inhaltsverzeichnis

20.3.2	DNS/DHCP	802
20.3.3	Novell Storage Services (NSS)	804
20.3.4	Novell Distributed Print Services (NDPS)	806
20.3.5	Z.E.N.works Starter Pack	807
20.4	Erweiterte Sicherheit	809
20.4.1	Kryptografische Dienste	810
20.4.2	Secure Authentication Services (SAS)	810
20.4.3	Public Key Infrastructure Services (PKIS)	810
20.5	Installation und Upgrade	811
20.6	Java-Unterstützung	813
20.7	Third-Party Add-ons	815
20.8	Cluster-Technologie	815
21	NDS für andere Plattformen	821
21.1	NDS for NT	821
21.1.1	Arbeitsweise von NDS for NT	823
21.1.2	Verwendung von Paßwörtern unter NDS for NT	825
21.1.3	Security IDs unter NDS for NT	827
21.1.4	Installation NDS for NT	827
21.1.5	Management Tools für NDS for NT	832
21.1.6	Deinstallation von NDS for NT	834
21.2	NDS for Solaris	835
21.2.1	Vorteile durch NDS for Solaris	836
21.2.2	Arbeitsweise von NDS for Solaris	838
21.2.3	Einrichtung von NDS for Solaris	840
21.2.4	Verwaltung der Benutzer-Accounts	840
21.2.5	Zusammenspiel mit anderen Novell-Produkten	841
21.2.6	NDS v8	842
21.2.7	NDS-v8-Verbesserungen	842
22	Windows NT	849
22.1	Windows NT Features	850
22.1.1	Erweiterbarkeit	852
22.1.2	Portierbarkeit	853
22.1.3	Zuverlässigkeit	854
22.1.4	Kompatibilität	854
22.1.5	Leistungsfähigkeit	855
22.2	Systemübersicht	856
22.2.1	Client/Server-Modell	857
22.2.2	Objektmodell	861
22.2.3	Symmetrisches Multiprocessing	862
22.3	Die Struktur von Windows NT	864
22.3.1	Protected Subsystem	864
22.3.2	Executive	866
22.4	Die wichtigsten Eigenschaften von Windows NT	870

Inhaltsverzeichnis

22.4.1	Der Logon-Prozeß	870
22.4.2	Environment-Subsysteme	872
22.4.3	Native Service	873
22.4.4	Objekte	873
22.4.5	Virtueller Speicher	874
22.4.6	I/O- und Dateisysteme	875
22.5	Die Netzwerkfunktionalitäten von Windows NT	876
22.5.1	Eingebaute Netzwerkkomponenten	879
22.5.2	Server	879
22.5.3	Transport-Protokolle	881
22.6	Der Einsatz der Windows-NT-Netzwerkfunktionen	882
22.7	Andere Betriebssysteme und deren Einsatz im Netz mit Windows NT	887
22.8	Sicherheitsmechanismen von Windows NT	888
22.8.1	Paßwörter unter Windows NT	893
22.8.2	Default Accounts	894
22.8.3	Zugriffsrechte für Directories und Dateien	898
22.9	Plattenverwaltung unter Windows NT	903
23	Windows NT Server	907
23.1	Windows NT Server – ein Überblick	908
23.2	Windows NT und Windows NT Server im Vergleich	913
23.3	Netzwerksicherheit	915
23.3.1	Domains und Trusted Domains	915
23.3.2	Modelle für Domains	920
23.3.3	Login unter Windows NT Server	924
23.3.4	Benutzer und Benutzergruppen	926
23.4	Verwalten der Benutzeraktivitäten	932
23.5	Verwalten der Benutzerumgebung	934
23.6	Verwalten von Netzwerkdateien	938
23.6.1	Auswahl des Dateisystems	939
23.6.2	Freigabe von Dateien/Directories für Anwender im Netzwerk	941
23.6.3	Zugriffsberechtigungen für das NTFS-Dateisystem	943
23.6.4	Zugriffsberechtigung beim Freigeben von Directories	945
23.6.5	Vergeben von Berechtigungen	946
23.6.6	Berechtigungen für FAT- und HPFS-Dateisysteme	947
23.6.7	Dateibesitzrecht	947
23.7	Drucken im Netzwerk unter Windows NT Server	948
23.7.1	Zurückstellen von Druckaufträgen	950
23.7.2	Prioritäten für Drucker vergeben	950
23.7.3	Einsatz von Print-Pools	950
23.7.4	Zugriff auf Drucker steuern	951
23.8	Fehlertoleranz	952
23.8.1	RAID-Level-Systeme	952

Inhaltsverzeichnis

23.8.2	Unterbrechungsfreie Stromversorgung	954
23.9	Remote Access Services (RAS)	956
23.10	Services for Macintosh	957
23.11	TCP/IP-Umgebung für Windows NT Server	961
23.12	NetWare-Einbindung	965
24	Windows 2000	967
24.1	Windows 2000 Management	968
24.1.1	Active Directory	969
24.1.2	Erweiterte Suchfunktionen	969
24.1.3	Dynamic DNS	970
24.1.4	Speicherverwaltung	970
24.1.5	Ordner »Eigene Dateien«	971
24.1.6	Backup-Dienstprogramm	971
24.1.7	Unterstützung des Distributed File System (DFS)	971
24.1.8	Microsoft Management Console (MMC)	972
24.1.9	Hardware-Assistent mit Gerätemanager	972
24.1.10	Windows Scripting Host (WSH)	973
24.1.11	Win32 Driver Model (WDM)	973
24.1.12	Plug&Play	973
24.2	Entwickeln und Verwenden von Anwendungen	974
24.2.1	DCOM	974
24.2.2	Microsoft Transaction Server	974
24.2.3	Microsoft Message Queue Server	974
24.2.4	Internet Information Server	975
24.2.5	Index Server	975
24.2.6	Automatische Installation von Anwendungen	975
24.3	Skalierbarkeit und Verfügbarkeit	976
24.3.1	64-Bit-VLM	976
24.3.2	Microsoft Cluster Server	976
24.3.3	Intelligent Input/Output System	976
24.3.4	Kerberos-Authentifizierung	977
24.3.5	Certificate Server für öffentliche Schlüssel	977
24.4	Weitere Funktionen für Windows NT	977
24.5	Active Directories	979
24.5.1	Überblick des Active Directory	981
24.5.2	Änderungen im internen Aufbau	984
25	Internet/Intranet und Internet Security	989
25.1	Einrichten eines Internet-Anschlusses	994
25.2	FireWall-Systeme	998
25.2.1	Paketfilterung (Screening Router)	1000
25.2.2	Application-Level Gateway	1002
25.2.3	FireWall-Architekturen	1003

Inhaltsverzeichnis

25.3	Der Einsatz eines Intranet	1005
25.4	Der Einsatz von VPN	1008
26	Electronic-Mail-Systeme	1013
26.1	Der CCITT-X.400-Standard	1013
26.1.1	Das funktionale X.400-Modell	1015
26.1.2	Meldungsspeicher (Message Store, MS)	1016
26.1.3	X.400-Nachrichtenstruktur	1017
26.1.4	Namen und Adressen	1020
26.1.5	Verfügbare Dienste	1022
26.1.6	Zeichensätze	1023
26.1.7	Verwaltungsbereiche (Management Domains)	1024
26.1.8	Protokolle	1026
26.1.9	Sicherheitsmodell	1028
26.2	Das Simple Mail Transfer Protocol (SMTP)	1030
26.2.1	Das SMTP-Modell	1031
26.2.2	Adressierungsschema	1032
26.3	Multipurpose Internet Mail Extension (MIME)	1033
26.4	Application Programming Interfaces (APIs)	1034
26.4.1	Common Messaging Calls (CMC)	1035
26.4.2	Messaging Application Programming Interface (MAPI)	1035
26.4.3	Vendor Independent Messaging (VIM)	1037
26.4.4	Novell Standard Message Format (SMF)	1037
26.5	Sonstige Mailing-Systeme	1038
27	Die Grundlagen der Directory Services (Verzeichnisdienste)	1041
27.1	Der CCITT-X.500-Standard	1041
27.1.1	Das funktionale Modell	1042
27.1.2	Das Informationsmodell	1043
27.1.3	Dienste bzw. Operationen	1045
27.1.4	Verteiltes Verzeichnis	1047
27.1.5	Verwaltungsbereiche (Management Domains)	1049
27.1.6	Protokolle	1049
27.1.7	Sicherheitsmechanismen	1051
28	Die Jahr-2000-Problematik	1053
28.1	Jahr-2000-Fähigkeit bei Microsoft	1056
28.1.1	Windows 2000	1057
28.2	Jahr-2000-Fähigkeit bei Novell	1058
	Stichwortverzeichnis	1073

Vorwort

Ein Sprichwort besagt: »Es ist nichts beständiger als die Veränderung«. Dieses Sprichwort trifft auch für den Bereich der Netzwerktechnik zu, und zwar für alle damit verbundenen Bereiche. Es ist noch nicht lange her, da sprach man davon, daß mit einem Twisted-Pair-Kabel Datenraten von nicht mehr als 100 MHz (das entspricht einer Datenübertragungskapazität von 155 Mbit/s) erreicht werden können. Ebenso ging man davon aus, daß Fast Ethernet der Endpunkt in der Ethernet-Technologie wäre. In beiden Fällen hat man sich grundlegend geirrt. Auf Twisted-Pair-Kabeln können derzeit Datenraten von bis zu 1000 MHz erreicht werden, und das Fast Ethernet wurde innerhalb kürzester Zeit durch die Gigabit-Ethernet-Technologie ergänzt. Ähnliche Entwicklungen können auch auf dem Gebiet der aktiven Netzwerkkomponenten, der Netzwerkbetriebssysteme oder der Netzwerkkarten beobachtet werden. Das gleiche gilt natürlich auch für den PC-Bereich selbst – glaubte man vor kurzem noch, mit einem 266-MHz-Rechner hätte man eine sehr schnelle Maschine, dann wird man schnell eines besseren belehrt, wenn man die neuen 550- bzw. 600-MHz-Rechner sieht (zum Zeitpunkt der Erstellung dieses Buches). Wenn Sie das Buch lesen, sind diese Zahlen vielleicht auch nicht mehr ganz aktuell. Daran sehen Sie noch deutlicher, wie schnelllebig unsere Zeit heute ist.

In meinen Seminaren über Lokale Netzwerke weise ich immer darauf hin, daß die Neueinsteiger in diese Materie binnen kurzer Zeit viel Neues und »Unvorstellbares« lernen müssen. Am Anfang ist es sehr schwer, immer alles richtig auseinanderzuhalten. Man wirft Begriffe, Definitionen und Funktionsweisen durcheinander, denn es bedarf einer geraumen Zeit, bis man die Fülle der Informationen verarbeitet hat. Besonders auffällig ist dies, wenn man Messen besucht. Immer wenn man einen Messestand verläßt, hat man den Eindruck, genau jenes eben besichtigte Produkt gesucht zu haben. Dann geht man weiter, läßt sich alles erklären, verläßt den Messestand und denkt sich wiederum, daß dies genau das Produkt sei, das man brauche. Und so geht es weiter, bis man am Abend im Hotel oder zu Hause sitzt und sich plötzlich fragt: »Was brauche ich genau, wer hat jetzt eigentlich die besseren Komponenten, worin unterscheiden sich die einzelnen Hersteller? Etwa nur im Preis? Oder nur in bestimmten Funktionen?« Bei der richtigen Entscheidung wird Ihnen mein Buch helfen.

Vorwort

Ich habe bereits 1983 begonnen, mich nicht nur mit Netzwerken zu beschäftigen, sondern diese auch aufzubauen und zu betreiben. Die Auswahlmöglichkeiten waren zum damaligen Zeitpunkt noch nicht so groß, es gab nur eine Handvoll Hersteller und Anbieter. Auf diese Art und Weise hatte ich die Möglichkeit, die gesamte Entwicklung nicht nur mitzuerleben, sondern auch einen »sanften Übergang« für die neuen Komponenten zu schaffen. Mit jedem Jahr konnte aber auch ich feststellen, daß immer höhere Aufwendungen betrieben werden mußten, um den aktuellen Wissensstand halten zu können. Das Ganze wird natürlich einfacher, wenn der Grundstock steht. Und genau dieses Ziel wird mit diesem Buch verfolgt: Ihnen als Leser, Einsteiger bzw. Netzwerkverwalter zum einen die Basis zu schaffen, um zu erkennen und zu wissen, was es mit der Netzwerktechnik überhaupt auf sich hat, und zum anderen soll den bereits versierten Lesern aufgezeigt werden, was sich auf diesem Gebiet Neues ergeben hat, wie die zukünftigen Trends aussehen und wo die Haken und Ösen zu sehen sind.

Wie bei allen meinen Büchern habe ich es nicht versäumt, das Ganze mit den notwendigen praktischen Erfahrungen anzureichern, um Ihnen den größtmöglichen Nutzen zu bieten.

Ich habe Netzwerke konzipiert, die nur mit vier PCs ausgestattet sind, aber auch solche, die insgesamt 3000 PCs miteinander verbinden und eine Vielzahl von Servern, LAN-WAN-Verbindungen und andere Netzdienste integrieren. Man kann sich vorstellen, daß die Voraussetzungen für das kleine Netzwerk ganz anders aussehen als die für das große. Die Erfahrung, die ich im Lauf der Jahre sammeln konnte, ist in dieses Buch eingegangen und wird Ihnen bei der Planung und Verwaltung oder Ihrer Arbeit im Netzwerk zugute kommen, falls Sie »nur« ein Benutzer sein sollten.

Vergleicht man die vor Ihnen liegende Auflage dieses Buchs mit den fünf vorherigen, dann kann man sehen, wie schnell die Entwicklung im Bereich der Netzwerktechnologie ist. Innerhalb kürzester Zeit stehen Möglichkeiten und Mechanismen zur Verfügung, an die man vor einigen Monaten noch gar nicht zu denken wagte. Einer der Gründe dafür, daß ständig neue Produkte auf den Markt kommen, liegt darin, daß die Anforderungen an Netzwerke, an die Kommunikationstechnik und an das Netzwerksbetriebssystem immer größer werden. Als Autor eines solchen Buchs ist man gefordert, die richtigen Tendenzen zu erkennen und (in Buchform!) zu verarbeiten. Durch meine Tätigkeit im Bereich der Netzwerkplanung fällt mir das relativ leicht, da ich dort immer wieder gezwungen bin, zukünftige, technologische Entwicklungen zu erkennen und für den Kunden in der richtigen Form zu präsentieren.

Vorwort

Sie sollen mit diesem Buch einen Überblick darüber bekommen, welche Möglichkeiten beim Aufbau von Netzwerken zur Verfügung stehen. Außerdem werden Sie erfahren, welche Netzwerk Betriebssysteme die einzelnen Hersteller (Novell, Microsoft) anbieten, mit denen LANs und WANs aufgebaut werden können. Da es auch ganz neue Dienste gibt, die beim Einsatz von LANs interessant sind oder werden, erhalten Sie Informationen über Internet, Intranets, Fire-Walls-Systeme und vieles andere mehr.

Dem Verlag ist an dieser Stelle besonders zu danken, daß es möglich war, wenige Tage vor Drucklegung aktuelle Ergänzungen in das Buch zu integrieren. Damit werden auch meine Aussagen in diesem Buch bezüglich Schnellebigkeit im Bereich der Netzwerktechnik noch mehr untermauert.

Bei aller Sorgfalt kann es vorkommen, daß sich an der einen oder anderen Stelle versehentlich Fehler in die vorliegenden Ausführungen eingeschlichen haben. Das bitte ich zu entschuldigen. Für Anregungen zur Verbesserung dieses Buchs bin ich jederzeit dankbar.

An dieser Stelle möchte ich mich bei meiner Frau und Geschäftsführerin in unserem gemeinsamen Unternehmen bedanken. Durch ihre Ausdauer, Geduld und Unterstützung, durch Diskussionen und Anregungen bei der Auswahl und Gestaltung der einzelnen Kapitel hat sie wie immer erheblich zum Gelingen dieses Buchs beigetragen. Ihre langjährige Erfahrung auf dem Gebiet der Netzwerktechnologie und im Schulungs- und Beratungsbereich über Netzwerke ist in das Buch eingegangen.

Bedanken möchte ich mich an dieser Stelle auch bei meinen Mitarbeitern Herrn Günter Thiel und Herrn Florian Eck für die Unterstützung, den ersten bzw. zweiten Teil des Buches vollständig zu lesen, um weitere Unterstützung bei der Überarbeitung der 6. Auflage geben zu können. Für beide Herren eine sicherlich nicht ganz einfache Aufgabe.

Dem Verlag Addison-Wesley, insbesondere meinem Lektor Rolf Pakendorf, danke ich für die ausgezeichnete Zusammenarbeit und zügige Realisierung und Koordination dieses Buchs.

Dank gebührt auch den folgenden Firmen und Personen für die Bereitstellung der notwendigen Unterlagen und Produkte, auf die ich mich in diesem Buch stützen konnte: Herrn Krogull von der Firma Novell für das schnelle und automatische Zusenden neuer Produkte und Unterlagen, Herrn Hein von der Firma Bay Networks für die prompte Unterstützung bei neuen Produkten. Eigentlich müßte ich mich auch beim Internet bedanken, da notwendige Informationen

Vorwort

zum Teil am schnellsten dort zur Verfügung gestellt werden. Bei der Erstellung eines Buchs dieser Form stellte ich sehr schnell fest, welche Vorteile mit dem Internet verbunden sind – ein unverzichtbares Medium.

München, Oktober 1999

Andreas Zenk

Einleitung

Sie halten die inzwischen 6. Auflage dieses Buchs in den Händen. Jeder spricht vom Jahrtausendwechsel, der kurz bevorsteht. Man weiß nicht genau, mit welchen Überraschungen man am 1.1.2000 konfrontiert wird. Da es nicht mehr so lange dauert bis zu diesem Ereignis, stellt sich natürlich auch die Frage, was im Bereich der Netzwerktechnik in den nächsten Monaten zu erwarten ist bzw. wie die derzeitigen Entwicklungen weitergehen werden. Da es sich bei der Netzwerktechnik um revolutionäre Entwicklungen handelt, die sich zum Teil tagtäglich ergeben, soll Ihnen dieses Buch helfen, nicht nur die richtige Entscheidung über den Einsatz neuer Netzwerktechnologien zu treffen, sondern es soll Ihnen auch ein Überblick gegeben werden, welche Techniken heute und morgen wahrscheinlich zur Verfügung stehen: im LAN, WAN, bei Netzwerkbetriebssystemen und im gesamten Dienstebereich, der sich mit Netzwerk und Netzwerktechnik beschäftigt.

Wenn man täglich mit Netzwerken zu tun hat, dann stellt man fest, daß sich Neues getan hat; man nimmt dieses auf und macht seinen Job mit der neuen Technologie und den neuen Rahmenbedingungen. Ist man jedoch gezwungen, ein Buch wie das vorliegende in regelmäßigen Abständen auf den aktuellen Stand zu bringen, dann stellt man erst fest, wie gravierend zum Teil diese Änderungen sind und in welch kurzen Abständen sich diese Neuerungen am Markt durchsetzen. Man sollte nie davon ausgehen, daß man irgendwann einen Stand erreicht hat, der sich nicht mehr ändern wird; ebenso läßt sich ein gewisser Entwicklungsstand nicht über einen längeren Zeitraum einfrieren. Meist wird man durch äußere Einflüsse gezwungen, neue Techniken einzusetzen, auch wenn man dies zuerst nicht wollte.

Dieses Buch soll allen Entscheidungsträgern, zukünftigen Netzadministratoren, bereits tätigen Netzwerkadministratoren und allen, die sich für Netzwerke interessieren, Unterstützung bieten, das umfassende Gebiet der Netzwerktechnik besser abgrenzen zu können. Es werden aber nicht nur rein theoretische Konzepte und Lösungsansätze behandelt, Sie erhalten vielmehr Informationen aus der Praxis für die Praxis, z.B. wie Installationen durchzuführen sind etc. Schließlich stimmen Theorie und Praxis nicht immer überein. Es handelt sich bei dem vorliegenden Buch *nicht* um ein Installationshandbuch irgendeines Produkts. Ziel dieses Buchs ist es, einen umfassenden Überblick zu verschaffen.

Einleitung

Ich wünsche Ihnen bei der Lektüre viel Spaß und hoffe, alle für Sie interessanten Bereiche aus dem Gebiet der Netzwerktechnologie abgedeckt zu haben. Wenn Sie der Meinung sind, daß wichtige Aspekte fehlen, bin ich für jede Anregung dankbar, um dies dann in der nächsten Auflage aufgreifen zu können.

Sie sind nicht gezwungen, dieses Buch Kapitel für Kapitel der Reihe nach zu lesen. Es kann durchaus als Nachschlagewerk dienen, um auf spezielle Fragen die richtigen Antworten zu finden. Die folgenden kurzen Kapitelzusammenfassungen sollen Ihnen helfen, sich bei der Lektüre besser orientieren zu können.

- Kapitel 1** Dieses Kapitel vermittelt als Einstieg in das Thema einen kurzen geschichtlichen Überblick. Wer die Geschichte der EDV kennt – oder wen sie nicht interessiert –, kann dieses Kapitel einfach überspringen.
- Kapitel 2** In diesem Kapitel wird dargestellt, was überhaupt unter Netzwerken zu verstehen ist und durch welche Merkmale sich verschiedene Netzwerke voneinander unterscheiden.
- Kapitel 3** Dieses Kapitel zeigt, durch welche Kenndaten lokale Netze voneinander unterschieden werden können. Es geht dabei vor allem um die Restriktionen bei der Verkabelung und um das, was allgemein beim Aufbau der unterschiedlichen Netzwerke zu beachten ist. Es wird erklärt, worin sich die einzelnen Topologien voneinander unterscheiden, so daß Sie eine Grundlage für die späteren Ausführungen zu den Netzwerkkonzeptionen haben.
- Kapitel 4** Da beim Netzwerkaufbau und bei den Netzwerktopologien der einzelnen Hersteller sehr große Unterschiede bestehen, wird in diesem Kapitel jede Topologie in ihrer Struktur und ihrem Verhalten näher untersucht. Sie erfahren alles Wichtige über Ethernet, Fast Ethernet, Gigabit Ethernet, Token-Ring, FDDI, ATM und High Speed Token-Ring. Dies dient als Vorbereitung für das Kapitel 5, in dem es um die konzeptionellen Aspekte der Netzwerke geht.
- Kapitel 5** Kleinere Netze sind relativ einfach und unproblematisch zu konfigurieren. Anders sieht es bei großen und komplexen Netzwerken aus. Dieses Kapitel soll zeigen, wie beim Aufbau größerer Netzwerke vorgegangen werden kann, um flexible und zukunftssichere Strukturen zu erhalten, die jederzeit erweiterbar sind. Es werden dabei auch die Vorschriften beschrieben, die beim Aufbau einer zukünftigen Verkabelung berücksichtigt werden müssen. Ebenso erfahren Sie alles über die in Frage kommenden unterschiedlichen Kupfer-Kabeltypen (Cat5, Cat6, Cat7), Glasfaserkabel und die Vorschriften, die beim Einsatz und beim Verlegen dieser Kabel zu berücksichtigen sind. Ebenso wird darauf eingegangen, welche Fehler bei der Kabelverlegung gemacht werden können und worauf vor allem geachtet werden muß.

Einleitung

- Kapitel 6** Ab einer bestimmten Netzwerkgröße ist der Einsatz eines geeigneten Netzwerkmanagement-Systems unumgänglich. Dieses Kapitel soll Ihnen zeigen, worauf geachtet werden muß, um eine richtige Entscheidung treffen zu können. Dazu wird ein allgemeiner Überblick über den SNMP-Standard gegeben, und anschließend werden anhand von Novell ManageWise und dem NetWare Services Manager von Novell die wichtigsten Aspekte und Funktionen dargelegt, die von einer geeigneten Netzwerkmanagement-Software zu erwarten sind.
- Kapitel 7** Dieses Kapitel beschreibt, welche Hauptaufgaben ein Netzwerk hat und welche Gründe für eine bestimmte Lösung sprechen. Dabei wird auch beschrieben, worin die Vor- und Nachteile liegen, bestimmte Aufgaben der Datenverarbeitung in LANs durchzuführen.
- Kapitel 8** Grundlage der Netzwerktechnik ist Kommunikation. Dieser Abschnitt beschäftigt sich mit den allgemeinen Kommunikationsgrundlagen, so daß Sie die Spezifika der Rechner-Rechner-Kommunikation im Netz verstehen lernen.
- Kapitel 9** Dieser Abschnitt über das ISO-Schichtenmodell darf in keinem Buch über Netzwerke fehlen, da darauf sehr viele Standards aufsetzen bzw. darüber immer wieder neue Standards definiert werden. Dieses Kapitel soll in leicht verständlicher Weise darstellen, wie das ISO-Schichtenmodell aufgebaut ist, worin dieses Modell besteht und welche Zusammenhänge in diesem Modell existieren.
- Kapitel 10** Beim Aufbau größerer Netzwerke muß immer wieder die Entscheidung getroffen werden, wie Kopplungen zwischen Netzen durchgeführt werden sollen. In diesem Kapitel wird beschrieben, wann eine Bridge, ein Router, ein Brouter oder ein Gateway benötigt wird. Zudem erhalten Sie einen Einblick über den Aufbau und die Arbeitsweise von Switching-Systemen (Layer-2 und Layer-3). Außerdem wird dargestellt, wie diese einzelnen Systeme arbeiten, wo die Vor- und Nachteile liegen und wann welches Koppelement für welchen Zweck eingesetzt wird.
- Kapitel 11** Hier wird die Einteilung von Rechnernetzen dargestellt. Es geht vor allem auch um die Klassifikation von LANs, MANs und WANs sowie den Aufbau dieser Netzwerkgebilde. Ebenso wird gezeigt, welche Möglichkeiten die Deutsche Telekom AG (DTAG) und Arcor zur Verfügung stellen, um Remote-Netzwerkverbindungen zu realisieren, d.h. allgemeine Kopplungen von Netzwerken. Einen Schwerpunkt bilden dabei ISDN, Datex-Dienste etc. und alles weitere, was damit zusammenhängt. Schließlich werden die MAN-Technologie und die DQDB-Technik beschrieben.

Einleitung

- Kapitel 12** Dieses Kapitel beschäftigt sich mit der Erstellung von Auswahlkriterien für LANs, die Planung eines Kriterienkatalogs, die Erläuterung der einzelnen Kriterien und die Entwicklung eines einfachen Leistungsmeßverfahrens für LANs. Anschließend wird gezeigt, wie eine Konzeption und Realisierung von LANs durchgeführt werden kann. Dazu gehören die Darstellung der Komponenten für PC-Netzwerke, die Phasen der Netzwerkinstallation und schließlich ein Vergleich zwischen der Mittleren Datentechnik und der LAN-Technologie.
- Kapitel 13** Bei der LAN-Technologie kommt man um die Produkte von Novell nicht herum. Deshalb soll Ihnen in diesem Kapitel die Entwicklungsgeschichte von Novell aufgezeigt werden – sie ist exemplarisch für diesen Bereich. Sie können daraus ersehen, wie im Laufe einer über zehnjährigen Firmengeschichte die Netzwerktechniken Schritt für Schritt verfeinert worden sind. Diese Übersicht hilft Ihnen auch bei der Einordnung der weiteren Betriebssystemtechniken. In diesem Kapitel wird auch beschrieben, welche zukünftigen Trends zu erwarten sind; weitere und genauere Informationen erhalten Sie in den darauffolgenden Kapiteln.
- Kapitel 14** Diese Kapitel soll einen allgemeinen Überblick über Netzwerkbetriebssystem-Techniken vermitteln. Zudem wird gezeigt, welche Anforderungen an Netzwerkbetriebssysteme gestellt werden und wie diese erfüllt werden können. Sie erhalten zudem eine Einführung in die Client/Server-Architektur, die die Basis für alle zukünftigen Konzepte sein wird und Hauptbestandteil der Konzeption von Microsoft beim Aufbau des NT Servers oder auch des Mail Exchange Servers ist. Aber Client/Server-Architekturen werden auch von einer Vielzahl anderer Hersteller eingesetzt.
- Kapitel 15** Dieses Kapitel behandelt die Techniken und Konzepte von NetWare 3.2. Sie erfahren von den grundlegenden Strukturen und Funktionsweisen für NetWare 3.2 und bekommen einen Überblick über die wichtigsten Sicherheits- und Performance-Mechanismen. In diesem Kapitel werden auch Techniken beschrieben, die zum Teil für NetWare 4 und NetWare 5 Gültigkeit haben und in ähnlicher Form auch für Windows NT 4.0 und Windows 2000 zur Verfügung stehen.
- Kapitel 16** In diesem Kapitel werden die fehlertoleranten Konzepte von NetWare besprochen. Kapitel 15 und Kapitel 16 dienen auch zum Vergleich von NetWare 4 und NetWare 5 mit den älteren Konzepten von Novell.
- Kapitel 17** In diesem Kapitel wird Ihnen die Benutzeroberfläche von NetWare 3.2 vorgestellt, damit Sie einen Eindruck davon bekommen, wie sich ein Netzwerk in der Praxis darstellt.

Einleitung

- Kapitel 18** Ausfallsicherheit wird immer mehr gefordert. Novell bietet mit seiner SFT-III-Lösung eine Möglichkeit, sich gegen den Ausfall eines gesamten Servers abzusichern. Dieses Kapitel zeigt, wie dieses Konzept aussieht und welche Voraussetzungen geschaffen werden müssen.
- Kapitel 19** Unter NetWare 3.2 erfolgt die Verwaltung der Benutzer, Gruppen etc. zentral in der Bindery des Servers. In einer Multi-Server-Umgebung bedeutet dies einen größeren Aufwand für die Verwaltung. Deshalb wurde von Novell NetWare 4.2 entwickelt, bei der unter anderem die Verwaltung aller Netzwerkressourcen in der globalen, verteilten und replizierbaren NDS-Datenbank erfolgt. Daneben gibt es weitere Neuerungen und Verbesserungen, die intraNetWare 4.11 gravierend von NetWare 3.2 unterscheiden. In diesem Kapitel sollen deshalb alle diese Unterschiede und vor allem auch die wesentlichen Neuerungen im Detail beschrieben werden.
- Kapitel 20** Die neueste Entwicklung von Novell ist NetWare 5, die sich im Vergleich zu NetWare 4.2 nochmals durch eine Vielzahl von Neuerungen abhebt. So ist die NDS nach wie vor die zentrale Datenbank zur Verwaltung der gesamten Netzwerkressourcen. Hinzugekommen sind eine Vielzahl neuer Sicherheitsmechanismen, ein neues Dateisystem, ein Multiprozessor-Kernel, ein neuer Druckmechanismus und viele Dinge mehr. Ein großer Schritt erfolgte auch beim Protokollmechanismus. So ist IPX nicht mehr das Standardprotokoll (wird aber noch unterstützt), sondern IP. Das heißt, alle internen Mechanismen sind auf das IP-Protokoll abgestimmt worden. Für diese Protokollwelt sind deshalb zusätzliche Neuerungen eingeführt worden, so zum Beispiel DNS/DHCP, mit einer vollständigen Integration in die NDS oder auch Dynamic DNS (DDNS), um nur einige Beispiele zu nennen. Lesen Sie dieses Kapitel, und Sie wissen, mit welchen neuen Funktionen NetWare 5 aufwarten kann.
- Kapitel 21** Die NDS von Novell ist inzwischen nicht nur für das Netzwerkbetriebssystem NetWare verfügbar, sondern durch die Konzeption von Novell auch für andere Betriebssystem-Plattformen erhältlich. Um Ihnen einen Überblick darüber zu geben, wie die NDS unter Windows NT und Sun Solaris eingesetzt werden kann, beschreibt dieses Kapitel den Aufbau und den Einsatz der NDS für diese beiden Plattformen. Zudem erhalten Sie in diesem Kapitel einen Überblick darüber, wie die neue NDS v8 aufgebaut ist und welche Vorteile damit zukünftig verbunden sind.
- Kapitel 22** Die neue Betriebssystemplattform von Microsoft ist eindeutig Windows. Zur größten Plattform dieser Serie – neben Windows 95/98 – zählt Windows NT. Windows NT setzt neue Maßstäbe für Workstation-Betriebssysteme; Windows 95 und Windows 98 werden langfri-

Einleitung

stig gesehen in Windows NT überführt werden. Die eingebauten Netzwerkfunktionen, das neue Design und die darauf aufbauenden Konzepte sprechen für sich. Dieses Kapitel soll Ihnen einen Eindruck über die Leistungsfähigkeit und die konzeptionellen Aspekte von Windows NT vermitteln.

Kapitel 23 Für große und leistungsfähige Netzwerke reichen die Funktionen von Windows NT nicht mehr aus. Eine Erweiterung erfährt Windows NT durch den Einsatz von Windows NT Server. Dieses Kapitel zeigt, um welche Funktionen Windows NT durch den Einsatz von Windows NT Server erweitert wird. Ebenso wird erläutert, wie man unter Windows NT Server mit den unterschiedlichen Domänenkonzepten umzugehen hat, und in welchen Fällen welche Struktur am besten eingesetzt wird. Ebenso wird auf die notwendigen WINS-Mechanismen eingegangen, die beim Einsatz von TCP/IP unter Windows NT notwendig sind; DHCP und RAS werden ebenfalls erläutert.

Kapitel 24 Mit Windows 2000 setzt auch Microsoft neue Maßstäbe für den Einsatz einer besseren und flexibleren Netzwerkinfrastruktur. Bei Microsoft heißt das Zauberwort in Zusammenhang mit Windows 2000 Active Directory System, bei dem es sich um eine Directory-Services-Struktur handelt. Neben diesen Änderungen bietet Windows 2000 wahrscheinlich noch eine Vielzahl weiterer Merkmale, die es von Windows NT 4.0 gravierend unterscheiden. Die Informationen in diesem Kapitel basieren auf der Betaversion.

Kapitel 25 Das Internet wird von Tag zu Tag beliebter. Jedes renommierte Unternehmen und viele Institutionen stellen Informationen im Internet zur Verfügung. Ein neues Schlagwort in diesem Zusammenhang ist Intranet bzw. Extranet. In diesem Kapitel werden Ihnen Möglichkeiten aufgezeigt, die mit dem Intranet/Internet zur Verfügung stehen, und erklärt, welche Maßnahmen Sie ergreifen müssen, um das Unternehmensnetz gegen unerwünschte Internetbesucher abzusichern. Ebenso werden die Möglichkeiten zur Netzwerkkopplung mit Hilfe der VPN-Technologie erläutert.

Kapitel 26 Da der Einsatz von E-Mail-Systemen immer wichtiger wird, sollen in diesem Kapitel die notwendigen Grundlagen aufgezeigt werden. Dies betrifft vor allem den X.400-Standard und alle damit zusammenhängenden Mechanismen.

Kapitel 27 Neben dem X.400-Standard sind auch die Directory Services entscheidend, um flexible und leistungsfähige Mailing-Systeme aufzubauen. In diesem Kapitel werden alle hierfür notwendigen Definitionen und Grundlagen geklärt. Dabei werden auch die Übereinstimmungen mit NDS und X.500 diskutiert.

Einleitung**Kapitel 28**

Keiner weiß genau, was am 1.1.2000 alles nicht mehr funktionieren wird. Worauf es beim Jahrtausendwechsel ankommt, was beachtet werden muß, wie Sie die Risiken vermeiden – dieses Kapitel verschafft Ihnen einen Überblick, was bei der Hardware und was bei der Software für Netzbetriebssysteme und Add-ons zu beachten ist. Es stellt vor, wie Novell und Microsoft sich auf den Jahrtausendwechsel vorbereiten und wie der aktuelle Stand zum Zeitpunkt der Erstellung dieses Buchs aussieht. Das Problem darf nicht unterschätzt werden: Deshalb erfahren Sie auch, wie Sie an weitere Informationen kommen.

1

Geschichtlicher Überblick

Die Technologie der Computersysteme entwickelt sich mittlerweile so rasant, daß es schwerfällt, den Überblick darüber zu behalten. Die Rechenleistungen der Computeranlagen steigen ständig, und die Computer werden immer kleiner und handlicher. Dabei hat nicht nur eine Evolution auf der Hardware-Ebene stattgefunden, auch auf dem Gebiet der Software-Entwicklung werden dem Anwender immer bessere und leistungsfähigere Programme zur Verfügung gestellt.

Ohne Phantasie, theoretische Konzepte und deren Umsetzung in die Praxis ist keine technologische Entwicklung denkbar. Dies trifft auch für die geschichtliche Entwicklung der Computer bzw. Rechnersysteme zu.

Die Ideen für die heutigen Computer reichen bis in das Jahr 1000 vor Christus zurück. Einer der Vorläufer unserer heutigen Rechner im Altertum war der Abakus. Er diente den Händlern und Gelehrten als mechanische Rechenhilfe und leistete hierbei wertvolle Dienste. Diese Rechenhilfen sind sogar heute noch in einigen Teilen dieser Welt in Gebrauch. Man kann mit Recht behaupten, daß es sich beim Abakus um die erste mechanische Rechenmaschine gehandelt hat.

Fortgeführt wurde diese Entwicklung durch Blaise Pascal. Im Jahr 1647 erfand er eine analoge Rechenmaschine. Bekannt wurde sie unter dem Namen »Pascaline«. Diese Rechenmaschine funktioniert ähnlich wie ein Kilometerzähler. Die Ziffern 0 bis 9 sind auf Rädern angebracht. Hat sich ein Rad um eine volle Umdrehung bewegt, wird das benachbarte Rad um eine Stelle weitergedreht. Damals war es noch äußerst schwierig, entsprechend genaue und zuverlässige Komponenten herzustellen.

1666 stellte Sir Samuel Moreland seine Additions- und Subtraktionsmaschine vor und sieben Jahre später eine Multipliziermaschine. Fast zur selben Zeit entwickelte Leibniz in Deutschland einen funktionsfähigen Rechner zur Multiplikation und Division von Zahlen. Auch Leibniz benutzte noch das Zehnersystem als Grundlage, hatte jedoch schon den Gedanken, die Binärarithmetik aufgrund ihrer Einfachheit in einem Rechner zu verwenden. Dies geschah 150 Jahre bevor die beiden Mathematiker Boole und De Morgan die Algebra soweit entwickelt hatten, um diese binäre Notation als Basis in Rechenmaschinen einsetzen zu können.

1 Geschichtlicher Überblick

Als »Vater der modernen Rechner« wird Charles Babbage bezeichnet. Er stellte seine Maschine 1821 der Royal Astronomical Society vor. Diese Anlage arbeitet mit dem Prinzip der Differenzen zwischen Zahlen, daher wird sie auch Differenziermaschine (Difference Engine) genannt.

Die Differenziermaschinen hatten nur ein sehr begrenztes Funktionspektrum. Um sie leistungsfähiger zu gestalten und eine größere Vielfalt von Berechnungen durchführen zu können, bedurfte es einer vollkommen neuen Konstruktion. Anfang 1830 entwickelte Babbage das Konzept einer Allzweckrechenmaschine: die analytische Maschine (Analytical Engine).

Babbage hatte erkannt, daß Computer aus fünf grundlegenden Elementen bestehen müssen:

■ *Eingabe*

Das ist die Möglichkeit, den Computer mit Zahlen zu füttern. Babbage verwendete hierfür Lochkarten, so wie sie Jacquard anfänglich für die Steuerung seiner Webstühle verwendet hatte. Wer die Entwicklung der Computer kennt, weiß, daß Lochkarten noch bis in die siebziger Jahre verwendet worden sind.

■ *Speicher*

Darunter versteht man die Möglichkeit, dem Computer ein Gedächtnis zu geben. Für die Berechnungen ist es unabdingbar, daß Ergebnisse für spätere Berechnungen zwischengespeichert werden.

■ *Arithmetische Einheit*

Sie dient zur Durchführung von Berechnungen.

■ *Leitwerk*

Die Aufgabenausführung wird durch Vorgabe eines Programms gesteuert. Bei heutigen Rechnern werden die arithmetische Einheit und das Leitwerk in Form der CPU (Central Processing Unit, also Zentraleinheit) zusammengefaßt.

■ *Ausgabe*

Was nützen die besten Berechnungen, wenn die Ergebnisse nicht sichtbar gemacht werden können? In der heutigen Zeit werden hierfür Bildschirme und Drucker verwendet. Babbage stellte sich eine Ausgabe mit Lochkarten vor.

Die nächste überragende Figur in der Geschichte der Computerentwicklung dürfte Hermann Hollerith gewesen sein. Für seine Maschinen wurden ebenfalls Lochkarten zur Eingabe von Daten verwendet. Die Hollerith-Tabulierer waren die ersten Maschinen, die keine mechanische Verarbeitung einsetzten. Dieser Ansatz wurde noch im gleichen Jahr, nämlich 1890, von einer der bekanntesten Firmen aus-

1 Geschichtlicher Überblick

gewertet und erfolgreich vermarktet. Es handelt sich dabei um die Firma IBM (International Business Machines), mittlerweile der Welt größter Computerhersteller.

Konrad Zuse verwendete bei der Zuse Z1 für die Ausführung von Binäroperationen bloß mechanische Elemente. Beim Nachfolgemodell wurden bereits elektronische Relais statt mechanischer Schalter eingesetzt. Als Eingabemedium dienten Lochstreifen.

Durch ein von IBM finanziertes Projekt wurde im Jahr 1943 die Harvard Mark I fertiggestellt. Im gleichen Jahr setzte man Colossus I zur Entschlüsselung von Nachrichten ein. Dies war der erste elektronische Rechner. Die Maschine arbeitete mit zweitausend Röhren.

Während des zweiten Weltkriegs erfuhr die Entwicklung auf dem Gebiet der Computertechnologie einen großen Schub. 1946 ging die ENIAC (Electronic Numerical Integrator and Calculator) in Betrieb. Hiermit konnten ballistische Tafeln für Kanonen und Geschosse berechnet werden. Dieser Computer bestand aus nicht weniger als 18000 Röhren. Trotzdem konnten damit nur zwanzig zehnstellige Zahlen gespeichert werden. Die Maschine anders zu programmieren, stellte einen enormen Aufwand dar.

Ein Wendepunkt in der Entwicklung des Computers wurde durch die Arbeiten von John von Neumanns eingeleitet. In der Informatik werden diese Entwicklungen auch als das Von-Neumann-Prinzip bezeichnet. Alle herkömmlichen Rechner basieren heute noch auf diesem Prinzip. Von Neumann realisierte das Konzept der Steuerung durch ein gespeichertes Programm auf elektronischen Digitalrechnern. Die legendäre Mark I arbeitete nach diesem Prinzip. Im Jahre 1948 verarbeitete dieser Rechnertyp sein erstes Programm.

Die Entwicklungen wurden stetig vorangetrieben. Motor waren einerseits die Bemühungen der Industrie, andererseits die Forschungsarbeiten in den Labors der Universitäten.

Da die ersten Rechner stromfressende und tonnenschwere Ungeheuer waren, wurde auch versucht, Computer nicht nur leistungsfähiger, sondern auch kleiner zu machen. Ein Rechner wie noch die ENIAC benötigte eine Stellfläche in der Größe eines Fußballfeldes, bei einem Stromverbrauch einer Kleinstadt und einem Gewicht von fast 30 Tonnen. Die Rechenleistung war jedoch wesentlich kleiner als die der ersten Homecomputer von Apple oder Commodore.

Einen Schritt in Richtung Miniaturisierung läuteten die Bell Telephone Laboratories 1948 ein. Zu dieser Zeit wurde der Transistor erfunden. Mit Hilfe der Transistoren konnten die Röhren ersetzt werden. Die Rechner benötigten damit nicht nur weniger Strom, neben der gesteigerten Rechenleistung waren sie auch nicht mehr so groß und schwer.

1 Geschichtlicher Überblick

Großrechner beherrschten lange Zeit auf dem Gebiet der Datenverarbeitung die Szene, obwohl Firmen wie DEC Rechner der mittleren Datentechnik (Minicomputer) auf den Markt brachten (PDP-8). Durch den Einsatz der integrierten Schaltkreise (ICs) war man jetzt in der Lage, die Computerleistung auf ein Stückchen Silizium zu integrieren, das nicht größer als der Daumennagel eines Menschen ist.

1971 stellte die Firma Intel den ersten Mikroprozessor vor. Eine vollständige Computerzentraleinheit war auf einer Fläche von 6x6 mm untergebracht, die gesamte Computerschaltung bestand aus 2250 Transistoren. Die Transistoren sind notwendig, um die arithmetische Einheit und das Leitwerk eines Rechners verwirklichen zu können.

Die Integration von immer mehr Leistung auf immer kleinerem Raum ist nach wie vor in vollem Gange. Es ist auch nicht abzusehen, wann dieser Prozeß abgeschlossen sein wird. Derzeit ist es möglich, auf einem Chip mehrere Millionen elektronische Bausteine – Transistoren, Kondensatoren, Dioden etc. – unterzubringen.

Früher oder später ist dieser Entwicklung jedoch eine Grenze gesetzt, dann nämlich, wenn die Abstände der Leiterbahnen auf den ICs so klein sind, daß es unter anderem zu Elektronenübersprüngen kommt und ein Funktionieren der Systeme nicht mehr möglich ist. Um dieses Problem zu umgehen, ist man inzwischen dabei, sich nach anderen Grundstoffen an Stelle von Silizium umzusehen.

Neben der technologischen (Hardware-)Entwicklung ist auch eine rasche Entwicklung im Bereich der Betriebssysteme und Anwendungsprogramme (Anwenderapplikationen) festzustellen. Anfangs konnten Computer nur von Fachleuten bedient werden. Vor allem durch den vermehrten Einsatz von Personalcomputern werden für Anwender die unterschiedlichsten Betriebssysteme und Anwendungsprogramme angeboten. Beim Betriebssystem handelt es sich um den wichtigsten Teil eines Computersystems.

Ein Computer kann eingeteilt werden in:

- Hardware (CPU, Speicher, I/O-Einheiten)
- Betriebssystem
- Anwendungsprogramme (Compiler, Textsysteme, Zeichenprogramme etc.)

Die Aufgabe des Betriebssystems besteht darin, die unterschiedlichen Ressourcen eines Computers zu verwalten. Die Betriebssysteme von Großrechnern unterscheiden sich dabei grundlegend von den Betriebssystemen auf PCs.

1 Geschichtlicher Überblick

Seit einigen Jahren kann man feststellen, daß die Preise für Hard- und Software im PC-Bereich ständig fallen und die Leistung der angebotenen Komponenten immer mehr steigt. Man kennt das inzwischen: Was heute gekauft wird, ist morgen bereits veraltet.

Fast jedes Unternehmen arbeitet mittlerweile mit PCs, und die Anforderungen an die Hard- und Software steigen stetig. Es vergeht kein Jahr, in dem es nicht mindestens einen neuen Software-Update gibt. Allerorten hört man Schlagwörter wie Lokales Netzwerk, Internet, Cyberspace, Web-Server, E-Mail, GroupWare, ATM, Hubs, Internet-Surfer, CompuServe, American Online, Online-Dienste, High-Speed-LAN usw. usf. Ein PC ist heute bei weitem nicht mehr das, was er noch vor einigen Jahren gewesen ist. Der Weg zum multifunktionalen Arbeitsplatz ist nicht mehr weit, wenn nicht sogar schon beschritten. Ein Unternehmen ohne Netzwerktechnik wird es langfristig gesehen nicht mehr geben, da die Notwendigkeit, die richtige Information zur richtigen Zeit am richtigen Ort verfügbar zu haben, stetig wächst, egal in welcher Branche.

Mit diesen Entwicklungen geht auch einher, daß die Leistungsfähigkeit der Computer immer größer werden muß. Dies betrifft nicht nur den Bereich der Server, sondern auch die Endgeräte im Netzwerk und im Standalone-System. Aufgrund dieser Entwicklungen muß festgestellt werden: Alles, was Sie heute kaufen, ist bereits morgen veraltet. Die Forderung nach leistungsfähigeren Endgeräten wird vor allem durch die zum Einsatz kommenden Anwendungen verursacht. Es ist auffallend, daß jeder neue Software-Update zur Folge hat, daß die Anwendung auf der neuen Rechnerplattform meist nicht mehr so schnell läuft wie zuvor. Ähnliches gilt übrigens auch für Client-Betriebssysteme und Server-Betriebssysteme. Die steigenden Anforderungen an Anwendungssoftware und damit auch an die Server und Workstations ziehen nach sich, daß die Anforderungen an das Netzwerk in einem Unternehmen immer größer werden und die Netzwerke deshalb immer leistungsfähiger werden müssen.

Dieses Buch soll deshalb nicht nur die Grundlagen schaffen, die benötigt werden, um Lokale Netzwerke aufbauen zu können, sondern es soll gleichzeitig auch Grenzen und Möglichkeiten der zum Einsatz kommenden Techniken zeigen und erläutern. Nicht immer ist das, was der Hersteller verspricht, auch das, was als Ergebnis tatsächlich erreicht wird. Deshalb sind vor dem Einsatz und Aufbau neuer Technologien die Anforderungen mit den Leistungsdaten der Komponenten ganz genau zu prüfen – nur so können böse Überraschungen vermieden werden.

1 Geschichtlicher Überblick

Als Beratungsunternehmen werden wir auch immer wieder gefragt, wie lange eine Investition für Lokale Netzwerke Bestand hat. Diese Frage ist nur sehr schwer zu beantworten, da fast täglich nicht nur neue Komponenten, sondern auch Updates und Verbesserungen auf den Markt kommen. Für das Produkt »x« eines renommierten Herstellers von Netzwerkkomponenten kommen wöchentlich Software-Updates, die in die aktiven Komponenten eingespielt werden können. Nachgefragt, wie denn dies zu begründen sei, erklärte mir der Hersteller, daß das Produkt zunächst soweit entwickelt wird, daß es funktioniert. Die restlichen Feinheiten werden dann im Laufe des Lebenszyklus dieses Produkts entwickelt und zur Verfügung gestellt.

Somit ist die Frage nach der Lebensdauer einer Investition mittlerweile einzig abhängig davon, wann der Kunde bereit ist, einen neuen Update durchzuführen. Über einen längeren Zeitraum wird man es jedoch nicht erreichen, das gesamte System »einzufrieren«, da man sonst vielleicht wichtige und notwendige Neuerungen verpaßt bzw. übersieht. Wenn man schon nicht bereit ist, ständig Neuerungen und Updates durchzuführen, so sollte man zumindest versuchen, auf dem aktuellen Stand zu bleiben.

Wie Sie im Laufe der Ausführungen in diesem Buch sehen werden, sollte auf jeden Fall darauf geachtet werden, daß der gesamte Bereich der Netzwerkverkabelung wesentlich länger Bestand hat als die restlichen Netzwerkkomponenten, da die Verkabelung den weit aufwendigeren und zum Teil auch teureren Part eines Netzwerks ausmacht.

Da ich mich in diesem Buch unter anderem mit den Möglichkeiten von Betriebssystemen für Lokale Netze und deren Leistungsfähigkeit befassen will, soll zunächst dargestellt werden, was unter Lokalen Netzen zu verstehen ist. Aufbauend auf diesen Definitionen und Grundlagen werden in den darauffolgenden Kapiteln wichtige Funktionen und Komponenten erläutert, die eng mit Lokalen Netzwerken zusammenhängen bzw. ohne deren Einsatz zum Teil Lokale Netzwerke nicht betrieben werden könnten.

2

Definitionsgrundlagen des Lokalen Netzwerks

Zu Beginn der elektronischen Datenverarbeitung gab es ausschließlich die zentrale Datenverarbeitung. Der Computer (Großrechner, Host, Mainframe) stand in einem klimatisierten Raum und konnte nur von Spezialisten bedient werden. Im Laufe der Entwicklung wurden diese Systeme weiter ausgebaut und benutzerfreundlicher. Ein erster Schritt in diese Richtung war der Einsatz von Terminals, also Bildschirmarbeitsplätzen. Anwender bekamen ein Terminal auf den Schreibtisch und konnten von diesem die einzelnen Arbeitsaufträge am Host anstoßen.

Es konnten jedoch nur die dem Anwender zur Verfügung gestellten Dienstleistungen in Anspruch genommen werden, d.h., nur die für ihn bereitgestellten Programme konnten ausgeführt werden. Genauso konnten nur Datenbestände, die sich auf diesem Computer befanden, ver- und bearbeitet werden. Die Terminals mußten in bestimmten Abständen zum Rechner installiert werden, da die technischen Möglichkeiten noch keine anderen Alternativen zur Verfügung stellten.

Diese technischen Einschränkungen brachten es mit sich, daß zum Beispiel in Zweigstellen von Firmen ebenfalls EDV eingesetzt und Datenbestände mit der Zentrale ausgetauscht werden mußten. Am Anfang wurde dies aufwendig durch das Verschicken von Lochkarten, später durch einen Datenträgeraustausch über Magnetbänder durchgeführt. Dann wurde die Datenkommunikation durch einfache DFÜ-Verbindungen (Daten-Fern-Übertragung) weiterentwickelt. Es handelte sich dabei um eine reine Punkt-zu-Punkt-Verbindung. Auf diese Weise konnten Nachrichten oder Dateien übermittelt werden. Später war es sogar möglich, komplette Verarbeitungsaufträge für den anderen Computer mit Hilfe von sogenannten RJE-Stationen (Remote Job Entry) zu übertragen.

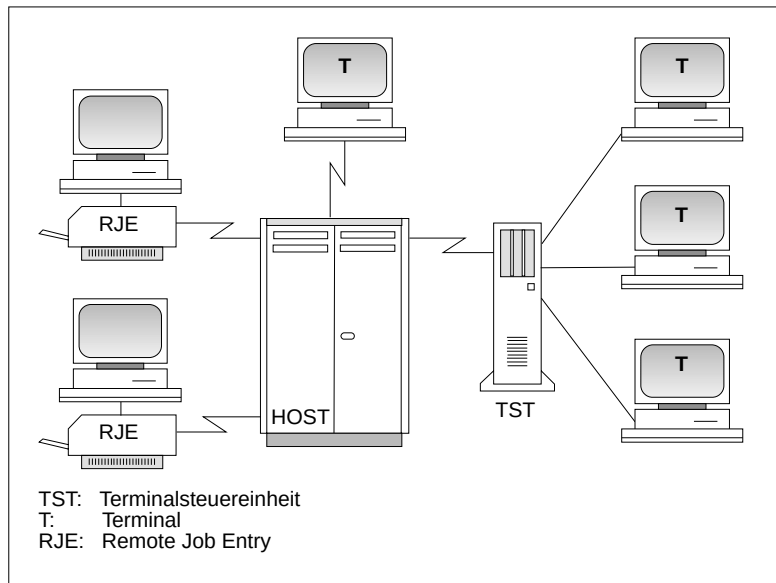
Mit dieser Rechner-Rechner-Kopplung war es jedoch nicht möglich, daß Arbeiten in der Stadt X mit Hilfe eines Terminals auf einem Rechner in der Stadt Y durchgeführt werden konnten. Der nächste Schritt bestand darin, Dialogterminals an weit entfernt stehenden Computern über Telefonleitung anzuschließen.

2 Definitionsgrundlagen des Lokalen Netzwerks

Die Punkt-zu-Punkt-Verbindungen wurden zu Mehr-Punkt-Verbindungen erweitert, über die mehrere Rechner und deren Anwender zusammengeschlossen werden konnten. Es entstanden die ersten Fernnetze, die den Nachrichtenaustausch mit beliebigen Teilnehmern und die gemeinsame Nutzung der Datenbestände erlaubten. Somit mußte kein komplizierter Datenträgeraustausch mehr durchgeführt werden. Änderungen von den Außenstellen wurden direkt auf dem zentralen Datenbestand durchgeführt (z. B. Buchungen von Reisebüros). Ich habe schon erwähnt, daß im Laufe der Computerentwicklung immer kleinere Systeme konzipiert und entwickelt worden sind. Es handelt sich dabei um die sogenannten Minicomputer. Auch diese Rechnerwelten konnten nach und nach in die Großrechnerwelt integriert werden.

Durch die Komprimierung der Rechenleistung auf kleinsten Raum ist es inzwischen möglich geworden, sich die hundert- bis tausendfache Rechenleistung einer ENIAC auf den Schreibtisch zu stellen und dies bei einem Gewicht von 3 bis 10 Kilogramm. Angesprochen sind hier die kleinen und leistungsfähigen Personalcomputer bzw. Notebooks, die mit dem Eintritt der IBM in diesen Wirtschaftszweig einen rasanten Aufschwung erlebt haben.

Abbildung 2.1
Zentralrechner mit
installierten Ein-/
Ausgabeeinheiten

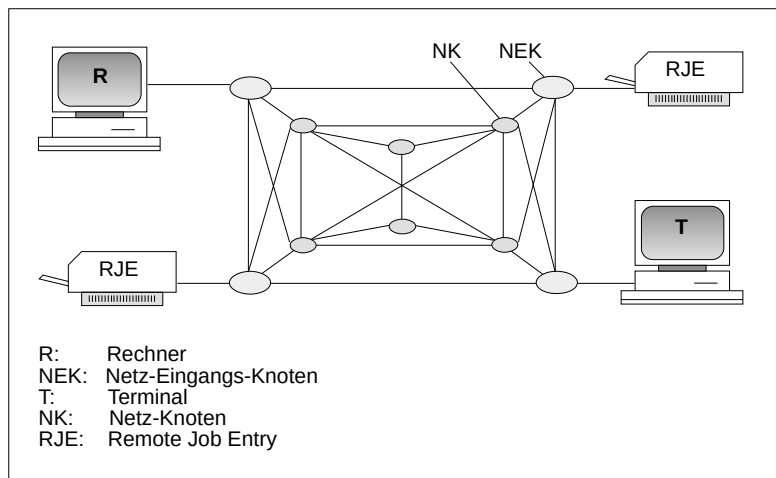


2 Definitionsgrundlagen des Lokalen Netzwerks

Wie sich in diesem Buch zeigen wird, besteht in sehr vielen Fällen auch bei den PCs der Bedarf nach Integration in die Mini- und Großrechnerwelt. Mit der Forderung nach der Vernetzung dieser Systeme innerhalb einer Firma wurden die ersten Ansätze für Local Area Networks aus der Taufe gehoben. Die Firmen Xerox, Intel und Digital Equipment entwickelten das erste Lokale Netzwerk. Es ist heute noch unter der Bezeichnung Ethernet bekannt.

In Abbildung 2.1 ist das Prinzip eines Zentralrechners mit den installierten Ein- und Ausgabeeinheiten dargestellt.

Abbildung 2.2
Aufbau von
Fernnetzen



In Abbildung 2.2 sehen Sie das Prinzip eines Fernnetzes (Wide Area Network). Ich werde Ihnen in einem gesonderten Kapitel zeigen, welche Möglichkeiten zur Verfügung stehen, um Wide Area Networks mit LANs aufzubauen.

Abbildung 2.3 zeigt das Grundprinzip eines LAN (Local Area Network).

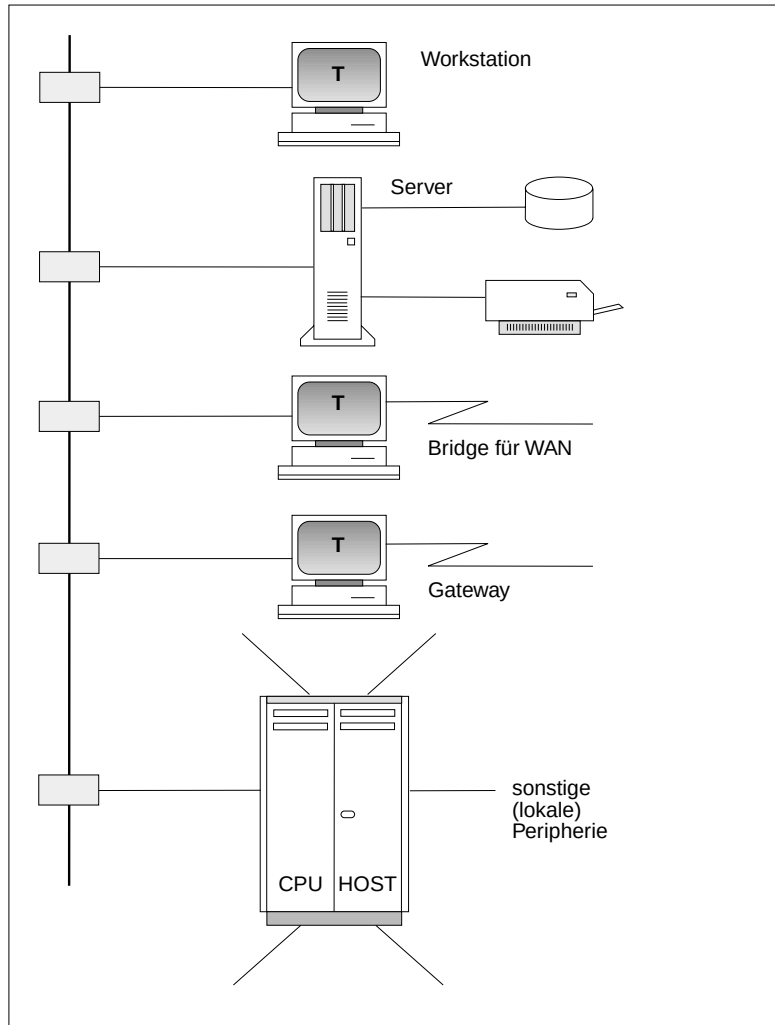
Es handelt sich dabei jedoch noch nicht um ein PC-LAN. Auf den Unterschied zwischen LANs und PC-LANs werde ich später noch eingehen. Die möglichen Einsatzbereiche Lokaler Netzwerke können sein:

- Ressourcen-Sharing
- Lastverbund
- Electronic-Mail
- Datei-Sharing (File-Sharing)

2 Definitionsgrundlagen des Lokalen Netzwerks

Durch den vermehrten Einsatz von PCs in den Büros ist eine rasante Entwicklung auf dem Gebiet der PC-LANs zu verzeichnen. Einen großen Einfluß übte dabei die Firma IBM aus, da durch den Einstieg von IBM in den PC-Bereich innerhalb kürzester Zeit immer leistungsfähigere und preiswertere kompatible PCs auf dem Markt verfügbar waren.

Abbildung 2.3
Allgemeiner Aufbau von Lokalen Netzwerken



Im Jahr 1981 verkaufte die Firma IBM in Amerika den ersten IBM-PC, der auf einem Intel-8088-Prozessor basierte. 1983 wurde das erste PC-LAN-Betriebssystem der Firma Novell verkauft: Novell NetWare

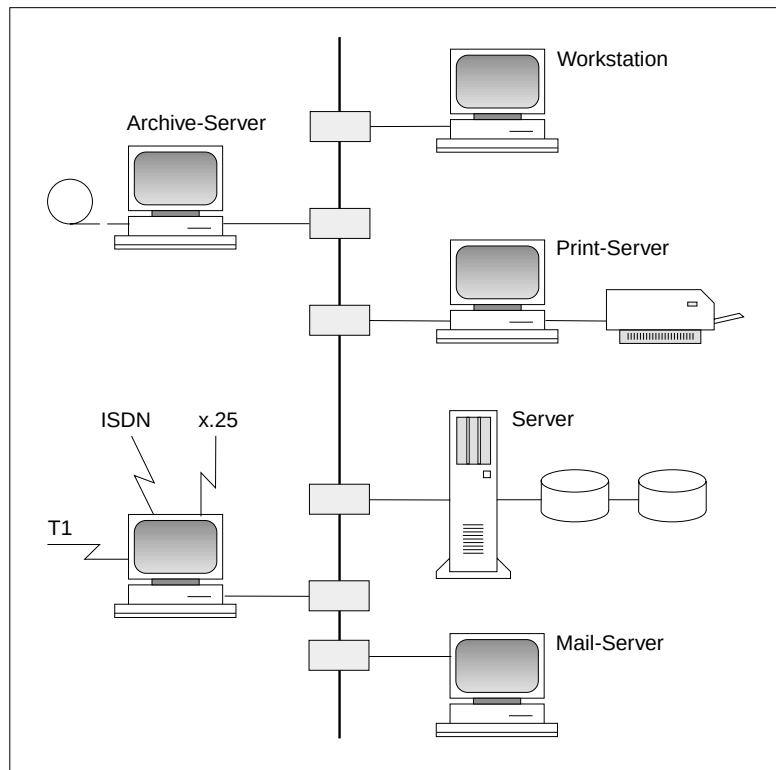
2 Definitionsgrundlagen des Lokalen Netzwerks

86. Seitdem werden ständig verbesserte und leistungsfähigere LAN-Betriebssysteme angeboten. Allgemein können Lokale Netze, speziell für PCs, wie folgt definiert werden:

Lokale Netze im PC-Bereich verbinden ausschließlich PCs und gegebenenfalls Geräte mit zentralen Funktionen miteinander. Es besteht keine Forderung nach Lastverbund.

Jeder PC erbringt seine eigene Rechenleistung. In Abbildung 2.4 ist der Aufbau eines Lokalen Netzes, ohne Berücksichtigung irgendeiner Architektur, dargestellt.

Abbildung 2.4
Aufbau von Lokalen Netzwerken



Die Merkmale von Lokalen Netzen sollen etwas genauer betrachtet werden:

In der Literatur gibt es eine sehr große Anzahl unterschiedlicher Definitionen, die im Grunde jedoch alle dasselbe zum Ausdruck bringen. Ich habe mich deshalb auf zwei Definitionen beschränkt. Anhand dieser Definitionen sollen die darin enthaltenen Aussagen und die damit verbundenen Merkmale näher betrachtet werden.

2 Definitionsgrundlagen des Lokalen Netzwerks

In einer Definition nach ISO (International Standard Organisation) ist zu lesen:

»Ein Lokales Netzwerk dient der bitseriellen Informationsübertragung zwischen miteinander verbundenen unabhängigen Geräten. Es befindet sich vollständig im rechtlichen Entscheidungsbereich des Benutzers und ist auf sein Gelände (gemeint ist das Firmengelände, Anm. des Autors) beschränkt.«

Auf dem Telematica-Kongreß in Stuttgart 1986 wurde von Gühr folgende Definition vorgenommen:

»Unter Lokalen Netzwerken (Local Area Network, LAN) werden spezielle Kommunikationsnetze verstanden, welche durch eine eng begrenzte räumliche Ausdehnung von nur wenigen Kilometern, ein gemeinsames breitbandiges Übertragungsnetz sowie eine dezentrale Steuerung gekennzeichnet sind. LANs eignen sich besonders gut zur Vernetzung von Rechnern, Arbeitsplatzsystemen (Workstations) [...] u. a. m., zwischen denen kurzzeitig große Datenmengen ausgetauscht werden müssen.«

Hier wird unter einem LAN zunächst eine nicht näher festgelegte Infrastruktur verstanden, an deren Peripherie sich gleichartige Systeme befinden. Jedes Endgerät sollte dabei in der Lage sein, eine Verbindung zu einem beliebigen anderen Gerät in diesem Netz herzustellen. Das bedeutet, daß jede Einheit mit jeder anderen Einheit in Verbindung treten kann. Wir werden noch sehen, daß sich dies zwar sehr einfach anhört, in der Praxis jedoch gar nicht so einfach realisierbar ist. Das LAN soll dabei so gestaltet sein, daß bei Ausfall einer Komponente nur die Ressource dieser ausgefallenen Einheit nicht mehr zur Verfügung steht. Ein Einfluß auf die anderen Kommunikationsbeziehungen sollte dabei nach Möglichkeit nicht entstehen.

Deshalb muß beim Aufbau eines LAN darauf geachtet werden, daß bei einem Ausfall einer einzelnen Komponente so viele Einzelfunktionen wie möglich zur Verfügung stehen. Diese Sicherheit kann in den meisten Fällen mit Hilfe eines redundanten Aufbaus einer Netzwerkstruktur erreicht werden. Eine Integration von sehr vielen Funktionalitäten in eine einzige Komponente (Server, Gateway, Bridge, Router etc.) führt also dazu, daß auf einen Schlag eine große Anzahl von Funktionen nicht mehr verfügbar ist, wenn genau diese Komponente ausfallen sollte.

Es läßt sich sagen, daß Sicherheit Redundanz bedeutet, Redundanz aber bedeutet höhere Kosten.

Wieweit er diesen wichtigen und kritischen Aspekt beim Auswahl- und Aufbauprozeß eines LAN berücksichtigen will, ist vom jeweiligen Betreiber selbst zu entscheiden. Wichtig ist nur, daß Sie sich für

2 Definitionsgrundlagen des Lokalen Netzwerks

Ihre jeweilige Umgebung und Situation für das Richtige entscheiden. Führende Hersteller im Hardware-Bereich bieten inzwischen ausfallsichere Hardware-Komponenten an, die speziell für den Einsatz als Server konzipiert sind. Ebenso bieten führende Hersteller von Netzwerkbetriebssystemen ausfallsichere und redundante Lösungen für das NOS (Network Operating System) an.

Häufig wird beim Aufbau eines LAN auch gefordert, daß eine Station nicht nur mit den Komponenten innerhalb desselben Netzes kommunizieren können muß. Dann ist es notwendig, Übergänge zu schaffen, um Verbindungen zu Partnern in anderen Netzwerken herstellen zu können oder diese ständig und permanent zur Verfügung zu haben. Es kann sich dabei um Netzwerke im gleichen Gebäude, auf dem gleichen Firmengelände oder in anderen Stadtteilen oder Städten handeln. Letzteres erfordert dann die Einbeziehung der öffentlichen Netze, die Ihnen durch die Telekom angeboten werden. Bei den zu koppelnden Netzwerken muß es sich allerdings nicht um den gleichen Typ Netzwerk handeln. Die dafür geeigneten Übergänge betreffen nicht nur die Anbindung an Host-Systeme (IBM, Siemens, DEC etc.) und firmeneigene LANs am gleichen Standort oder an einem anderen Standort (remote Kopplung), sondern auch die Zugänge zu Online-Diensten (CompuServe, American Online, T-Online etc.), die Anbindung an das Internet oder andere Netzwerke einzelner Hersteller (herstellerspezifische Kundennetze).

Wenn man beide Definitionen zusammenfaßt, dann können folgende relevante Eigenschaften von LANs bestimmt werden.

Ausdehnung

Ein Lokales Netzwerk ist in seiner Ausdehnung auf das eigene Firmengelände beschränkt. Es werden keine Dienste der Telekom eingesetzt. Sobald sich das Netzwerk über das eigene Firmengelände hinaus ausdehnen soll, müssen die Dienste der Telekom oder anderen Telekommunikationsanbieter in Anspruch genommen werden. In diesem Fall handelt es sich auch nicht mehr um ein Lokales Netzwerk, sondern um ein Wide Area Network (WAN). Dieses kann sich sogar über die ganze Welt erstrecken.

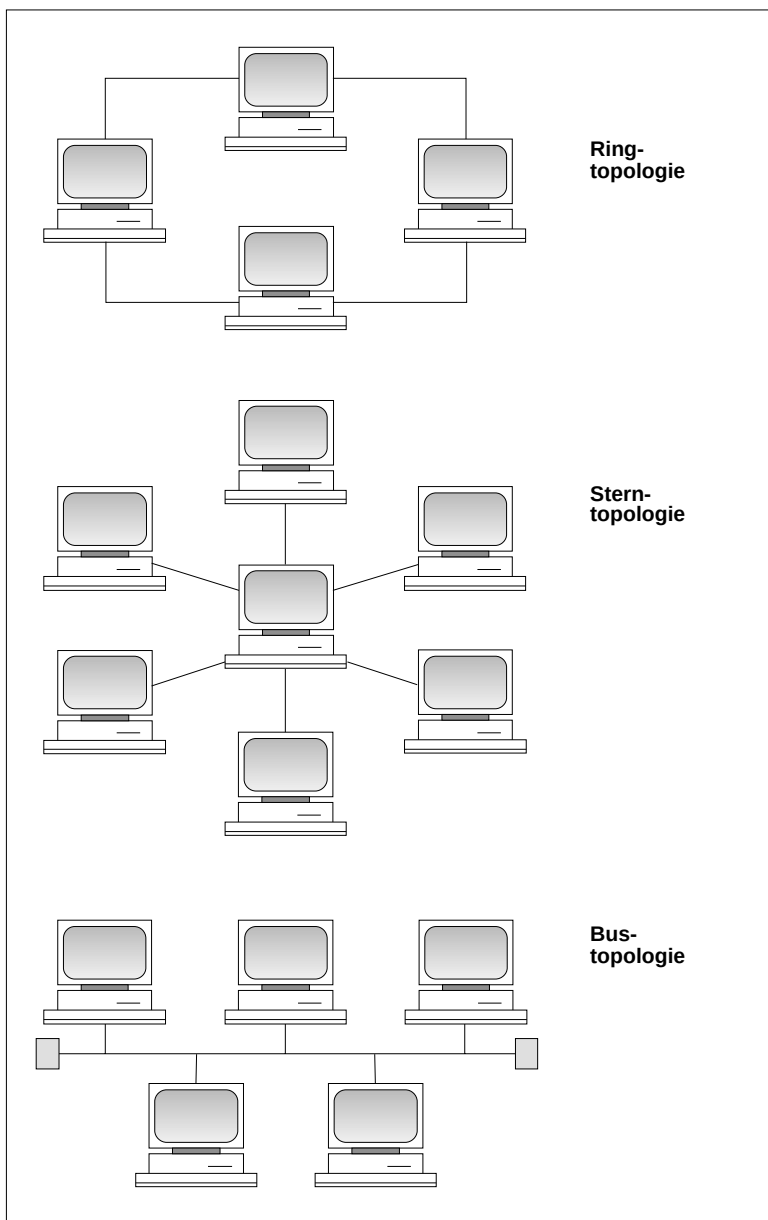
Topologie

Unter der Topologie ist die Art und Weise zu verstehen, wie Rechner und Kommunikationssysteme miteinander verbunden werden können. Im Laufe der Zeit haben sich drei Grundformen der topologischen Verbindungsmöglichkeiten etabliert: Ring-, Stern- und Bustopologie.

2 Definitionsgrundlagen des Lokalen Netzwerks

In Abbildung 2.5 sind diese drei Grundformen allgemein dargestellt. Ein eigenes Kapitel wird sich mit den Vor- und Nachteilen dieser Topologien befassen.

Abbildung 2.5
Drei Standard-
topologien für den
Aufbau des LAN



2 Definitionsgrundlagen des Lokalen Netzwerks

Übertragungsmedium

In Lokalen Netzwerken wird üblicherweise mit Übertragungsraten von 10 Mbit/s bis 100 Mbit/s gearbeitet. Inzwischen gibt es jedoch Hersteller, die Komponenten anbieten, um mit bis zu 1000 Mbit/s arbeiten zu können. Als Übertragungsmedien kommen derzeit in Betracht:

- Twisted-Pair-Kabel (4- bzw. 8-adrige Kabel gemäß CAT-5-, CAT-6-, CAT-7-Spezifikation)
- Koaxialkabel in verschiedenen Ausführungen (z.B. 50-, 75- oder 93-Ohm-Kabel)
- Glasfaserkabel (Lichtwellenleiter)

Als Übertragungstechnik kann zwischen Breitband- und Basisbandübertragung unterschieden werden. Dieser Unterschied soll später betrachtet werden.

Die eingesetzten Übertragungsmedien und Übertragungstechniken sind von LAN zu LAN unterschiedlich. Zu beachten ist dabei nur, daß unter bestimmten Umgebungsbedingungen nur spezielle Übertragungsmedien einsetzbar sind.

Steuerung

Bei Fernnetzen werden zur Steuerung der Informationsübertragung und der Kommunikation von Rechnern sogenannte Knotenrechner (s. Abbildung 2.2) verwendet. Diese Knotenrechner arbeiten meist so, daß die zu übermittelnden Informationen (siehe Datenformate) aufgenommen werden und auf einer weiteren Leitung zum nächsten Knotenrechner geleitet werden, bis das Informationspaket beim Empfänger angekommen ist.

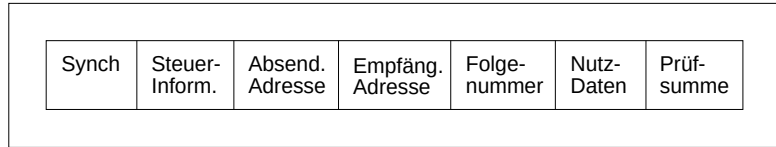
Die Topologie bei diesen Netzen (Fernnetzen oder LANs) und die Steuerung der Übertragung ist wesentlich komplexer als bei Lokalen Netzwerken. Bei LANs sind alle Kommunikationseinheiten an ein und dasselbe Medium (z.B. Koaxialkabel) angeschlossen. Es wird keine Flußsteuerung wie im vorher geschilderten Fall bei Fernnetzen benötigt. Bei der Informationsübertragung wird der Zugang zum Netz über ein sogenanntes Zugangsverfahren realisiert.

Datenformate

In Abbildung 2.6 ist der prinzipielle Aufbau eines Datenpakets dargestellt, so wie es in etwa bei der Übertragung von Informationen in Netzwerken Verwendung findet. Es sei jedoch darauf hingewiesen, daß der Aufbau dieser Datenpakete sich in einigen Punkten bei unterschiedlichen Protokollen von der Datenkommunikation unterscheidet.

2 Definitionsgrundlagen des Lokalen Netzwerks

Abbildung 2.6
Der Aufbau eines
Datenpakets



Generell ist es jedoch so, daß die Übertragung innerhalb eines Netzwerks (Lokales Netz oder Fernnetz) in Datenblöcken erfolgt. Die Länge des Nutzdatenfelds ist hierbei festgelegt (in Abhängigkeit des Protokolls).

Angenommen, dieses Feld darf maximal 2000 Byte (Zeichen) groß sein, dann bedeutet dies, daß ein Datensatz von 3500 Byte (Zeichen) Länge in zwei Etappen übertragen werden muß. Zuerst wird das erste Datenpaket mit 2000 Byte Nutzdaten übertragen und dann die restlichen 1500 Byte. Es können also immer nur Nutzdaten von maximal 2000 Byte innerhalb eines Datensatzes (Frame) übertragen werden. Größere Datenpakete müssen in je 2000 Byte großen Blocks übermittelt werden.

Beteiligte Stationen

In Lokalen Netzen sind meist Rechnersysteme, Ein- und Ausgabegeräte, Speichermedien und spezielle Peripheriegeräte (z.B. für die Prozeßsteuerung) integriert. Bei Fernnetzen hingegen sind nur die Rechner miteinander verbunden, da es aufgrund der relativ geringen Übertragungsgeschwindigkeiten oft viel zu lange dauern würde, auf spezielle Subsysteme zuzugreifen.

Der Einsatz von LANs erlebte in den letzten Jahren einen enormen Aufschwung. Für diese Entwicklung und das große Interesse muß es Gründe geben – ich will Ihnen die wichtigsten im folgenden Abschnitt auflisten und erläutern.

- Server-Funktionen
- Netzwerkressourcen-Sharing
- Wirtschaftliche Erweiterung der PC-Basis
- Möglichkeit, Netzwerksoftware zu nutzen
- Electronic-Mail
- Einrichten von Workgroups
- Zentralisiertes Management
- Erweiterte Sicherheit
- Betriebssystembasis auf dem PC
- Erweiterung der unternehmensweiten Struktur

2 Definitionsgrundlagen des Lokalen Netzwerks

Server-Funktionen

Dem Server-Konzept liegt zugrunde, daß ein zentrales System im Netzwerk, der Server, notwendige Dienstleistungen allen im Netz angeschlossenen Einheiten zur Verfügung stellt. Es ist dabei nicht festgelegt, daß sich dieser Server an einem bestimmten Ort befinden muß, d.h., der Standort des Servers kann frei gewählt werden. Unter Umständen kann er auch über eine WAN-Verbindung integriert werden. Dies ist jedoch aufgrund der zu transportierenden Datenmengen nur in Ausnahmefällen zu empfehlen. Über eine WAN-Kopplung sollten nur die benötigten Datenmengen übertragen und kein kompletter Serverbetrieb aufgebaut werden.

Auf einem Server können inzwischen mehrere Dienste gemeinsam installiert werden. Ein Server kann damit die unterschiedlichsten Aufgaben erledigen. Die wichtigsten werde ich nachfolgend aufzeigen.

File-Server

Unter einem File-Server (oder Datei-Server) ist ein Rechner zu verstehen, der zur Verwaltung und Bereitstellung von Dateien dient. Jeder berechnigte Anwender im Netz kann Dateien von diesem Server laden, ändern oder löschen. Dafür müssen Mechanismen zur Verfügung gestellt werden, die einen gemeinsamen Zugriff auf Dateien erlauben. Denken Sie beispielsweise an ein Auftragssystem: In einem solchen System müssen mehrere Mitarbeiter die Möglichkeit haben, in ein und derselben Datei unterschiedliche Datensätze zu bearbeiten. Diese Aufgabe muß sowohl die Applikation als auch das File-Server-Betriebssystem gewährleisten. Für den Anwender entsteht jedoch der Eindruck, als wären die Datenbestände »lokal« nur für ihn vorhanden. In den Anfängen der LANs für den PC-Betrieb war dies die grundsätzliche Funktionalität, die von einem Netzwerkbetriebssystem auf einem Server zur Verfügung gestellt wurde. Generell gilt, daß dem Anwender die lokale Arbeitsumgebung um die Möglichkeiten des Servers erweitert wird. D.h., man besitzt eine größere Plattenkapazität, mehr Drucker und andere zentralisierte Dienste.

Ein Zugriff auf die Ressourcen am Server ist allerdings nur dann möglich, wenn an den Benutzer die dazu benötigten Rechte vergeben worden sind. Diese Rechte werden dem Anwender durch den Netzwerkverwalter zugewiesen. Hierüber werden Sie mehr im Abschnitt über das Einrichten von NetWare und Windows NT erfahren.

Programm-Server

File-Server und Programm-Server sind eigentlich die gleiche Einheit. Da es sich bei Programmen, abstrakt betrachtet, um nichts anderes handelt als um Dateien, werden diese auch auf dem File-Server abgespeichert und bei Bedarf vom Anwender von diesem geladen. Ebenso wie bei der Verwaltung von Datendateien können Programme zentral auf einem Rechner, dem Server, gehalten werden;

2 Definitionsgrundlagen des Lokalen Netzwerks

damit kann auch die zentrale Wartung und Pflege von Programmen gewährleistet werden. Dies stellt sicher, daß alle Arbeitsplätze im Netz mit der gleichen Version des Programms arbeiten und alle den gleichen aktuellen Datenbestand verwenden. Redundante Daten- und Programmhaltung wird somit vermieden.

Zudem gibt es von sehr vielen Herstellern inzwischen netzwerkfähige Applikationen. Diese sind in der Regel nicht nur preisgünstiger als entsprechende Standalone-Versionen, sondern Sie ersparen sich beim Update auf eine neue Programmversion auch eine Menge Zeit, wenn sämtliche Programme auf dem Server verwaltet werden. Sie müssen die neue Version nur auf den Server einspielen und nicht mehr jeden einzelnen Arbeitsplatz auf die neue Version umstellen.

Über Zusatzfunktionen kann gewährleistet werden, daß benutzer-spezifische Teile des Programms, die unter Umständen auf den lokalen Platten abgelegt werden müssen, automatisch auf den Arbeitsplätzen über den Server geladen werden. D.h., sobald sich der Benutzer nach einer Umstellung am Server anmeldet, werden die notwendigen Änderungen sofort auf die Platte des Benutzers kopiert, ohne daß dieser davon etwas merkt.

In besonderen Fällen können Sie bei der Installation von Netzwerken in Verbindung mit einem Server aus Sicherheitsgründen noch einen Schritt weitergehen. Arbeitsplätze können bei Bedarf ohne jegliche periphere Speicherkapazität ausgestattet werden; das sind sogenannte diskless Workstations. In solchen Fällen werden nicht nur Programme und Daten vom Server geladen, sondern es wird auch das PC-Betriebssystem über besondere Einrichtungen von der Platte des Servers geladen. Eine unerwünschte Manipulation von Daten oder das Einspielen von Daten von der Workstation kann damit nicht mehr erfolgen. Diese Mechanismen werden vermehrt eingesetzt, da immer häufiger Viren durch nicht geprüfte Disketten ins LAN gelangen.

Print-Server

Sehr wirtschaftlich ist es, spezielle Systeme im Netz einzusetzen, denen sogenannte Print-Server-Funktionen übertragen werden. Im Netzwerkbetrieb ist es dann nicht mehr erforderlich, jeden Arbeitsplatz mit teuren und leistungsfähigen Druckern auszustatten. Je nach Anwendungsfall können ein oder mehr Print-Server eingesetzt werden, welche die Aufgabe haben, die definierten Drucker im LAN zu verwalten und die entsprechenden Druckaufträge auszugeben.

Die Drucker können dabei direkt am Print-Server angeschlossen sein. Es besteht jedoch auch die Möglichkeit, einen Netzwerkdruker an einer Workstation zu installieren, um diese allen Benutzern im LAN zur Verfügung zu stellen. Seit längerem gibt es auch Möglich-

2 Definitionsgrundlagen des Lokalen Netzwerks

keiten, Drucker direkt als Node im Netz zu installieren, d.h., diese Drucker besitzen dann eine eigene Netzwerkadapterkarte. Für Drucker, die diese Möglichkeit nicht besitzen, kann eine kleine Black Box als Koppellement für Drucker installiert werden. Diese Black Box besitzt dann eine bestimmte Anzahl von Schnittstellen (parallel, seriell), an die Drucker angeschlossen werden können. Drucker mit integrierter Netzwerkadapterkarte werden z.B. von HP angeboten. Black-Box-Systeme gibt es z.B. von Intel (Intel NetPort). Die Firma Extended Systems z.B. stellt eigene Netzwerkadapter für HP-Drucker her und kleine Pocket-Print-Server, die direkt an die parallele Schnittstelle aufgesteckt werden und mit einem Netzwerkananschluß versehen sind.

Kommunikations-Server

Kommunikations-Server haben die Aufgabe, die Verbindung zu anderen Netzen herzustellen. Es kann sich dabei um die Kommunikation mit anderen LANs handeln, um den Anschluß an das öffentliche Datennetz oder um den Anschluß an MDTs oder Mainframes. Der Vorteil liegt darin, daß von jedem beliebigen Arbeitsplatz aus die Verbindung zu den jeweiligen Systemen hergestellt werden kann, sofern der Benutzer eine Berechtigung besitzt. Der Server steuert die notwendigen Vorgänge, um eine reibungslose Kommunikation zu ermöglichen. Die Workstation selbst benötigt keinen direkten Anschluß an das andere Netz, die MDT oder den Host, da alles über den entsprechenden Kommunikations-Server im Netzwerk abgearbeitet wird.

Es besteht dabei die Möglichkeit, bestimmte Funktionen auf den Server zu legen, der bereits als File-Server und Print-Server fungiert, oder einen eigenen separaten Kommunikations-Server zu installieren. Die Entscheidung für eine der beiden Installationen hängt davon ab, wie belastet der Server bereits ist und welche Sicherheitsanforderungen an das Netzwerk gestellt werden. Beim Ausfall des File-Servers würde auch der Kommunikations-Server ausfallen, wenn beide Funktionen auf der gleichen Maschine laufen. Bei einer getrennten Installation kann der Kommunikations-Server weiter genutzt werden, auch wenn der File-Server ausgefallen ist.

Fax-Server

Der komfortablen Einrichtung, Faxe zentral vom Arbeitsplatz und der jeweiligen gerade im Einsatz befindlichen Anwendung versenden zu können, kommt in einer vernetzten Umgebung immer mehr Bedeutung zu. Damit dies alles realisiert werden kann, wird hierfür im Netz ein sogenannter Fax-Server installiert, der außer der installierten Netzwerkbetriebssystem-Basis und der Fax-Software auch noch einen Anschluß zur TK-Anlage oder einem separaten Telefonanschluß haben muß. Die Anschlüsse können als normale analoge oder digitale Anschlüsse (ISDN) gewählt werden. Zudem kann man den Fax-Server in Abhängigkeit von der benötigten Leistung mit einer oder mehreren

2 Definitionsgrundlagen des Lokalen Netzwerks

Anschlußleitungen (auch gemischt) ausstatten. Der Fax-Server dient nun dazu, sowohl eingehende als auch ausgehende Faxe zu bedienen. Hierzu wird auf dem jeweiligen Arbeitsplatz eine Fax-Client-Software installiert. In den meisten Fällen installiert die Software dabei einen weiteren Druckertreiber, der für die Übertragung der Faxe in die Faxwarteschlange zuständig ist. Von dieser Faxwarteschlange liest der Fax-Server die eingetragenen Dateien aus, konvertiert diese entsprechend den G3-Fax-Richtlinien, wählt die Faxnummer der Gegenstelle und überträgt anschließend das Fax. Mittels der Fax-Client-Software kann der Mitarbeiter den Status seiner Faxeinträge überwachen. Das gleiche Prinzip gilt ebenso für eingehende Faxe, nur in umgekehrter Reihenfolge. Für jeden Anwender kann dabei ein eigener persönlicher Bereich eingerichtet werden, in den dann das jeweilige persönliche Fax automatisch vom Fax-Server übertragen wird. Voraussetzung hierfür ist jedoch, daß jedem Faxteilnehmer im Unternehmen eine »virtuelle« Faxnummer zugewiesen wird, sofern der Fax-Server an einer TK-Anlage angeschlossen ist. Der Fax-Server wird dann so konfiguriert, daß die Faxnummer einem Benutzer zugewiesen wird. Jedes eingehende Fax kann anhand der Nebenstellenummer dem jeweiligen Mitarbeiter zugewiesen werden. Man erkennt bereits anhand dieser kurzen Beschreibung, daß es sich tatsächlich um eine sehr komfortable Einrichtung handelt, die man im Laufe der Zeit nicht mehr missen möchte.

Hat man für das eigene Netzwerk auch noch ein Mailing-System installiert, kann man die Funktionalität der Fax-Server noch zusätzlich um die Funktion ergänzen, daß ein eingehendes Fax automatisch in den Briefkasten des Mitarbeiters übertragen wird. Auf diese Art und Weise bekommt der Mitarbeiter seine Faxe automatisch per Electronic-Mail übermittelt. Dadurch ist man nicht mehr gezwungen, ständig zu prüfen, ob sich in den Faxeingängen neu eingetroffene Faxe befinden. Hierfür wird ebenfalls jedem Mitarbeiter eine Faxnummer zugewiesen und damit eine Beziehung zum Postfach hergestellt. Meistens geht man dazu über, daß man eine zusätzliche Nebenstellenziffer für die Faxnummer verwendet und somit nur eine Ergänzung zur bereits bestehenden Nebenstellentelefonnummer herstellt. Hat ein Mitarbeiter z.B. die Nebenstelle -315, dann wählt man als neue, vierte Nebenstellenziffer zum Beispiel 7 und weist dem Mitarbeiter somit die Faxnummer 7315 zu. D.h., jeder Telefondurchwahl wird für das Faxen einfach die Zahl 7 vorangestellt. Zu beachten ist bei der Installation, daß es nicht nur unterschiedliche Lösungen der einzelnen Hersteller gibt, sondern daß diese Lösungen auch für die unterschiedlichen Netzwerkbetriebssysteme angeboten werden. Im Prinzip arbeiten jedoch alle Lösungen, die eingehende

2 Definitionsgrundlagen des Lokalen Netzwerks

Faxe direkt in das Postfach des Mitarbeiters transferieren, nach dem gleichen Schema. Unterschiede bestehen jedoch im Preis, in der Gesamtfunktion und den unterstützten Mailing-Systemen.

Mail-Server

Ein weiterer wichtiger Einsatzbereich des LAN ist Electronic-Mail: Einfach und komfortabel können Mailings intern und extern ausgetauscht werden. Intern soll hier bedeuten, daß Mitarbeiter innerhalb des Unternehmens per Mail erreicht werden können, und extern, daß es sich um Mitarbeiter von Fremdfirmen handelt, die per Mail über das Internet erreicht werden können. Auf dem Mail-Server werden die ein- und ausgehenden Nachrichten der Mitarbeiter gespeichert. Dieser Bereich wird auch als Postfach (Post Office) bezeichnet, und jeder Mitarbeiter, der in der Lage sein soll, Nachrichten auszutauschen, muß mit einem Postfach ausgestattet sein. In Abhängigkeit von der Unternehmensgröße und der Verteilung des Unternehmens auf unterschiedliche Standorte können in einem Netzwerk auch mehrere Mail-Server installiert sein. Dies muß bei der Planung der gesamten Mail-Umgebung entschieden und entsprechend implementiert werden. Beim Mailing-Austausch zwischen zwei »Fremdfirmen« ist es nicht immer gegeben, daß beide Firmen das gleiche Mailing-System einsetzen. Damit Anwender unterschiedlicher Mailing-Systeme untereinander Nachrichten austauschen können, gibt es einen »standardisierten« Austauschmechanismus. Hierfür wird zu beiden Seiten der Mailing-Systeme ein sogenanntes SMTP-Gateway eingerichtet. Der Begriff SMTP steht hierbei für Simple Mail Transfer Protocol, ein Mechanismus, der aus dem TCP/IP kommt und hauptsächlich für den Mailing-Austausch über das Internet verwendet wird. Inzwischen wird dieses Verfahren aber auch innerhalb von LANs genutzt, um damit spezielle Kommunikationsaufgaben erfüllen zu können. So nutzen z.B. manche Hersteller dieses Protokoll bei der automatisierten Übertragung eingehender Faxe in das Mailing-System, um die Verbindung zwischen dem eigenen Mailing-System und dem Fax-Server herstellen zu können.

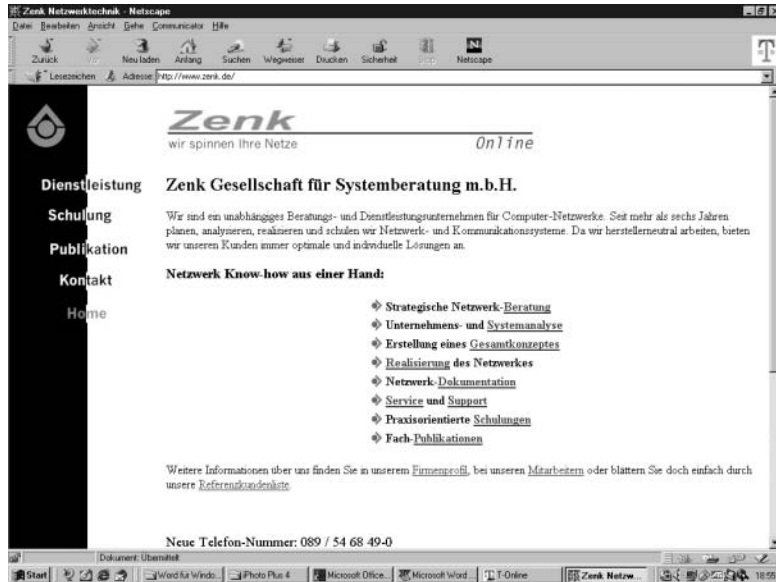
Web-Server

Dieser Begriff ist in Verbindung mit LANs und Internet- bzw. Intranet-Mechanismen immer wieder zu hören. Bei dieser Komponente handelt es sich um einen Server (unter Unix, NetWare oder Windows NT), der auf dem dazugehörigen Web-Server installiert ist (z.B. Apache unter Unix, Fast Track Server unter NetWare oder Internet Information Server unter Windows NT). Die Aufgabe eines Web-Servers besteht darin, den Workstations, die mit einem Web-Browser (Netscape Communicator oder Internet Explorer) darauf zugreifen, bestimmte hierfür hinterlegte Informationen zurückzugeben. Auf dem Web-Server liegen hierzu in einem bestimmten Format (HTTP) Web-Seiten, auf die nacheinander über eine Einstiegsstartseite zugegriffen werden kann. Über sogenannte Links wird die Ein-

2 Definitionsgrundlagen des Lokalen Netzwerks

stiegsseite auf die restlichen Seiten verzweigt. Für den Zugriff auf die Web-Seiten muß eine Web-Adresse zur Verfügung gestellt werden. Es handelt sich um Adressen, die meist in der Form www.zenk.de genutzt werden. Wenn Sie z.B. auf die Web-Seite der Zenk GmbH über www.zenk.de verzweigen, dann erhalten Sie derzeit das in Abbildung 2.7 aufgeführte Eingangsbild.

Abbildung 2.7
Die Web-Seite der
Zenk GmbH



Bei vielen anderen Firmen ist im Laufe der Zeit zu erkennen, daß die Web-Seiten ständig und permanent geändert werden. So kann es durchaus sein, daß beim Besuch der Web-Seite der Zenk GmbH diese vielleicht etwas anders aussieht als in Abbildung 2.7 dargestellt.

Archive-Server

Ein Archive-Server ist ein Streamer in Verbindung mit einer passenden Streamer-Software, um die zentrale Datensicherung im Netzwerk durchführen zu können. Bei der Auswahl der Streamer-Software ist es wichtig, darauf zu achten, daß sie in der Lage ist, alle Dateien und die dazugehörigen Informationen, die von der Netzwerk-Betriebssystemsoftware benötigt werden, zu sichern. Sie können zwar einen Server unter NetWare auch mit dem herkömmlichen DOS-Backup sichern, anschließend fehlen Ihnen jedoch alle benötigten Dateiattribute, Zugangsberechtigungen für Dateien und Directories, also alles, um einen kompletten Restore nach einem Server-Absturz durchführen zu können. Sie hätten dann zwar alle Dateien wieder auf den Platten des Servers, müßten aber das Einrichten der Benutzerplätze und alles, was dazugehört, per Hand nachholen.

2 Definitionsgrundlagen des Lokalen Netzwerks

Die Archive-Server-Software gibt es, je nach Hersteller, entweder nur lauffähig auf dem Server (die Überwachung und Steuerung erfolgt von einer Workstation aus im Netz) oder nur lauffähig auf einer dedizierten oder nicht dedizierten Workstation im Netzwerk oder auch beides. Die neuen Softwareprodukte erlauben es auch, zentral eine Datensicherung der lokalen Platten der Workstations durchzuführen, d.h., Sie können damit den Anwender von der leidigen Arbeit der Datensicherung entlasten; dafür haben Sie als Netzwerkadministrator mehr zu tun.

Aufgrund der Plattenkapazitäten sollten Sie an den Einsatz von 4-mm- oder 8-mm-Streamer-Einheiten denken. Auf einem 4-mm-Band können derzeit bis zu 24 Gbyte und auf einem 8-mm-Band bis zu 70 Gbyte Daten gespeichert werden. Wem dies nicht ausreicht, der kann sich einen Autoloader/Stacker installieren, mit dem ein automatischer Bandwechsel durchgeführt wird, wenn das aktuelle Band voll ist. Mit diesen Systemen können dann sehr große Datenmengen gespeichert werden. Zu dem Zeitpunkt, zu dem Sie dieses Buch lesen, kann die Technik diesbezüglich jedoch schon wieder weiter fortgeschritten sein.

Apropos: Sie müssen sich damit abfinden, daß die Systeme, die Sie heute kaufen, morgen schon wieder veraltet sind. Andererseits gilt, daß heute gekaufte Systeme morgen viel billiger sind. Sie können aber nicht ewig warten, sonst haben Sie bis zu Ihrer Pensionierung noch kein Netzwerk installiert.

Sie sehen anhand dieser Ausführungen über Server-Funktionen, daß es eine Vielzahl von Anwendungen gibt, die auf dem Server laufen müssen, um entsprechende Server-Funktionen im Netzwerk zur Verfügung stellen zu können. Dabei wird auch immer wieder die Überlegung angestellt bzw. die Frage gestellt, ob man alle diese Funktionen auf einem Server implementieren soll oder verteilt auf mehreren Server-Maschinen. Diese Fragen lassen sich nur hinsichtlich der Ausfallsicherheit und der Kosten und Ihrer Präferenzen beantworten. Man kann sehr wohl alle notwendigen Funktionen auf eine entsprechend leistungsfähige Server-Maschine implementieren. Zwar braucht man dann weniger Hardware-Equipment, geht dafür aber das Risiko ein, daß beim Ausfall dieser zentralen Server-Maschine so ziemlich alle Netzwerk-Funktionen respektive Server-Funktionen ausfallen. Aus diesem Aspekt heraus ist es zu empfehlen, alle Server-Funktionen auf mehrere Server-Plattformen zu verteilen, damit man beim Ausfall einzelner Komponenten nicht einen Totalausfall über sich ergehen lassen muß. Die Erhöhung der Ausfallsicherheit ist also immer mit zusätzlichen Kosten verbunden.

2 Definitionsgrundlagen des Lokalen Netzwerks

Netzwerkressourcen-Sharing

Zu den Ressourcen im Netzwerk, die in einem LAN gemeinsam genutzt werden können, zählen Drucker, Plotter, periphere Speicherkapazitäten, MDTs, Host-Systeme, CD-ROMs, WORMs und dergleichen mehr. Somit läßt sich durch das LAN eine kostengünstige Nutzung teurer Peripherie erreichen.

Wirtschaftliche Erweiterung der PC-Basis

Netzwerke bieten eine wirtschaftlich sinnvolle Möglichkeit, die Anzahl der Computer in einem Unternehmen durch den Einsatz preisgünstiger Systeme zu erweitern, da diese nicht mehr mit allen peripheren Subsystemen ausgestattet sein müssen. Sie werden durch Ressourcen-Sharing allen zentral zur Verfügung gestellt. Voraussetzung hierfür muß jedoch sein, daß eine Infrastruktur verfügbar ist (Verkabelung), mit der es möglich ist, schnell und einfach neue Arbeitsplätze zu installieren, um diesen dann alle notwendigen Ressourcen freizugeben. Welche Möglichkeiten es bezüglich der Infrastruktur gibt, werde ich in nachfolgenden Kapiteln zeigen.

Möglichkeit, Netzwerksoftware zu nutzen

Es wurde bereits angesprochen, daß der Einsatz von LANs durch die Einsatzmöglichkeit netzwerkfähiger Software interessant wird. Damit können Mehrfachlizenzen kostengünstiger gekauft und installiert werden. Es ist jedoch darauf zu achten, daß die Software auch die Möglichkeiten eines LAN unterstützt, also Datei-Sharing, Record-Locking und die Fähigkeiten, anwenderspezifische Umgebungen festzulegen. Der letzte Aspekt ist deshalb besonders wichtig, da in einem LAN nicht jeder PC mit der gleichen Hardware ausgestattet ist (z. B. anderer Bildschirm, unterschiedliche Speicherausstattung, verschiedene Einstellung der Bildschirmfarben und Default-Laufwerke). Da die Programmsoftware nur einmal auf dem Server installiert wird, müssen diese Einstellungen für jeden Benutzer individuell einstellbar sein.

Electronic-Mail

Electronic-Mail wird eingesetzt, um Benutzern oder Benutzergruppen Nachrichten oder gesamte Dokumente über das Netzwerk schicken zu können, unabhängig davon, ob diese im gleichen LAN oder über remote Verbindungen erreichbar sind. Die Nachrichten werden dabei in elektronischen Briefkästen auf dem Server für den jeweiligen Empfänger gespeichert. Dieser kann die Nachricht oder das Dokument lesen, ausdrucken oder eine Antwort versenden. Über eine

2 Definitionsgrundlagen des Lokalen Netzwerks

Alarmfunktion kann in den meisten Systemen der Benutzer informiert werden, wenn eine Nachricht für ihn eingetroffen ist.

Der sinnvolle Einsatz von Electronic-Mail-Systemen in einem Unternehmen steht und fällt mit der Akzeptanz durch den Anwender. Verwendet keiner das Electronic-Mail-System, um Nachrichten und Dokumente zu versenden, oder liest keiner die für ihn eingetroffenen Nachrichten, nützen die schönsten und komfortabelsten Systeme nichts.

Bei der Auswahl der Electronic-Mail-Systeme ist darauf zu achten, in welchen Umgebungen sie benötigt werden. Auf diesem Gebiet haben sich zwei Standards etabliert. Zudem existieren einige proprietäre Systeme großer renommierter Hersteller. Im PC-Bereich werden in Verbindung mit LANs zumeist Electronic-Mail-Systeme auf Basis des MHS-Protokolls eingesetzt. Als ISO-Standard wurde X.400 verabschiedet, der von vielen anderen Herstellern eingesetzt wird. MHS ist zwar eine Teilmenge von X.400, es wurde jedoch soweit zugunsten der Performance reduziert, daß keine Kompatibilität mehr zu X.400 existiert. Einen Übergang von MHS zu X.400 und vice versa kann jedoch über eigene MHS/X.400-Gateways hergestellt werden.

Es gibt auch proprietäre Systeme wie zum Beispiel All-in-one von DEC oder Dissos/Profs von IBM, die nicht zueinander kompatibel sind. Um Kommunikationsmöglichkeiten aufbauen zu können, werden auch hierfür Gateways von Drittherstellern angeboten. MS-Mail von Microsoft bietet zum Beispiel Gateways, um die Anbindung zu einer Vielzahl von anderen Electronic-Mail-Systemen herstellen zu können.

Sie sehen, daß es vor einer Entscheidung für ein Electronic-Mail-System unbedingt notwendig ist, die Randbedingungen abzuklären, um sich nicht eine Insellösung im Netzwerk zu installieren.

Einrichten von Workgroups

Eine Anzahl von Benutzern kann innerhalb einer Abteilung oder auch abteilungsübergreifend an einem gemeinsamen Projekt arbeiten. Durch den Einsatz von Netzwerken und der jeweiligen Netzwerk-Betriebssystemsoftware auf dem Server ist es möglich, einer Gruppe von Benutzern spezielle Directories und Ressourcen zuzuweisen, auf die keine anderen Benutzer im Netzwerk Zugriff haben. Bei Bedarf können diese Zuweisungen geändert werden. Das Versenden von Nachrichten, die für alle Anwender im Netzwerk gelten, kann ohne Einschränkung durchgeführt werden. Auf diese Weise ist es möglich, daß auf einem gemeinsamen Server unterschiedliche Arbeitsgruppen oder Abteilungen arbeiten, ohne daß sie sich gegenseitig behindern oder gar Daten zu Gesicht bekommen, die für sie nicht bestimmt sind.

2 Definitionsgrundlagen des Lokalen Netzwerks

Zentralisiertes Management

Da in der Regel alle Ressourcen zentralisiert auf dem Server oder über das Netzwerkbetriebssystem verwaltet werden, wird das Management solcher Ressourcen wesentlich vereinfacht. In letzter Zeit werden dabei immer mehr Produkte entwickelt und angeboten, mit denen Managementfunktionen in einem Netzwerk noch besser gestaltet werden können. Langfristig gesehen geht es dabei jedoch nicht nur um die Verwaltung der Netzwerkressourcen, sondern auch um die Möglichkeiten, die einzelnen Verkabelungskomponenten zu überwachen und zu steuern. Ich werde in einem eigenen Kapitel kurz auf die wichtigsten Aspekte des Netzwerkmanagements eingehen.

Erweiterte Sicherheit

Bisher mußte ich bei Schulungen, Beratungen und Projektarbeiten immer wieder feststellen, daß die eingesetzten Mechanismen zum Schutz eines unberechtigten Zugriffs auf die lokalen Ressourcen eines PC unzureichend sind. Durch die Zentralisierung der Programm- und Datenbestände auf einem File-Server kann dieses Sicherheitsloch der PCs geschlossen werden. In den heutigen Systemen sind generell Funktionen enthalten, um festzulegen, mit welchen Rechten ein Benutzer auf Dateien und Directories zugreifen darf, wann dieser sich am Server anmelden kann, von welcher Workstation dies gestattet wird und wie andere Ressourcen im Netzwerk zur Verfügung gestellt werden. Welche Möglichkeiten Ihnen hierbei Novell NetWare und Windows 2000 zur Verfügung stellt, wird unter anderem in diesem Buch behandelt.

Betriebssystembasis auf dem PC

Die größte Betriebssystembasis auf dem PC bildet immer noch Windows 95/98 bzw. Windows NT. Allerdings sind auch Unix-, Macintosh- und OS/2-Systemen relativ weit verbreitet. In einem Netzwerk soll und muß die Möglichkeit bestehen, alle diese PCs mit den oben genannten Betriebssystemen einsetzen zu können. Wie Sie noch sehen werden, bieten NetWare und Windows NT hierfür eine elegante Möglichkeit. Es ist dabei nicht nur so, daß mit diesen unterschiedlichen PCs Daten und Programme vom Server geladen werden können, sondern diese Systeme können ihre Daten in ihrer eigenen Dateinamenskonvention abspeichern und bearbeiten. Der Anwender sieht also seine gewohnte Umgebung. Umgekehrt können jedoch auch andere Workstations auf Daten zugreifen, die unter einem anderen Betriebssystem abgelegt worden sind, sofern das jeweilige Programm kompatibel zum Dateiformat ist. Da die einzelnen Betriebssysteme jedoch unterschiedliche Dateinamenskonventionen

2 Definitionsgrundlagen des Lokalen Netzwerks

einsetzen, müssen unter Umständen bei der Namenskonvertierung Änderungen durchgeführt werden; ein Macintosh-Dateiname darf z. B. länger sein als der Dateiname unter DOS. Wie dies erfolgt, wird später näher erläutert werden. Bei Novell wird diese Funktion für NetWare als NetWare Name Space Support bezeichnet.

Erweiterung der unternehmensweiten Struktur

Durch den Einsatz von Lokalen Netzen und der Kopplung dieser LANs miteinander ist es wesentlich einfacher, bislang getrennte Bereiche miteinander zu vereinen. Die Bildung von Workgroups sowie damit verbunden die Kommunikation und der Datenaustausch innerhalb dieser Workgroups werden wesentlich vereinfacht. Mußten bislang notwendige Daten anderer Abteilungen über Postweg versandt werden, kann dies durch die Kopplung von LANs schneller vonstatten gehen bzw. gleich ein direkter Zugriff erfolgen. Erst vor kurzem stellte ich ein Konzept auf, wie mit Hilfe einer LAN-Kopplung der Datenaustausch einer Programmierabteilung vereinfacht werden konnte. Dabei befand sich der eine Teil der Abteilung in Deutschland, der andere in Amerika. Der Abgleich der Programme erfolgte jede Nacht. Der Datenaustausch oder gemeinsame Zugriff auf spezielle Datenbestände zwischen einzelnen Abteilungen kann aber auch schneller und einfacher realisiert werden.

Bald werden wir in einem Unternehmen auf jedem Schreibtisch einen PC vorfinden, der in ein Netzwerk integriert ist. Dieser Arbeitsplatz wird aber nicht nur Zugriff auf die internen Ressourcen des Unternehmens haben, sondern über das Internet auch Zugang zu einer Vielzahl weiterer Informationen. Ziel wird es sein, einen Arbeitsplatz zur Verfügung zu stellen, der dem Anwender auf alle notwendigen Informationen Zugriff gewährt bzw. den Zugang zu diesen Informationen zur Verfügung stellt, ohne daß sich der Anwender allzu viele Gedanken machen muß, wie er an diese Informationen gelangt. Eine vernünftige Planung der Netzwerkinfrastruktur ist gefordert, um ein flächendeckendes Netzwerk sukzessive aufbauen zu können. Diese Planung betrifft aber nicht nur das physikalische Netzwerk mit seinen aktiven und passiven Netzwerkkomponenten, sondern hat auch weitreichende Auswirkungen auf die einzusetzenden Netzwerkbetriebssysteme, Mail-System, Fax-Server, Web-Server und eine Vielzahl weiterer Software-Komponenten.

Wie solche Lösungen aussehen könnten, werde ich Ihnen bei der Betrachtung der Netzwerktopologien und in weiteren Kapiteln über Netzwerkbetriebssysteme näher erläutern.

3

Kenndaten Lokaler Netzwerke

Es gibt mehrere Klassifikationen Lokaler Netzwerke, nach denen diese unterschieden und eingeteilt werden können. Die Grobeinteilung kann erfolgen in:

- Topologie
- Übertragungsmedien
- Übertragungstechnik
- Zugriffsverfahren

Die räumliche Ausdehnung von Lokalen Netzen ist vom Übertragungsverfahren, vom Übertragungsmedium und von der Übertragungsgeschwindigkeit, mit der gearbeitet wird, abhängig.

Die beteiligten Stationen werden sowohl durch die Anwendung im Netzwerk als auch vom Netzwerkbetriebssystem bestimmt.

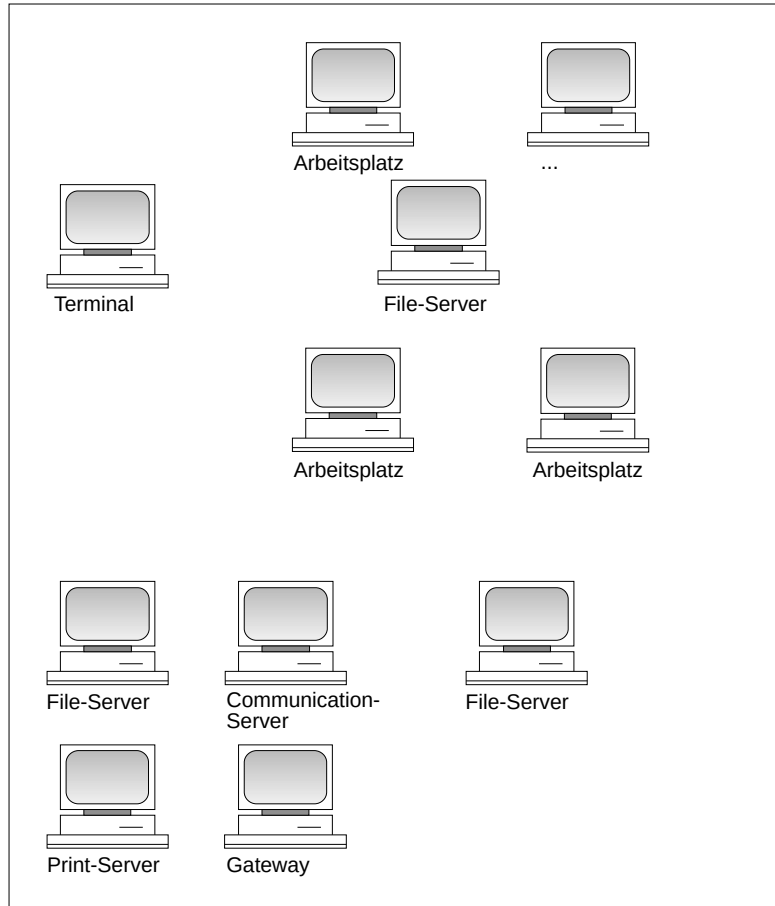
Das Datenformat, das bei der Kommunikation und der Datenübertragung verwendet wird, hängt vom verwendeten Protokoll ab.

3.1 Topologische Strukturen Lokaler Netze

Im Folgenden sollen die Stern-, Bus- und Ringstruktur Lokaler Netze behandelt werden. Abbildung 3.1 stellt die Ausgangssituation dar. Anhand dieses Beispiels werden nun die einzelnen topologischen Grundlagen und deren Eigenschaften erläutert.

3 Kenndaten Lokaler Netzwerke

Abbildung 3.1
Zu vernetzende
PCs mit ihren
unterschiedlichen
Funktionen



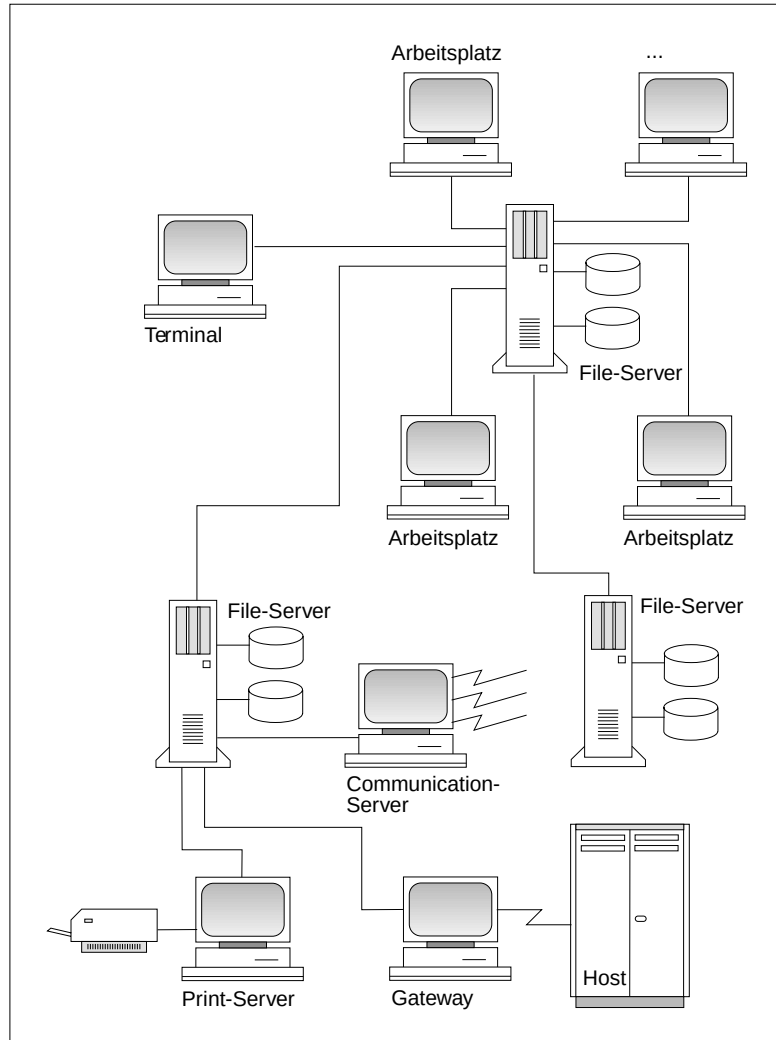
3.1.1 Sterntopologie

In ihrer herkömmlichen Form handelt es sich um die älteste Form zum Aufbau von Netzwerken. Sie ist Basis vieler heutiger Informationsnetzwerke. Denken Sie zum Beispiel an Terminalnetzwerke, Verkabelung der MDTs oder Telefonnebenstellenanlagen.

Die Sterntopologie, wie sie in Abbildung 3.2 dargestellt wird, ist von der Auslegung des Betriebssystems her die einfachste Struktur. Sie wurde in den letzten 20 Jahren häufig eingesetzt, wird inzwischen jedoch immer seltener verwendet, da ihr die anderen Topologien weit überlegen sind. Ein klassisches Großrechnersystem der IBM ist nach wie vor nach diesem Prinzip verkabelt. In der Mitte befindet sich der Host (Mainframe), sternförmig daran angeschlossen sind die einzelnen I/O-Systeme.

3.1 Topologische Strukturen Lokaler Netze

Abbildung 3.2
LAN, basierend auf
Sterntopologie



Der zentrale Knotenrechner (File-Server, Mainframe, Mini) hat die Verantwortung für die gesamte Kommunikation im Netzwerk und steuert den Verkehr im Netz.

Will eine Station einer anderen Station auch nur eine Nachricht schicken, läuft dies immer über den zentralen File-Server. Dieser nimmt die Nachricht auf und übermittelt sie an die Zielstation.

Es gibt verschiedene Möglichkeiten der Zugriffsregelung, wie also die einzelnen Workstations mit dem Server kommunizieren. Bei einer Methode sendet jede Station die Anforderungen an den zentra-

3 Kenndaten Lokaler Netzwerke

len Rechner und wartet auf die entsprechenden Ergebnisse. Dies kann dazu führen, daß der File-Server bei sehr vielen Anforderungen überlastet wird.

Die Workstations müssen dann entsprechend »gebremst« werden, damit keine Anforderungen verlorengehen und der File-Server die entsprechenden Anfragen auch schnell beantworten kann. Um das vernünftig umsetzen zu können, ist es notwendig, daß der Server mit einer ausreichenden Pufferkapazität ausgestattet wird, so daß die Überlastungssituation nicht zu schnell eintreten kann.

Die andere Methode ist das Polling-Verfahren. Bei dieser Zugriffsvariante bei Sternsystemen fragt der zentrale File-Server nach einem bestimmten Verfahren nacheinander alle Stationen ab, ob diese Übertragungswünsche haben. Trifft der Rechner auf eine Station, die übertragen will, wird sie bedient. Damit das Verfahren auch »fair« ist, ist es notwendig, daß nach Abarbeitung der gerade aktiven Station die unmittelbar nachfolgenden behandelt werden. Es darf auf keinen Fall so sein, daß ein und dieselbe Station für längere Zeit den File-Server exklusiv benutzt, weil die Übertragungswünsche so groß sind.

Da für jeden Übertragungswunsch der File-Server einbezogen werden muß, ist eine Peer-to-peer-Kommunikation (von Programm zu Programm also) innerhalb des Systems nicht möglich, wie es zum Beispiel bei Bus- und Ringsystemen der Fall ist.

Daraus ergibt sich ein Nachteil: Der Server des Systems unterliegt einer sehr hohen Belastung und sollte deshalb auch entsprechend leistungsfähig sein. Bei Ausfall des File-Servers ist das gesamte Netzwerk lahmgelegt. Keine Workstation ist mehr in der Lage zu arbeiten. Zudem ist der Verkabelungsaufwand sehr groß, da von jeder Station ein Kabel zur Zentrale verlegt werden muß.

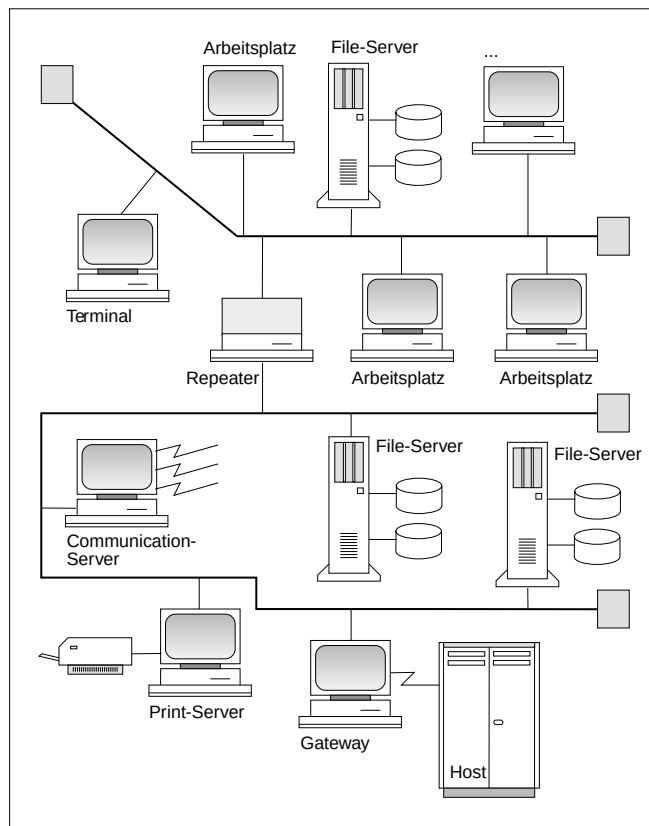
Eine andere Form der Sterntopologie stellt nicht den Server zentral in den Mittelpunkt der Datenverarbeitung, sondern verwendet ausschließlich für den physikalischen Aufbau der Verkabelung eine sternförmige Struktur. Diese Formen der Verkabelung sind vor allem dann vorzufinden, wenn Netzwerke auf Basis von Twisted-Pair-Verkabelung aufgebaut werden. Es gibt jedoch auch ein Netzwerk in Form einer Koaxialverkabelung, die auf einer Sterntopologie aufbaut. Es handelt sich dabei um ARCNET. ARCNET hat jedoch heute im Prinzip keine Bedeutung mehr. Wesentlich wichtiger in Bezug auf die sternförmige Verkabelung ist eine neue Netzwerktechnik, die inzwischen in aller Munde ist: ATM. Es handelt sich um ein sehr leistungsfähiges Netzwerk, das aufgrund der physikalischen Struktur rein sternförmig aufgebaut werden muß. In einem späteren Kapitel werde ich die Funktionsweise und den Aufbau von ATM-Netzwerken ausführlicher erläutern.

3.1 Topologische Strukturen Lokaler Netze

3.1.2 Bustopologie

In Abbildung 3.3 ist der Aufbau eines Netzes basierend auf einer Bustopologie zu sehen. Bei dieser Methode sind alle Stationen an einem gemeinsamen passiven Medium, dem Bus, angeschlossen. Jede Station kann frei kommunizieren, jeder mit jedem also, ohne Zuhilfenahme einer gesondert deklarierten Master-Station, während man im Vergleich dazu den File-Server beim Sternnetz als Master bezeichnen würde.

Abbildung 3.3
LAN, basierend auf
Bustopologie



Daten, die über den Bus zu einer Empfängerstation übertragen werden sollen, werden somit von allen Stationen empfangen, allerdings nur von der Station ausgewertet, für die die Daten bestimmt sind.

3 Kenndaten Lokaler Netzwerke

Die Vorteile bei dieser Topologie sind folgende:

- Die Struktur ist leicht erweiterbar.
- Das Anfügen oder Abklemmen von einzelnen Stationen ist meist während des Betriebs möglich, ohne daß das gesamte Netzwerk ausfällt oder Netzwerkfehler auftreten.
- Die Busverkabelung ist modular.

Es gibt jedoch auch bei dieser Art der Verkabelung ein paar Nachteile:

- Die Struktur ist anfällig gegenüber einem Ausfall des Mediums.
- Je nach eingesetztem Protokoll treten unvorhersehbare Wartezeiten bei der Kommunikation der Stationen auf.
- Die Längenausdehnung ist begrenzt.

Bekannt wurde dieses System durch Ethernet. Auf die Eigenschaften von Ethernet werde ich später noch genauer eingehen.

3.1.3 Ringtopologie

Bei einer Ringstruktur, wie sie in Abbildung 3.4 dargestellt ist, wird ähnlich wie bei Bussystemen ein gemeinsames Übertragungsmedium verwendet, nur daß dieses zu einem Ring zusammengeschlossen ist. Jede Station hat einen eindeutigen Vorgänger und einen eindeutigen Nachfolger. Die zu übertragende Information wird von einer Station an die nachfolgende gesandt. Diese nimmt die Information auf und überprüft, ob sie für sie bestimmt ist. Ist dies nicht der Fall, gibt diese Station wiederum die Information an die nachfolgende weiter. Das wird so lange durchgeführt, bis die Nachricht beim Empfänger eingetroffen ist.

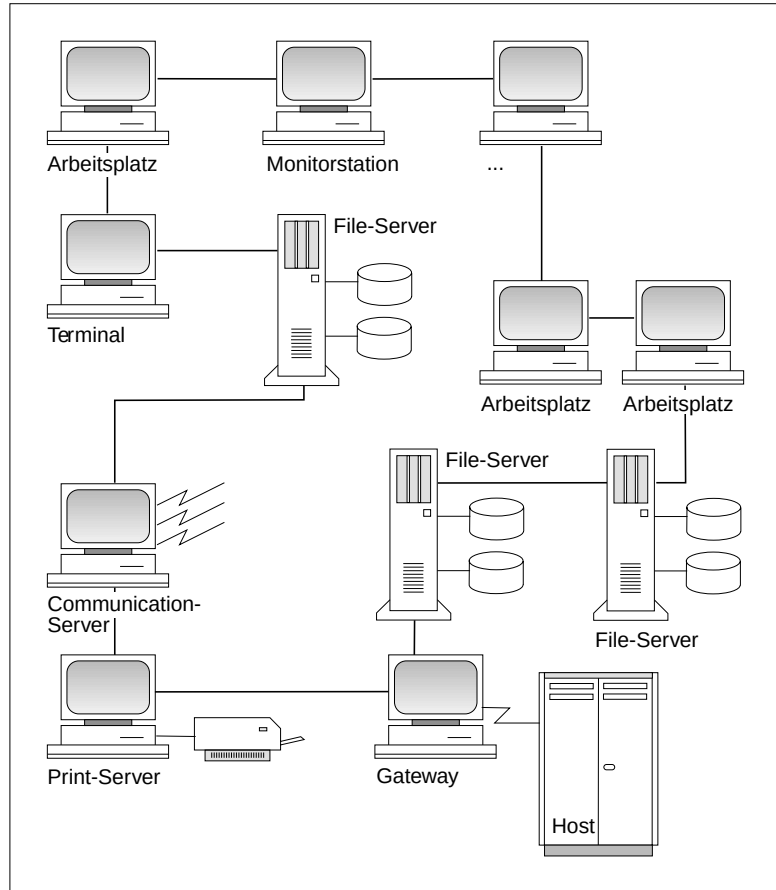
Eine Ringstruktur läßt sich relativ leicht erweitern, arbeitet mit einer minimalen Leitungsanzahl und hat einen geringen Zuwachs der Verkabelungslänge bei neu einzufügenden Stationen.

Der Nachteil dieser Struktur wird jedoch schon durch die Beschreibung erkennbar. Fällt eine Station aus bzw. wird durch Kabelbruch oder ähnliches die Verbindung zwischen zwei Stationen gestört, ist der gesamte Ring lahmgelegt, da die Nachricht nicht mehr durch das Ringsystem transportiert werden kann.

Es gibt mehrere Lösungsansätze, um dies zu verhindern, zum Beispiel die Verwendung einer redundanten Verkabelung. Damit könnte bei einem Ausfall die defekte Station auf einer Ersatzleitung umgangen werden. Es wäre auch möglich, die Übertragung nicht nur in einer Richtung zuzulassen, sondern bei einem Ausfall einer Station das System quasi von »hinten« aufzurollen, also in der Gegenrichtung zu übertragen.

3.1 Topologische Strukturen Lokaler Netze

Abbildung 3.4
LAN, basierend auf
Ringtopologie



Die Nachrichtenübertragung ist proportional zur Anzahl der Stationen, da jede Nachricht durch jede Station transportiert werden muß.

In der Gesamtsumme können die Kabellängen dieser Topologie sehr schnell sehr groß werden.

Aufgrund der aufgeführten Nachteile, vor allem Probleme wie den Stationsausfall oder Kabelbruch, gibt es diese Art der Topologie in Reinform nicht. Es existieren bessere und sicherere Möglichkeiten, die zwar nach dem Prinzip des Rings arbeiten, aber was die Verkabelung angeht, kein echter Ring sind.

Bekannte Beispiele sind ARCNET der Firma Data-Point (Ringstruktur auf Busverkabelung – heute nahezu bedeutungslos) bzw. der Token-Ring von IBM (physikalischer Stern und ein logischer Ring); auf sie wird in einem späteren Kapitel noch eingegangen.

3 Kenndaten Lokaler Netzwerke

Im Laufe der Entwicklung haben sich auch Mischformen dieser drei Topologien entwickelt, die jedoch nicht unbedingt überall sinnvoll eingesetzt werden können.

Beim Aufbau von großen Netzwerken ist es äußerst schwierig, über eine einzige Netzwerkverkabelung alle notwendigen Bereiche abzudecken. Zum einen wird das physikalische Netzwerk dadurch zu groß, zum anderen reichen unter Umständen die physikalischen Spezifikationen nicht aus, um das gesamte Netzwerk in einer einzigen Verkabelung realisieren zu können. Es hat sich deshalb eine Technik der Verkabelung entwickelt, die als Backbone bezeichnet wird. Inzwischen wird für die Realisation großer und komplexer Netzwerke auch strukturierte Verkabelung eingesetzt.

Ein möglicher Aufbau dieses Systems ist in Abbildung 3.5 skizziert.

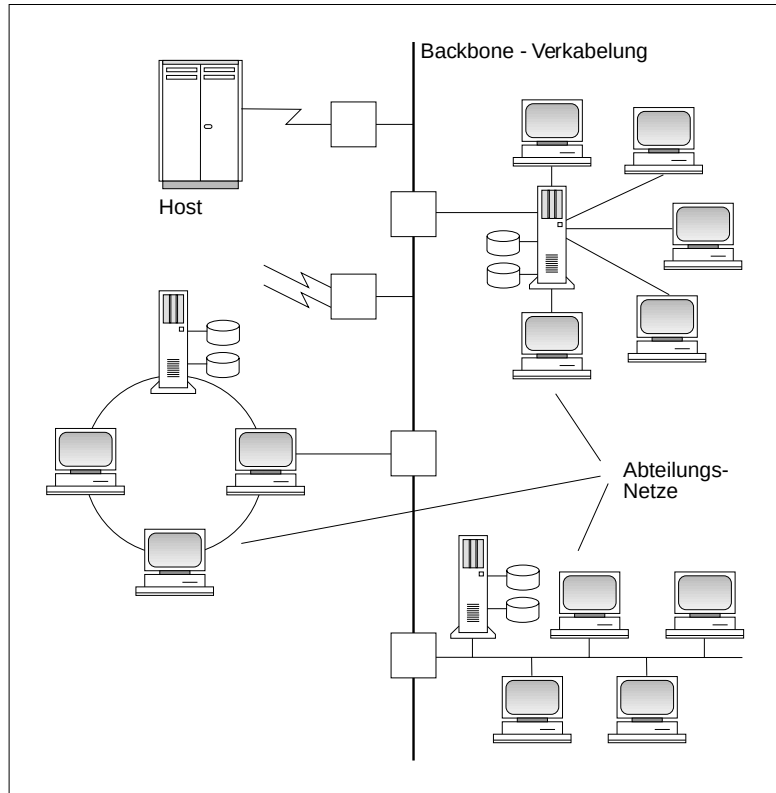
Bei dieser Art des Netzwerkaufbaus verwendet man ein zentrales, das gesamte Unternehmen umspannende Netzwerk als Rückgrat (Backbone) der Verkabelung, um darin mit Hilfe von Koppellementen alle anderen Subnetze des Unternehmens anzubinden. Damit ist es möglich, ein unternehmensweites Netzwerk aufzubauen, in dem jeder mit jedem kommunizieren kann. Als Backbone kann im Prinzip jedes Netz und jede Verkabelung eingesetzt werden. Um den hohen Anforderungen eines Backbone-Netzwerks gerecht werden zu können, wurde allerdings ein leistungsfähiges Hochgeschwindigkeits-Netzwerk als Trägersystem entwickelt. Man kann als Backbone-Netzwerk also auch Ethernet- oder Token-Ring-Netzwerke verwenden, es werden in der Regel aber FDDI-, Fast-Ethernet-, Gigabit-Ethernet- oder ATM-Netzwerke eingesetzt.

Die Kopplung der Subnetze an den Backbone erfolgt durch Koppellemente, die eine logische Trennung der Netze durchführt (Bridges, Router, Brouter oder Switches), d.h., solange die Stationen auf ihrem eigenen Netzwerk arbeiten, ist der Backbone als Übertragungsmedium nicht notwendig.

Wird netzübergreifend gearbeitet, d.h., Daten werden von einem Server benötigt, die in einem anderen Subnetz gespeichert sind, oder es wird auf Komponenten zugegriffen, die sich direkt im Backbone befinden, steht dem Anwender ein leistungsfähiges Netzwerk, der Backbone, zur Verfügung. In dieses Backbone-Netz können in der Regel alle eingesetzten Rechnersysteme und die damit verbundenen Netzwerkarchitekturen eingebunden werden.

3.2 Übertragungsmedien

Abbildung 3.5
LANs, die an einem
Backbone ange-
schlossen sind



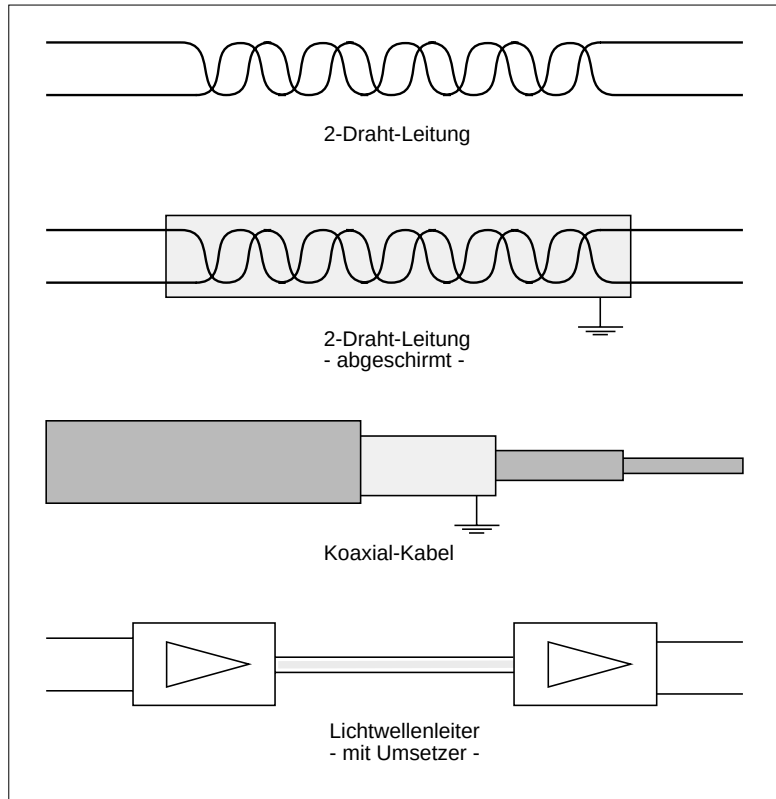
Es kann sich um Mainframes, MDTs, PCs, Communication-Server, Archive-Server etc. handeln, die in ein Gesamtnetzwerk zusammengeführt werden. In der neueren Fachliteratur wird die Backbone-Verkabelung auch als Primärverkabelung bezeichnet. Der weitere Ausbau der Subnetze kann in Form einer Sekundär- und Tertiärverkabelung durchgeführt werden. Bei der Besprechung von FDDI als spezielles Backbone-Netzwerk in einem späteren Kapitel werde ich auf diese Art des Aufbaus von Netzen noch genauer eingehen.

3.2 Übertragungsmedien

Ein Lokales Netz ist nicht nur durch seine topologischen Eigenschaften bestimmt, sondern auch durch die Art der verwendeten Übertragungsmedien, mit denen es arbeiten kann.

3 Kenndaten Lokaler Netzwerke

Abbildung 3.6
Unterschiedliche
Kabeltypen für den
Aufbau von LANs



Man unterscheidet folgende Übertragungsmedien (siehe Abbildung 3.6):

- verdrehte Zweidrahtleiter (Telefonkabel)
- verdrehte Vierdrahtleiter (IBM-Verkabelung bzw. CAT-5-Verkabelung in geschirmter und ungeschirmter Ausführung)
- Koaxialkabel
- Lichtwellenleiter (Glasfaserkabel)

Die verwendeten Kabeltypen unterscheiden sich nicht nur in ihren Kosten, sondern auch durch die möglichen Übertragungsraten, die Anfälligkeit gegenüber elektromagnetischen Störungen, Verlegbarkeit (Biegeradien, Durchmesser) und die überbrückbaren Entfernungen (Dämpfung, Einstreuung).

Verdrillte Kupferkabel (Twisted-Pair)

Die verdrehte Kupferdoppelader ist schon lange durch den Einsatz im Fernmeldewesen bekannt und stellt das kostengünstigste Verkabelungssystem dar. Dabei werden Paare von Kupferdrähten zu einer Spiralförmigkeit verdreht, wodurch im Vergleich zur nicht verdrehten Dop-

3.2 Übertragungsmedien

pelader Störeinflüsse von außen keinen besonders großen negativen Effekt mehr ausüben können (sofern die Störstrahlungen nicht zu groß werden).

Bei der Verdrillung der Adern hat man inzwischen unterschiedliche Techniken entwickelt, um die Leistungsfähigkeit, d.h. die möglichen Übertragungsraten, noch weiter zu erhöhen. So werden zum Beispiel paarweise verdrehte Kabel angeboten oder besondere Sternviererverseilung (auch verdrehte Kabel). Bei der Sternviererverseilung sind alle vier Adern (nicht mehr jedes Paar einzeln) und dann diese Paare schließlich nochmals ineinander verdreht.

Man unterscheidet bei Twisted-Pair-Kabeln zwischen Unshielded- (UTP) und Shielded-Twisted-Pair (STP). Shielded-Twisted-Pair-Kabel besitzen eine Abschirmung um jedes Adernpaar. Diese sind dann miteinander verdreht, und darum wird nochmals ein Metallmantelgeflecht gelegt.

Beim Unshielded-Twisted-Pair-Kabel sind, je nach Hersteller, die vier Adern verdreht (oder Sternviererverseilung), dann mit einer Metallfolie umgeben und schließlich mit einem Metallmantelgeflecht versehen.

UTP-Kabel sind bezüglich der Verkabelung wesentlich einfacher zu handhaben, da diese Kabel dünner und flexibler sind als normale STP-Kabel. Mag man den Prognosen glauben schenken, dann wird sich auf dem Gebiet der Verkabelung, vor allem wenn es um strukturierte Verkabelung geht, das UTP-Kabel durchsetzen (meist in Verbindung mit Lichtleiterverkabelung).

Koaxialkabel

Das Koaxialkabel kennt wahrscheinlich jeder, da dieser Kabeltyp für den Antennenanschluß des Fernsehers benutzt wird. Auch die IBM verwendet spezielle Koaxialkabel für den Anschluß von Terminals an die Steuereinheiten des IBM-Großrechners. Das Koaxialkabel besteht aus einem äußeren Leiter, der einen innenliegenden Leiter vollständig umschließt und dadurch abschirmt. Die beiden Leiter werden durch einen Isolator, das Dielektrikum, voneinander getrennt.

Koaxialkabel werden in den verschiedensten Ausführungen angeboten und eingesetzt. Dies hängt davon ab, welche Netzwerktypen eingesetzt werden sollen. Weit verbreitet sind 50-Ohm-Kabel für Ethernet, 75-Ohm-Kabel für Breitbandnetze oder 93-Ohm-Kabel für ARCNET-Netzwerke. Die Kabel können einen Durchmesser von 3 Millimeter bis zu 1,5 Zentimeter haben.

Die Bedeutung der Koaxialkabeltechnik weicht aber immer mehr der UTP-Verkabelungstechnik, weil mit ihr eine wesentlich höhere Flexibilität erreicht werden kann. Es ist inzwischen möglich, über ein

3 Kenndaten Lokaler Netzwerke

und dasselbe UTP- bzw. STP-Kabel Ethernet-, Token-Ring-, CDDI-, ATM- oder ARCNET-Netzwerke aufzubauen. Der Trend geht in die Richtung, dasselbe Kabel für alle notwendigen Kommunikationsdienste (inklusive Telefon, ISDN etc.) verwenden zu können. Wenn es jedoch um den Aufbau kleinerer Netze geht, wird bis auf weiteres die herkömmliche Koaxialverkabelung in Verbindung mit Ethernet eingesetzt werden, da diese preiswerter ist. Es zeichnet sich jedoch ab, daß auch diese Technik in kleineren Netzen der Twisted-Pair-Technologie weicht, da auch die aufwendigen Komponenten immer preiswerter werden. Der Aufbau von Token-Ring-, FDDI- oder ATM-Netzwerken in einem kleinen Unternehmen würde zu hohe Kosten verursachen. Geht es jedoch darum, leistungsfähige Netzwerke aufzubauen und dennoch preiswerte Komponenten dafür verwenden zu können, sollte man inzwischen Fast Ethernet bzw. Gigabit Ethernet näher in Betracht ziehen, da gerade auf diesem Gebiet die Leistungen permanent zunehmen und die Preise hingegen ständig fallen. Sie werden später noch sehen, daß es beim Einsatz von Twisted-Pair-Kabeln immer um eine sternförmige Verkabelung geht. Die Komponenten hierzu sind teurer, und Sie benötigen wesentlich mehr Kabel, als dies bei einer Busverkabelung (Koaxialkabel) der Fall ist.

Lichtleiterkabel (Glasfaser)

Beim Einsatz von Kupferkabeln (metallische Leiter) werden die Binärdaten in Form von elektrischen Signalen übertragen. Die Umwandlung der Binärdaten in diese elektrischen Signale wird unter anderem von der Netzwerkadapterkarte durchgeführt. Der Lichtleiter hingegen transportiert die Binärdaten in Form von Lichtsignalen. Ein wesentliches Merkmal dieser Verkabelungsart ist die hohe Übertragungskapazität, die erzielt werden kann. Es sind Kapazitäten denkbar, die im Bereich von einigen Gbit/s liegen. Zudem können die Lichtsignale nicht durch elektrische oder elektromagnetische Störquellen beeinflusst werden. Wenn LANs in Produktionsbetrieben installiert werden sollen, die durch sehr hohe magnetische Störstrahlungen beeinflusst sind, können meist nur noch Lichtleiterkabel verwendet werden, da ansonsten eine störungsfreie Übertragung nicht mehr gewährleistet werden kann. Inzwischen werden von vielen Herstellern Komponenten angeboten, mit denen es möglich ist, gemischt Kupfer- und Lichtleiterverkabelung einzusetzen. Das heißt, in den Bereichen, wo es ausreicht, werden Kupferkabel verlegt, wenn es die Umgebung dagegen erfordert, wird mit Lichtleiterkabeln gearbeitet.

3.2 Übertragungsmedien

Die weiteren Merkmale der Lichtwellenleiter sind:

- Sehr hohe Abhörsicherheit im Gegensatz zum Kupferkabel, ein Einkoppeln in den Lichtleiter ist fast unmöglich.
- Es tritt kein Nebensprechen auf, so wie es aus dem Fernsprechbereich bekannt ist. Schlechte Twisted-Pair-Kabel weisen übrigens das gleiche Problem auf.
- Durch die Übertragung von Lichtsignalen eignet sich dieses Medium besonders gut in explosionsgefährdeten Umgebungen.
- Ohne daß Verstärker (Repeater) eingesetzt werden müssen, liegen die überbrückbaren Entfernungen im Kilometerbereich (in Abhängigkeit vom Kabel).

Zusammengefaßt ergeben sich folgende charakteristische Eigenschaften:

- *Verdrillte Zweidrahtleitung*
 - am billigsten
 - 9.6 Kbit/s bis mehrere 100 Kbit/s
 - am stör anfälligsten
 - leicht zu verlegen
 - geringe Ausdehnung
- *Verdrillte Vierdrahtleiter* (spezielle Kabel, je ein Paar verdrillt und abgeschirmt, die Leiterpaare selbst sind dann noch einmal mit einem Metallmantel abgeschirmt – UTP bzw. STP)
 - relativ teuer (im Vergleich zum Zweidrahtleiter)
 - 4 Mbit/s bis 16 Mbit/s, das IBM-Verkabelungssystem ist für diesen speziellen Leitertyp bis 16 Mbit/s getestet
 - die neuen Kabeltypen müssen den Anforderungen CAT 5 oder höher entsprechen
 - die Anforderung an ordnungsgemäße Verkabelung steigt mit zunehmenden Übertragungsgeschwindigkeiten (derzeit mehr als 1 Gbit/s über TWP-Verkabelung möglich)
 - Standardkabellänge ≤ 90 Meter (s. Kapitel »Netzwerkkonzeption«)
- *Koaxialkabel* (Basisband)
 - mittlere Preislage
 - hohe Übertragungsraten bis 50 Mbit/s
 - relativ gute Verlegung
 - noch besser gegen Störanfälligkeit abgesichert
 - relativ große Entfernungen möglich
- *Koaxialkabel* (Breitband)
 - können sehr teuer werden
 - Übertragungsraten bis 500 Mbit/s möglich
 - relativ gute Verlegung
 - gutes Verhalten gegen Störeinflüsse
 - große Entfernungen möglich

3 Kenndaten Lokaler Netzwerke

- *Lichtwellenleiter* (Glasfaserkabel)
 - momentan noch die teuersten
 - Übertragungsraten im Gigabit-Bereich
 - leicht zu verlegen
 - Störeinflüsse von außen können die Übertragung nicht beeinträchtigen
 - enorm hohe Entfernungen möglich

Es hängt von der Leistung und den Umgebungsbedingungen des Lokalen Netzes ab, welchen Kabeltyp Sie verwenden wollen. Der Lichtwellenleiter kann inzwischen bei allen Standardtopologien gemischt verwendet werden. An den Stellen also, wo normales Kupferkabel ausreicht, sollten Sie diese Verkabelung verwenden. Ist es jedoch aufgrund der Umgebungsbedingungen nicht möglich, z.B. wegen zu starker elektromagnetischer Einstrahlung in Produktionsstätten, verwenden Sie für diesen Teilstrang das nicht störanfällige Glasfaserkabel. Die entsprechenden Umsetzer und Adapter sind bereits verfügbar. Wenn sich der Einsatz dieser Systeme immer mehr durchsetzt, werden im Lauf der Zeit auch die Kosten für den Lichtwellenleiter sinken. In bestimmten Situationen müssen Kostenvergleiche für »Fiber to the Desk« und herkömmlichen TWP-Verkabelungen durchgeführt werden, um eine optimale Entscheidungsgrundlage zu haben. In einigen Jahren ist es wahrscheinlich üblich, einheitlich Glasfaserverkabelungen durchzuführen.

3.3 Übertragungstechnologie (Basisband versus Breitband)

Jedes Verkabelungssystem arbeitet mit einer bestimmten Übertragungsbandbreite. Diese Bandbreite ist ausschlaggebend für die maximale Übertragungsgeschwindigkeit, mit der ein Lokales Netzwerk arbeiten kann. Wenn wir von einer Übertragungsleistung von 10 Mbit pro Sekunde sprechen, bedeutet dies, daß die Signale mit 10 MHz über das Medium Kabel übertragen werden. Diese 10-MHz-Frequenz ist die Übertragungsbandbreite des Netzes.

Bei der Basisbandtechnologie wird die gesamte Bandbreite für die Übertragung der Signale verwendet. Es kann somit nur zu einem Zeitpunkt in einer Richtung übertragen werden. Eine Darstellung dieses Prinzips finden Sie in Abbildung 3.7.

Im Gegensatz dazu können bei der Breitbandtechnologie zu einem Zeitpunkt mehrere unterschiedliche Übertragungen über ein und dasselbe Kabel erfolgen.

3.3 Übertragungstechnologie (Basisband versus Breitband)

Ein typisches Breitbandnetz kennen Sie aus dem täglichen Leben. Wenn Sie sich Ihren Fernseher zu Hause ansehen, werden Sie feststellen, daß an diesem nur ein Kabel an der Rückseite mit der Fernsehantenne verbunden ist. Dennoch ist es möglich, daß Sie mehr als ein Programm über nur ein vorhandenes Kabel (Koaxialkabel) empfangen können.

Abbildung 3.7
Basisband-Netz-
werktechnologie

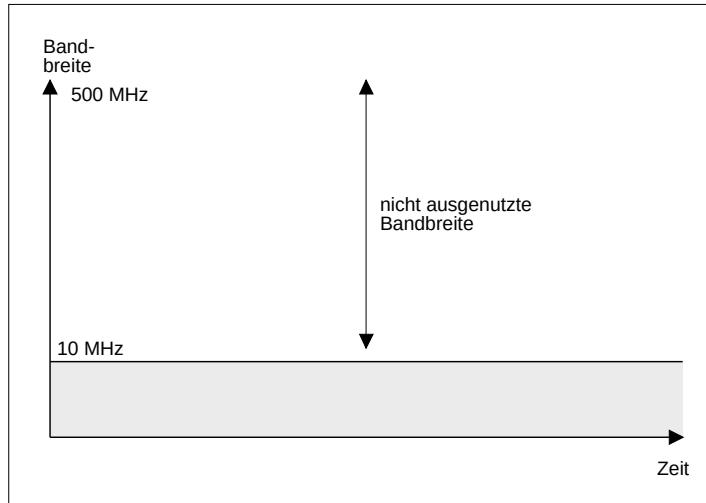
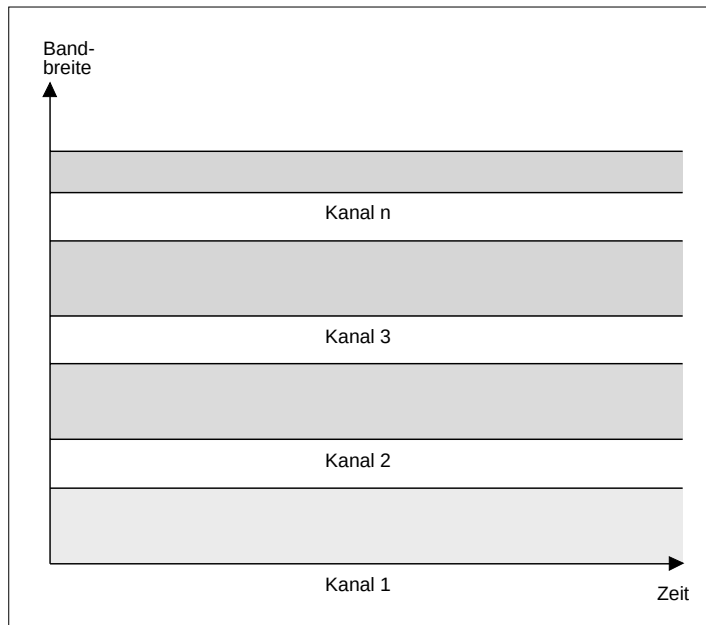


Abbildung 3.8
Breitband-Netz-
werktechnologie



3 Kenndaten Lokaler Netzwerke

Das Breitbandsystem teilt das gesamte Frequenzspektrum, das zur Verfügung steht, in kleinere Frequenzbänder ein. Jedem Übertragungsdienst wird auf diese Weise ein ganz bestimmtes Frequenzspektrum zugewiesen, auf dem die Übertragung zu erfolgen hat. Um dies auch durchführen zu können, muß das zu übertragende Signal auf eine bestimmte Trägerfrequenz für einen dafür definierten Kanal aufmoduliert werden. Auf der Seite des Empfängers wird dieses modulierte Signal wieder demoduliert, d.h., die Trägerfrequenz wird herausgefiltert, und das ursprüngliche Nutzsignal (die Daten) steht zur Verfügung. Die entsprechenden Einrichtungen, die dies bewerkstelligen, werden deshalb auch als MODEM (MODulator und DEMoulator) bezeichnet. In Abbildung 3.8 ist dieses Prinzip dargestellt.

Das ISDN-Projekt (Integrated Services Digital Network) der Telekom zielt zum Beispiel darauf ab, ein Breitbandsystem zur Verfügung zu stellen, das es gestattet, über ein Kabel gleichzeitig bewegte Bilder (Videokonferenzen, Fernsehübertragung), Daten, Sprache (Telefonieren) und Festbilder zu übertragen. Für diese Dienste wird es dann ausreichend sein, einen multifunktionalen Arbeitsplatz einzurichten, der nur noch eine Anschlußleitung besitzt.

Für diese Art von Informationsübertragung eignen sich am besten Lichtwellenleiter, da diese in einem Frequenzbereich von bis zu einigen Giga-Hertz betrieben werden können.

3.4 Zugriffsverfahren in Lokalen Netzen

Aus den bisher beschriebenen Kennzeichen Lokaler Netze wissen Sie, daß LANs unter anderem dadurch gekennzeichnet sind, daß alle angeschlossenen Stationen zur Kommunikation und Datenübertragung ein und dasselbe Transportmedium (Kabel) verwenden müssen. Ein Beispiel aus dem Alltag soll dies verdeutlichen.

Stellen Sie sich eine große, lange Straße in einer Stadt vor. In diese Straße münden lauter Nebenstraßen ein. Die große, lange Straße soll unser Übertragungsmedium im Netzwerk symbolisieren, und die Nebenstraßen sind unsere angeschlossenen Arbeitsstationen. Die Straßen werden von Verkehrsteilnehmern zur Beförderung von Waren genutzt (auf Lokale Netze umgesetzt: der Transport von Informationen). Jeder, der Waren befördern will, muß von den Nebenstraßen auf die große, lange Straße einbiegen.

Wenn dieses Einreihen in den Verkehrsfluß im Straßenverkehr nicht geregelt werden würde (durch Ampeln, Vorfahrtsschilder, Verkehrspolizisten), entstünde das reinste Chaos. Sie kennen dies bestimmt – sobald die Ampel an einer Kreuzung ausfällt, ist der Verkehrsfluß ge-

3.4 Zugriffsverfahren in Lokalen Netzen

stört, und es bilden sich Staus. Genauso verhält es sich in Lokalen Netzen, da nur ein Übertragungsmedium für alle Teilnehmer zum Transport von Daten zur Verfügung steht. Es muß genau festgelegt werden, wer zu welchem Zeitpunkt das Kabel zur Datenübertragung verwenden darf. Zwei gleichzeitige Nutzer sind bei den herkömmlichen Verfahren nicht erlaubt. Im Lauf der Zeit haben sich drei Verfahren als Standard für die Kommunikationsregelung in Lokalen Netzen durchgesetzt. Dies sind:

- CSMA/CD (für Bussysteme)
- Token-Passing (für Ringtopologie)
- Token-Bus (für Bustopologie mit Token-Verfahren)

Wir werden im folgenden Abschnitt diese drei Verfahren der Reihe nach genauer behandeln.

Da im LAN für alle Stationen nur ein Übertragungsmedium zur Verfügung steht, muß auf irgendeine Weise geregelt werden, wer zu welchem Zeitpunkt dieses Medium zum Senden seiner Daten nutzen darf. Da es für die verschiedensten LAN-Topologien auch unterschiedliche Zugangsverfahren gibt, werden von IEEE diesbezüglich verschiedene Standards festgelegt, die auch als IEEE-802-Standards bezeichnet werden (zum ISO-Standard s. Kapitel 9).

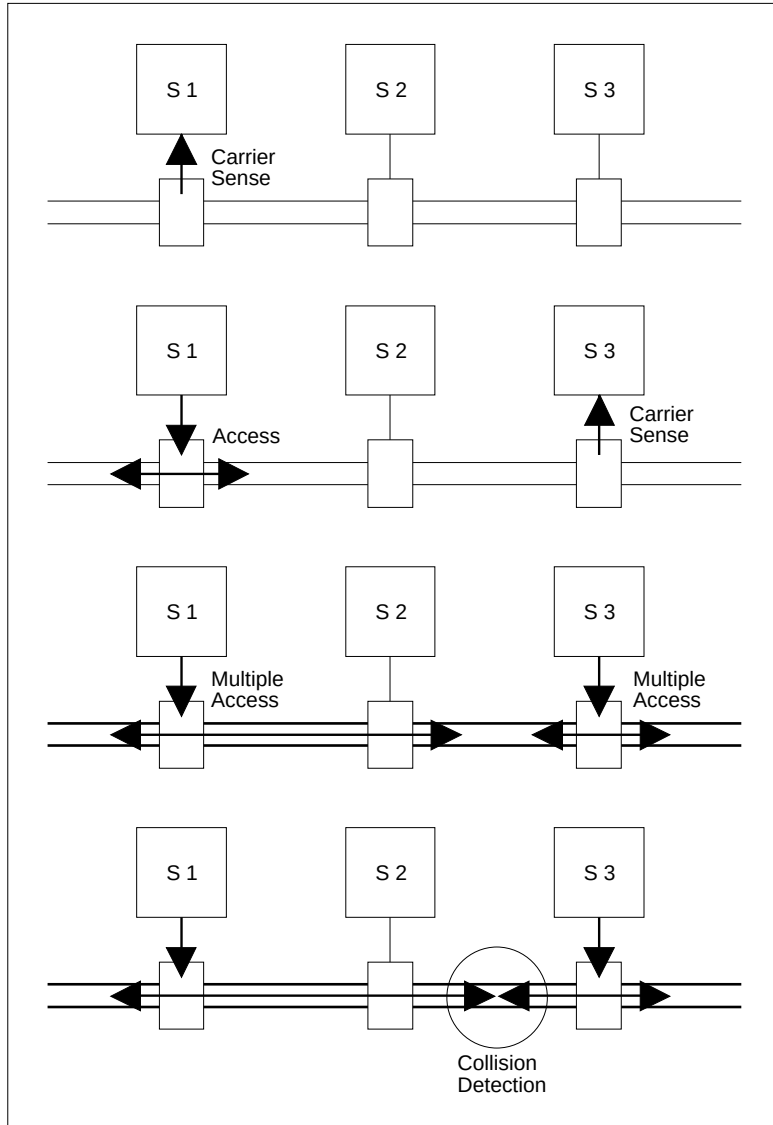
3.4.1 CSMA/CD-Zugriffsverfahren (IEEE 802.3)

An dieser Stelle sei auf folgende Unterschiede hingewiesen:

- In der Literatur werden der IEEE-802.3- und der Ethernet-Standard gleichgesetzt. Beide Varianten unterscheiden sich jedoch grundlegend, so daß es nicht möglich ist, LANs, die auf IEEE-802.3- und Ethernet-Standard basieren, miteinander zu mischen. Wenn wir im folgenden von Ethernet sprechen, meinen wir damit den IEEE-802.3-Standard.
- Im 802.3-Standard wird neben den Spezifikationen für die Schicht 1 (Physical Layer, Medium Attachment, Physical Signaling) vor allem auch das Zugriffsverfahren für das gemeinsam benutzte Medium, das Übertragungsmittel für die Kommunikation im Netz, festgelegt. Das heißt, dieser Standard definiert die MAC-Ebene, Media Access Control, eine Unterschicht der Ebene 2. Die für Ethernet definierte Zugriffsmethode wird als CSMA/CD bezeichnet (Carrier Sense Multiple Access with Collision Detection Access Method). Wir wollen uns im folgenden dieses Verfahren etwas genauer ansehen.
- Der IEEE-802.3-Standard definiert die CSMA-Variante für das 1-persistent-Protokoll. An dieser Stelle sei deshalb nur erwähnt, daß es für das Zugriffsverfahren CSMA mehrere Abwandlungen gibt, zum Beispiel CSMA/CA oder CSMA/CE.

3 Kenndaten Lokaler Netzwerke

Abbildung 3.9
Das CSMA/CD-
Zugangsverfahren



In Abbildung 3.9 sehen Sie eine Darstellung des CSMA/CD-Verfahrens. Die Zuteilung der Genehmigung, welche sendewillige Station wann über das Kabel verfügen darf, wird wie folgt festgelegt:

1. Die sendewillige Station überwacht, ob der Kanal frei ist oder gerade von einer anderen Station zur Datenübertragung benutzt wird (carrier sense, listen before talking).

3.4 Zugriffsverfahren in Lokalen Netzen

2. Ist der Kanal frei, beginnt die Station zu übertragen. Die Übertragung wird jedoch frühestens 9,6 Mikro-Sekunden (interframe gap) nach Freiwerden des Mediums begonnen.
3. Ist der Kanal jedoch belegt, wird er weiter überwacht und abgehört, bis er als nicht mehr belegt erkannt wird. Wird der Kanal dann als frei vorgefunden, wird sofort mit der Übertragung begonnen.
4. Während die Übertragung der Station durchgeführt wird, wird der Kanal weiter abgehört, d.h., die eigene Übertragung wird zusätzlich überwacht. Dieser Mechanismus wird auch als *listen while talking* bezeichnet.
5. Da das Signal der momentan sendenden Station eine gewisse Zeit braucht, bis es bei allen Rechnern angekommen ist, kann der Fall eintreten, daß eine weitere sendewillige Station den Kanal als frei vorfindet, während das Signal der anderen bei dieser noch nicht angekommen ist (multiple access).
Dann treffen auf dem Kanal die Signale von zwei Stationen aufeinander, und die Übertragung bzw. die Signale sind zerstört. Da jede sendende Station die eigenen Signale auch mit abhört, wird eine solche Kollision erkannt und die Übertragung sofort abgebrochen. Anschließend wird ein spezielles Störsignal (jam signal) auf den Kanal gegeben.
6. Nach Absenden des Störsignals wird eine bestimmte Zeit gewartet (backoff) und dann die CSMA-Übertragung erneut versucht.

Diese Wartezeit wird nach bestimmten Regeln festgelegt. Die Berechnung der Zeit erfolgt nach dem Truncated-binary-exponential-back-off-Verfahren. Die Verzögerungszeit wird mit $i \cdot \text{SlotTime}$ festgelegt. Die SlotTime entspricht dabei der Übertragungszeit für 64 Byte. Die Zahl i ist der zufällige Wert einer gleichverteilten Zufallsgröße (eine natürliche Zahl) im Intervall: $0 \leq i \leq 2k$, wobei $k = \min(n, 10)$ ist und n die Durchnummerierung des Wiederholungsversuchs für dieselbe Sendung repräsentiert. Nach 10 vergeblichen Sendeversuchen wird das Back-off-Intervall nicht weiter vergrößert. Nach 16 Fehlversuchen wird eine Fehlermeldung erzeugt. Daran ist zu erkennen, daß man durch den Algorithmus versucht, sich an steigende Netzlasten anzupassen. Es ist auch zu erkennen, daß Neubewerber dabei im Vorteil sind. Da zu den Neubewerbern alle Wiederholungsversuche kommen, stellt bei hohen Verkehrslasten der Kollisions-Overhead eine zusätzliche, die Konfliktwahrscheinlichkeit erhöhende Last dar.

3 Kenndaten Lokaler Netzwerke

Es gibt drei Typen von Algorithmen zur Festlegung der Aktion, die eine Station durchführen muß, wenn diese den Kanal als belegt vorfindet:

- *1-persistent*

Dies ist das Verfahren, das im 802.3-Standard festgelegt worden ist.

- *Non-persistent*

Die Station wartet eine Zeitdauer zufälliger Länge, bevor sie den Kanal wieder abhört.

- *p-persistent*

Die Station hört den Kanal so lange ab, bis er frei ist, dann sendet sie mit der Wahrscheinlichkeit p . Mit der Wahrscheinlichkeit $1-p$ wartet sie eine festgelegte Zeit, dann hört sie den Kanal erneut ab, d.h., sie wiederholt die Prozedur.

Das CSMA/CD-Verfahren ist mit Ethernet bekanntgeworden. Ein Nachteil von CSMA/CD ist, daß dieses Verfahren nicht deterministisch ist, d.h., es kann nicht genau festgelegt werden, zu welchem Zeitpunkt die einzelne Station senden wird. Für Realzeitsteuerung ist dieses Verfahren deswegen nicht zu gebrauchen.

Zudem kann der Durchsatz bei einer bestimmten Anzahl aktiver Stationen und einer gewissen Grenzlast des Systems sehr langsam werden bzw. gar zum Stillstand kommen.

Dieser Grenzbereich hängt von mehreren Faktoren ab, die wir in einem späteren Kapitel näher behandeln wollen.

3.4.2 Token-Passing-Zugriffsverfahren (IEEE 802.5)

Das Token-Passing-Verfahren wird in der Fachliteratur oft auch Token-Ring-Verfahren, sequentielle Token-Methode oder Newhall-Verfahren genannt. Das Newhall-Verfahren geht auf den Erfinder dieses Zugriffsverfahrens zurück (Newhall und Farmer, 1969).

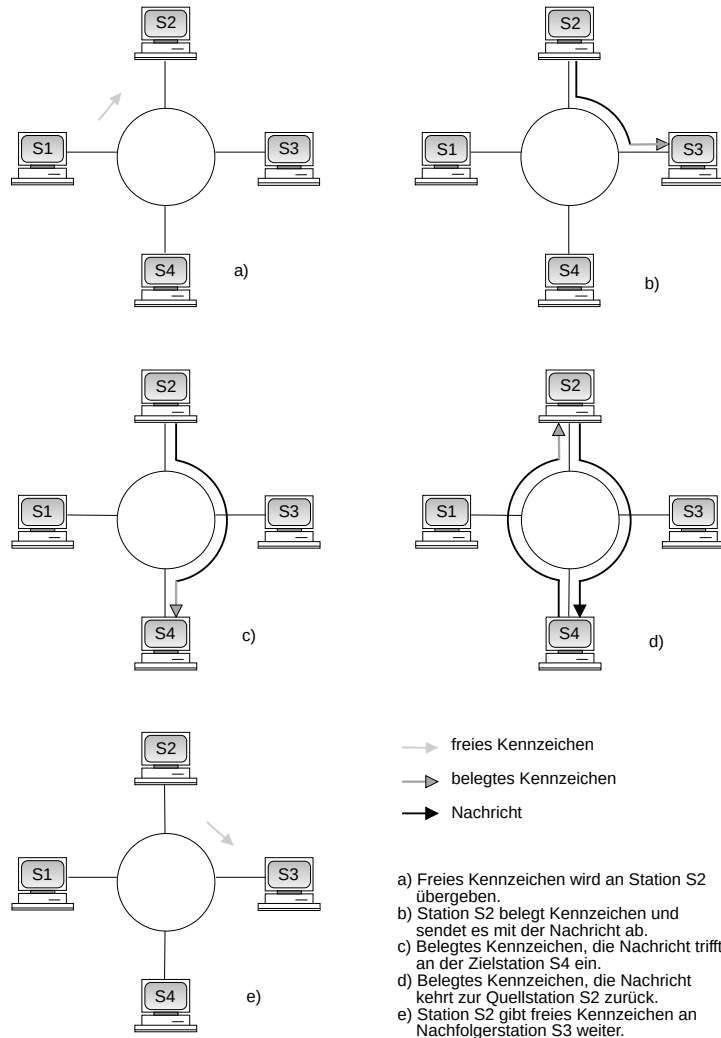
Abbildung 3.10 zeigt das Prinzip des Token-Passing-Verfahrens.

Ein Token ist ein spezielles Bitmuster, eine Datenstruktur, die dazu dient, das Zugriffsverfahren in einem Ring zu steuern.

Beim Token-Ring kreist ein Token (Berechtigungsmarke) im Ring und gibt den jeweiligen Stationen die Erlaubnis zu senden. Im Ring kann zu einem Zeitpunkt, wie bei allen bisher besprochenen Zugangsverfahren, nur eine Station senden. Diese Station muß das Token besitzen. Eine Station, die senden will, kann dies nur dann durchführen, wenn sie ein als *frei* markiertes Token empfängt.

3.4 Zugriffsverfahren in Lokalen Netzen

Abbildung 3.10
Das Token-
Passing-Zugangs-
verfahren



Sie ändert sodann den Zustand des Tokens in *belegt* und sendet ihre Daten direkt im Anschluß an das Belegt-Token. Stehen in der Station keine Daten an, die gesendet werden müssen, so gibt sie das Frei-Token sofort an die nachfolgende Station weiter. Empfängt eine Station ein Token, das als belegt gekennzeichnet ist, weiß diese, daß anschließend Nachrichten eingehen werden. Jede Station, außer der, die die Nachrichten gesendet hat, überprüft sodann, ob die mitübertragene Empfängeradresse mit der eigenen Stationsadresse übereinstimmt. Bei Übereinstimmung kopiert die betroffene Station die

3 Kenndaten Lokaler Netzwerke

Nachricht in den hierfür vorgesehenen Pufferbereich. Danach wird der gesamte Nachrichten-Frame (Token und Nachricht) an die nächste Station weitergegeben. Der komplette Frame wird dann auf alle Fälle zur nächsten Station weitergegeben. Dabei wird jedoch ein sogenanntes Antwortbit gesetzt, das für den Sender der Nachricht notwendig ist. Die gesendete Nachricht kreist genau einmal um den Ring und trifft nach einem Umlauf wieder beim Sender ein. Die Station, die die Nachricht versendet hat, nimmt den Frame wieder vom Ring. Diese Station erzeugt anschließend ein neues Frei-Token und übergibt dieses an die nächste Station weiter, wenn die Übermittlung der Nachricht abgeschlossen ist und das Belegt-Token, das einmal im Ring gekreist ist, beim Sender der Nachricht wieder eingetroffen ist. Trifft beim Sender der Nachricht ein Frame ein, der nicht die eigene Quellenadresse enthält, muß ein Fehler aufgetreten sein, also mehr als ein Token im Netz existieren, und es wird daher kein Frei-Token erzeugt. Die Fehlerbeseitigung ist Aufgabe der *Monitorstation* (siehe weiter unten).

Zu bemerken ist noch, daß jede Station eine Verweilzeit von 1 Bit in ihrem Ring-Interface benötigt, um Bits während der Weiterleitung ändern zu können. Sendet eine Station ein Frei-Token, so hat die Folgestation die Möglichkeit, sich das Token anzueignen und selbst Nachrichten zu versenden. Unter sehr starker Last des Rings erfolgt der Zugang zum Ring nach einer *Round-Robin-Methode*. Unter Kenntnis der maximalen Nachrichtenlänge ist es nun möglich, die maximal auftretende Wartezeit für den Ringzugang zu berechnen.

Da die Quellstation die eigene Nachricht wieder empfängt und entfernt, kann die Nachricht eine Antwort der Empfängerstation enthalten. Dies erlaubt es dem Sender festzustellen, ob die Empfängerstation aktiv ist oder nicht, ob sie beschäftigt ist (dann wurde die Nachricht nicht kopiert und unquittiert weitergegeben), ob die Nachricht richtig empfangen worden ist oder im ungünstigsten Falle nochmal gesendet werden muß oder ob von einer anderen Station im Ring ein Fehler entdeckt worden ist.

In Abbildung 3.11 bzw. Abbildung 3.12 ist der Aufbau des Tokens und des Nachrichtenpakets aufgezeigt.

Wie in Abbildung 3.12 zu sehen ist, besteht die Möglichkeit, im Token einen Prioritätsindikator anzugeben. Was kann mit dieser Angabe bewirkt werden?

Eine Station, die ein Datenpaket mit hoher Priorität senden will, kann in das Belegt-Token ihre Prioritätsstufe eintragen. Wenn der momentane Sender ein Frei-Token erzeugt, besitzt das neue Frei-Token diese hohe Priorität.

3.4 Zugriffsverfahren in Lokalen Netzen

Abbildung 3.11
Der Aufbau des
802.5-Frame-
Formats

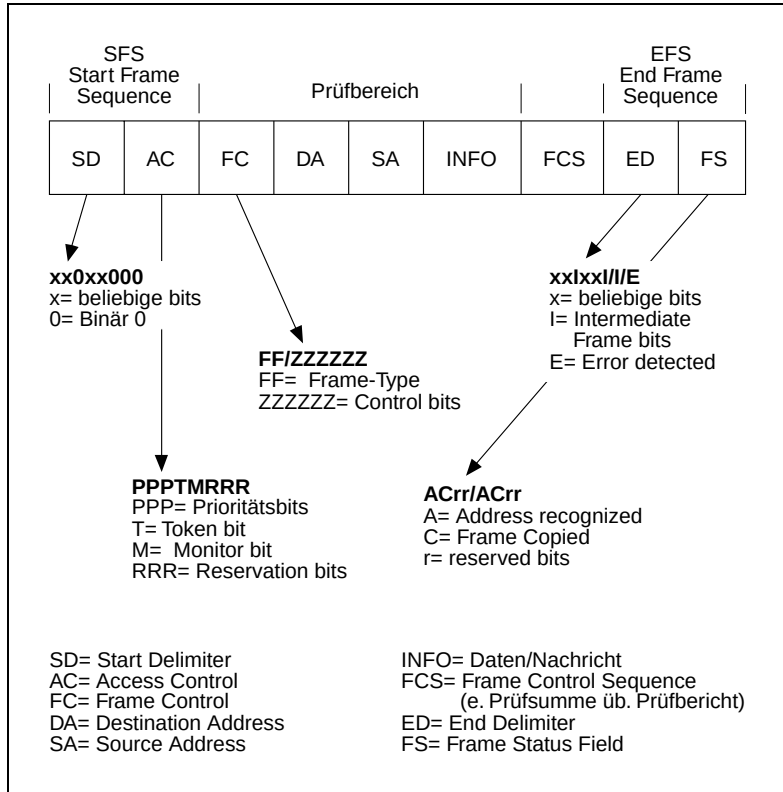
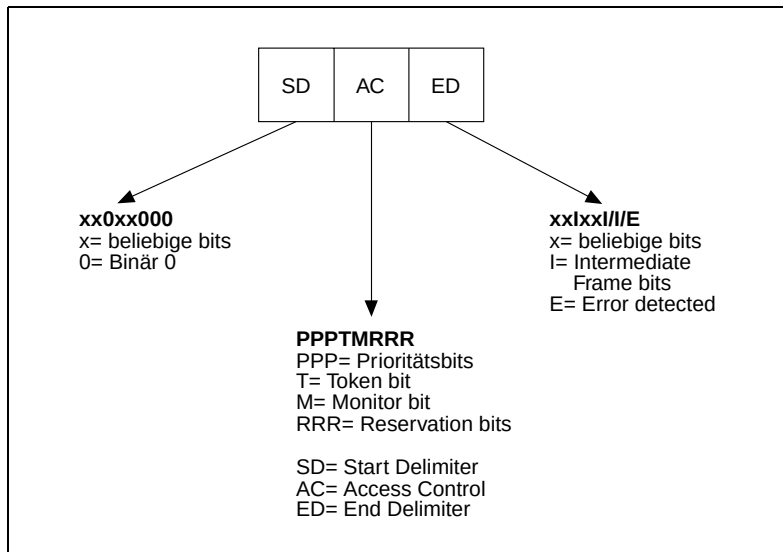


Abbildung 3.12
Der Aufbau des
802.5-Token-
Formats



3 Kenndaten Lokaler Netzwerke

Eine Station mit einer niedrigeren Priorität kann sich dann das Frei-Token nicht aneignen, um selbst Daten zu übertragen. Das Frei-Token mit der hohen Priorität wird so lange im Ring weitergereicht, bis die Station mit der hohen Priorität erreicht ist. Sind keine Datenpakete von dieser Station mehr zu übertragen, setzt diese die Prioritätsstufe wieder auf den ursprünglichen Zustand zurück, und das gewöhnliche Verhalten im Token-Ring-Netz ist wiederhergestellt.

Es wurde bereits angedeutet, daß es im Token-Ring-Netz eine sogenannte *Monitorstation* gibt. Generell ist es so, daß eine aktive Station als Monitorstation ausgezeichnet ist. Normalerweise besitzt die erste aktive Station, also die Station, die als erste im Netz eingeschaltet worden ist, diesen Status. Die Monitorstation ist für die Erkennung von Fehlern zuständig, d. h. für die Erkennung des Verlusts eines Tokens oder eines ständig kreisenden Belegt-Tokens. Ein Token-Verlust wird ganz einfach durch einen Zeitüberwachungsmechanismus erkannt. Dadurch, daß die maximale Zeit für ein einmalig zirkulierendes Frei-Token bekannt ist, erkennt dies die Monitorstation, wenn innerhalb dieser Zeit kein Frei-Token die Station passiert. Ist dieser Timeout abgelaufen, erzeugt die aktive Monitorstation ein neues Frei-Token, damit im Netz weitergearbeitet werden kann. Dieser Mechanismus kann ebenfalls für die erstmalige Erzeugung eines Frei-Tokens beim Starten des Netzes eingesetzt werden.

Ein ständig zirkulierendes Belegt-Token wird von der Monitorstation wie folgt erkannt und bereinigt:

Ein an der Monitorstation vorbeikommendes Belegt-Token wird durch Setzen eines bestimmten Bits im Token auf 1 markiert. Erkennt dann die Monitorstation ein Belegt-Token, das dieses Bit bereits gesetzt hat, dann weiß sie, daß das Datenpaket schon einmal um den Ring gelaufen und vom Sender bzw. von der Quelle nicht vom Ring entfernt worden ist. Dieser Fehler wird dadurch behoben, daß das Belegt-Token in ein Frei-Token umgewandelt wird. Im Token-Ring-Netz kann jede Station aktiver Monitor werden. Um zu vermeiden, daß mehrere Stationen die Rolle des aktiven Monitors übernehmen, können unterschiedliche Timeout-Zeiten oder ein spezieller Wettbewerbs-Auflösungsalgorithmus verwendet werden. Ebenfalls wird durch einen Protokollmechanismus dafür gesorgt, daß bei Ausfall oder nicht mehr existentem aktiven Monitor eine andere Station deren Aufgabe übernimmt.

3.4 Zugriffsverfahren in Lokalen Netzen

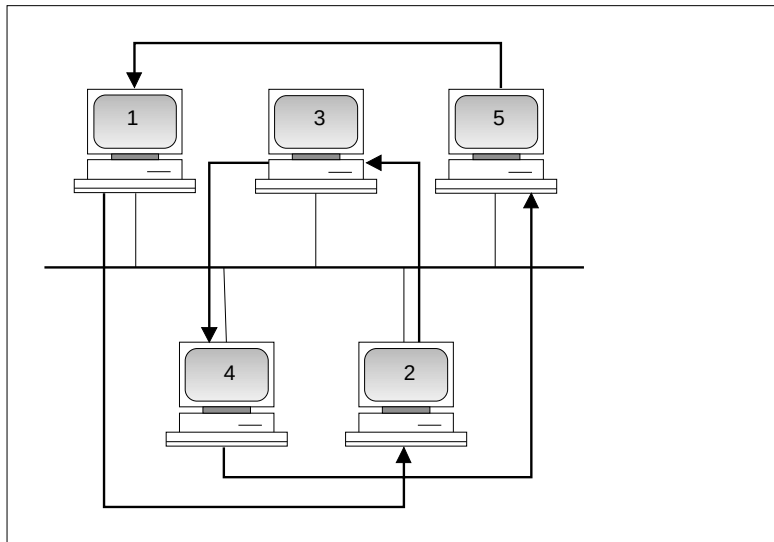
Bei der Token-Ring- bzw. Token-Passing-Methode kann man drei Merkmale erkennen:

1. Die Zugriffsmethode ist deterministisch und bezüglich der Steuerung dezentral gestaltet. Mit Hilfe mathematischer Verfahren läßt sich genau berechnen, wie lange eine Station im ungünstigsten Fall warten müßte, bis sie wieder senden darf.
2. Es handelt sich bei diesem Verfahren um ein »faïres« Verfahren, da jede Station pro freiem Token-Zyklus die Möglichkeit erhält, Daten zu übertragen.
3. Für Realzeitanwendungen kann eine obere Zeitschranke gewährleistet werden, bis ein Kanalzugriff für eine Station gewährt wird.

3.4.3 Token-Bus-Zugriffsverfahren (Token-Ring auf Bussystemen – IEEE 802.4)

Beim Token-Bus-Verfahren der Firma Datapoint handelt es sich physikalisch um eine Bustopologie, auf der jedoch protokollmäßig ein Ring implementiert ist. Von der Steuerung des Zugriffs wird das gleiche Token-Prinzip verwendet wie bereits oben beschrieben.

Abbildung 3.13
Token-Passing auf
Bustopologie



Beim Aufbau des logischen Rings muß von den einzelnen Stationen nur eine Tabelle geführt werden, wer Vorgänger bzw. Nachfolger der Station ist (siehe Abbildung 3.13). Mit Hilfe dieser Information ist es einfach, den logischen Ring auf der Busstruktur aufrechtzuerhalten.

3 Kenndaten Lokaler Netzwerke

Da Token-Bus die gleichen Vorteile bietet, wie beim Token-Passing-Zugriffsverfahren bereits beschrieben, wird dieses Protokoll für das MAP-Projekt (Manufacturing Automation Protocol) der Firma General Motors in den Standard aufgenommen. General Motors gab nur den Entwicklungsauftrag und ist nicht, wie oft behauptet wird, der Hersteller dieses Verfahrens.

Die mit dem Bus verbundenen Stationen bilden einen logischen Ring. Dieser logische Ring wird durch spezielle Mechanismen des eingesetzten Protokolls aufgebaut. Bei diesem Protokoll (Token-Passing, wir werden dieses Verfahren noch bei der Besprechung des Token-Ring-Protokolls antreffen) kreist ein spezielles »Paket«, Token genannt, auf diesem Ring. Das Token kann zwei Zustände annehmen: frei oder belegt. Die Station, die Daten über das Netz senden will, muß warten, bis sie ein freies Token erhält. Das Token wird dabei in einer geordneten Reihenfolge zwischen den Stationen transportiert, so daß eine Ringstruktur entsteht. Dabei muß jede Station Informationen darüber besitzen, wer ihr Nachfolger bzw. ihr Vorgänger ist. Diese Informationen pflegt jede Station durch das Führen einer Tabelle, in die eingetragen wird, welche Station Vorgänger und welche Nachfolger dieser einen Station ist. Ausschlaggebend hierfür sind die Node-Adressen der einzelnen Stationen, um den entsprechenden Adreßeintrag durchführen zu können. Aufgrund der Busverkabelung ist im Gegensatz zum klassischen Token-Ring-Verfahren die Reihenfolge der Stationen unabhängig von ihrer physikalischen Position im Netz.

Die Station, die das freie Token besitzt, kann Nachrichten senden oder Anforderungen an andere Stationen absetzen. Solange sie das Frei-Token besitzt, fungiert sie praktisch als Masterstation. Hat eine Station ihre Aufgaben erledigt oder ist ihre Zeit abgelaufen, muß sie das Token, als *Frei-Token* gekennzeichnet, an die in der Reihenfolge nächste Station weitergeben. Dies geschieht mittels einer Token-Übergabekontrollnachricht. Das Nachrichtenprioritätsschema ist vergleichbar mit dem des Token-Rings.

Bei der Verwaltung des Tokens sind folgende Gesichtspunkte zu beachten:

Aufnahme in den Ring

Da kein Netzwerk während des Betriebs statisch ist, weil neue Stationen hinzukommen oder die Arbeit beenden, muß diesen die Möglichkeit gegeben werden, periodisch in den Ring aufgenommen zu werden. Damit das geschehen kann, generiert die Station, die gerade das Token besitzt, periodisch eine Solicit-successor-Nachricht.

3.4 Zugriffsverfahren in Lokalen Netzen

Dieser Nachrichtenblock bewirkt, daß andere Stationen mit einer Adresse zwischen ihrer eigenen und der ihres Nachfolgers mit einer Anforderung für die Aufnahme in den Ring antworten. Die Station wartet eine gewisse Zeit. Die Zeitdauer entspricht dem Antwortfenster (mindestens jedoch doppelt so lange, wie die Ausbreitung des Signals von einem Ende zum anderen braucht). Existiert eine Aufnahmeanforderung, d.h., es muß eine neue Station in den Ring integriert werden, dann nimmt die das Token besitzende Station die neue Station als ihren Nachfolger in die Tabelle auf und sendet ihr das Frei-Token zu. Die Sendeberechtigung geht an die neu aufgenommene Station über. Wird eine Aufnahmeanforderung von mehr als einer Station gesendet, kollidieren diese »Rückmeldungen« und werden verstümmelt.

In diesem Fall sendet die das Token besitzende Station eine »resolve-contention«-Nachricht und wartet auf vier Antwortfenster. Die an der Kollision beteiligten Stationen verwenden die ersten beiden Bits ihrer Adresse, um das für ihre Anforderung zu benutzende Antwortfenster identifizieren zu können. Bemerkt die neue Station dabei einen Datenverkehr, bevor ihr Fenster an der Reihe ist, sendet sie keine Aufnahmeanforderung zurück. Tritt jedoch wieder eine Kollision auf, durchlaufen die an der Kollision beteiligten Stationen wieder eine Phase zur Kollisionsauflösung, die dann allerdings auf den nächsten beiden Adreßbits basiert. Dies geht so lange, bis eine eindeutige Anforderung über das Netz gelangt oder die maximale Anzahl von Versuchen überschritten ist.

Löschen aus dem Ring

Will eine Station den Ring verlassen, sendet sie, wenn sie das Token erhält, eine *Set-successor-Nachricht* an ihren Vorgänger. Die *Set-successor-Nachricht* enthält dabei die Information, wer der Nachfolger dieser Station ist. Der Vorgänger der Station schickt entsprechend eine Nachricht an seinen Nachfolger.

Doppeltes Token

Hört eine das Token besitzende Station eine andere Station senden, verwirft diese das Token und kehrt in den Empfangsmodus zurück.

Ausfall des Nachfolgers

Wird ein Token an den Nachfolger weitergegeben, muß dieser innerhalb des Antwortfensters antworten. Die das Token noch innehabende Station führt einen weiteren Versuch durch. Antwortet der Nachfolger immer noch nicht, sendet sie eine *Who-follows-Nach-*

3 Kenndaten Lokaler Netzwerke

richt. Mit dieser Nachricht versucht sie den Nachfolger der ausgefallenen Station zu finden. Die das Token besitzende Station sollte dann eine *Set-successor-Antwort* erhalten.

Nachdem sie diese Nachricht erhalten hat, berichtet sie ihre Nachfolgerinformation und gibt das Token weiter. Wenn notwendig, wird die *Who-follows-Nachricht* auch ein weiteres Mal gesendet. Ist dann jedoch immer noch kein Nachfolger ausfindig gemacht, sendet die das Token besitzende Station eine *Any-successor-Nachricht*. Zu diesem Zeitpunkt ist die Station froh, irgendeine andere Station als Nachfolger zu bekommen. Erhält sie immer noch keine Antwort, nimmt sie an, daß sie isoliert im Netz arbeitet, und schaltet in den Empfangsstatus um.

Initialisierung des Rings

Dieser Vorgang tritt in zwei Fällen ein:

1. Starten des Netzwerks
2. Verlust des Tokens

Der Verlust des Tokens wird bemerkt, wenn eine oder mehrere Stationen feststellen, daß für eine bestimmte Zeitdauer keinerlei Aktivität auf dem Bus ist. Ist in einer Station die Zeitüberwachung für die Ringinaktivität abgelaufen, dann gibt diese eine *Claim-token-Nachricht* auf den Bus. Dabei auftretende Kollisionen werden unter der Verwendung von Adressen wie oben bereits beschrieben aufgelöst.

Der Token-Passing-Bus zeichnet sich durch eine sehr komplexe Token-Verwaltung aus. Bei kleiner Last ist die Leistung dieses Verfahrens schlechter als CSMA/CD. Unter zunehmender Last ist er jedoch dem CSMA/CD-Verfahren überlegen. Treten keine Fehler auf, kann eine obere Grenze für die Verzögerung einer Nachricht angegeben werden. Der Bus kann länger sein als für CSMA/CD-Verfahren, da keine Notwendigkeit besteht, während des Sendens den Bus abzuhören, und die elektrischen Restriktionen weniger ins Gewicht fallen.

4

Netzwerkaufbau und Netzwerktopologien

Unter einem Netzwerk kann man ein modulares, erweiterbares und anpassungsfähiges System verstehen, das an den jeweiligen Bedarf der einzelnen Unternehmen angeglichen werden kann. Die Modularität erleichtert es, neue Komponenten hinzuzufügen oder bestehende Komponenten zu entfernen und an anderer Stelle wieder einzufügen. Im letzten Kapitel wurden bereits die Netzwerktopologie und das zugehörige Zugriffsverfahren gegenübergestellt. Ich will Ihnen in diesem Kapitel Ethernet, Token-Ring, Fast Ethernet, Gigabit Ethernet, FDDI und ATM näher vorstellen.

- Ethernet bietet im ursprünglichen Sinn eine lineare Busstruktur mit CSMA/CD-Zugriffsverfahren. Wie Sie noch sehen werden, kann Ethernet inzwischen auch als sternförmige Verkabelungsstruktur aufgebaut werden. Als Kabeltyp kommen Thin- oder Thick-Ethernet (Koaxialkabel), Twisted-Pair oder Glasfaserkabel in Frage.
- Token-Ring ist eine sternförmige Verkabelungsstruktur, die mit Hilfe spezieller Verkabelungskomponenten einen Ring bildet. Als Zugriffsverfahren werden Token-Passing und als Kabeltyp Twisted-Pair, Unshielded-Twisted-Pair oder Glasfaserkabel verwendet.
- Fast Ethernet ist eine Weiterentwicklung der herkömmlichen Ethernet-Technologie, um High-Speed-LANs aufbauen zu können. Mit dieser Netzwerktechnik sind Übertragungsgeschwindigkeiten von 100 Mbit/s möglich.
- Gigabit Ethernet und Fast Ethernet haben das 100VG-AnyLAN vom Markt verdrängt. 100VG-AnyLAN war eine High-Speed-LAN-Entwicklung von HP. Auch diese LAN-Technik hat Übertragungsgeschwindigkeiten von 100 Mbit/s zugelassen. Wie so oft haben sich leider zwei Lager für 100-Mbit/s-Ethernet-Netzwerke gebildet: die Technik von DEC und die von HP. Die nächsten Monate werden zeigen, welcher Hersteller sich am Markt behaupten kann – so stand es in der 4. Auflage. Inzwischen ist bekannt, daß HP diese Entwicklung aufgrund zu geringer Marktdurchdringung aufgegeben hat. Dafür hat sich eine noch schnellere Ethernet-Variante am Markt etabliert – anfangs von allen Herstellern, die keine adäquaten Komponenten anbieten konnten, belächelt. Inzwischen werden jedoch von allen führenden Herstellern entsprechende Komponenten und Produkte für Gigabit Ethernet angeboten und zur Verfügung gestellt. Bei Gigabit Ethernet handelt es sich ähnlich

4 Netzwerkaufbau und Netzwerktopologien

wie bei Fast Ethernet um eine Ethernet-Technologie, um noch schnellere High-Speed-LANs aufbauen zu können: Mit ihr können mit 1000 Mbit/s im Netz Datenübertragungen durchgeführt werden.

- FDDI (Fibre Distributed Data Interface) bildet ein Hochgeschwindigkeitsnetz auf Basis einer Ringstruktur und Token-Passing-Zugriffsverfahren. Standardmäßig wird für dieses Netzwerk eine reine Glasfaserverkabelung verwendet. Es gibt jedoch inzwischen Produkte, mit denen FDDI auf Unshielded-Twisted-Pair-Kabel eingesetzt werden können. Dann sind jedoch die überbrückbaren Längen wesentlich geringer.
- Bei der Diskussion um den Einsatz von High-Speed-LANs kommt immer häufiger der Begriff ATM in die Diskussion. Bei genauer Betrachtung soll ATM die Netzwerktechnik der Zukunft werden. Aufgrund der großen Bedeutung von ATM soll abschließend in diesem Kapitel diese neue Technik näher betrachtet werden.

Wenn man die neuen Installationsbasen auf dem Gebiet der Lokalen Netze betrachtet, stellt man fest, daß sich immer mehr die Twisted-Pair-Verkabelung durchsetzt. Ein Grund hierfür ist darin zu sehen, daß über diesen Kabeltyp inzwischen alle Topologien eingesetzt werden können. Die Bedeutung der 50-Ohm-Koaxkabel für Ethernet und 93-Ohm-Kabel für ARCNET nimmt zumindest für größere, flexible und zukunftsichere Verkabelungsstrategien immer mehr ab. Bei kleineren Netzen ist es von der jeweiligen Umgebungssituation abhängig, auf welche Weise das Netz aufgebaut und verkabelt wird.

Wenn ein LAN in einer organisatorischen Einheit zu installieren ist, dann stehen vor allem folgende Fragestellungen im Mittelpunkt der Betrachtung:

- Welche Datenendeinrichtungen (PCs, MDTs, spez. Peripherie) sollen vernetzt werden?
- Existieren bereits Netzwerke, und wie können diese sinnvoll mitgenutzt werden, oder wie können zu ihnen Verbindungen hergestellt werden, wenn die Notwendigkeit dazu besteht?
- Mit welcher Topologie soll das Netzwerk aufgebaut werden?
- Mit welchen Übertragungsmedien soll verkabelt werden?
- Existieren bereits Kabelschächte, und ist in diesen noch Platz für die neu zu verlegenden Kabel?
- Können bereits vorhandene Kabel genutzt werden?
- Welche Arten von Daten sollen übertragen werden?
- Handelt es sich dabei um Daten, Text, Sprache oder Bild?
- Welche Datenmengen muß das Netz zur Spitzenlast übertragen können?

4 Netzwerkaufbau und Netzwerktopologien

- Mit welcher Übertragungstechnik (Basisband oder Breitband) wird die Verkabelung geplant?
- Welches Zugriffsverfahren (s. IEEE-Standards) soll zum Einsatz kommen?
- Wie weit liegen die einzelnen Stationen voneinander entfernt (maximale bzw. minimale Entfernung)?
- Welcher bzw. wie viele Server sollen eingesetzt werden?
- Wie hoch muß die maximale Übertragungskapazität sein?
- Welche Rolle spielt die Datensicherheit im Netzwerk?
- Welche Maßnahmen müssen gegen Ausfall des Servers übernommen werden?
- Wie viele Stationen arbeiten gleichzeitig im Netzwerk?
- Welches Netzwerkbetriebssystem erfüllt die gestellten Anforderungen?
- Welche Applikationen sollen im Netzwerk betrieben werden?
- Besteht die Forderung nach netzwerkfähiger Software? Wenn ja, existiert diese, und ist sie auch für das ausgewählte Netzwerkbetriebssystem verfügbar?
- Zu welchen anderen Netzen (Nebenstellenanlagen, andere LANs, öffentliche Netze, WANs oder Host-Rechnernetze) sind Schnittstellen, d.h. Gateways, erwünscht oder notwendig?
- Welche Betriebssystemvarianten werden auf den Workstations eingesetzt?
- Welche Workstations sollen eingesetzt werden (PCs, PS/2, MACs, Notebooks oder Unix-Systeme)?
- Wird sich das Netzwerk nur auf eine Abteilung beziehen, oder soll es abteilungsübergreifend eingesetzt werden?
- Soll die Hardware und Software von einem Hersteller geliefert werden, oder ist eine Umgebung mit Produkten verschiedener Hersteller sinnvoller oder gar unausweichlich?

Dies sind nur die wichtigsten Aspekte. Diese Liste ist lange nicht vollständig, genausowenig entspricht die Reihenfolge der Punkte ihrer Wichtigkeit. Für jeden Anwendungsfall wird ein anderer Punkt größere Bedeutung haben. Sie sollen bei dieser Zusammenstellung nur ein ungefähres Gefühl dafür bekommen, welche Probleme beim Aufbau und bei der Auswahl von LANs zu berücksichtigen sind. Die wichtigsten Bestandteile eines LAN lassen sich wie folgt deklarieren:

- Zu vernetzende Dateneneinrichtungen (MS-DOS-Rechner, OS/2-Rechner, Windows-95-Rechner, Windows-NT-Rechner, MACs, Unix-Systeme etc.)
- Verkabelungssystem (Twisted-Pair-Kabel, Koaxial-Kabel, IBM-Verkabelungssystem (STP-Kabel), Lichtleiterkabel)
- Anschlußsystem jeder Station (Breitband- oder Basisbandanschluß)

4 Netzwerkaufbau und Netzwerktopologien

- Gemeinsam nutzbare Ressourcen (Hard- und Software, Drucker, periphere Speicher, Streamer, Scanner, Plotter, Gateways, Bridges, Datenbestände etc.)
- Netzwerkbetriebssystem (z.B. Novell NetWare in der notwendigen Ausbaustufe oder NT Server)

Betrachten wir nun die Netzwerke, die gegenwärtig am häufigsten eingesetzt werden bzw. deren Bedeutung in Zukunft immer größer werden wird.

4.1 Ethernet-LANs

Ethernet wird bereits seit Jahren von allen Token-Ring-, FDDI- und inzwischen auch den ATM-Verfechtern totgesagt. Aber, wie man sagt, Totgesagte leben länger – und genau diese Weisheit bewahrt sich bei Ethernet. Die Ethernet-Technologie feiert im Jahr 1998 den 25. Geburtstag. Im Mai 1973 hat Bob Metcalfe bei Xerox Corp. das Übertragungsverfahren für Ethernet entwickelt. Seit dieser Zeit hat sich eine Vielzahl von Entwicklungen ergeben. Man denke nur an den Übergang von Thick-Ethernet auf Thin-Ethernet, die unterschiedlichen Übertragungsgeschwindigkeiten im unteren Transferbereich und die revolutionäre Twisted-Pair-Technik für Ethernet, die man sich heute gar nicht mehr wegdenken kann. Hinzu kam in den letzten Jahren die 100-Mbit/s-Fast-Ethernet-Technologie. Auch dieser neuen Technologie wurde keine Zukunft versprochen, wobei sich jedoch am Markt das genaue Gegenteil erwiesen hat. Ähnlich sieht es mit der neuesten Technik, Gigabit Ethernet, aus. Anfänglich belächelte man dieses neue Ethernet-System und bescheinigte ihm keine Zukunftsaussichten. Auch hier hat man sich kräftig geirrt. Inzwischen gibt es von fast allen Herstellern entsprechende Komponenten, um einfach und kostengünstig Gigabit-Ethernet-Netzwerke aufbauen zu können.

Von Hawaii aus begann der Eroberungszug von Ethernet, und es stellt immer noch das am häufigsten installierte Netzwerk dar. Laut Aussagen von IDC soll sich dieser Trend noch fortsetzen. So geht IDC davon aus, daß im Jahr 2000 weltweit 84 Prozent aller installierten Netzwerkkarten mit Ethernet- oder Fast-Ethernet-Ports ausgestattet sind (Aussagen zu Gigabit Ethernet existieren hierzu leider noch nicht).

Nach Aussagen von Experten ist mit Gigabit Ethernet jedoch noch nicht das Ende der technischen Möglichkeiten erreicht. Man schätzt, daß im Bereich des Machbaren eine Gigabit-Variante liegt, die um den Faktor zehn schneller sein soll. Diese hohen Geschwindigkeiten

4.1 Ethernet-LANs

haben aber auch ihren »Preis« – die maximal erlaubten Kabellängen sind zum Teil wesentlich kürzer als bei Standard Ethernet und Fast Ethernet. Hierzu jedoch zu einem späteren Zeitpunkt mehr.

Ethernet ist und bleibt somit das bisher am weitesten verbreitete und auch bekannteste Basisband-Bussystem, basierend auf Koaxialkabeltechnik. Es stützt sich auf das von der Firma Xerox entwickelte und bereits 1973 implementierte und danach sukzessive ausgebaut experimentelle Ethernet-System.

Die Bezeichnung ETHERNET ist ein geschütztes Warenzeichen der Firma Xerox. Die Firmen *Digital Equipment*, *Intel* und *Xerox* (DIX-Firmenkonsortium) haben ein kommerzielles Ethernet-LAN auf Basis des CSMA/CD-Zugriffsverfahrens für ein Basisband-Koaxialkabel entwickelt. Dieses Netzwerk arbeitet mit einer Übertragungsgeschwindigkeit von 10 Mbit/s und wurde Anfang 1980 auf den Markt gebracht. Ein Ethernet-Netz kann inzwischen auf zweierlei Art und Weise aufgebaut werden. Entweder durch Einsatz der *Thick-Wire-Verkabelung* (*Yellow-Cable*) oder mit Hilfe der *Thin-Wire-Verkabelung* (*Cheapernet*). Betrachten wir zunächst die Komponenten für Thick-Ethernet-Verkabelung. Häufig werden in Berichten Thin-Ethernet-Verkabelung und Cheapernet-Verkabelung gleichbedeutend verwendet. Dies ist jedoch nicht der Fall. Thin-Ethernet-Kabel und Cheapernet-Kabel unterscheiden sich grundlegend, so daß diese beiden Kabeltypen im gleichen Netzwerk nicht miteinander gemischt werden dürfen. Eine Kopplung über Bridge-Rechner, Router oder Repeater hingegen ist durchaus erlaubt.

Neben Ethernet gibt es den ISO-Standard IEEE 802.3, der ebenfalls Ethernet-Netzwerke repräsentiert. Der Unterschied zwischen Ethernet und IEEE 802.3 ist nicht besonders groß, jedoch hat er zur Folge, daß beide Systeme nicht miteinander kompatibel sind. In diesem Fall geht es nicht um die technische Spezifikation (Netzwerkaufbau), sondern um das Frameformat, welches in beiden Fällen benutzt wird. NetWare unterstützt auf einfache Weise beide Standards. Es ist dabei jedoch zu beachten, daß bei der Installation von NetWare angegeben werden muß, ob DIX-Ethernet (Ethernet II) oder IEEE 802.3 verwendet werden soll.

Mit welchen Kabeln Ethernet auch aufgebaut wird, ob IEEE 802.3 oder Ethernet II, es handelt sich immer um ein Netzwerk mit einer Übertragungsgeschwindigkeit von 10 Mbit/s. Für die unterschiedlichsten Verkabelungsmöglichkeiten haben sich auch entsprechende Bezeichnungen am Markt etabliert.

4 Netzwerkaufbau und Netzwerktopologien

Diese Standardangaben sind wie folgt zu interpretieren.

xxBBByy

xx: Übertragungsgeschwindigkeit

BBB: Basisband oder Breitband

yy: Länge eines Segments (yy*100); Ausnahme: Twisted-Pair

Die Standardbezeichnungen sind wie folgt:

- 10Base5-Koaxkabel mit einer maximalen Segmentlänge von bis zu 500 Metern und Basisbandtechnik. Mit diesem Kabeltyp ist Ethernet groß geworden, auch bekannt unter der Bezeichnung Thick-Ethernet. Es wird heute immer seltener eingesetzt.
- 10Base2-Koaxkabel mit einer Segmentlänge von bis zu 185 Metern und Basisbandtechnologie. Man unterscheidet zwei Kabeltypen: Thin-Ethernet, doppelt geschirmtes Kabel, und Cheapernet, einfach geschirmtes Kabel. Die beiden Kabel weisen dadurch eine unterschiedliche Dämpfung auf und dürfen nicht im gleichen Segment gemischt werden.
- 10Base-T-Twisted-Pair-Verkabelung mit sternförmigem Aufbau und einer maximalen Kabellänge von bis zu 100 Metern.
- 10Broad5-Koaxialkabel mit einer maximalen Segmentlänge von 3600 Metern auf Basis einer Breitbandtechnologie.
- 10Base-F-Glasfasersegmente mit einer Übertragungsgeschwindigkeit von 10 Mbit/s.

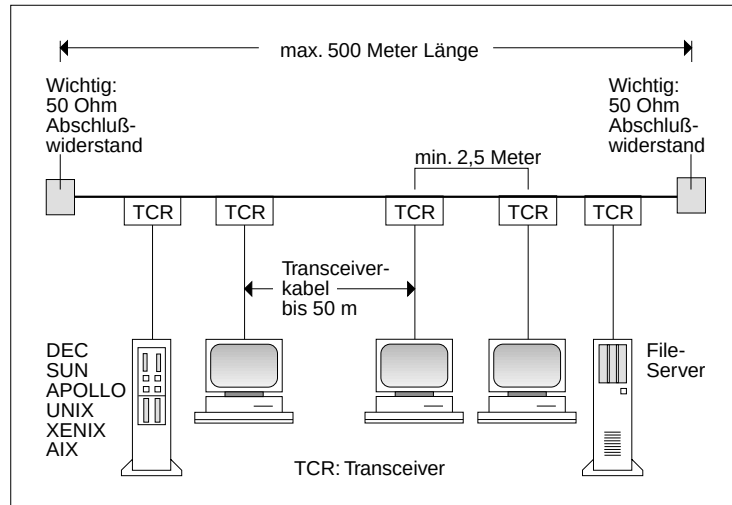
Aufgrund der Installationsbasen werde ich mich in den nachfolgenden Ausführungen auf 10Base5, 10Base2 und 10Base-T beschränken.

4.1.1 Thick-Ethernet

In diesem Abschnitt wollen wir einen Überblick über die wichtigsten Komponenten von Ethernet-LANs geben. Behandelt werden dabei Koax- und Link-Segmente, Transceiver, Transceiverkabel, Controller, Repeater und Fan-out-Units. Die nachfolgende Abbildung zeigt den Aufbau eines Thick-Ethernet-LAN.

4.1 Ethernet-LANs

Abbildung 4.1
Aufbau eines
Thick-Ethernet-
LAN



Das Koaxialkabelsegment

Als Übertragungsmedium werden Koaxialkabel mit 50 Ohm Impedanz eingesetzt. Für die Verkabelung wird dabei das dicke, gelbe Ethernet-Kabel verwendet, anders als beim anschließend behandelten Thin-Ethernet. Diese Kabelsegmente können aus einem oder mehreren gekoppelten Koaxialkabelstücken bestehen und dürfen dabei eine Länge von 500 m nicht überschreiten. Die einzelnen Kabelstücke werden in diesem Fall mit sogenannten N-Barrel-Steckern gekoppelt.

Nach Möglichkeit sollten bei der Verkabelung jedoch nur Einkabelstück-Segmente verwendet werden, um auftretende Signalreflexionen an den Verbindungssteckern zu vermeiden. Soll ein Segment bis zur maximalen Ausbaustufe von 500 m später erweitert werden, kann es jedoch notwendig werden, weitere Kabelstücke anzukoppeln. Dabei ist folgendes zu beachten:

- Wird ein Koaxialkabelsegment aus mehreren Koaxialkabelstücken zusammengesetzt, dann sollte jedes Teilstück ein ungerades Vielfaches von 23,4 m sein.
- Die Kabellängen können beliebig miteinander kombiniert und zu Segmenten unterschiedlicher Länge zusammengesetzt werden, ohne daß sich die Signalreflexionen an den Verbindungsstellen phasenmäßig so aufaddieren, daß es zu Störungen im Netzwerkbetrieb kommt. Dabei sollte jedoch darauf geachtet werden, daß die einzelnen Koaxialkabelstücke von einem Hersteller stammen und dieselben physikalischen Eigenschaften aufweisen, z.B. Durchmesser, Impedanz, Dämpfungsverhalten.

4 Netzwerkaufbau und Netzwerktopologien

An beiden Enden eines Koaxialkabelsegments wird und muß ein *Abschlußwiderstand* (Wellenabschlußwiderstand) aufgeschraubt werden. Die wesentlichen Charakteristika des Ethernet-Yellow-Kabels sind:

- Impedanz des Koaxialkabels: 50 Ohm
- Schutzbeschichtung: PVC, Teflon, Fluorpolymere
- Markierungsringe im Abstand von 2,5 m ($\pm 0,5$ cm) für Transceiveranschlüsse
- Wellenabschlußwiderstand an beiden Enden eines Segments von 50 Ohm
- Maximale Segmentlänge: 500 Meter

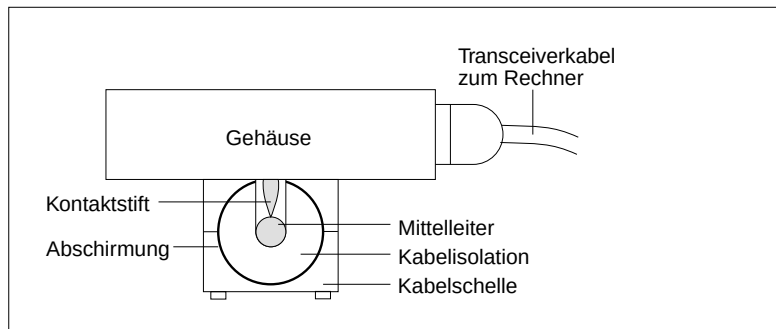
Pro Koaxsegment dürfen nicht mehr als 100 Transceiver angeschlossen werden. Zwischen den Transceivern muß ein Abstand von mindestens 2,5 Metern (Markierungen am Kabel) oder ein Vielfaches davon eingehalten werden. Dies ist notwendig, damit sich Signalreflexionen am TAP-Anschluß nicht phasenmäßig aufaddieren können. Der TAP-Anschluß stellt die Verbindung des Transceivers zum Innenleiter des Koaxkabel her.

Transceiver

Das Wort Transceiver ist eine Kombination der beiden Begriffe Transmitter (Sender) und Receiver (Empfänger) und bedeutet soviel wie Sende- und Empfangseinheit. Die ist notwendig, um eine Station physikalisch an das Koaxialkabel anschließen zu können.

Pro Koaxsegment von max. 500 m Länge dürfen nicht mehr als 100 Transceiver (jeweils mindestens 2,5 m voneinander entfernt) angeschlossen werden. Die mechanisch-elektrische Ankopplung eines Transceivers wird über einen TAP-Anschluß ermöglicht. Dabei wird mit dem Handbohrer des Installationskits das Koaxialkabel an einer Markierung fast bis zum Innenleiter angebohrt.

Abbildung 4.2
Aufbau und
Funktion eines
Transceivers



4.1 Ethernet-LANs

In das kleine Loch wird dann ein Zapfen gedreht. Dieser TAP-Anschluß stellt den mechanisch-elektrischen Anschluß her. Bei sachgemäßer Installation des Transceivers am Koaxialkabel wird der Netzbetrieb nicht unterbrochen, d.h., die Anbringung eines Transceivers kann während des Netzbetriebs erfolgen.

Die Aufgabe des Transceivers soll hier noch einmal zusammengefaßt werden:

- Koaxialkabelsignalisierung, Weiterleitung von kodierten bitseriellen Datenströmen auf das Koaxialkabel
- Die Signalisierung muß repeaterfrei bis zu einer Übertragungsstrecke von 500 m gewährleistet werden
- Empfangen von bitseriellen Datenströmen vom Koaxialkabel
- Kollisionserkennung
- Carrier Sense
- Unterstützung einer Datenrate von 10 Mbit/s

Transceiverkabel

Das Transceiverkabel, häufig auch Drop-Kabel genannt, verbindet die Netzwerkadapterkarte mit dem Transceiver. Das Transceiverkabel darf nicht länger als 50 m sein. Auf Seiten der Station endet das Transceiverkabel in einem männlichen und auf Seite des Transceivers in einem weiblichen 15poligen Subminiaturstecker.

Da das Transceiverkabel relativ starr und somit inflexibel zu verlegen ist, werden auch dünnere Kabelversionen (z.B. von DEC) angeboten. Bei diesen Kabeln sind die Leitungsdurchmesser geringer, daher sind auch die elektrischen Kenngrößen schlechter. Entsprechend reduziert sich bei diesen Kabeln die Maximallänge. Im DEC-Fall darf das Transceiverkabel dann nicht länger als 12,5 m sein.

Netzwerkadapterkarte

Die Kommunikationssoftware ist, wie noch ausführlich besprochen wird, eine Station in einem Lokalen Netz und entsprechend dem ISO/OSI-Referenzmodell in sieben Schichten unterteilt. Die unteren vier Schichten realisieren das Transportsystem, die oberen Schichten repräsentieren die vom Transportsystem unabhängigen Dienstleistungen. Letztere arbeiten sehr eng mit dem Betriebssystem des jeweiligen Rechners zusammen. Deshalb erscheint es sinnvoll, die Protokollsoftware, die durch das Transportsystem realisiert wird, auf einem eigenständigen Netzwerk-Controller zu implementieren. Dadurch wird der Stationsrechner von der Abarbeitung dieser Aufgaben entlastet.

4 Netzwerkaufbau und Netzwerktopologien

Zum heutigen Zeitpunkt werden Adapterkarten angeboten, auf denen die Funktionen bis zur Ebene 2 und sogar bis zur Ebene 4 (auf der Karte) integriert sind. Netzwerkadapterkarten werden von den unterschiedlichsten Herstellern angeboten.

Dies sind unter anderem:

- Adaptec (früher COGENT)
- Compaq
- Hewlett Packard
- 3COM
- IBM
- Intel
- Cabletron
- Schneider & Koch
- Compu-Shack

Daneben gibt es ein paar hilfreiche Mittel, um Kabelsegmente miteinander zu verbinden bzw. am Anfang und Ende zu terminieren. Somit ist es möglich, ein defektes Thick-Ethernet-Kabel nicht gleich sofort komplett austauschen zu müssen, sondern mit einfachen Methoden wieder instandzusetzen. Folgende Elemente stehen zur Verfügung:

N-Series male Connectors

Diese Thick-Ethernet Cable Connectors werden an beiden Enden des Kabels installiert, wenn T-Connector-Transceiver verwendet werden. Bei vorinstallierten Kabeln sind diese Connectors bereits installiert.

N-Series Barrel Connectors

Mit diesen Connectors werden zwei Kabelstücke miteinander verbunden. Bei einem Kabelbruch zum Beispiel kann man auf diese Weise die defekte Stelle wieder reparieren.

N-Series-Terminatoren

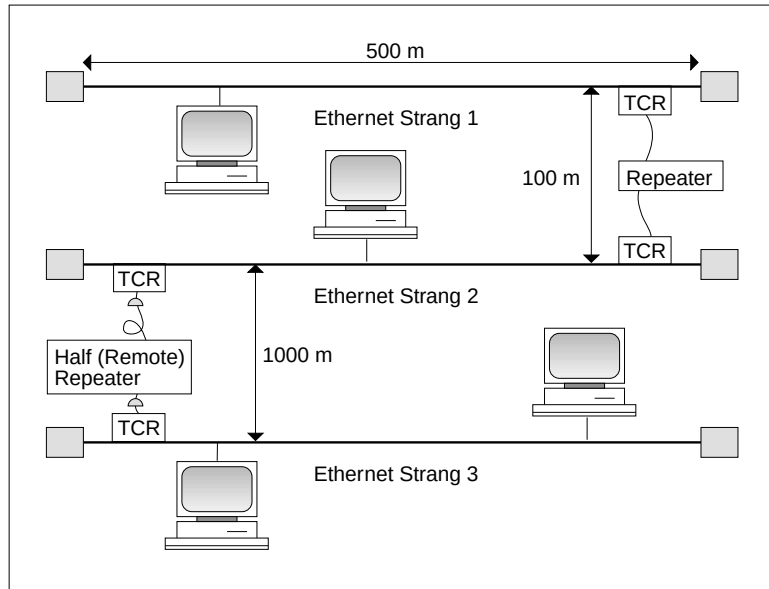
Wie bereits erwähnt, muß das Thick-Ethernet-Kabel an beiden Enden terminiert werden. Hierzu wird ein 50-Ohm-N-Series-Terminator verwendet. Für jedes Kabelsegment wird der eine Terminator mit der Erdung des Gebäudes verbunden, der andere in der Regel nicht.

Repeater

Repeater werden dann eingesetzt, wenn die Topologie über die einzuhaltende 500-m-Koaxialkabel-Segmentlänge hinaus erweitert werden muß. Hierbei sind zwei unterschiedliche Kopplungsmöglichkeiten zu beachten:

4.1 Ethernet-LANs

Abbildung 4.3
Kopplung von
Ethernet-LANs mit
Repeater



Local Repeater

Local Repeater verbinden zwei Kabelsegmente miteinander, wenn diese weniger als 100 m voneinander entfernt sind. Der Repeater wird dann mit einem Transceiver-Kabel und je einem Transceiver an jedes Kabelsegment angeschlossen. Ein Repeater regeneriert und wiederholt alle Signale eines jeden Segments und gibt diese auf das andere Segment weiter.

Liegen die Segmente weiter als 100 m voneinander entfernt, können nur noch Remote-Repeater eingesetzt werden.

Remote-Repeater

Beim Einsatz von Remote-Repeatern wird die gesamte Repeater-Funktion über zwei Repeater-Hälften erbracht. Diese sind über eine Duplex-Glasfaserstrecke miteinander verbunden. Die maximale Länge dieser Glasfaserstrecke darf insgesamt nicht über 1000 m liegen, wenn mehrere Remote-Repeater auf dem gleichen Datenweg installiert sind. Jeder Remote-Repeater wird über ein Transceiverkabel mit einem Transceiver des jeweiligen Segments gekoppelt. Da das Transceiverkabel maximal 50 m lang sein darf, ergibt sich eine Gesamtentfernung der beiden Segmente von maximal 1100 m. Die zu überbrückende Strecke inklusive beider Repeater-Hälften verhält sich dabei bezüglich der Netzauslegung wie ein einzelner Local-Repeater.

4 Netzwerkaufbau und Netzwerktopologien

Repeater können so konfiguriert werden, daß sie ein defektes Segment isolieren können. Der Netzbetrieb kann jedoch auf den anderen Segmenten ohne Störung fortgeführt werden. Die Repeater haben folgende Aufgaben zu erfüllen:

- Weiterleiten der Daten
- Signalregenerierung
- Carrier Sense und Datenwiederholung
- Kollisionserkennung
- Jam-Signalgenerierung
- Testfunktionen

Ein Repeater muß nicht unbedingt am Ende eines Koaxialkabelsegments installiert werden. Der Anschluß kann an einer beliebigen Stelle des Segments erfolgen. Der Abstand zwischen zwei Transceivern von mindestens 2,5 m muß jedoch beachtet werden.

Fan-Out-Unit

Im Lauf der Zeit hat sich bei der Installation von Ethernet-LANs herausgestellt, daß man sehr oft vor dem Problem steht, innerhalb eines Raums mehrere Ethernet-Endgeräte an das Netz anschließen zu müssen. Bei der herkömmlichen Vorgehensweise würde dies bedeuten, daß pro Endgerät ein Transceiver benötigt wird und daß ein Minimalabstand der Transceiver von 2,5 m eingehalten werden muß. Wegen der letzteren Spezifikation war man oft gezwungen, künstliche Kabelschleifen einzufügen, um diese Abstände auch gewährleisten zu können. Deshalb haben einige Hersteller sogenannte Fan-Out-Units, auch Multi-Port-Transceiver genannt, entwickelt. Herkömmliche Fan-Out-Units erlauben den Anschluß von bis zu acht Endgeräten über die normalen Transceiverkabel. Das Fan-Out-Unit selbst wird über ein Transceiverkabel und einen einzigen Transceiver an das Koaxialkabel angeschlossen. Ein zusätzlicher Vorteil dieser Multiport-Transceiver ist die Möglichkeit der Serienschaltung zweier Fan-Out-Units (zweistufige Kaskadierung).

Eine Fan-Out-Unit muß nicht unbedingt an ein Ethernet-Kabel angeschlossen sein. Im Stand-alone-Betrieb erlaubt dies die Bildung eines eigenständigen Mini-Ethernet-Netzes. Wenn Sie die Möglichkeit durchrechnen, stellen Sie fest, daß damit ein Ethernet-Netz durch Serienschaltung der Fan-Out-Units von maximal 64 Endgeräten aufgebaut werden kann, ohne daß Sie einen Meter Yellow-Cable benötigen (immer unter Beachtung der einzuhaltenden Transceiver-Kabellängen).

4.1 Ethernet-LANs

Systemausbaustufen

In diesem Abschnitt wollen wir zusammenfassend die Ausbaustufen des physikalischen Übertragungssystems für die IEEE-802.3-Spezifikation betrachten. Es werden die Komponenten und Restriktionen einer Minimalkonfiguration und die Kopplungsmöglichkeiten von Segmenten bis hin zur Konfiguration mit maximalem Signalweg abgehandelt.

Minimale Systemkonfiguration

Wenn wir ein Ethernet aufbauen, das der minimalen 802.3-Spezifikation Rechnung tragen soll, besteht dieses Netz aus einem einzigen Koaxialkabelsegment, wobei dieses wiederum aus mehreren Kabelstücken zusammengesetzt sein kann, aber nicht länger als 500 Meter ist. An dieses Koaxialkabelsegment werden dann mit Hilfe der Transceiver die einzelnen Stationen oder Repeater angeschlossen. Station bzw. Repeater werden dabei mit dem Transceiver-Kabel verbunden. An beiden Enden des Kabels muß der richtige Wellenabschlußwiderstand angebracht werden, um auftretende Signalreflexionen zu verhindern. Man spricht hier auch von einer *Signalsenke*. Der Abstand zwischen zwei Transceivern auf dem Koaxialkabelsegment sollte mindestens 2,5 Meter betragen. Sind die Abstände größer zu wählen, sollte der Abstand ein Vielfaches dieser 2,5 Meter sein. Auf diese Weise wird verhindert, daß sich die Signalreflexionen an den Transceiver-Anschlüssen phasenmäßig aufaddieren können. Die maximale Anzahl von Transceivern auf einem 500-Meter-Segment ist mit 100 festgelegt. Das Transceiverkabel, d. h. der Abstand von Station zu Transceiver, darf maximal 50 Meter betragen. Wenn all diese Vorschriften für den Aufbau eines minimal ausgestatteten Ethernet-Strangs unter Thick-Ethernet-Verkabelung eingehalten werden, treten beim Betrieb eines solchen Netzes keinerlei Schwierigkeiten auf, außer Sie haben irgendwelche wichtigen Installationsanweisungen nicht beachtet.

Kopplung von Segmenten

Da in speziellen Fällen die 500-Meter-Koaxialkabel-Segmentlänge nicht ausreicht, kann die physikalische Topologie durch den Einsatz von Repeater-Komponenten erweitert werden. Durch die Installation von Repeatern können zwei oder mehrere Segmente miteinander verbunden werden.

Die Segmente bestehen aus den Repeatern, zwei Transceiverkabeln und zwei Transceivern. Die Transceiver-Kabel können optional sein, da die Transceiver gegebenenfalls in den Repeater-Komponenten in-

4 Netzwerkaufbau und Netzwerktopologien

tegiert sind. Mit diesen Repeater-Komponenten können Koaxialkabelsegmente verbunden werden, die höchstens 100 Meter voneinander entfernt sind. Müssen größere Entfernungen überbrückt werden, sollten sogenannte *Link-Segmente* (Remote-Repeater) eingesetzt werden. Wie aus der obigen Beschreibung bereits hervorging, realisiert jedes Link-Segment eine Punkt-zu-Punkt-Verbindung zwischen zwei Repeater-Komponenten. An dieser Verbindung dürfen keine weiteren Transceiver angeschlossen werden. Zwei entfernt liegende Koaxialkabelsegmente können somit über diese Repeater-Komponenten und ein Link-Segment gekoppelt werden. Im Signalweg zwischen zwei beliebigen Stationen dürfen höchstens zwei Link-Segmente eingesetzt werden. Als Übertragungsmedium für dieses Link-Segment wird Glasfaser bzw. ein Lichtleiterkabel verwendet.

Konfiguration mit maximaler Ausdehnung

Gemäß den 802.3-Festlegungen sind für die Übertragung von Signalen zwischen zwei beliebigen Stationen folgende Restriktionen zu beachten:

Im Übertragungsweg zwischen zwei Stationen dürfen höchstens zwei Stations-Transceiver-Kabel, drei Koaxialkabelsegmente und zwei Link-Segmente installiert sein. Statt der Link-Segment-Kopplung kann die Verbindung auch mit Local-Repeatern hergestellt werden.

Unter Beachtung der IEEE-802.3-Erweiterungen von 1986, die für das Link-Segment den Einsatz von Lichtwellenleitern vorsieht (Fibre Optic Interrepeater Link) und eine maximale Glasfaser-Link-Entfernung zwischen zwei beliebigen Stationen von 1000 m festlegt, ergibt sich für den maximalen Abstand zwischen zwei Stationen:

Zwei Transceiver-Kabel	100 m
Drei Koaxialkabelsegmente	1500 m
Insgesamt zulässige Länge des Link-Segments	1000 m
Vier Transceiver-Kabel (vier Remote-Repeater-Komponenten)	200 m
Maximaler Abstand zwischen zwei Stationen	2800 m

Wird auf den Einsatz von Link-Segmenten verzichtet, ergibt sich ein maximaler Signalweg zwischen zwei beliebigen Stationen von 1800 m.

4.1 Ethernet-LANs

Kopplung eigenständiger Netzwerke

Durch den vermehrten Informationsbedarf ist es bei heutigen Unternehmensformen nicht mehr möglich, diese Anforderung mit nur einem Netz zu erfüllen. In der Praxis kommt es deshalb nicht selten vor, daß eine Vielzahl von Netzen miteinander verbunden werden soll, um im Bedarfsfall Informationen aus anderen Datenbeständen, die nicht die eigenen sind, aufzurufen.

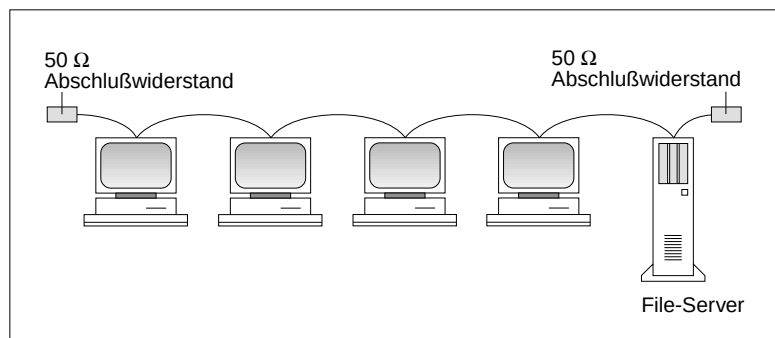
Hier können dann Fälle auftreten, wo nicht nur IEEE-802.3- oder Ethernet-Netze gekoppelt werden müssen, sondern auch Netze mit unterschiedlicher Struktur und unterschiedlichen Protokollen. Es können folgende Kopplungsmöglichkeiten unterschieden werden:

- Verknüpfung mit Repeatern (s. oben)
- Verknüpfung mit Bridges (s. spätere Beschreibung)
- Verknüpfung mit Routern
- Verknüpfung mit Gateways

4.1.2 Thin-Ethernet

Das unter der Bezeichnung Cheapernet bekanntgewordene CSMA/CD-Netz stellt ein preiswertes Ethernet-Derivat dar. Bei der Installation sollte darauf geachtet werden, welcher Kabeltyp zum Einsatz kommt, da sich Thin-Ethernet-Kabel und Cheapernet-Kabel nicht miteinander mischen lassen. In der Literatur werden diese beiden Typen meistens gleichgesetzt, obwohl dies nicht korrekt ist. Das Cheapernet unterscheidet sich vom Thick-Ethernet durch die kürzere Ausdehnung der Koaxialkabelsegmente und das eingesetzte Koaxialkabel. Die Übertragungsrate von 10 Mbit/s und das MAC-Protokoll sind gleich.

Abbildung 4.4
Aufbau eines Thin-
Ethernet-LAN



4 Netzwerkaufbau und Netzwerktopologien

Da sich die Spezifikationen für die Installation jedoch nicht unterscheiden, werden im nachfolgenden die Bezeichnungen Thin-Ethernet und Cheapernet wahlweise verwendet werden. Es sei nochmals darauf hingewiesen, daß bei der Installation eine Mischung beider Kabeltypen nicht möglich ist.

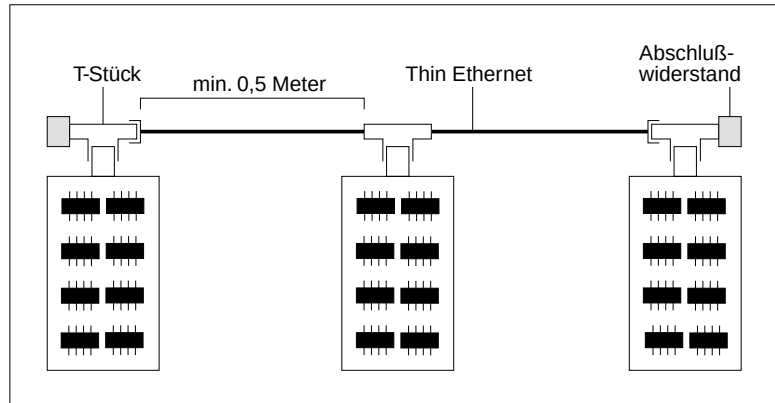
Cheapernet verwendet das im Vergleich zum Yellow-Cable preiswertere und leichtere RG58-A/U-Koaxialkabel sowie BNC-T-Stecker zum mechanischen Anschluß der einzelnen Stationen. Der Transceiver kann an den BNC-T-Stecker angeschlossen werden. Wenn Sie jedoch die Ethernet-Karten betrachten, sind auf diesen oft bereits zwei Anschlüsse vorhanden, ein 15poliger Transceiver-Anschluß und ein BNC-Anschluß. Wird über den vorhandenen BNC-Stecker angekoppelt, muß die Karte entsprechend eingestellt werden, da dann der integrierte Transceiver auf der Karte (VLSI-Controllerboard) die Einkopplung und die Arbeit im Netz übernimmt. Da sich Cheapernet von Ethernet nur auf der physikalischen Ebene unterscheidet (es wird ein anderes Übertragungsmedium eingesetzt) und ansonsten gleiche Funktionalität vorherrscht (CSMA/CD und 10 Mbit/s Übertragungsgeschwindigkeit) dürfen Cheapernet-Segmente problemlos über Repeater mit Standardkoaxial- und/oder Lichtleitersegmenten gekoppelt werden. Die maximale Ausdehnung eines Cheapernet-Segments darf nicht über 185 m hinausgehen, und es können auf dieser Länge auch nur maximal 30 Stationen angeschlossen sein. Die Stationen werden über den BNC-T-Stecker mit dem Kabel verbunden. Anders als bei Thick-Ethernet-Verkabelung wird dabei das Kabel an der jeweiligen Station unterbrochen (durch den BNC-T-Stecker). Ein problemloses Einkoppeln von neuen Stationen ist nicht mehr möglich, da das Kabelsegment geöffnet werden muß und aufgrund dessen ein Netzstillstand hervorgerufen wird. Ebenso darf im laufenden Betrieb der BNC-T-Stecker nicht von einer Station entfernt werden, da es dann zu Schwierigkeiten beim Wellenwiderstand kommen kann.

Die Entfernung von zwei Stationen, die nebeneinander installiert werden sollen, muß mindestens 0,5 m betragen. Auch beim Einsatz von Cheapernet ist zu beachten, daß an beiden Enden des Segments Wellenabschlußwiderstände eingesetzt werden (Signalsenke).

Bei Cheapernet ist eine Verbindung zum normalen Ethernet (Thick-Ethernet) durch den Einsatz von Repeatern möglich. Es gibt jedoch einige Hersteller, die sogenannte Multi-Port-Repeater anbieten. Über diese Multi-Port-Repeater kann ein Anschluß am Thick-Ethernet erfolgen, die anderen Anschlüsse werden für Cheapernet-Segmente verwendet.

4.1 Ethernet-LANs

Abbildung 4.5
Anbindung einer
Workstation an
Thin-Ethernet



So wie bereits für Thick-Ethernet ausgeführt, gibt es auch für Thin-Ethernet (Cheapernet) BNC Barrel Connectors, um zwei Kabelsegmente miteinander zu verbinden.

An dieser Stelle sei jedoch ausdrücklich darauf hingewiesen, daß die Anzahl der Barrel Connectors sowohl für Thin-Ethernet als auch für Thick-Ethernet so gering wie möglich sein sollte, da jeder Barrel Connector eine Dämpfung des Signals erzeugt.

4.1.3 Twisted-Pair-Ethernet

Inzwischen hat sich bei der Verkabelung für Ethernet-Netzwerke immer mehr der Einsatz von Twisted-Pair-Kabeln durchgesetzt. Die Standardbezeichnung hierfür ist 10BASE-T. 10BASE-T bietet die meisten Vorteile von Ethernet, basierend jedoch auf einer neuen Verkabelungsform, d.h., es ist nach wie vor ein CSMA/CD-Zugriffsverfahren mit einer Übertragungsgeschwindigkeit von 10 Mbit/s. Bei dieser Verkabelungsform handelt es sich nicht um eine Busstruktur, sondern um eine sternförmige Verkabelung. Zu diesem Zweck werden Ethernet Twisted Pair Concentrator verwendet.

10BASE-T ist kompatibel mit allen anderen Ethernet-Standards. Dadurch stehen auch Produkte zur Verfügung, die den Übergang von einem zum anderen Kabelmedium realisieren. Man kann also zum Beispiel Repeater verwenden, um von Thin-Ethernet auf Twisted-Pair-Ethernet zu wechseln. Somit ist eine problemlose Integration in bestehende Ethernet-Segmente möglich bzw. der Einsatz unterschiedlichster Ethernet-Strukturen, je nach Einsatzgebiet, erlaubt und machbar.

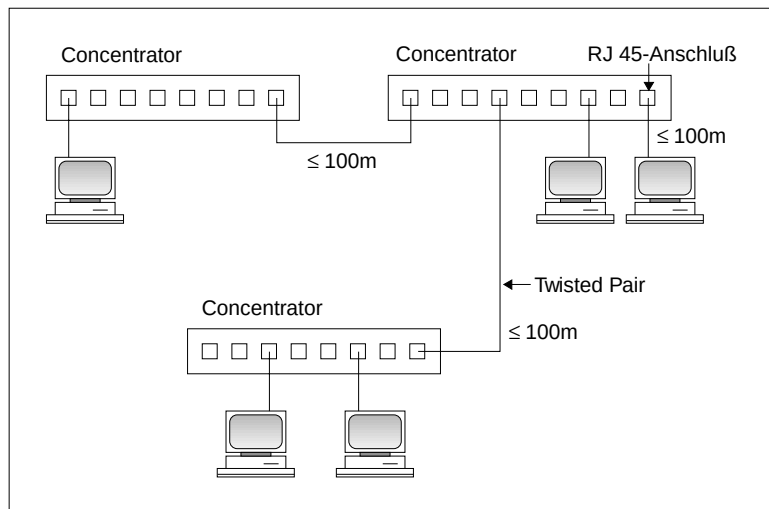
4 Netzwerkaufbau und Netzwerktopologien

Bislang werden bei fast allen Ethernet-Karten die Anschlüsse für Thin-Ethernet und Thick-Ethernet unterstützt. Neuere Karten unterstützen zusätzlich noch Twisted-Pair. Sie werden oft als Three-in-one-Karten bezeichnet. Andere Hersteller bieten als Anschlußmöglichkeiten Thick-Ethernet und Twisted-Pair oder die Kombination Thin-Ethernet und Twisted-Pair an.

In der 10BASE-T-Spezifikation ist eine Kabeltestfunktion definiert, bezeichnet als Link Status Test. Über diese Funktion testet das System ständig die Twisted-Pair-Verkabelung auf offene Kabel oder Kurzschlüsse im Kabel. Das Monitoring der Verkabelung wird mit Hilfe spezieller Verkabelungskomponenten und entsprechender Software ermöglicht.

In der nachfolgenden Abbildung wird eine mögliche Twisted-Pair-Verkabelung dargestellt. Hier ist bereits zu sehen, daß die Entfernung zwischen Station Concentrator und Concentrator Concentrator maximal 100 m betragen kann. Sie wissen bereits, daß Sie für den Anschluß von Nodes an Thick-Ethernet einen Transceiver benötigen. Angenommen, Sie haben nur ältere Ethernet-Karten und wollen diese dennoch unter Twisted-Pair-Verkabelung einsetzen, was dann? Eine Möglichkeit wäre die Verwendung eines Repeaters, der von Twisted-Pair auf Thick-Ethernet umsetzen kann.

Abbildung 4.6
Aufbau von
10BASE-T-
Ethernet-LANs



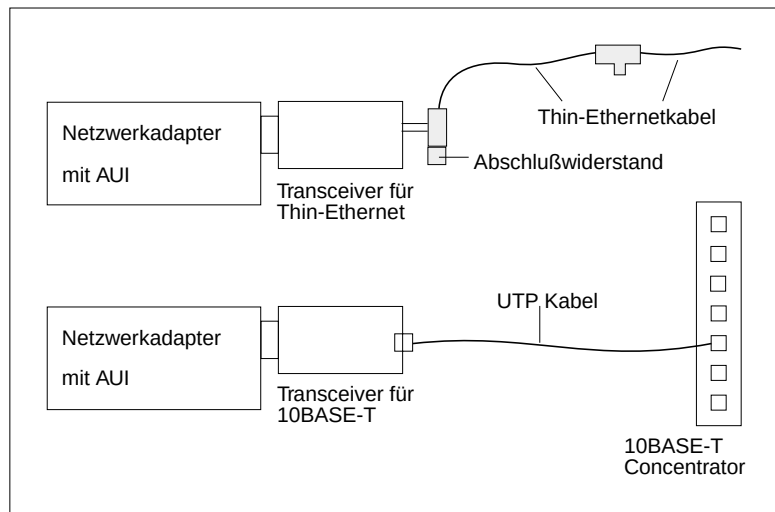
Inzwischen werden jedoch Transceiver nicht nur für den Anschluß an Thick-Ethernet angeboten, sondern auch für den Anschluß an Twisted-Pair und Thin-Ethernet. Auf diese Weise läßt sich ein ganz flexibles und ständig erweiterbares System aufbauen. Es gibt zum

4.1 Ethernet-LANs

Beispiel spezielle Netzwerkadapter für Ethernet, die nur einen Transceiveranschluß besitzen. Wenn Sie diese dennoch unter Thick-Ethernet oder Twisted-Pair-Ethernet einsetzen wollen, dann besorgen Sie sich einfach einen Transceiver für 10BASE2 oder 10BASE-T.

In der nachfolgenden Abbildung sind die unterschiedlichen Möglichkeiten aufgezeigt, die mit diesen Transceivern verfügbar sind.

Abbildung 4.7
Einsatzmöglich-
keiten unterschied-
licher Transceiver



In Abbildung 4.6 ist zu sehen, wie Workstations und Endgeräte an den zentralen Concentrator angeschlossen werden. Jeder Concentrator, genauer gesagt, jeder Anschlußpunkt des Concentrators führt eine Repeater-Funktion aus, d.h., die Signale werden an jedem Anschlußpunkt verstärkt.

Wenn eine Station Datensignale erzeugt, treffen sie beim Concentrator ein, der sie an alle anderen aktiven Anschlußports weiterleitet. Sie sehen anhand Abbildung 4.6 auch, daß an einen Anschlußpunkt wiederum ein Concentrator angeschlossen werden kann. Die 10BASE-T-Concentrator können auf diese Weise kaskadiert werden.

Endgeräte werden an den Concentrator über ein Twisted-Pair-Kabel angeschlossen. In der Regel handelt es sich dabei um ein 100-Ohm-Unshielded-Twisted-Pair-Kabel. Es ist aber auch durchaus möglich, das technisch sicherere, aber auch etwas teurere 100-Ohm-Shielded-Twisted-Pair-Kabel zu verwenden.

Es gibt jedoch auch Concentrator, die es gestatten, das 150-Ohm-Shielded-Twisted-Pair-Kabel zu verwenden, das von IBM für den Aufbau von Token-Ring-Netzen standardisiert worden ist. Hierfür

4 Netzwerkaufbau und Netzwerktopologien

wird der Markt jedoch immer »dünner«. Statt sich mühsam einen passenden Hub für ein verlegtes 150-Ohm-Kabel zu suchen, besteht auch noch die Möglichkeit, mit Hilfe von Impedanzwandlern 100 Ohm auf 150 Ohm und umgekehrt umsetzen zu lassen. Somit ist es einfach möglich, vom Concentrator mit 100 Ohm auf den Impedanzwandler zu gehen, der dann auf 150 Ohm für das IBM-Typ-I-Kabel umsetzt. An der Netzwerkdose für den PC-Anschluß wird dann wieder von 150 Ohm auf 100 Ohm umgesetzt, um entsprechend mit 100 Ohm Impedanz den Netzkartenanschluß durchführen zu können. Solche Impedanzwandler gibt es als externe Geräte, die dann zwischen Netzkartenanschluß und Netzwerkdose bzw. Concentrator-Anschluß und Verteilerfeld-Anschluß geschaltet werden müssen. Die Firma Dätwyler stellt hierfür deshalb eine besondere Technik zur Verfügung. Man muß für die Impedanzwandlung keine externen Geräte zwischenschalten, sondern tauscht im Verteilerschrank einfach das Patchfeld aus (hier erfolgt die erste Umwandlung von 100 Ohm auf 150 Ohm), und die ursprüngliche Token-Ring-Anschlußdose im Kabelkanal wird gegen eine Twisted-Pair-Dose mit integrierten Impedanzwandler ersetzt.

Die Entwicklung des 10BASE-T-Standards wurde maßgeblich von folgenden Firmen beeinflusst:

AT&T, Hewlett-Packard, SynOptics, Wang, Western Digital, 3Com, Advanced Micro David Systems, DEC, Intel, National Semiconductor, NCR, Ungermann-Bass und Racal Interlan. Sie sehen, alles bekannte und renommierte Hersteller qualitativ hochwertiger Netzwerkkomponenten.

Durch den 10BASE-T-Standard sollen folgende wesentlichen Ziele erreicht werden:

1. Es soll eine Möglichkeit geschaffen und definiert werden, die physikalische Verbindung im LAN über Twisted-Pair-Kabel durchzuführen. In der amerikanischen Literatur finden Sie an dieser Stelle sehr oft den Hinweis, eine bestehende Telefonverkabelung nutzen zu können. Das sollten Sie bei unseren Telefonkabeln vermeiden, da sie nicht den Qualitätsanforderungen entsprechen. Für eine Twisted-Pair-Verkabelung sollten spezielle Twisted-Pair-Kabel eingesetzt werden.
2. Die Produkte, die diesem Standard entsprechen, sollen nicht nur preisgünstig, sondern auch leicht zu installieren und zu bedienen sein. Die Praxis zeigt, daß diese Forderungen sehr gut zu erfüllen sind.
3. Die Richtlinien müssen kompatibel mit den bereits entwickelten und sich im Einsatz befindlichen Netzwerkschnittstellen sein. D.h., der Schutz der Investitionen muß gewährleistet sein. Da sich

4.1 Ethernet-LANs

alle bisher am Markt befindlichen Produkte ohne Schwierigkeiten in bestehende Netzwerke eingliedern lassen, wird auch diese Forderung ausreichend erfüllt.

4. Die Implementierung unter den bereits bestehenden Standards darf durch den Zusatz nicht in Frage gestellt werden. Damit soll die Kompatibilität aller 802.3-Produkte auf Twisted-Pair-Verkabelung gewährleistet werden. Auch hier zeigt die Praxis, daß dies voll erfüllt wird. Es gibt inzwischen Koppellemente zwischen Thin-Ethernet und Twisted-Pair oder auch Thick-Ethernet und Twisted-Pair. Das sind Repeater, die nicht größer sind als eine Zigarettenschachtel, oder auch Twisted-Pair-Transceiver, die noch kleiner sind als eine Zigarettenschachtel.

10BASE-T entspricht zwar dem 802.3-Standard, aber aufgrund der technischen Notwendigkeit mußten wichtige Änderungen hinzugefügt werden:

1. 10BASE-T ist strukturell eine sternförmige Verkabelung. Die Segmentlänge (Concentrator Node, Concentrator Concentrator) beträgt dabei nicht mehr als 100 Meter mit einem eingebauten Link-Status-Test für die Verbindung.
2. Repeater müssen in der Lage sein, Netzwerksegmente abzutrennen, falls es zu Störungen auf diesem Segment kommt. Da jeder Anschlußpunkt separat verstärkt wird, heißt das im Falle einer Störung, hinter diesem Anschlußpunkt den Port automatisch zu schließen, ohne die weitere Funktionsfähigkeit der restlichen Ports zu beeinflussen.
3. Der größte Teil des neuen Standards betrifft allerdings die Festlegungen für die Verbindung über verdrehte Zweidrahtleitungen (Twisted-Pair). Dabei werden die funktionellen, elektrischen und mechanischen Spezifikationen für 10BASE-T-MAUs (Media Access Unit) festgelegt. Eine MAU ist zuständig für den korrekten Anschluß und die Verbindung zum Netzwerk. Es kontrolliert die Verbindung zwischen dem Node (PC, Drucker etc.) oder dem Concentrator Port und dem Kabel.

Die MAU selbst wird wieder in zwei Bereiche unterteilt: das Physical Medium Attachment (PMA) und das Medium Dependent Interface (MDI). Das PMA enthält die Schaltungstechnik, das MDI stellt die mechanische und elektrische Schnittstelle zwischen dem Kabelsegment und der MAU dar. Aufgrund dieser getroffenen Festlegungen ist bereits ersichtlich, daß alle Implementierungen auf der MDI-Ebene kompatibel sein müssen, um solche Lokalen Netze miteinander koppeln bzw. Komponenten von Drittherstellern ohne Schwierigkeiten einsetzen zu können. Es muß zum Beispiel möglich sein, Concentrator und Netzadapterkarten verschiedener Hersteller mit-

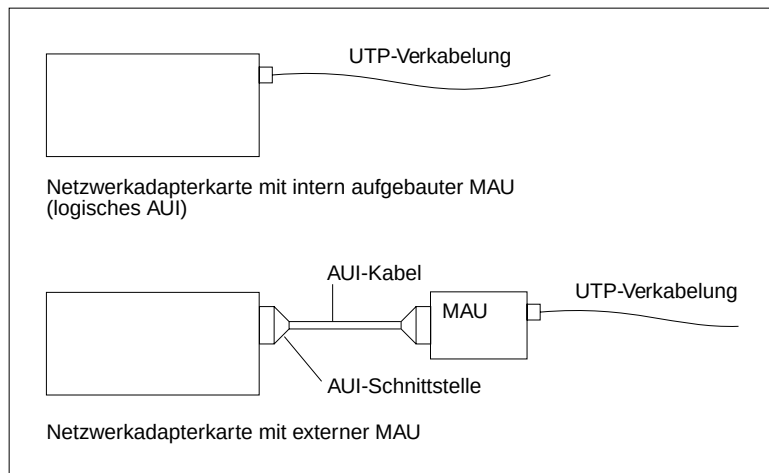
4 Netzwerkaufbau und Netzwerktopologien

einander zu mischen. Auf MAU-Ebene allerdings haben die Hersteller für die Umsetzung der Schaltungen eine ziemlich große Freiheit.

Die MAU stellt bestimmte Dienste bereit. Dies betrifft unter anderem den Transport von Informationen zur physikalischen Signalebene des Eingabegeräts. Die Verbindung wird über eine sogenannte AUI (Attachment Unit Interface) hergestellt. Entsprechend dem 802.3-Standard ist die AUI-Schnittstelle zwischen der MAU und dem Eingabegerät bzw. dem Concentrator Port.

Die MAU kann dabei entweder bereits im Eingabegerät oder im Concentrator enthalten sein oder aber auch als externes Gerät realisiert werden. Beim Einsatz einer externen MAU existiert eine physikalische AUI. Dies kann durch ein Kabel realisiert werden, das die MAU mit dem AUI-Port der Netzadapterkarte verbindet. Handelt es sich hingegen um eine eingebaute MAU, wird lediglich eine logische AUI benötigt. In Abbildung 4.8 ist der Unterschied zwischen diesen beiden Techniken dargestellt.

Abbildung 4.8
Interne und
externe MAU



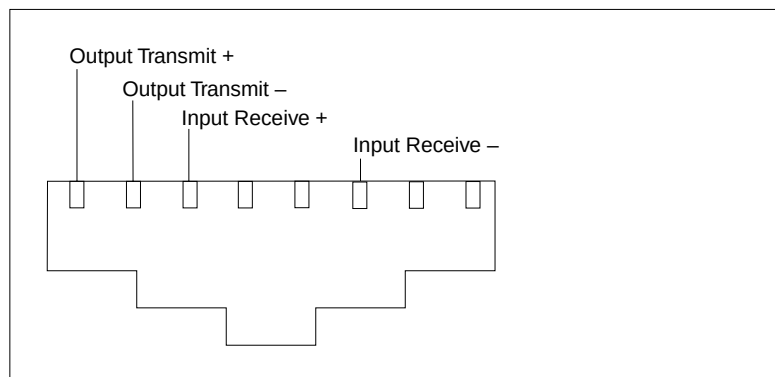
Wie bereits erwähnt, existiert für 10BASE-T ein Verbindungstest, der klärt, ob der Kontakt zwischen Concentrator (Repeater) und Endgerät noch aktiv ist. Dabei gehen vom Concentrator in regelmäßigen Abständen Signale an die MAUs. Antwortet eine MAU nicht mehr, wird die Verbindung zu diesem Endgerät unterbrochen und eine Meldung ausgegeben (sofern eine Managementfunktion zur Verfügung steht), daß der Test nicht erfolgreich gewesen ist. Fängt die MAU plötzlich wieder an, Signale auszusenden, wird ohne Ihr Zutun der Concentrator Port geöffnet und die Station in das Netz integriert.

4.1 Ethernet-LANs

Die Sterntopologie lässt sich generell leichter installieren und überwachen. Fällt in einem 10BASE-T-Netzwerk ein Segment aus, wird nur dieses Segment abgeschaltet (der einzelne Port) und nicht das gesamte Netzwerk, wie dies bei einer Bustopologie der Fall wäre. Alle 10BASE-T-Concentrator (Repeater) müssen einen sogenannten Auto-Partition-/Reconnection-Algorithmus unterstützen. Dieser Algorithmus erlaubt dem Concentrator (Repeater) das automatische Abschalten eines Ports, wenn dieser einen Fehler aufweist, und das automatische Reaktivieren des Ports, wenn der Fehler behoben ist. Auf diese Weise wird nur der defekte Port deaktiviert und nicht der gesamte Repeater.

An beiden Enden des Verbindungskabels wird zum Anschluß an den Concentrator (Repeater) ein RJ45-Stecker verwendet. In Abbildung 4.9 ist die Pinbelegung für diesen Anschlußstecker aufgezeigt.

Abbildung 4.9
Steckerbelegung
(RJ45) für
10-BASE-T

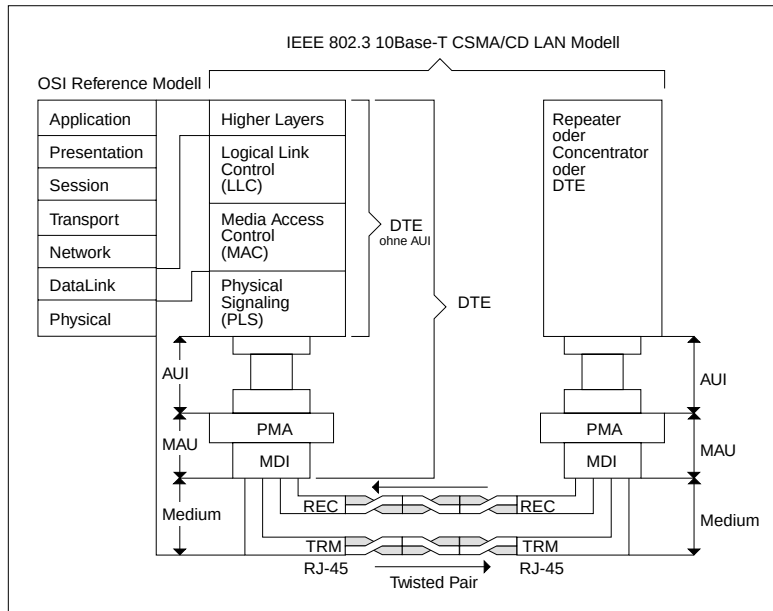


Durch die zur Verfügung stehenden Möglichkeiten, die 10BASE-T-Komponenten zum Aufbau und zur Überwachung von LANs bereitzustellen, wird die Fehlerdiagnose wesentlich vereinfacht. Gute Netzadapterkarten und Concentrator (Repeater) haben pro Port eine eigene LED für den Link State. Diese leuchtet (meist grün), wenn die Verbindung zwischen Concentrator (Repeater) und Netzadapterkarte oder dem nächsten Concentrator in Ordnung ist. Man hat hier bereits optisch die Möglichkeit, die korrekte Verbindung zu überprüfen.

In der folgenden Abbildung ist dargestellt, wie 10BASE-T im OSI-Modell eingegliedert ist.

4 Netzwerkaufbau und Netzwerktopologien

Abbildung 4.10
10BASE-T im
ISO-OSI-Schichten-
modell



Die Anzahl der Ports an einem Concentrator unterscheidet sich von Hersteller zu Hersteller. Die Auswahl der entsprechenden Concentrator hängt von der jeweiligen Situation ab, d.h., wie viele Nodes vernetzt werden sollen, um die geeigneten Komponenten auszuwählen. In der Regel dürfen bis zu 12 Concentrator kaskadiert werden, um die entsprechende Port-Anzahl zur Verfügung zu haben bzw. die entsprechenden Längen überbrücken zu können.

Eine weitere wichtige und marktbeherrschende Netzwerktopologie bildet der Token-Ring. Dessen Möglichkeiten sollen im nächsten Abschnitt erläutert werden.

4.2 Token-Ring-LANs

Der Aufbau von Token-Ring-Netzwerken unterscheidet sich grundsätzlich von dem Aufbau der im vorigen Kapitel besprochenen Ethernet-Netze, allerdings nur, solange man auf klassische Bustopologie setzt. Wie Sie noch sehen werden, ist die Verkabelung physikalisch gesehen eine sternförmige Struktur, ähnlich wie Sie es bereits von 10BASE-T kennengelernt haben. In den folgenden Abschnitten will ich Ihnen zeigen, wie Token-Ring-Netze aufgebaut werden können.

4.2 Token-Ring-LANs

4.2.1 IBM-Token-Ring-Netzwerk

Das IBM-Token-Ring-Netzwerk basiert auf den bereits erwähnten internationalen Standards für Lokale Netze, IEEE 802.5. Bevor wir uns näher mit den technischen Spezifikationen dieses Netzwerks auseinandersetzen, wollen wir uns zuerst das IBM-Verkabelungssystem etwas genauer ansehen. Bemerkt sei an dieser Stelle, daß das IBM-Token-Ring-Netz genau auf dieses Verkabelungssystem aufbaut.

Das IBM-Verkabelungssystem

Wie Sie bereits aus den Ausführungen zu Beginn dieses Buchs wissen, kann bei der Verkabelung von Gebäuden, für den Aufbau von LANs und den Anschluß von Datenstationen eine Vielzahl unterschiedlicher Kabeltypen eingesetzt werden. Jeder dieser Kabeltypen zeichnet sich durch spezielle technische und physikalische Eigenschaften aus, die für die vorgesehenen Einsatzbereiche optimale Einsatzbedingungen gewährleisten. Ausschlaggebend für die Verwendung der einzelnen Kabeltypen sind neben technischen Aspekten vor allem auch Wirtschaftlichkeit und Migrationsfähigkeit für zukünftige Verkabelungsvorhaben.

Weil unterschiedliche Netzwerke oft auch verschiedene Kabeltypen erfordern, ist bis heute in Firmen vielfach Mehrfachverkabelung notwendig. Damit sind natürlich erhöhte Kosten verbunden.

Dies schlägt sich vor allem dann negativ nieder, wenn eine sehr hohe Dichte von Datenendgeräten besteht und zudem eine Vielfalt unterschiedlicher Systeme eingesetzt werden muß. Der Aufwand für eventuelle Änderungen und die damit verbundenen Kosten dürfen dabei nicht vernachlässigt werden.

Bei IBM werden selbst die einzelnen Systeme über unterschiedliche Kabeltypen miteinander verknüpft, und dazu müssen auch noch unterschiedliche Steckdosen verwendet werden.

So wird beispielsweise beim System IBM 3600/4700 ein Klinkenstecker verwendet, während hingegen die mit Twinax-Kabel angeschlossenen Systeme, IBM 5250, Spezialstecker verwenden. Bildschirme und Drucker der IBM-Host-Welt (3270-Welt) werden über BNC-Stecker angeschlossen, während Ringleitungssysteme der IBM 8100 oder der IBM 4300 mit IBM-Spezialsteckern angeschlossen werden.

Diese unterschiedlichen Anschlußvoraussetzungen können nur durch den Einsatz einer einheitlichen Datensteckdose und einer einheitlichen Verkabelung für alle Gerätetypen umgangen werden. Mittlerweile wurden erste Schritte unternommen, um dies zu erreichen.

4 Netzwerkaufbau und Netzwerktopologien

Der IBM-Datenstecker, der für das IBM-Token-Ring-Netzwerk benötigt wird, erfüllt diese Anforderung und ist zudem von der IEEE genormt. Für die Montage des IBM-Datensteckers steht ein Einsatz für eine Standardeinbaudose zur Verfügung. In diesen Einsatz kann von der Rückseite der mit dem Kabel versehene Datenstecker eingeklinkt und arretiert werden. Nach Einschub dieser Kombination in die Installationsdose wird die Frontseite mit einer Abdeckplatte abgeschlossen. Der Anschluß eines Endgeräts an die montierte Wandsteckdose erfolgt mit dem gleichen Steckertyp, der dabei nur um 180 Grad gedreht werden muß. IBM bezeichnet diesen Stecker auch als *hermaphroditischen Stecker*, da nur noch ein Steckertyp benötigt wird, um die Endgeräte anschließen zu können, im Gegensatz zu den bisherigen Steckerverbindungen, die zwischen männlichen und weiblichen Steckern unterscheiden mußten.

Für das IBM-Verkabelungssystem stehen insgesamt sieben verschiedene Kabeltypen zur Verfügung. Im Folgenden sollen deren grundsätzliche Unterschiede dargestellt werden.

Typ-1-Kabel

Dieses Kabel besteht aus zwei verdrehten Doppeladern aus massivem Kupferdraht, die mit einer doppelten Abschirmung versehen sind. Die kunststoffisolierten Leiter sind farbcodiert und finden sich in drei Kabelversionen wieder, die für die stationäre Verkabelung gedacht sind. Bei der Standardversion handelt es sich um die am meisten verwendete Typen für Bereiche, die keinen besonderen Anforderungen unterliegen.

Die teflummantelte Version ist für Bereiche gedacht, die besonderen feuerpolizeilichen Bestimmungen unterliegen (dieses Kabel wird jedoch nur in den USA ausgeliefert, da in der BRD andere Vorschriften bestehen). Die dritte Version ist für Außenmontage gedacht und zeichnet sich im wesentlichen durch eine besondere physische Stabilität aus.

Typ-2-Kabel

Dieser Kabeltyp ist im Aufbau mit dem Typ-1-Kabel vollkommen identisch. Zusätzlich sind jedoch noch vier einfache Doppeladern außerhalb der Abschirmung untergebracht, die für spezielle Zwecke eingesetzt werden, zum Beispiel, um darüber Telefone anzuschließen, oder, wie es die Firma *Proteon* für die eigenen voll kompatiblen Ringleitungsverteiler vorsieht, um den Ring zu überwachen und Fehler zu lokalisieren.

Typ-3-Kabel

Das Typ-3-Kabel entspricht einem Telefonkabel und kann auch für die Verkabelung eines Token-Ring-Netzes eingesetzt werden. Hierbei sind jedoch bestimmte Einschränkungen zu beachten, auf die ich später noch zu sprechen komme.

4.2 Token-Ring-LANs

- Typ-5-Kabel** Dieser Kabeltyp wird für Glasfaserstrecken verwendet. Das Typ-5-Glasfaserkabel ist für 100/140 Micron spezifiziert. Dieser Kabeltyp wird inzwischen jedoch nicht einmal mehr von IBM empfohlen, da bereits fast alle anderen LWL-Typen eingesetzt werden können.
- Typ-6-Kabel** Das Typ-6-Kabel ist eine flexible Ausführung des Typ-1-Kabels und sollte nur für die direkte Verbindung von Endgerät und Ringleitungsverteiler oder Endgerät und Wandsteckdose eingesetzt werden. Für alle anderen Anschlüsse sollten die besseren Kabeltypen (1, 2 oder 5) eingesetzt werden. Auch die physikalischen Eigenschaften dieses Kabels entsprechen nicht denen der anderen Typen; daher lassen sich keine so großen Entfernungen überbrücken. Die Innenleiter des Kabels bestehen aus gedrehten Kupferlitzen und nicht aus massivem Kupferdraht wie beim Typ-1- oder Typ-2-Kabel.
- Typ-8-Kabel** Bei diesem Kabeltyp der IBM handelt es sich um ein spezielles Flachkabel, das es erlaubt, Endgeräte nachträglich zu installieren, ohne vorhandene Kabelschächte zur Kabelverlegung zu verwenden. Das Kabel kann unter den Teppichboden zur Datensteckdose hin verlegt werden.
- Typ-9-Kabel** Das Typ-9-Kabel ist ein spezielles brandgesichertes Teflonkabel für das IBM-Verkabelungssystem und entspricht bezüglich der physikalischen Eigenschaften dem Typ-1-Teflonkabel. Der einzige Unterschied liegt im Preis.
- Das Typ-9-Kabel ist eine billigere Ausführung und wird vorwiegend in den USA benutzt, da dort üblicherweise die Kabelverlegung in den Klimaschächten erfolgt. Dieses Kabel entspricht jedoch nicht der deutschen feuerpolizeilichen Bestimmung.
- Bei den beschriebenen Kabeltypen werden verdrehte Kupferdoppeladern verwendet, außer es handelt sich um das Typ-5-Kabel (Fibre Optic). Bei den verdrehten Kupferadern handelt es sich um ein sogenanntes *symmetrisches Medium*, das die Eigenschaft besitzt, relativ unempfindlich gegen magnetische Störungen zu sein, was sich positiv auf die Zuverlässigkeit der Datenübertragung auswirkt.
- Die Kabel aus Kupferadern zeichnen sich zudem dadurch aus, daß sie vor allem für den Anschluß von Endgeräten zwischen Verteilerraum und Anschlußpunkt einfach und zuverlässig installiert werden können. Dies ist wichtig, da es sich bei diesen Installationen meist um eine große Anzahl von Anschlüssen handelt und an den Anschlußpunkten nicht selten erschwerte Arbeitsbedingungen vorherrschen.
- Damit das Kabel zusätzlich gegen Störungen von außen abgesichert werden kann, ist dieses zusätzlich mit einer doppelten Abschirmung versehen, die einerseits das Erdpotential trägt, andererseits einen weiteren Schutz gegen elektrische Störungen bietet.

4 Netzwerkaufbau und Netzwerktopologien

Da in einem Ringnetz Sender und Empfänger permanent aktiv sind und die Leitungen des Sende- und Empfangssignals sehr eng nebeneinanderliegen, ist der Einsatz eines symmetrischen Mediums, wie der verdrehten Doppelader, von großem Vorteil. Diese Kabelform gewährleistet, daß relativ wenig Energie von der Sende- auf die Empfangsleitung übergehen kann (der sogenannte Effekt des Nebensprechens).

Außerdem erlaubt der Einsatz eines Doppeladerpaares, Gleichstromkomponenten zu übertragen, um zum Beispiel durch zusätzliche Steuerung in einem Kabelverteiler die dynamische Einfügung eines Endgeräts in den Ring vorzunehmen. Es ist somit möglich, eine automatische Überbrückung bei Ausfall einer Station oder einer Anschlußleitung vorzunehmen und einen Schleifentest vom Endgerät aus zu implementieren.

Beim Einsatz von Token-Ring-Systemen mit dem IBM-Verkabelungssystem sind für den Anschluß von Endgeräten und bei Verwendung von Wandsteckdosen Datenstecker entwickelt worden, die gleichzeitig als Stecker oder als Buchse verwendet werden können. Diese Steckertypen werden auch unter der Bezeichnung *hermaphroditischer Stecker* geführt. Der Stecker verfügt über mehrere Möglichkeiten der Kanalzuführung. Das Kabel kann entweder senkrecht nach oben oder nach unten herausgeführt werden. Es ist aber auch möglich, das Kabel von hinten oder unter einem Winkel von 45 Grad zu montieren. Damit ist eine gewisse Flexibilität erreicht worden, die es erlaubt, auch komplizierte Installationsbedingungen gut zu meistern.

Betrachtet man den Stecker und die Montage der Kabel etwas näher, stellt man fest, daß diese unter dem Gesichtspunkt größtmöglicher Einfachheit und Zuverlässigkeit bei der Installation entwickelt worden sind. Für den Anschluß der Kupferleiter und den Zusammenbau des Steckers sind beispielsweise keinerlei Lötarbeiten erforderlich, es müssen auch keine Spezialwerkzeuge verwendet werden. Für die Montage genügen eine Zange zum Abschneiden des Kabels und ein Messer oder Abisolierwerkzeug zum Freilegen der Kupferleiter. Die Anschlüsse an den goldplattierten Kontakten sind mit einer Farbcodierung versehen, die derjenigen der einzelnen Kupferadern entspricht. Ein Vertauschen der Leiter ist dadurch bei sorgfältigem Arbeiten fast ausgeschlossen. Die Leiter werden an den Anschlüssen nur eingeklemmt und dadurch automatisch »aufgeschlitzt«, genauso wie bei Quetschverbindern für Flachbandkabel. Ein explizites Abisolieren der einzelnen Leiterkabel entfällt somit gänzlich.

Für Schleifentests, für den Einsatz in bestehenden Systemkonfigurationen oder für den Einsatz in zukünftigen Token-Ring-Netzen verfügt der Stecker über einen automatischen Schleifenschluß (paar-

4.2 Token-Ring-LANs

weise Verbindung zweier Kontakte). Dieser Schleifenschluß wird für jeden der zu einer Verbindung gehörigen Stecker im Moment der Auftrennung der Steckverbindung wirksam.

Folgendes Zubehör wird nur kurz beschrieben, da eine detaillierte Beschreibung den Rahmen dieses Buchs sprengen würde.

Bestandteile des IBM-Verkabelungssystems sind normalerweise ein oder mehrere Verteiler. An diesen zentralen Punkten werden die einzelnen von den Anschlußdosen herkommenden und zum Beispiel an das Rechenzentrum weiterführenden Kabel miteinander verknüpft oder durch entsprechende Hardware-Einrichtungen konzentriert. Für diesen Verteiler wird von der Firma IBM ein sogenannter Verteilerrahmen angeboten. Dieser Verteilerrahmen kann in 19-Zoll-Gestelle eingesetzt werden. Der Verteilerrahmen enthält 64 Aussparungen, in die von hinten die Anschlußkabel, versehen mit IBM-Datensteckern, eingeklinkt und verriegelt werden können. Von vorne können somit nach Bedarf Verbindungskabel zu Konzentratoren oder zu weiterführenden Kabeln, die in einem anderen Verteilerrahmen aufgelegt sein können, gesteckt werden. Die einzelnen Steckerpunkte des Verteilerrahmens sind mit Spalten- und Zeilenmarkierungen versehen, damit eine leichte Lokalisierung der Positionen möglich ist.

In diese 19-Zoll-Gestelle können neben den Verteilerrahmen spezielle Koax-Anschlußplatten eingebaut werden, die es erlauben, 3270-Systeme über den Verteilerrahmen auf einen anderen Kabeltyp umzusetzen. Die Koax-Anschlußplatte enthält insgesamt 24 BNC-Doppelbuchsen, an die jeweils von hinten und von vorne Koaxialstecker angeschlossen werden können. Entsprechende Verbindungskabel zur Weiterführung zu einem anderen Kabeltyp werden von IBM angeboten.

Inzwischen geht man jedoch dazu über, eine vollständig einheitliche Verkabelung auf Basis einer Twisted-Pair-Verkabelung (mindestens CAT 5) und der RJ45-Stecker-Technik durchzuführen. Damit ist gewährleistet, daß man die verlegten Kabel und Stecker für jede zukünftige Netzwerktechnik verwenden kann, egal ob es sich dabei um Ethernet, Token-Ring, CDDI oder ATM handelt. Ausschlaggebend ist dabei nur, daß die eingesetzten Verkabelungskomponenten mit dieser Art Twisted-Pair-Kabel umgehen können, da es sich in der Regel um 100-Ohm-Kabel handelt, anders als bei der traditionellen IBM-Verkabelungstechnik, die auf Basis einer 150-Ohm-Kabelstruktur aufgebaut worden ist bzw. zum Teil immer noch wird. Will man jedoch offen für die Zukunft sein, wird man alles auf Grundlage der 100-Ohm-Twisted-Pair-Verkabelung und der RJ45-Stecker-Technik installieren.

4 Netzwerkaufbau und Netzwerktopologien

Zu beachten ist dabei nur, daß jedes Netzwerk beim Einsatz einer Twisted-Pair-Verkabelung und den RJ45-Steckern unterschiedliche Belegungen verwendet. Bei der Beschreibung der Ethernet-Twisted-Pair-Verkabelung wurde bereits darauf hingewiesen, daß der RJ45-Stecker aus insgesamt acht Anschlüssen besteht, geeignet für ein 4-paariges Twisted-Pair-Kabel. Man kann jedoch auch 2-paarige Kabel verwenden, wenn man die richtige Belegung der Kabelkontakte berücksichtigt. Gemäß der Standarddefinition für eine strukturierte Verkabelung mit Twisted-Pair-Kabeln und RJ45-Steckern sind für die einzelnen Netzwerke die folgenden Stiftbelegungen des RJ45-Steckers definiert:

	Ethernet	Token-Ring	CDDI
Pin 1	X		X
Pin 2	X		X
Pin 3	X	X	
Pin 4		X	
Pin 5		X	
Pin 6	X	X	
Pin 7			X
Pin 8			X

Man sieht also, daß es nicht ohne weiteres möglich ist, die aktiven Verkabelungskomponenten gegen eine andere Netzwerktechnik zu tauschen, wenn man nicht auch bei der Belegung der Steckerkontakte darauf achtet, ob diese mit dem neuen Netzwerk (Übergang von Ethernet zu CDDI) zusammenpassen. Dieses Problem läßt sich entweder dadurch lösen, daß man von Anfang an gleich vierpaarige Kabel verlegt und jedes Adernpaar in der Dose und im Patch-Feld des Verteilerraums auflegt. Oder man muß beim Einsatz von zweiadrigen Kabeln entweder codierbare Anschlußdosen verwenden oder mit Hilfe der Patchkabel auf die richtige Belegung für den Anschluß der Netzwerkadapterkarte achten und dem aktiven Verteiler die korrekte Pinbelegung ermöglichen.

Aufbau eines IBM-Token-Ring-Netzes

Wie bereits mehrfach erwähnt, basieren das IBM-Token-Ring-Netz und alle hiermit kompatiblen Netze auf dem IEEE-802.5-Standard. Die Token-Ring-Architektur setzt grundsätzlich keine Grenzen bezüglich der eingesetzten Übertragungsgeschwindigkeit. Die anschließend zu besprechenden Spezifikationen und Möglichkeiten

4.2 Token-Ring-LANs

orientieren sich am 4-Mbit/s-Token-Ring der IBM. Ich werde Ihnen anschließend die Spezifikationen für den 16-Mbit/s-Token-Ring aufzeigen. In den meisten Fällen wird inzwischen zwar dieser Token-Ring installiert, aber dennoch soll zuerst der 4-Mbit/s-Token-Ring erläutert werden. Fast alle neuen Token-Ring-Karten lassen es zu, zwischen 4 Mbit/s und 16 Mbit/s zu wählen.

IBM beschreibt die eigene Architektur aufgrund der eingesetzten Komponenten als *logischen Ring*, der aus einer Struktur physischer untereinander verbundener *Sternnetze* resultiert. Die Übertragungsmedien werden durch das IBM-Verkabelungssystem festgelegt. Wie Sie später noch sehen werden, kann es sich dabei um mehrfach abgeschirmte Kupferdoppeladern hoher Qualität oder um optische Leiter handeln.

Die maximale Ausbaufähigkeit eines einzelnen Token-Rings ist auf 260 anschließbare Komponenten begrenzt. Der Grund für diese Limitierung ist in der physikalischen Arbeitsweise des Token-Ring-Netztes begründet und hat ihre Ursache in dem auftretenden *Jitter-Effekt*.

Die Beiträge von IBM an IEEE bezüglich der Implementierung eines Token-Ring-Netzwerks gehen von einer physischen Sternverkabelung aus. Dabei enthält jedes Kabel, das zum Endgerät führt, einen Pfad für die Hin- sowie einen Pfad für die Rückleitung. Durch spezielle Verknüpfungen im Sternpunkt ist es möglich, ein Ringnetz aufzubauen.

Die Komponenten, die die Aufgabe dieses Sternpunkts übernehmen, werden als *Ringleitungsverteiler*, *Wire-Center* oder *Multi Station Access Unit* bezeichnet. Es kann sich dabei um einzelne Komponenten handeln oder im Zuge einer strukturierten Verkabelung um Einschübe eines Hub-Systems. Je nach Größe und Ausdehnung des Netzwerks wird man sich für die eine oder andere Lösung entscheiden. In den nachfolgenden Ausführungen werden wir die Bezeichnung RLV (Ringleitungsverteiler) verwenden.

Ein typischer passiver RLV enthält Anschlußpunkte für maximal acht anschließbare Endgeräte. Andere Hersteller bieten jedoch auch RLVs für mehr als acht Anschlüsse an. IBM hat zum Beispiel den 8230 RLV mit insgesamt 80 Anschlußpunkten. Dieser passive RLV kann entweder in ein 19-Zoll-Gestell, eventuell zusammen mit anderen IBM-Komponenten oder 19-Zoll-kompatiblen Systemen, eingebaut werden, oder er kann in einem eigenen Gehäuse untergebracht und in Wand- oder Tischmontage eingesetzt werden. Der RLV der IBM enthält selbst keine eigene Stromversorgung (im Gegensatz zu anderen kompatiblen RLVs). Der IBM-RLV benötigt zur Ausführung seiner Funktion die Ansteuerung des entsprechenden Endgeräts. Durch die

4 Netzwerkaufbau und Netzwerktopologien

Ansteuerung des Endgeräts wird gewährleistet, daß Endgeräte automatisch in den Ring eingefügt werden und bei Bedarf oder im Fehlerfall auch wieder aus dem Ring entfernt werden können.

Gibt es mehr als acht Endgeräte (bzw. sind alle Anschlußpunkte des RLV belegt) können zur Vergrößerung des Rings mehrere RLVs zusammengeschaltet werden. Hierfür besitzt jeder RLV neben den entsprechenden Anschlüssen für die Endgeräte auf der rechten Seite einen Ring-Output- (RO) und auf der linken Seite einen Ring-Input-Anschluß (RI). Beim RO-Anschluß wird die Verbindung zum nächsten RLV hergestellt, wohingegen beim RI-Anschluß das Kabel des letzten RLV angesteckt wird.

Wird ein Endgerät in den Ring eingefügt, so findet nach Einschalten des Geräts zunächst ein interner Adaptertest statt. Anschließend wird die im Ringleitungsverteiler noch kurzgeschlossene Anschlußleitung mit einem Testmuster beschickt, so daß die Funktionsweise des Adapters und der Verbindungsleitung überprüft werden kann. Schließlich wird vom Endgerät veranlaßt, daß durch Anlegen einer Versorgungsspannung (Phantomspannung) an die im Ringleitungsverteiler befindliche Relaisschaltung diese sich öffnet und das Endgerät somit in den Ring eingefügt ist. Diese Phantomspannung fließt anschließend ständig zwischen Endgerät und RLV. Sobald sie fehlt (z.B. bei gezogenem Stecker) schließt das Relais am RLV.

Anhand der Abbildung 4.11 soll die Funktionsweise des RLV näher erläutert werden.

Die Anschlußpositionen für die einzelnen Endgeräte – wie bereits besprochen: acht Stück oder mehr – werden durch eine Relaisschaltung abgeschlossen. Damit ist beim Fehlen von angeschlossenen Endgeräten oder wenn dieses ausgeschaltet sind, der Ring im Ringleitungsverteiler geschlossen. Im Moment der Inbetriebnahme eines Endgeräts wird von diesem – wie bereits besprochen – dafür gesorgt, daß es durch die Aktivierung des Relais in den Ring eingeschaltet wird. Das bedeutet, daß die Signale nun auch durch das Endgerät (Funktion des Rings) geschleust werden. Dieser Vorgang findet für alle Endgeräte nach Inbetriebnahme statt.

Tritt ein Fehler auf, zum Beispiel eine durchtrennte Leitung, ein abgeschaltetes Endgerät oder Stromausfall des Endgeräts, wird dieser Anschlußpunkt wegen der fehlenden Aktivierung durch das Endgerät wieder kurzgeschlossen und die Ringstruktur somit erneut hergestellt (siehe Abbildung 4.12).

4.2 Token-Ring-LANs

Abbildung 4.11
Die Funktions-
weise des Ring-
leitungsverteilers

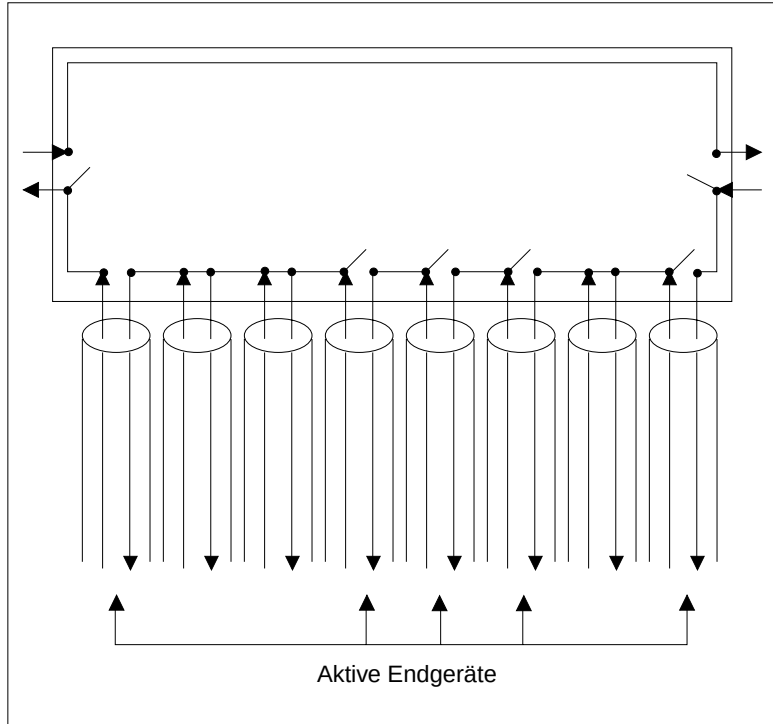
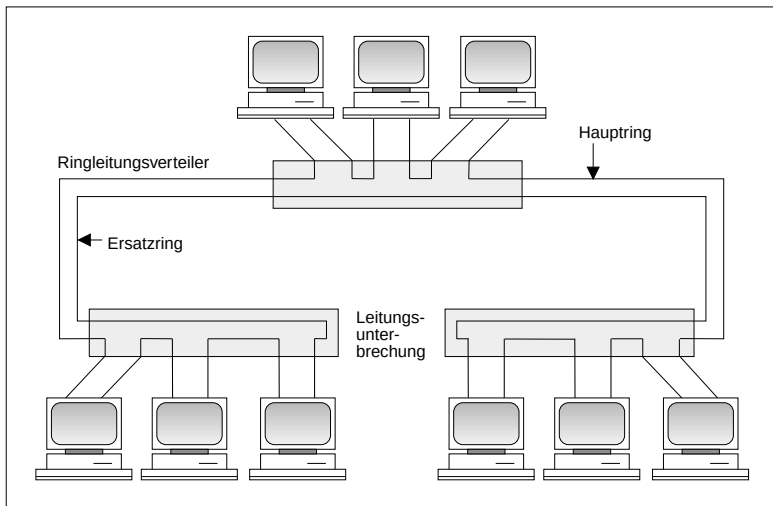


Abbildung 4.12
Ersatzschaltung
im Fehlerfall



4 Netzwerkaufbau und Netzwerktopologien

Für die Anschlüsse der weiterführenden Leitungen zu anderen RLVs, RI- bzw. RO-Schaltung, gilt dieses Verfahren allerdings nicht. An diesen beiden Anschlußpunkten findet der jeweilige Kurzschluß bzw. das Auftrennen der Leitung durch das Einfügen des Datensteckers statt. Dies liegt daran, daß an diesen Anschlußpunkten keine Endgeräte angeschlossen werden und somit auch keine Aktivierung des Relais erfolgen kann. Diese Funktionsweise älterer Ringleitungsverteiler für RI und RO hat jedoch einen entscheidenden Nachteil: Da die Verbindung von RI zu RO durch Steckerkontakt erfolgt, bedeutet dies bei einem Kabelbruch zwischen den beiden RLVs, daß der Ring unterbrochen ist und somit »steht«, da kein automatisches Schließen erfolgen kann.

Bei den älteren RLVs mußte man in solchen Fehlersituationen wissen, zwischen welchen RLVs der Fehler liegt und die Kabel mit der Hand ziehen, um die Kontakte für den RI des einen RLV und den RO des anderen RLV zu schließen und den Ring wieder funktionsfähig zu machen.

Dieser Mißstand wurde von anderen Herstellern bereits früh erkannt und beseitigt, indem auch die RI- und RO-Anschlüsse über Relais gesichert werden. Im Fall eines Kabelbruchs zwischen zwei RLVs fehlt die Phantomspannung, die Relais schließen automatisch und erhalten den Ring aufrecht. Die IBM nutzte diese Technik erst mit den RLVs 8230 und allen späteren Weiterentwicklungen, um dadurch ebenfalls einen verbesserten Ausfallmechanismus gewährleisten zu können, indem der Ring automatisch geschlossen wird.

Die erste Generation RLVs der IBM wurde unter der Bezeichnung IBM 8228 geführt. Wenn Sie also in IBM-Beschreibungen in Verbindung mit Token-Ring-Netzen etwas über IBM-8228-Geräte lesen, sind damit Ringleitungsverteiler gemeint. Für den Aufbau von Token-Ring-Netzen sind bestimmte Längenrestriktionen zu beachten, wenn Sie diese Netze ohne zusätzliche Verstärkereinrichtungen betreiben wollen. Diese Längenangaben beziehen sich auf die Verkabelung mit den vorgeschriebenen IBM-Kabeltypen, die bereits weiter oben beschrieben worden sind. In allen anderen Fällen sind die Spezifikationen der einzelnen Hersteller durchzulesen; hier sind Informationen über die Längenrestriktionen zu finden. Da jeder Hersteller unterschiedliche Komponenten verwendet, sind auch andere Spezifikationen und Restriktionen damit verbunden. Die nachfolgenden Ausführungen sollen zumindest einen groben Überblick geben, welche Restriktionen in einer normalen Standardumgebung zu erwarten sind.

4.2 Token-Ring-LANs

Wenn Sie sich dafür entscheiden, statt der klassischen IBM-Verkabelung die 100-Ohm-Twisted-Pair-Verkabelung einzusetzen, lässt sich die Längenrestriktion sehr leicht definieren: 100 Meter (genau 90 Meter zwischen Verteilerraum / Dose und insgesamt 10 Meter für Patchkabel).

Die bislang beschriebenen Komponenten werden zwar nicht mehr unbedingt bei Standardinstallationen eingesetzt, es lassen sich dadurch aber sehr einfach die Schwierigkeiten erkennen, die beim Aufbau von Token-Ring-LANs auftreten können. Beim Aufbau komplexer Token-Ring-LANs sind auf alle Fälle die technischen Spezifikationen des Herstellers zu berücksichtigen, um alle notwendigen Anforderungen erfüllen zu können.

In der nachfolgenden Tabelle sind die Restriktionen der Datenkabel Typ 1 und 2 bzw. Datenkabel Typ 3 wiedergegeben.

	Datenkabel Typ 1/2	Datenkabel Typ 3
Datenrate getestet	16 Mbit/s	4 Mbit/s
Kabellänge Verteilerraum–Anschlußdose		
1 Verteilerraum	max. 300 m*	max. 100 m
Mehrere Verteilerräume	max. 100 m	max. 45 m
Kabellänge Verteilerraum–Verteilerraum		
Ohne Verstärker	max. 200 m*	max. 100 m T 1
Mit IBM 8218	max. 750 m*	max. 600 m
Mit IBM 8219	max. 2000 m	max. 2000 m
	(bei Kaskadenschaltung > 2000 m)	
Unterstützte Anzahl der Endgeräte	max. 260	max. 72
Anzahl der RLVs	max. 33	max. 9
Anzahl Verteilerräume	max. 12	max. 2
Filter im Endgerätestecker notwendig	nein	ja

* nur 4 Mbit/s

Beim Einsatz des Typ-9-Kabels sind als Längenangaben zwei Drittel von Typ 1 zu nehmen. Der Kabeltyp 6 sollte nur als Lobe-Kabel für die Verbindung von Endgerät und Wandsteckdose eingesetzt werden und auf keinen Fall für eine RLV-RLV-Kopplung.

4 Netzwerkaufbau und Netzwerktopologien

Reichen die Entfernungen zwischen den RLVs für den Aufbau von Token-Ring-Netzen nicht aus, bietet IBM hierfür entsprechende Komponenten an, um größere Strecken überbrücken zu können. Es handelt sich dabei um einen *Leitungsverstärker IBM 8218* (nur für 4 Mbit/s) und um einen *Lichtleiter-Umsetzer IBM 8219* (nur für 4 Mbit/s) (s. obige Tabelle).

Der IBM 8218 ist als Erweiterungsbaustein des IBM-Token-Ring-Netzes zu verstehen. Die Aufgabe des Leitungsverstärkers besteht darin, größere Entfernungen zwischen zwei Ringleitungsverteilern auf der Basis von 4 Mbit/s Übertragungsgeschwindigkeit zuzulassen. Im Gegensatz zum Ringleitungsverteiler der IBM, der ein passives Verhalten aufweist (er wird ohne Stromversorgung betrieben), benötigt der Leitungsverstärker einen eigenen Netzanschluß. Die Hauptaufgabe dieser Komponente besteht darin, die Datensignale zu verstärken, zu resynchronisieren und zu regenerieren. Da der RLV nur eine Übertragungsrichtung verstärkt und regeneriert, müssen die Verstärker paarweise pro Leitung eingesetzt werden. Für die Verbindung RLV1-RO und RLV2-RI benötigen Sie somit insgesamt vier Leitungsverstärker, zwei Stück pro Leitung. Der Leitungsverstärker kann einzeln oder in einem 19-Zoll-Gestell (maximal sieben Stück) montiert werden. In Abbildung 4.13 ist eine typische Konfiguration mit Einsatz eines Leitungsverstärkers aufgezeigt.

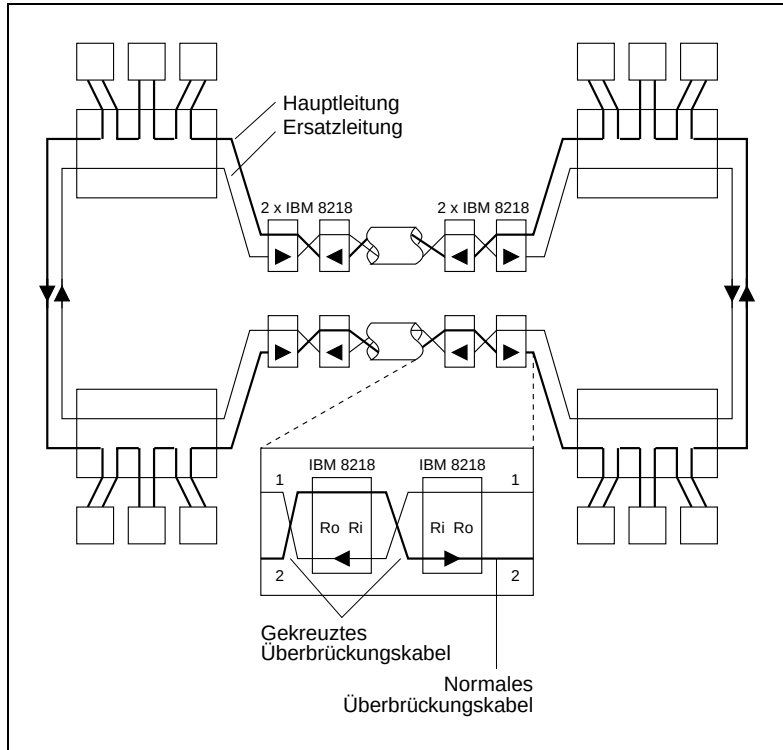
Wie Sie in diesem Bild sehen können, sind zwischen zwei RLVs, die mit Typ-1-Kabel verbunden sind, je zwei Leitungsverstärker vorge schaltet. Der Grund für die angeordneten, hintereinandergeschalteten Verstärker an jedem Kabelende liegt im Verstärkerverhalten und in der Token-Ring-Struktur. Da im Verbindungskabel der RLVs sowohl Haupt- als auch Ersatzleitung untergebracht sind, läßt sich keine andere Anordnung finden.

Da beide Leitungen, Haupt- und Ersatzleitung, verstärkt werden sollen und der Ringleitungsverteiler nur in einer Richtung verstärken kann, muß die aufgezeigte Schaltungsanordnung so gewählt werden. Um eine Entfernung von maximal 750 Metern zwischen RLVs überbrücken zu können, sind also vier IBM 8218 (pro Kabel) notwendig.

Reichen diese 750 Meter Entfernung auch nicht aus, kann dies mit einem Token-Ring-Lichtleiterumsetzer wesentlich weiter überbrückt werden. Beim Lichtleiterumsetzer handelt es sich im Endeffekt um eine Komponente, die zum selben Zweck eingesetzt wird wie der vorher beschriebene Leitungsverstärker.

4.2 Token-Ring-LANs

Abbildung 4.13
Der Einsatz eines
Leitungsverstär-
kers für Token-
Ring-LANs

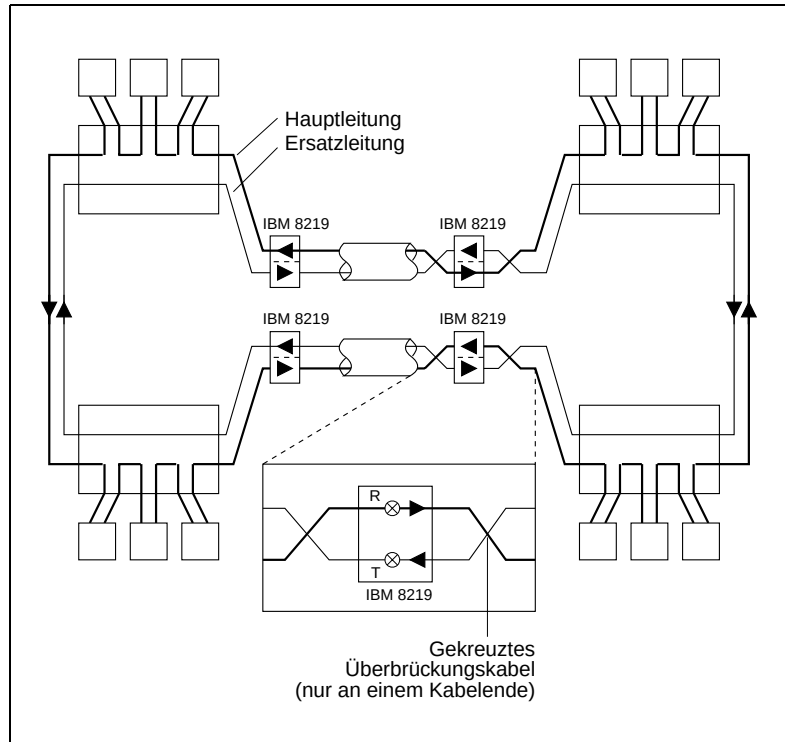


Auch diese Einheit kann als Bestandteil des 4-Mbit/s-Token-Ring-Netzwerks eingesetzt werden. Hier wird zur Inbetriebnahme ebenfalls eine eigene Stromversorgung benötigt. Damit kann man die Entfernung zwischen zwei RLVs auf bis zu 2000 Meter ausdehnen. Voraussetzung ist der Einsatz optischer Leiter zwischen zwei paarweise betriebenen Lichtleiterumsetzern. Die angegebene Maximalentfernung kann nur dann erreicht werden, wenn das Kabel Typ 5 des IBM-Verkabelungssystems eingesetzt wird (Fibre Optic 100/140 Mikron). Der Lichtleiterumsetzer wandelt dabei das auf dem Kupferkabel ankommende elektrische Datensignal in ein optisches (Licht-)Signal für die Lichtleiterkabel um und führt die umgekehrte Funktion auf der anderen Seite aus. Im Gegensatz zum Leitungsverstärker wird pro Leitungsende nur ein einziges Gerät benötigt.

In Abbildung 4.14 ist ein Konfigurationsbeispiel gezeigt, mit dem eine maximale Entfernung von 2000 Metern überbrückt werden kann. Da der Lichtleiterumsetzer in der Lage ist, sowohl die Hauptleitung als auch die Ersatzleitung umzusetzen, ist lediglich ein Paar Lichtleiterumsetzer pro Kabelstrang notwendig.

4 Netzwerkaufbau und Netzwerktopologien

Abbildung 4.14
Der Einsatz von
Lichtleiterumset-
zern in Token-
Ring-LANs



Hierbei ist jedoch zu beachten, daß am Übergang zu den RLVs an einem Ende ein normales, am anderen Ende hingegen ein gekreuztes Überbrückungskabel verwendet werden muß.

Wir wollen im nächsten Abschnitt die Möglichkeiten des 16-Mbit/s-Token-Rings, die technischen Komponenten und die strategischen Aspekte etwas genauer betrachten.

IBMs 16-Mbit/s-Token-Ring

Mit dieser Produktvariante können Token-Ring-Systeme aufgebaut werden, die mit einer Geschwindigkeit von 16 Mbit/s arbeiten. Somit steht eine wesentlich höhere Übertragungsgeschwindigkeit und Übertragungskapazität zur Verfügung. Wenn es um den neuen Aufbau von LANs unter einem Token-Ring geht, sollte man sich ausschließlich für diese Technik entscheiden. Es gibt jedoch noch genügend ältere Installationen, die mit 4 Mbit/s betrieben und erweitert werden müssen. Deshalb bieten neue Token-Ring-Karten die Möglichkeit, zwischen 4 und 16 Mbit/s umstellen zu können.

4.2 Token-Ring-LANs

Für den 16-Mbit/s-Token-Ring sind zusätzliche Performance-Verbesserungen dank der Erweiterung der Token-Ring-Architektur ermöglicht worden. Mit Hilfe einer sogenannten Early-Token-Release-Funktion, auf die wir später noch genauer eingehen wollen, kann der Durchsatz im Netz erheblich verbessert werden. Die neue Early-Token-Release-Funktion stellt übrigens eine Erweiterung des internationalen Standards IEEE 802.5 für 16-Mbit/s-Token-Ring-Netze dar. Für das 16-Mbit/s-Token-Ring-Netz wurde auch ein neuer Token-Ring-Lichtleiterumsetzer vorgestellt, der sowohl Übertragungsraten von 4 Mbit/s als auch 16 Mbit/s auf optischen Leitern unterstützt. Dieser Lichtleiterumsetzer wird als IBM 8220 bezeichnet und stellt eine intelligente Komponente dar. In Fehlerfällen kann dieser Umsetzer automatisch auf den Ersatzring umschalten. Damit wird eine hohe Zuverlässigkeit in Token-Ring-Netzen erreicht.

Für den Anschluß von Arbeitsplatzgeräten (PCs, ATs, PS/2-Modelle) werden neue Adapterkarten angeboten, die wahlweise mit 4 oder 16 Mbit/s betrieben werden können. Auch für eine Vielzahl von Steuereinheiten und Prozessoren der IBM-Host-Welt stehen neue Karten zur Verfügung, die auch wahlweise mit 4 oder 16 Mbit/s arbeiten können (direkte Einbindung von Host-Systemen, MDT in Token-Ring-Netze).

Das neue 16-Mbit/s-Token-Ring-Netz zeichnet sich insbesondere dadurch aus, daß die Kapazität des Netzes auch im Lastbereich noch sehr gute Ergebnisse liefert. Somit ist es denkbar, Netzstrukturen aufzubauen, die es erlauben, den steigenden Anforderungen bezüglich Übertragungskapazität im *Inhouse*-Bereich mehr als gerecht zu werden. Mit der vermehrten Einführung von Grafikanwendungen, CAD/CAM, Übertragung von Programmen, verteilten Datenbanken und dergleichen mehr sind Netzwerke erforderlich, die sehr hohe Datenraten aufweisen. Folgende Einsatzkriterien für das 16-Mbit/s-Token-Ring-Netz sind denkbar:

- In vielen Fällen war es so, daß 16-Mbit/s-Token-Ring-Netze als Backbone-Ringe aufgebaut werden. Ein Backbone-Ring ist im allgemeinen dadurch gekennzeichnet, daß an ihn keine Arbeitsplatzrechner angeschlossen sind, sondern nur Bridge-Rechner oder Gateways zu Großrechnersystemen oder Minicomputern. Dieser Einsatz ist vor allem dann sinnvoll, wenn ein bislang stark belastetes Einzelringsystem in mehrere Ringe aufgeteilt werden soll, die wiederum ihre gemeinsame Kommunikation und die Kommunikation mit dem Host über ein Backbone-Netz abwickeln können. Da jedoch vom Backbone immer mehr Leistung gefordert wird, setzt man inzwischen im Backbone wesentlich höhere Übertragungsgeschwindigkeiten ein.

4 Netzwerkaufbau und Netzwerktopologien

- Bei Backbone-Ringen ist es auch denkbar, Doppelringe herzustellen, die über Bridges miteinander verbunden sind. Dadurch erhöht sich nicht nur der Durchsatz, es können durch die Funktion der Lastverteilung auch extrem hohe Zuverlässigkeiten erzielt werden. Dies ist vor allem dann von großem Interesse, wenn sich Backbone-Netze über ein weites Firmenareal erstrecken.
- Es spricht aber nichts dagegen, auch Arbeitsplatzrechner an ein 16-Mbit/s-Token-Ring-Netz anzuschließen. Es kann entweder ein eigenes 16-Mbit/s-Token-Ring-Netz aufgebaut werden, oder spezielle Arbeitsplätze werden direkt mit dem 16-Mbit/s-Backbone verbunden. Man könnte sich zum Beispiel vorstellen, daß ein Server mit einer bestimmten Funktion, die für alle verfügbar sein soll, mit diesem Backbone-Netz verbunden wird.
- Als Gateway werden die Rechner oder Komponenten in einem Netz bezeichnet, die die Verbindung vom LAN zum Host oder Minicomputer herstellen. Da mit diesem Gateway unter Umständen sehr viele Anwender gleichzeitig arbeiten, ist es nicht notwendig, daß der Gateway-Rechner selbst eine entsprechende Kapazität aufweist, sondern es reicht aus, wenn er mit hohen Übertragungsgeschwindigkeiten die Daten weitergeben kann.

Die 16-Mbit/s-Adapterkarten können wahlweise mit 16 Mbit/s oder 4 Mbit/s Übertragungsgeschwindigkeit betrieben werden. Es kann somit aus Kompatibilitätsgründen zunächst mit anderen 4-Mbit/s-Karten gearbeitet werden und später, wenn alle 4-Mbit/s-Karten ersetzt werden sollen, die 16-Mbit/s-Karte, die bisher mit 4-Mbit/s betrieben worden ist, auf die höhere Geschwindigkeit umgestellt werden. Der Übergang auf eine andere Geschwindigkeit kann im Bedarfsfall durch einen Jumper oder Schalter auf der Karte oder bei den PS/2-Modellen über das System Setup erfolgen; bei anderen Herstellern ist es auch denkbar, dies über eine Generierungsoption in der Software oder im Mikrocode durchzuführen.

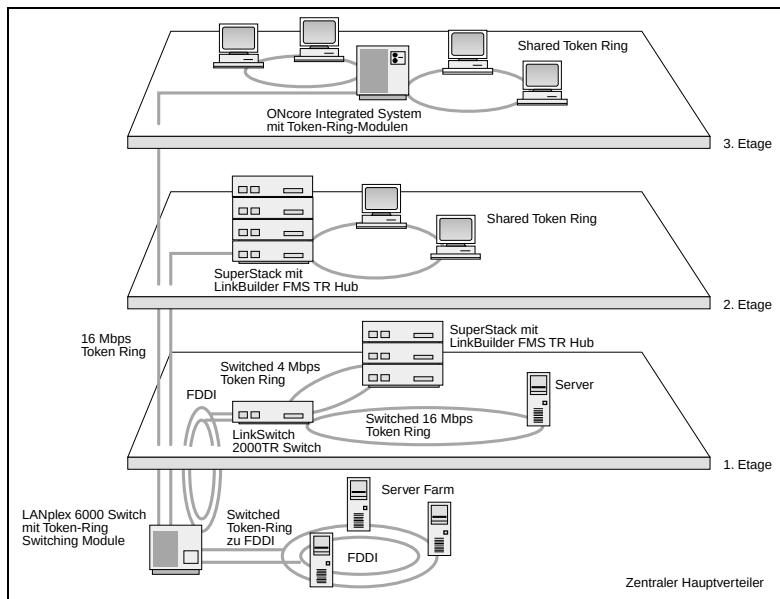
Auch der Einsatz des 16-Mbit/s-Token-Rings von IBM basiert auf dem Einsatz des IBM-Verkabelungssystems. Wir haben uns bereits bei der Behandlung des 4-Mbit/s-Token-Rings mit der Frage beschäftigt, welche Längenrestriktionen im Einzelfall zu beachten sind. Die gleiche Frage wollen wir uns nun für den 16-Mbit/s-Token-Ring stellen.

Der Betrieb des Token-Ring-Netzes mit 16 Mbit/s sieht nach wie vor den Einsatz des IBM-Verkabelungssystems vor. Wegen der stark erhöhten Übertragungsfrequenz bei 16 Mbit/s gegenüber 4 Mbit/s sind jedoch einige Einschränkungen zu beachten.

4.2 Token-Ring-LANs

Die bei der Einführung des IBM-Verkabelungssystems für das IBM-Token-Ring-Netz getroffenen Empfehlungen hinsichtlich der Leitungsentfernung zwischen Arbeitsplatzgerät und Verteilerraum von 100 Metern gelten auch bei 16-Mbit/s-Netzwerken. Damit sind die getätigten Investitionen eines bereits installierten Token-Ring-Netzes hinsichtlich dieser Verkabelung gesichert. Unter Berücksichtigung der oben genannten technischen Gegebenheiten muß allerdings beim Übergang auf die höhere Übertragungsgeschwindigkeit eine Reduktion der maximal anschließbaren Komponenten bei der Beibehaltung einer bestimmten Kabellänge in Kauf genommen werden. Dies bedeutet im Fall eines einzigen Verteilerraums und Anschlußkabellängen von 100 Metern die maximale Ausbaufähigkeit des Systems auf acht Ringleitungsverteiler und damit 96 Endgeräte. Sofern die Anschlußlängen geringer sind, können auch mehr als 96 Endgeräte an diesem Token-Ring angeschlossen werden. Die Daten hierfür sind den entsprechenden Tabellen des Installationshandbuchs für das IBM-Verkabelungssystem zu entnehmen.

Abbildung 4.15
Ein Konfigurationsbeispiel für durch Hub-Systeme aufgebaute LANs



Die Ringleitungsverteiler der neuen Generation sind nicht mehr in passiver Form, sondern als aktive Komponenten konzipiert. Damit sind auch vielfältige Möglichkeiten bezüglich Netzwerkmanagement verbunden. Eine Überwachung und Steuerung dieser Netzwerkkomponenten wird wesentlich einfacher. Kleine und große Netzwerke lassen sich dadurch optimal steuern. Neben dem Einsatz einzelner

4 Netzwerkaufbau und Netzwerktopologien

Ringleitungsverteiler sind im Zuge der Hub-Technologie Ringleitungsverteiler in Form von Einschubmodulen zu berücksichtigen. In Abhängigkeit von der Netzwerkgröße erfolgt der Aufbau eines Netzwerks entweder mit kleinen externen Ringleitungsverteilern oder mit Hilfe der leistungsfähigen Hub-Technologie. Hub-Systeme haben den großen Vorteil, daß damit nicht nur ein Netzwerktyp eingesetzt werden kann, sondern über unterschiedliche Einschubmodule und Einschubkoppellemente Token-Ring-Netzwerke, Ethernet-Netzwerke oder FDDI-Netzwerke aufgebaut werden können. In Abbildung 4.15 ist dargestellt, wie ein größeres komplexes Netzwerk mit Hilfe von Hub-Systemen aufgebaut werden könnte. Dabei ist sehr schön zu sehen, daß ein Hub in der Lage ist, unterschiedliche Netzwerke zu unterstützen und zu verbinden.

Early Token Release

Das Prinzip des Early Token Release ist eine Erweiterung der Token-Ring-Architektur für 16-Mbit/s-Token-Ring-Netze. Es ist im IEEE-802.5-Standard verankert. Von dieser Betriebsweise kann im 16-Mbit/s-Token-Ring-Netz wahlweise Gebrauch gemacht werden. Bei der 4-Mbit/s-Token-Ring-Architektur würde aus einem rotierenden Token ein Frame, sobald das Token von der Station, die Daten sendet, mit Adreßinformation versehen und ein Datensatz samt Nachsatz (Trailer) angefügt wird. Die den Frame erzeugende Station ist im Normalfall als einzige berechtigt, einen neuen Token zu erzeugen.

Dies geschieht jedoch nicht vor Erhalt des letzten Zeichens des Nachsatzes, der erfolgt, nachdem dieser Frame den Ring einmal umkreist hat.

Betrachtet man diese Technik genauer, dann läßt sich erkennen, daß bei hohen Übertragungsgeschwindigkeiten und großer Netzlänge oder im Falle von kurzen Nachrichten die Ausnutzung des Rings nicht sehr effektiv ist. Sogenannte Idle-Zeichen belegen den Ring, während andere Stationen auf ein Frei-Token warten müssen, um Daten übertragen zu können. Die neue Funktion des Early Token Release vermeidet dieses Problem und erlaubt auch bei hoher Geschwindigkeit, großer Netzlänge und relativ kurzen Nachrichten eine wesentlich bessere Ausnutzung des Rings.

Die Funktionsweise des Early Token Release ist jedoch nicht neu. Bereits vor vielen Jahren hat die Firma Proteon ein ProNET10 (10 Mbit/s) und ein ProNET80 (80 Mbit/s) auf den Markt gebracht und damals schon die Methode implementiert. Im Vergleich zum 4-Mbit/s-Token-Ring besteht die Möglichkeit, daß mehrere Datenblöcke zur gleichen Zeit auf dem Ring vorhanden sind. Das Token

4.2 Token-Ring-LANs

wird somit nicht festgehalten, bis die Daten beim Absender wieder eingetroffen sind, sondern es wird an die Daten angehängt. Es kennzeichnet das Ende des Frames. Jede Station, die das Token sieht, weiß somit, daß hier die Daten zu Ende sind, und kann eigene Daten an dieser Stelle hinzufügen. Die Quittierung des Datenempfangs erfolgt durch das Setzen einer Marke. Diese Marke wird beim Absender ausgelesen. Wird die Übertragung als erfolgreich erkannt, nimmt dieser die Daten aus dem Ring.

Dieses Verfahren bringt jedoch nur bei großen Ringen mit hoher Übertragungsgeschwindigkeit einen spürbaren und meßbaren Vorteil. In allen anderen Fällen ist die Idle-Zeit des Token-Rings so kurz, daß das genannte Verfahren keinen Performance-Gewinn bringt. Verdeutlicht werden kann die Situation, wenn man sich vor Augen hält, daß in einem 4-Mbit/s-Token-Ring ein 250 Byte langer Datensatz auf dem Token-Ring eine Länge von nicht weniger als 100 km aufweist. Bei einem 5 km langen Token-Ring bedeutet dies, daß im ungünstigsten Falle nur 2,5% der möglichen Kapazität ungenutzt bleiben, da auf das Token gewartet werden muß. Beim 16-Mbit/s-Token-Ring und einer Länge von 25 km läßt sich hingegen unter Verwendung des Early-Token-Release-Verfahrens bei einer Übertragung von 250 Byte langen Datensätzen eine fast fünfzigprozentige Steigerung des Durchsatzes erzielen.

Das Early-Token-Release-Verfahren darf nicht mit einem Mehr-Token-Verfahren verwechselt werden. Dieses Mehr-Token-Verfahren wird bei noch schnelleren Netzen auf Token-Ring-Basis eingesetzt. Beim Early-Token-Release-Verfahren befindet sich zwar nach wie vor nur ein Token auf der Leitung, aber dafür mehrere Frames gleichzeitig.

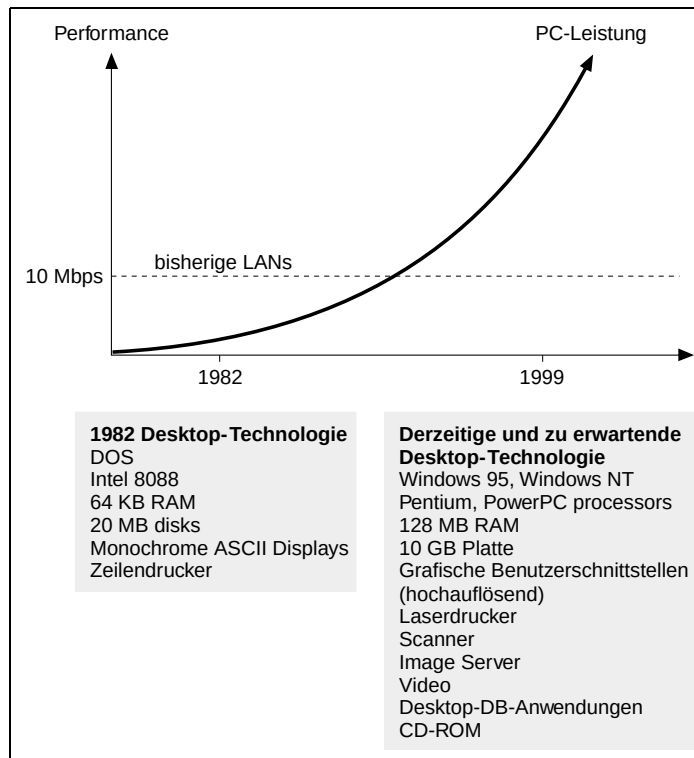
In einem späteren Kapitel werde ich noch auf neue Techniken eingehen, die es erlauben, Token-Ring-Netze und dazugehörige Netzwerkmanagement-Funktionen zu installieren. Es wird auch um eine Integration von Ethernet, Token-Ring, FDDI oder ATM gehen. Als Schlagwort sei hier nur die Hub-Technologie genannt.

Wenn ein Netzwerk installiert worden ist, kann man davon ausgehen, daß immer wieder neue PCs hinzugefügt werden sollen. Zumindest steigen die Anforderungen an das Netzwerk. Da die Leistungsfähigkeit der PCs und die Software, die eingesetzt wird, größer wird, wird auch die Anforderung an das LAN größer. Anwendungen, die bislang nur auf Host-Systemen implementiert worden sind, werden inzwischen auf PCs eingesetzt, da Pentium-Prozessoren in Verbindung mit LANs und neuen externen Speichermedien in der Lage sind, diese sogenannten Mission-Critical-Applikationen problemlos einzusetzen. In Abbildung 4.16 ist dargestellt, welche Anforderungen zukünftig an PCs, LANs und die eingesetzten Anwendungen ge-

4 Netzwerkaufbau und Netzwerktopologien

stellt werden. Langfristig gesehen werden Übertragungsraten von 10 Mbit/s bzw. 16 Mbit/s nicht mehr reichen. Für bestimmte Anwendungsgebiete werden High-Speed-LANs benötigt.

Abbildung 4.16
Steigende Anforderungen an Endgeräte und LAN-Technik



Um auch dieser Forderung gerecht werden zu können, begann man vor einigen Jahren, 100-Mbit/s-LANs auch für den normalen LAN-Bereich zu entwickeln. Hochgeschwindigkeit war bis dahin eine Domäne des Backbone-Bereichs. Aufgrund der preisgünstigen Entwicklungen kann man sich hohe Geschwindigkeiten auch bis zum Arbeitsplatz leisten. Die nachfolgenden Ausführungen sollen zeigen, welche Möglichkeiten hierfür derzeit geboten werden, wie diese High-Speed-LANs aufgebaut sind und wie sie arbeiten.

Zu beachten ist, daß es sich hierbei zum einen um neue Techniken handelt (ATM bzw. die alte FDDI-Technologie) und zum anderen um Weiterentwicklungen im Ethernet-Bereich (Fast Ethernet bzw. Gigabit Ethernet). Somit können auch für den Netzwerkananschluß von herkömmlichen Arbeitsplatzrechnern schnelle und preiswerte Fast Ethernet-Anschlüsse zur Verfügung gestellt werden. Die Token-Ring-Entwicklung, so scheint es, hat sich auf der 16-Mbit/s-Technologie

4.3 Fast Ethernet LANs

ausgeruht und hat die neu entstandenen Anforderungen »verschlafen«. Zum Zeitpunkt der Erstellung dieses Buches gab es erkennbare Entwicklungstendenzen für einen 100 Mbit/s-High-Speed-Token-Ring (HSTR), jedoch noch keine große Auswahl am Markt verfügbarer Produkte. Es ist auch bis jetzt nicht erkennbar, wie sich diese Entwicklung am Markt durchsetzen wird. Ein wesentlich größeres Problem dürfte die Tatsache darstellen, daß die herkömmlichen Token-Ring-Produkte immer noch um 25% bis 50% teurer sind als Ethernet-Komponenten. Die ersten Herstelleraussagen für den HSTR besagen, daß diese Komponenten um etwa 25% teurer sein sollen, als die jetzigen Token-Ring-Produkte. Wenn sich daran nichts ändern sollte, dann ist bereits jetzt zu erkennen, daß HSTR nicht den Durchbruch erleben wird. Zudem sind in vielen Fällen Tendenzen zu erkennen, daß Netzwerkkomponenten zuerst für den größeren und preiswerteren Ethernet-Markt verfügbar sind statt für Token-Ring.

4.3 Fast Ethernet LANs

Die Entwicklungsgeschichte von Ethernet begann 1973 im Palo Alto Research Center (PARC) von Xerox. Seit dieser Zeit wurden unterschiedliche Versionen standardisiert. Die Versionen 1.0 und 2.0 von DEC, Intel und Xerox (DIX) aus den Jahren 1980 bzw. 1982 waren die ersten Versionen. Später wurde Ethernet vom IEEE (Institute of Electrical and Electronic Engineers) und vom ANSI (American National Standards Institute) dem »Standard 802.3 Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications« angepaßt.

Die internationale Anerkennung erfolgte 1989 durch die International Organization for Standards and International Electrotechnical Commission und den ISO/IEC-8802-3-Standard.

Aufgrund dieser Standards konnten in kurzer Zeit durch eine Vielzahl von Herstellern kompatible Ethernet-Produkte verfügbar gemacht werden. Beim Ethernet-Standard handelt es sich wie gesagt um ein 10-Mbit/s-Netzwerk. Ursprünglich als 10Base5 durch das IEEE-802.3-Komitee bezeichnet, wurde daraus eine neue Spezifikation entwickelt: 10Base2, das nicht mehr Thick-Ethernet-, sondern Thin-Ethernet-Kabel zum Aufbau eines LANs verwendet. Die letzte Anpassung bekam die Bezeichnung 10Base-T – ein Verweis darauf, daß Ethernet auf einer Twisted-Pair-Verkabelung eingesetzt wird.

Ethernet=
CSMA/CD

Alle bisherigen Ethernet-Entwicklungen haben daran nichts geändert. Das heißt, sämtliche 802.3-Standards (10Base5, 10Base2, 10Broad36, 10Base-F, 10Base-T) verwenden die gleiche CSMA/CD-Spezifikation.

4 Netzwerkaufbau und Netzwerktopologien

Was ist Fast Ethernet?

Fast Ethernet bietet die zehnfache Geschwindigkeit gegenüber dem herkömmlichen Ethernet, d.h., statt mit 10 Mbit/s arbeitet Fast Ethernet mit einer Übertragungsgeschwindigkeit von 100 Mbit/s. Ebenso wie 10Base-T wird Fast Ethernet über eine Twisted-Pair-Verkabelung betrieben. Somit wird eine sternförmige Verkabelung benötigt. Wichtigstes Merkmal für Fast Ethernet ist, daß nach wie vor das CSMA/CD-Zugriffsverfahren eingesetzt wird.

Fast Ethernet ist Ethernet

Ethernet oder IEEE 802.3 definiert ein Kommunikationsprotokoll, das prinzipiell in zwei Teile gegliedert ist. Zum einen gibt es die Definition der MAC-Ebene (Media Access Control Layer), in der sowohl das Format der Informationen für die Datenübertragung festgelegt wird als auch die Frage, wie der Zugang zum Netz gesteuert wird. Der Ethernet MAC Layer ist CSMA/CD (Carrier Sense Multiple Access with Collision Detection). Auf der zweiten Ebene des Ethernet-Protokolls – dem Physical Layer – wird die Kommunikation zwischen der Verkabelung und der MAC-Ebene geregelt.

Obwohl derzeit nicht jeder Arbeitsplatz 100 Mbit/s Übertragungsgeschwindigkeit benötigt, ist doch eine steigende Tendenz zu beobachten, vor allem bei Netzwerkneuplanungen, sich gleich in Richtung High-Speed-LAN zu bewegen. Aufgrund der Einfachheit von Fast Ethernet wird einem nicht nur der Neueinstieg in diese Technik, sondern auch eine Umstellung von 10-Mbit/s-Ethernet auf Fast Ethernet erleichtert.

Die Frage ist dabei nur noch, ob man Fast Ethernet, CDDI, ATM oder gar 100VG-AnyLAN verwenden soll. Die Vorteile von Fast Ethernet sind unter anderem:

- Hohe Übertragungsgeschwindigkeit
- Standardisierte Technik (mit jahrelanger Erfahrung)
- Kostengünstige Migration mit maximalem Einsatz bestehenden Equipments, Verkabelungsstrukturen, Netzwerkmanagementsystemen
- Unterstützung durch alle führenden Hersteller auf allen Gebieten der Netzwerkprodukte
- Optimale Ressourcennutzung

Die oben aufgeführten Optionen sollen etwas näher betrachtet werden, damit Sie einen besseren Eindruck von der Leistungsfähigkeit von Fast Ethernet erhalten.

Hohe Übertragungsgeschwindigkeit

Einer der maßgeblichen Gründe für den Einsatz von Fast Ethernet in Abteilungsnetzen (Workgroups) besteht in der Möglichkeit, durch Fast Ethernet die kurzfristigen Anforderungen nur weniger Anwen-

4.3 Fast Ethernet LANs

der bzw. die immer größer werdenden Datenmengen im LAN (durch schnelle PCs und leistungsfähige Anwendungen) optimal zu bedienen. Immer häufiger werden neben herkömmlicher Datenverarbeitung (Text, Tabellen etc.) umfangreiche Datenmengen über das Netzwerk transportiert (grafische Datenverarbeitung, 3D-Grafiken, Animation, Bewegtbildübertragung etc.). Problematisch ist, daß eine große Leistungsfähigkeit des LAN nicht kontinuierlich benötigt wird. Das heißt, das High-Speed-LAN muß in der Lage sein, den sogenannten Burst im Netz abwickeln zu können. Dabei kann es zu Kollisionen kommen, die unter Umständen Performance-Verbesserungen wieder kaputtmachen. Zudem kann man davon ausgehen, daß Fast Ethernet ebenso wie 100VGAny-LAN nur Übergangslösungen sind. Spätestens wenn ATM standardisiert ist und »preisgünstig« eingesetzt werden kann, sollten diese beiden Produktbereiche an Bedeutung verlieren.

Standardisierte Technik

Fast Ethernet ist eine konsequente Weiterentwicklung von 10Base-T. Daher behält man als Zugriffsverfahren CSMA/CD, so wie es in dem Ethernet MAC Layer spezifiziert ist. Man kann deshalb auch sagen, Fast Ethernet oder 100Base-T ist herkömmliche 10Base-T-Technik, nur zehnmal schneller. Deshalb sind auch die Kollisionen, die bei diesem Verfahren auftreten, bezogen auf die Gesamtlast des Netzwerks, zu berücksichtigen. Man könnte somit behaupten, das LAN ist nicht nur zehnmal schneller als bisher, auch die Kollisionen treten zehnmal häufiger auf als vorher. Von Vorteil ist in jedem Fall, daß die Entwicklung von Hubs, Ethernet-Karten oder anderen Fast-Ethernet-Komponenten relativ wenig Schwierigkeiten bereitet, da Fast Ethernet auf der bewährten Technik aufbaut.

Kostengünstige Migration

Da die 100Base-T-Technologie sich gegenüber der 10Base-T-Technologie kaum verändert hat, kann 100Base-T einfach und schnell in eine bestehende 10Base-T-Umgebung eingeführt werden. Eine Migration kann auf den folgenden Gebieten einfach und wirtschaftlich durchgeführt werden:

Netzwerk- verkabelung

Durch die 100Base-T-Media-Spezifikation (100Base-TX, 100Base-T4 und 100Base-FX) kann Fast Ethernet auf allen Twisted-Pair-Verkabelungen der Kategorie 3, 4 oder 5 (UTP), Shielded Twisted-Pair (STP) und LWL-Kabeln eingesetzt werden.

Administrative Vorteile

Netzwerkverwalter können in der Regel bestehende Analyse-Tools weiter verwenden und müssen sich auf keine neuen Protokolle oder Verkabelungsvorschriften umstellen.

4 Netzwerkaufbau und Netzwerktopologien

Management-Software	Fast-Ethernet-LANs können mit bestehenden SNMP-basierten Netzwerkmanagement-Systemen und den für Fast Ethernet verfügbaren MIBs (Management Information Base) überwacht werden.
Software-Unterstützung	Bestehende Anwendungen und Netzwerksoftware laufen ohne Änderungen auf Basis von Fast Ethernet.
Flexible Migration	Die neu entwickelten 10/100-Dual-Speed-Autosensing-Netzwerkadapter können in einer 10Base-T und 100Base-T-Umgebung eingesetzt werden, ohne daß an der Netzwerkkarte eine Einstellung durchgeführt werden müßte. Somit kann beim kurzfristigen Mischbetrieb kein Fehler auftreten. Ebenso wird durch den Einsatz von 10-100-Mbit/s-Ethernet-Switching-Hubs eine sanfte Migration auf 100Base-T unterstützt und erleichtert.

Unterstützung durch führende Hersteller

Jeder führende Hersteller von Ethernet-Komponenten unterstützt heute auch 100Base-T. Mehr als 80 führende Hersteller für Netzwerkadapter, Hubs, Switches, Workstations und andere Komponenten stellen passende Produkte zur Verfügung. Hierzu zählen unter anderem Firmen wie Intel, 3Com, Sun Microsystems, SMC, Cabletron, Cisco oder auch Nortel Networks. Die meisten dieser Hersteller sind Mitglied der Fast Ethernet Alliance (FEA), ein Zusammenschluß von Firmen, die den Einsatz von Fast Ethernet forcieren und die Interoperabilität von Fast Ethernet gewährleisten. Hierzu werden von der FEA Standardtestprogramme entwickelt.

Optimale Ressourcennutzung

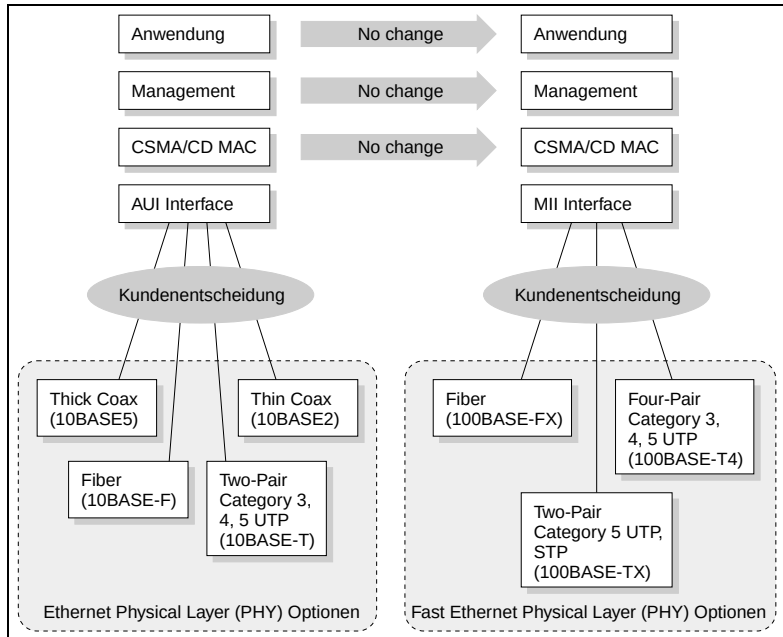
Da die Standards für Fast Ethernet vollständig existieren und Produkte hierfür von einer Vielzahl von Firmen angeboten werden, bietet Fast Ethernet ein günstiges Preis-Leistungs-Verhältnis. Für die zehnfache Performance muß man derzeit weniger als die doppelten Kosten im Vergleich zu 10Base-T kalkulieren. Und die Preise für Fast-Ethernet-Komponenten werden ständig nach unten korrigiert: In einigen Jahren dürften sie für Fast Ethernet den Stand erreicht haben, der heute für herkömmliche Ethernet-Komponenten bezahlt werden muß.

4.3.1 Die Technologie hinter Fast Ethernet

Es wurde bereits erwähnt, daß 100Base-T im Prinzip eine Erweiterung von 10Base-T ist. Abbildung 4.17 zeigt, wo die Unterschiede zu finden sind.

4.3 Fast Ethernet LANs

Abbildung 4.17
Kompatibilität
zwischen Ethernet
und Fast Ethernet



Es ist zu erkennen, daß Fast Ethernet die bestehende 802.3-MAC-Ebene verwendet und über die MII-Schnittstelle die Verbindung zu einer der drei möglichen PHY-Komponenten herstellt. Die MII-Spezifikation ist ähnlich der AUI-Schnittstelle. Fast Ethernet unterstützt drei Kabelspezifikationen: 100Base-TX, 100Base-T4 und 100Base-FX. Der 100Base-T-Standard legt ebenfalls den Aufbau von 100Base-T-Repeater und Managementschnittstellen fest. Beim Aufbau des Fast Ethernet MAC reduzierte IEEE die Bitzeit – also die Dauer der Bitübertragung – dem 10-Mbit/s-CSMA/CD-MAC-Layer um den Faktor 10, um damit eine zehnfach höhere Geschwindigkeit zu erreichen. Da die Ethernet-MAC-Spezifikation bereits geschwindigkeitsunabhängig ist, ergibt sich keine Änderung in der Funktionalität. Somit sind Paketformat, Paketlänge, Error Control und Managementinformation identisch mit dem 10Base-T-Standard.

Nachfolgend ist aufgeführt, welche Parameterwerte für Fast Ethernet definiert sein müssen. Dabei fällt auf, daß es sich um die gleichen Spezifikationen handelt, die man auch für eine Standard-Ethernet-Spezifikation vorfindet.

4 Netzwerkaufbau und Netzwerktopologien

Parameter	Wert
SlotTime	512 bit-times
InterFrameGap	960 ns
AttemptLimit	16
BackoffLimit	10
JamSize	32 bits
MaxFrameSize	1518 octets
MinFrameSize	512 bits (64 octets)
AddressSize	48 bits

Alternativen der Verkabelung

Für Fast Ethernet sind drei unterschiedliche Physical Layers definiert:

- 100Base-TX, für 2-paarige Verkabelung (EIA 568 Category 5) UTP- und STP-Kabel
- 100Base-T4, für eine 4-paarige Verkabelung (Category 3, 4 oder 5) UTP-Kabel
- 100Base-FX, für eine Verkabelung auf Basis von LWL-Kabel

Aufgrund dieser drei vorhandenen Spezifikationen ist man mit Fast Ethernet flexibel genug, um so ziemlich in jeder Umgebung passende Kabel zu finden bzw. zu verwenden, vor allem dann, wenn man von einer bestehenden 10Base-T-Verkabelung auf Fast Ethernet umstellen will. Auf diese Weise bleibt die bereits getätigte Investition geschützt, und man kann dennoch auf High-Speed-LANs umsteigen. Durch den geeigneten Einsatz von aktiven Fast-Ethernet-Komponenten (Hub-System) kann eine Mischung von 100Base-TX, 100Base-T4 und 100Base-FX durchgeführt werden, so wie man dies bereits mit herkömmlichen Ethernet-Komponenten und passenden Repeatern realisieren konnte.

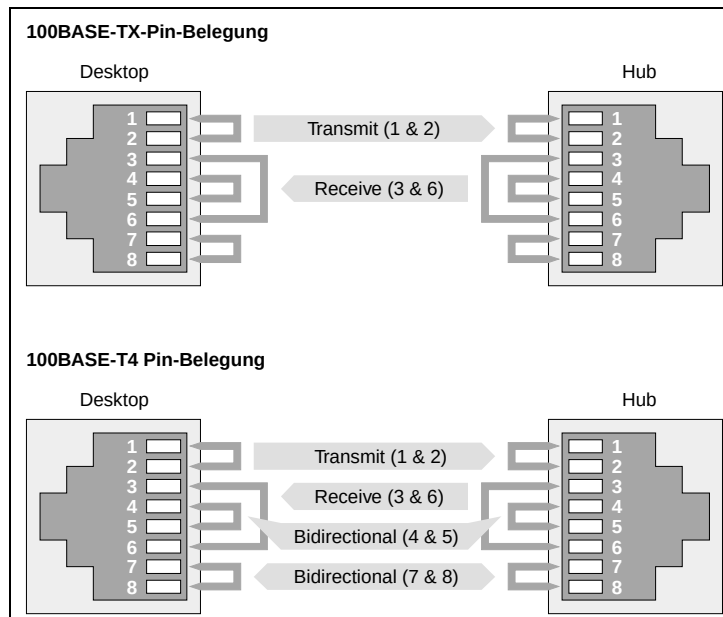
Die 100Base-TX-Entwicklung basiert auf der FDDI/CDDI-Physical-Media-Dependent-Spezifikation (PDM), entwickelt und anerkannt durch das American National Standards Institute (ANSI) X3T9.5. Für den Ethernet MAC Layer stehen somit die gleichen Transceiver und PHY-Chips zur Verfügung, die bereits für FDDI und CDDI entwickelt worden sind. Da diese Chips im großen Umfang verfügbar sind, haben bereits die ersten Fast-Ethernet-Produkte 100Base-TX unterstützt. Dadurch kann 100Base-TX auf 2-paarigen UTP-CAT-5-Kabeln eingesetzt werden, eine Installationsbasis, die bereits in einer Vielzahl von installierten Netzwerken vorzufinden ist.

Die 100Base-T4-Technik wurde entwickelt, um Fast Ethernet auch über CAT-3-UTP-Verkabelungen einsetzen zu können. Dieser Kabel-

4.3 Fast Ethernet LANs

typ ist in älteren Twisted-Pair-Verkabelungen vorzufinden. Zu beachten ist nur, daß eine 4-paarige UTP-CAT-3-, -4- oder -5-Verkabelung benötigt wird. In Abbildung 4.18 ist dargestellt, wie die Pinbelegung für 100Base-TX und 100Base-T4 aussehen muß. Dabei ist eindeutig festzustellen, daß in beiden Fällen die Standard-Paarbelegung 1/2 und 3/6 verwendet wird. Zusätzlich nutzt 100Base-T4 die zwei weiteren Paare 4/5 und 7/8 zur Datenübertragung.

Abbildung 4.18
Pinbelegung für
100Base-TX- und
100Base-T4-Netz-
werke



10/100 Auto-Negotiation

Um eine Umstellung von bestehenden 10-Mbit/s-Netzwerken auf Fast Ethernet mit 100 Mbit/s zu erleichtern, beinhaltet der 100Base-T-Standard einen Mechanismus zur automatischen Erkennung der Netzwerkgeschwindigkeit, den sogenannten Auto-Negotiation-Vorgang, auch als NWay bezeichnet.

Diese optionale Funktion ermöglicht es einem Netzwerkadapter oder Switch, sowohl mit 10Base-T- als auch mit 100Base-T-Übertragungsgeschwindigkeiten zu arbeiten, ohne daß der Anwender etwas einstellen muß. Das heißt, die Netzwerkkarte erkennt, ob es sich um ein Fast-Ethernet-Netzwerk handelt, bzw. der Hub erkennt, ob am Anschlußport beispielsweise eine 10-Mbit/s-Netzwerkkarte angebunden ist. Damit wird die optimal mögliche Geschwindigkeit eingesetzt und verwendet.

4 Netzwerkaufbau und Netzwerktopologien

Der Auto-Negotiation-Mechanismus kann nur in Dual-Funktions-Karten verfügbar gemacht werden. Dies ist daran zu erkennen, daß die Karten immer in der Form 10/100 ausgewiesen werden.

Inzwischen gibt es auch 10/100 Auto-Negotiation für Concentrator bzw. Hub-Systeme. Wenn man dann noch 10/100 Auto-Negotiation für die Netzwerkadapter verwendet, dann sollte dieser Mechanismus nur auf der Netzwerkadapterkarte oder nur am Port des Hub bzw. Concentrator verwendet werden. Ist Auto-Negotiation für beide Anschlüsse eingestellt, dann weiß keiner der Komponenten, welche Geschwindigkeit genutzt werden soll, da keine Referenzgeschwindigkeit vorliegt. Dies ist in etwa so, als würden zwei freundliche Menschen vor einem Eingang stehen, und jeder versucht dem anderen den Vortritt zu lassen. In diesem Fall müssen beide Personen jämmerlich vor dem Eingang verhungern, da keiner von beiden als erster durch den Eingang gehen wird.

4.3.2

Base-T-Regeln zum Topologieaufbau

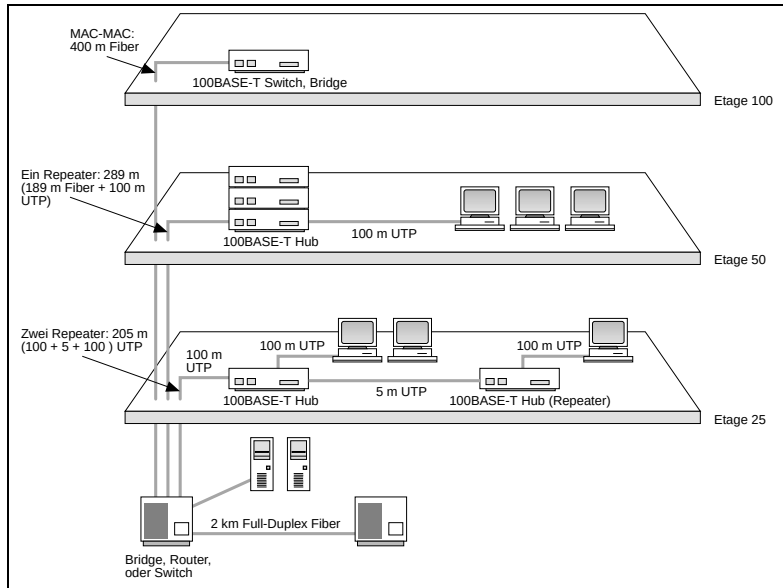
Wie bei allen Twisted-Pair-Verkabelungen muß auch für 100Base-T die 100-Meter Regel für den Anschluß von Endgeräten an einen Hub eingehalten werden (s. Kapitel 5: Netzwerkkonzeption). Im Vergleich zum herkömmlichen 10Base-T-Standard unterscheiden sich die restlichen Regeln für Entfernungsfestlegungen in einem 100Base-T-Netzwerk zum Teil grundlegend wegen der höheren Geschwindigkeit (100 Mbit/s statt 10 Mbit/s).

Beim Aufbau von 100Base-T-Netzwerken dürfen zwischen Sendestation und Empfängerstation maximal zwei Repeater auftreten, und die maximale Netzwerkausdehnung (Entfernung zwischen Sender und Empfänger) beträgt 205 Meter beim Einsatz von UTP-Kabeln und 400 Meter beim Einsatz von Glasfaserverbindungen.

Die geringere Netzwerkausdehnung ist keine so große Einschränkung (so wie dies auf den ersten Blick aussehen könnte), da bei strukturierten Verkabelungen in der Regel LWL-Verbindungen zwischen Backbone- und Etagen-Verteiler eingesetzt werden. In der nachfolgenden Abbildung 4.19 ist eine mögliche Konfiguration anhand einer Collapsed-Backbone-Struktur dargestellt. An den jeweiligen Verbindungspunkten sind zur besseren Verständlichkeit die erlaubten Kabellängen aufgeführt. Anhand dieser Angaben ist zu ersehen, daß sich mit Fast Ethernet auch größere Netzwerkstrukturen aufbauen lassen.

4.3 Fast Ethernet LANs

Abbildung 4.19
Längenrestriktion
für 100Base-T



Zusammengefaßt die wichtigsten Restriktionen:

- Die maximale Kabellänge für UTP-Kabel zwischen Endgerät und Hub beträgt 100 Meter.
- Für Verbindungen zwischen MAC-MAC (d.h. vom Switch zum Switch oder vom Endgerät zum Switch) und dem Einsatz von Halbduplex 100BaseFX ist eine maximale Länge von 400 Metern gestattet.
- In einer Single-Repeater-Topologie (ein Stackable Hub pro Verteilerebene und eine LWL-Verbindung zum Collapsed Backbone) ist eine LWL-Verbindung von 189 Metern erlaubt. Zusätzlich darf die UTP-Verbindung zwischen Hub (Stackable Hub) und Endgerät 100 Meter betragen.
- In einer 2-Repeater-Topologie darf die UTP-Kabellänge zwischen Station-Repeater-Repeater-Station nicht mehr als 205 Meter betragen.
- Daneben gibt es auch noch eine Vollduplexvariante für 100Base-FX (LWL-Verbindung), um zwei Koppelemente im Netzwerk (Switch, Bridge oder Router) über maximal zwei Kilometer lange LWL-Kabel miteinander zu verbinden.

Eine weit verbreitete Netzwerktopologie im Bereich der High-Speed-LANs, vor allem im Backbone-Bereich, bildet FDDI. Da der Einsatz von FDDI in komplexen Netzwerkumgebungen nicht wegzudenken ist, sollen der Aufbau und die Funktionsweise näher beschrieben werden.

4.4

FDDI-LANs

FDDI (Fibre Distributed Data Interface) ist mit Ausnahme einer Komponente eine von ANSI vorgeschlagene ISO-Norm und wird unter der Bezeichnung ANSI X3T9.5 geführt. Es handelt sich um einen Token-Ring mit einer Übertragungsgeschwindigkeit von 100 Mbit/s. Das FDDI-Protokoll wurde dabei speziell für eine hohe Bandbreite und für die Verwendung eines reinen Glasfasersystems entwickelt. Es gibt zwar inzwischen auch Produkte, die es erlauben, FDDI über Unshielded-Twisted-Pair-Kabel zu betreiben, aber die überbrückbaren Längenausdehnungen sind dabei wesentlich geringer als beim FDDI-Glasfasersystem.

In einem FDDI-Ring können auf einer Gesamtlänge von 100 Kilometern bis zu 500 Stationen eingebunden werden. Die Entfernung von zwei Stationen darf maximal zwei Kilometer betragen, vorausgesetzt der FDDI-Ring wird mit Glasfaserkabeln aufgebaut. Deshalb wird der FDDI-Ring nicht nur als leistungsfähiges Hochgeschwindigkeitsnetz eingesetzt, sondern in sehr vielen Fällen als Backbone-System für größere, strukturierte Verkabelungskonzepte, wenn zugleich gefordert wird, einen leistungsfähigen Backbone nutzen zu können. Für den Aufbau von FDDI-Ringen werden Glasfaserkabel des Typs 50/125 µm bzw. 62,5/125 µm verwendet.

Da inzwischen häufig diskutiert wird, diese Übertragungsgeschwindigkeit auch bis zum Endgerät zur Verfügung zu stellen, steht FDDI auch für Unshielded- und Shielded-Twisted-Pair-Verkabelungen zur Verfügung. Mittlerweile gibt es auch immer mehr Verkabelungen dieses Kabeltyps.

Zur Überbrückung von Leitungsfehlern ist FDDI so konzipiert, daß das Netzwerk aus zwei Ringen (Primär- und Sekundärring) aufgebaut ist, die beide in entgegengesetzter Richtung betrieben werden. Der Sekundärring wird in der Regel als reiner Backup-Ring betrieben. Das ANSI-Komitee schließt allerdings eine Verwendung des Sekundärrings zur Kapazitätssteigerung nicht aus. Man spricht in diesem Fall von der sogenannten Dual-MAC-Option. In diesem Buch wird uns allerdings nur die typische FDDI-Form interessieren.

Die FDDI-Topologie ist mit dem Token-Ring vergleichbar. Es existieren Stationen mit zwei oder vier Glasfaseranschlüssen. Stationen mit vier Glasfaseranschlüssen werden direkt an den Doppelglasfaser-Ring angebunden, d.h., sie sind sowohl auf dem Primär- als auch auf dem Sekundärring angeschlossen. Man bezeichnet diese Endgeräte als Class-A-Stationen. Für Stationen mit zwei Anschlüssen (Class-B-

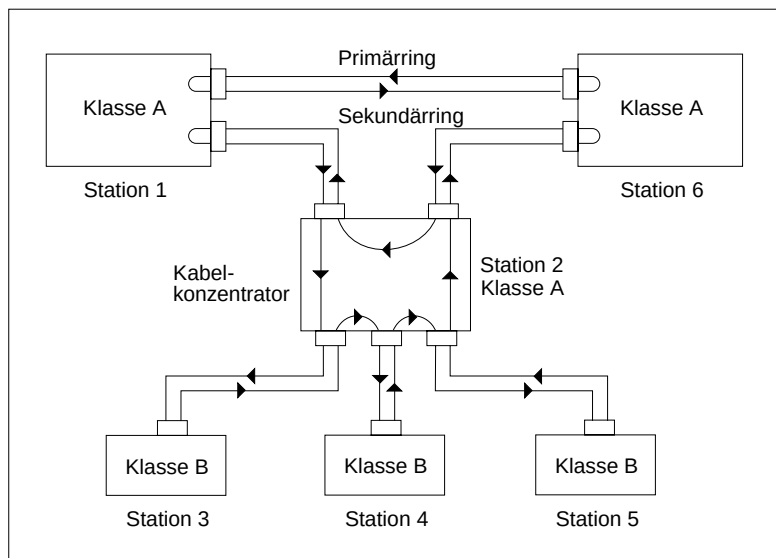
4.4 FDDI-LANS

Stationen) gibt es einen Concentrator (Class-A), der an den Primär-ring angeschlossen ist und die Backup-Funktion in der Art eines Ringleitungsverteilers übernehmen kann.

Die A-Stationen und der C-Concentrator besitzen eine intelligente Komponente, um Leitungsausfälle zu überbrücken. Diese intelligente Komponente wird als Station Manager (STM) bezeichnet. Dieser Station Manager ist in der Lage, Leitungsfehler zwischen A- bzw. C-Stationen und auf den Leitungen zu B-Stationen zu erkennen. Erstere werden durch die Benutzung des Sekundärrings in einer Art automatischer Rekonfiguration behoben. Letztere führen zum Ausfall der B-Station und werden innerhalb des C-Concentrator überbrückt.

Das von FDDI verwendete Zugriffsverfahren entspricht im wesentlichen dem Token-Ring-Protokoll nach IEEE 802.5. Der grundsätzliche Unterschied besteht darin, wie das Frei-Token durch die sendende Station nach Abschluß einer Datenübertragung erzeugt wird.

Abbildung 4.20
FDDI-Ring-
topologie



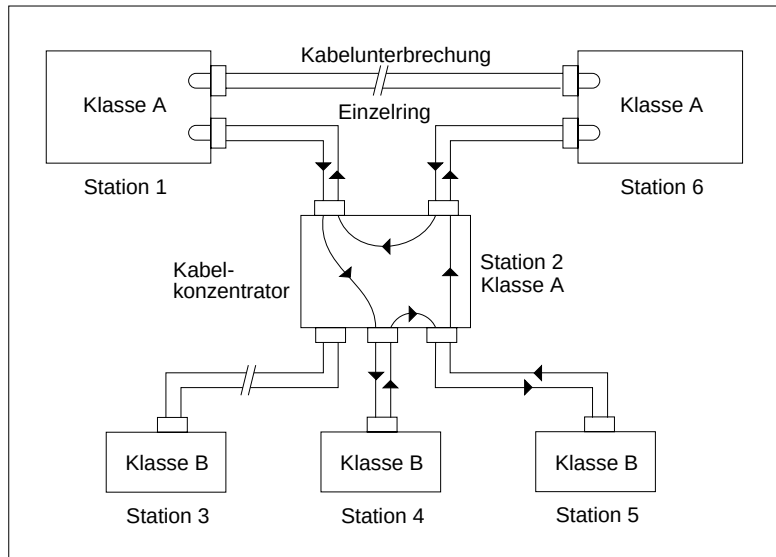
Das FDDI-Protokoll legt fest, daß eine Station das Frei-Token unmittelbar nach Aussenden des letzten Datenpakets innerhalb der maximalen Sendedauer auf den Ring geben kann, während bei IEEE 802.5 das Frei-Token erst nach Eintreffen des (einzigen) Datenpakets bei der sendenden Station auf den Ring gegeben werden darf. FDDI läßt die Sendung mehrerer Datenpakete innerhalb eines Token-Besitzes zu, IEEE 802.5 nur die Sendung eines einzigen Datenpakets.

4 Netzwerkaufbau und Netzwerktopologien

Somit ist das FDDI-Protokoll vergleichbar mit dem Early-Token-Release-Verfahren, wie dies beim 16-Mbit/s-Token-Ring eingesetzt werden kann.

In den Abbildungen 4.20 und 4.21 ist dargestellt, wie FDDI im Normalbetrieb und wie ein rekonfigurierter FDDI nach einer Leitungsstörung aussieht.

Abbildung 4.21
Rekonfigurier-
barer FDDI-Ring



Innerhalb von FDDI gibt es einen synchronen Verkehr mit höherer Priorität und einen asynchronen Verkehr mit niedriger Priorität. Dabei ist es durchaus möglich, innerhalb einer Station für den asynchronen Verkehr weitere Prioritätsänderungen durchzuführen. Auf diese Weise wird die Auslastung des FDDI-Rings wesentlich verbessert.

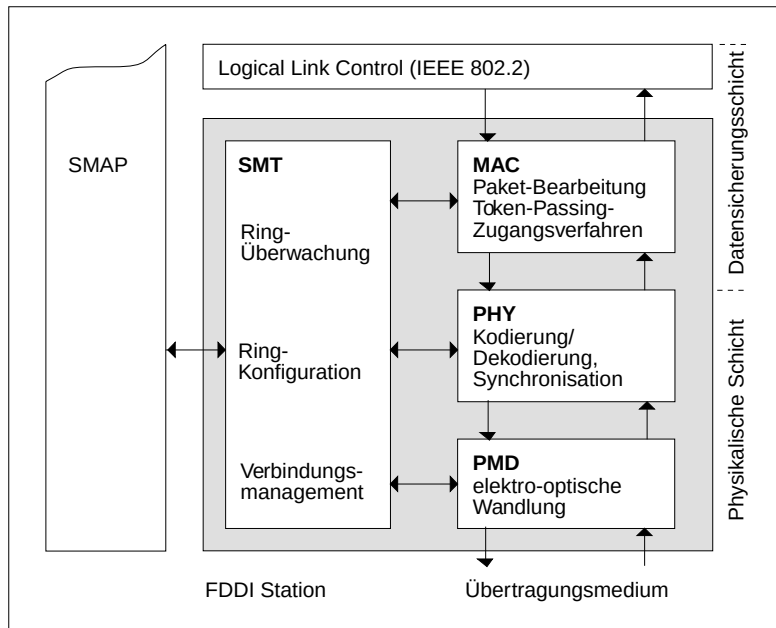
An dem in Kapitel 9 ausführlich behandelten ISO/OSI-Schichtenmodell können Sie sehen, daß die Datensicherungsschicht (Ebene 2) in die Schicht 2a (Media Access Control – MAC) und 2b (Logical Link Control – LLC) unterteilt wird. FDDI umfaßt vier Standarddokumente, die sowohl die physikalische Schicht als auch das Medienzugangsverfahren umfassen und eine Verbindung zwischen Übertragungsmedium und der Teilebene 2b realisieren:

- Media Access Control (MAC)
- Physical Layer Protocol (PHY)
- Physical Layer Medium Dependent (PMD)
- Station Management (SMT)

4.4 FDDI-LANs

Die notwendigen Komponenten für FDDI und deren Zusammenspiel sind in der nachfolgenden Abbildung dargestellt.

Abbildung 4.22
FFDI-Komponenten-
Blockdiagramm



Die Aufgaben und Funktionen dieser einzelnen Ebenen sollen anschließend kurz erläutert werden. Eine zu umfangreiche Beschreibung würde den Rahmen dieses Buchs sprengen, inzwischen gibt es über FDDI aber gute Literatur.

FDDI – Media Access Control

Das Medienzugangsverfahren arbeitet nach dem Prinzip des Token-Passing. Die Übertragung einer Nachricht wird von der Schicht 2b angestoßen. Die Nachricht wird mit der Aufforderung zur Übertragung an die MAC-Schicht weitergereicht. Die MAC-Schicht generiert aus dieser Nachricht eine PDU (Protocol Data Unit, auch Frame genannt) zur Übertragung an die entsprechende Zielstation.

Zur Übertragung muß die sendewillige Station auf ein freies Token warten, das sie in ein belegtes Token umwandelt und daran die eigene Nachricht anfügt und überträgt. Die Umwandlung des freien Tokens in ein belegtes Token ist bei FDDI anders realisiert, wie Sie dies von IEEE 802.5 her kennen. Bei FDDI wird das freie Token vom Ring entfernt, und anschließend wird mit der Übertragung begonnen, d.h., es gibt kein explizites Belegt-Token. Die Nachricht, also

4 Netzwerkaufbau und Netzwerktopologien

das zu übertragende Datenpaket, wird durch eine Start-Ende-Kennung markiert.

Damit FDDI auch effizient ist, arbeitet FDDI mit dem bereits bekannten und sinnvollen Early-Token-Release-Verfahren. FDDI unterstützt im wesentlichen zwei Dienste:

1. Die Übertragung herkömmlicher asynchroner Daten, z.B. File-Transfer
2. Die Übertragung synchroner Daten, z.B. digitale Sprache

Beide Dienste übertragen Daten paketweise. Den synchronen Diensten werden dabei Prioritäten eingeräumt, indem das Station-Management einen entsprechenden Bandbreitenkanal hierfür reserviert. Die verbleibende Bandbreite kann von asynchronen Diensten in Anspruch genommen werden.

Auch FDDI besitzt eingebaute Überwachungsfunktionen, ähnlich wie sie für IEEE 802.5 existieren. Es handelt sich dabei um folgende Funktionen des FDDI-MAC-Protokolls:

Ring Monitoring Im Gegensatz zum IEEE 802.5, bei dem eine explizite Monitorstation die Überwachung des Rings übernimmt und alle anderen Stationen als passive Monitore fungieren, sind die MAC-Monitorfunktionen beim FDDI zur Ringüberwachung dezentral auf alle angeschlossenen Stationen des Rings verteilt.

Jede FDDI-Station überwacht den FDDI-Ring ständig auf auftretende Fehler, die unter Umständen eine Neuinitialisierung des Rings erforderlich machen. Als auftretende Fehler werden Inaktivität oder auch nicht erlaubte Aktivitäten auf dem FDDI-Ring erkannt.

Die Inaktivität wird durch den Ablauf eines Valid-Timers festgestellt. Nicht erlaubte Aktivitäten wie zum Beispiel Protokollstörungen werden durch mehrfaches Ablaufen des Token-Rotation-Timers oder durch Kontrollprozesse des Station Management (SMT) erkannt. Damit diese Störungen auch behoben werden können, sind im MAC-Protokoll unterschiedliche Fehlerbehebungsprozeduren eingerichtet.

Es handelt sich dabei um:

Claim-Token-Prozeß Da jede Station im FDDI als aktiver Monitor arbeitet, können somit auch mehrere Monitore eine Störung des Protokolls erkennen. Jede dieser Stationen generiert daraufhin einen sogenannten Claim-Token-Prozeß. Innerhalb dieses Prozesses konkurrieren die Stationen um das Recht, ein neues Frei-Token generieren zu dürfen, indem sie immer wieder Bid-Frames erzeugen und übertragen. Gleichzeitig achtet jede Station auf das Eintreffen von Bid-Frames anderer Stationen.

4.4 FDDI-LANs

Die Station mit der kürzeren TTRT-Zeit, die Sollzeit für die Rotation des Tokens, erhält in diesem Fall den Zuschlag. Der Claim-Prozeß ist dann abgeschlossen, sobald eine Station ihr eigenes Claim-Paket wiedererhält. Diese Station darf nun den Ring neu initiieren und ein neues Frei-Token erzeugen.

Beacon-Prozeß Wenn der Claim-Token-Prozeß nicht zum gewünschten Erfolg führt, muß eine schwerwiegende Störung vorliegen, z.B. eine physikalische Ringunterbrechung. In diesem Fall bzw. wenn das SMT eine entsprechende Aufforderung gibt, startet die Station einen Beacon-Prozeß.

Sinn und Zweck ist, alle Stationen davon in Kenntnis zu setzen, daß eine logische Unterbrechung des Rings aufgetreten ist. Gleichzeitig wird die Rekonfiguration des Rings unterstützt, die durch das Station Management durchgeführt wird. Beim Starten des Beacon-Prozesses beginnt die Station, kontinuierlich Beacon-Frames zu übertragen. Da jede Station ein eintreffendes Beacon-Frame weiterleiten muß und eigene Übertragungen zurückzustellen sind, ist der FDDI-Ring vollständig mit Beacon-Frames ausgefüllt, die sich in Übertragungsrichtung unmittelbar hinter der Störung befinden.

Erhält die Station ihr Beacon-Frame zurück, ist die Ringunterbrechung behoben, z.B. durch Überbrückung der fehlerhaften Station. In diesem Fall wird von der Station unmittelbar danach der Claim-Token-Prozeß eingeleitet.

FDDI Physical Layer Protocol (PHY)

Durch das FDDI Physical Layer Protocol wird der obere Teil der physikalischen Schicht entsprechend dem ISO/OSI-Schichtenmodell beschrieben. Es wird dadurch das Bindeglied zwischen PMD und MAC zur Verfügung gestellt.

Die wesentliche Aufgabe dieser Schicht besteht darin, die physikalischen Verbindungen zwischen PHY-Instanzen benachbarter FDDI-Knoten aufrechtzuerhalten und gegebenenfalls auch wiederherzustellen. Zum anderen werden auf dieser Schicht auch die Verfahren zur Kodierung und Dekodierung der Information definiert. Diese Schicht legt auch fest, wie der Sendetakt und die Regeneration des Sendetakts zur Synchronisation der Station erfolgen müssen, damit eine serielle Datenübertragung durchgeführt werden kann.

Im Gegensatz zu IEEE 802.5 wird der Sendetakt von jeder FDDI-Station dezentral durch einen eigenen Oszillator erzeugt. Der Empfangstakt wird aus dem einlaufenden Bitstrom erhalten. Dabei wird eine maximale Abweichung von 0,01% der Nominaldatenrate als Ab-

4 Netzwerkaufbau und Netzwerktopologien

weichung zwischen Signaltaktung einlaufender Signale und dem lokalen Oszillator zugelassen. Um einen eventuellen Unterschied zwischen Empfangs- und Sendetakt ausgleichen zu können, wird das einlaufende Signal durch einen Pufferspeicher geschleust, der die Frequenzunterschiede kompensieren kann.

Im Gegensatz zu FDDI arbeitet der IEEE-802.5-Token-Ring mit einem zentralen Oszillator, der jeweils vom aktiven Monitor bereitgestellt wird. Auch hier führt der verwendete Pufferspeicher zu einer Netzlimitierung. Beim IEEE-802.5-Token-Ring beträgt die Limitierung 260 Stationen, unter der Voraussetzung, daß mit Typ-1-Kabeln und passiven Ringleitungsverteilern gearbeitet wird. Man sollte sich beim Token-Ring in Abhängigkeit von den eingesetzten Komponenten beim Hersteller erkundigen, ob andere Beschränkungen gelten, als sie durch den Standard festgelegt sind.

FDDI Physical Medium Dependent (PMD)

Diese Ebene stellt eine digitale Punkt-zu-Punkt-Verbindung zwischen FDDI-Knoten zur Verfügung. Die wesentliche Hauptaufgabe dieser Ebene liegt in der Festlegung der physikalischen Eigenschaften des Übertragungsmediums. Dies umfaßt auch die Festlegung der Steckertechnik, der Sende- und Empfangseinheiten, einen (optionalen) optischen Bypass und die Schnittstellen zu PHY und dem Station Management (SMT).

In der anfänglichen Entwicklung wurde für FDDI eine multimodale Gradientenindexfaser als Übertragungsmedium festgelegt, genormt und eingesetzt. Im Lauf der Zeit stellte man fest, daß man weit größere Entfernungen als »nur« zwei Kilometer zwischen zwei benachbarten Knoten überwinden will. Deshalb sind auch Monomode-Glasfaserkabel in Verbindung mit Laserdioden in den Standard aufgenommen worden. Diese ermöglichen es, bis zu 60 Kilometer zwischen zwei FDDI-Knoten zurückzulegen.

Die jüngsten Bestrebungen gehen in die Richtung, FDDI bis zum Endgerät verfügbar zu machen, dann jedoch nicht mit Glasfaserkabeln, auch wenn die immer billiger werden, sondern mit Kupferkabeln. Mehrere Hersteller arbeiten seit ein paar Jahren verstärkt an einer Lösung verdrahter Vierdraht-Kupferkabel (Copper Distributed Data Interface – CDDI). Diese Technik wird sowohl für geschirmte Vierdrahtleitungen (STP) in Typ-1-Qualität gemäß IBM-Verkabelungssystem als auch für Unshielded Twisted-Pair (UTP) angeboten. Dabei sollen in der Regel Distanzen von bis zu 100 Metern zwischen FDDI-Knoten überwunden werden können.

4.4 FDDI-LANs

FDDI Station Management (SMT)

Auf dieser Ebene befinden sich sowohl die Funktionen und Komponenten als auch die Schnittstellen, die zur Initiierung und zum Betrieb des FDDI-Rings notwendig sind. Außerdem werden Prozeduren definiert, die im Fehlerfall ausgeführt werden und eine Rekonfiguration des Rings durchführen können.

Nachdem Sie nun wissen, wie FDDI im großen und ganzen funktioniert, will ich noch aufzeigen, welche unterschiedlichen Stationstypen für FDDI zur Verfügung stehen und welche Stationstypen zu welchem Zweck benötigt werden.

FDDI-Stationstypen

Zum Aufbau von FDDI läßt das Station Management verschiedene Konfigurationen von FDDI-Stationen zu. Es gibt zwei Klassen von Stationstypen, sie unterscheiden sich darin, wie sie an den Primärring bzw. an den Sekundärring angeschlossen werden. Eine weitere Klassenbildung wird durch die Medienzugangskomponenten (MAC) gebildet, mit denen eine FDDI-Station ausgestattet ist.

Es ergeben sich folgende Aufteilungen:

- Stationen mit einer Verbindung zu beiden Ringen und einer MAC-Komponente: Single MAC Dual Attachment Station (SM DAS)
- Stationen mit einer Verbindung zu beiden Ringen und zwei MAC-Komponenten: Dual MAC Dual Attachment Station (DM DAS)
- Stationen mit einer Verbindung zum Primärring mit MAC-Komponente: Single Attachment Station (SAS)
- Konzentrator mit einer Verbindung zu beiden Ringen (die MAC-Ebene ist optional): Dual Attachment Concentrator (DAC)
- Konzentrator mit nur einer Verbindung zum Primärring (MAC optional): Single Attachment Concentrator (SAC)

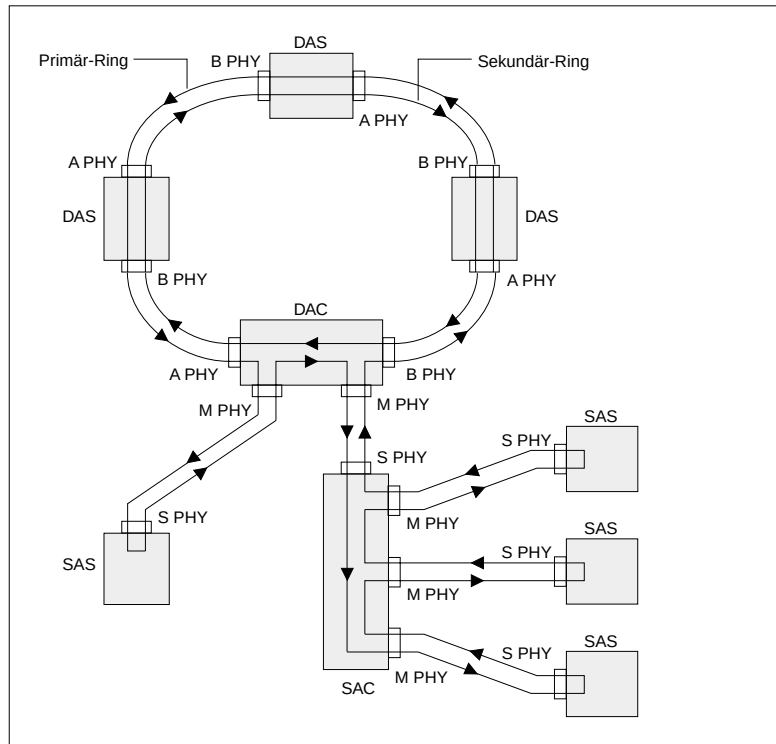
Dual-Attachment-Knoten (SM DAS, DM DAS und DAC) lassen sich direkt in den Doppelring (Primär- und Sekundärring) einbinden. Jeder Knoten dieses Typs enthält zwei Ports, die mit A und B bezeichnet werden. Der Port A ist in diesem Fall mit der eingehenden LWL-Faser des Primärrings und der ausgehenden Faser des Sekundärrings verbunden. Der Port B ist mit der eingehenden LWL-Faser des Sekundärrings und der ausgehenden Faser des Primärrings verbunden. Der Anschluß sieht nun so aus, daß bei Dual Attachment Stations der Port A eines Knotens mit dem Port B seines Nachbarknotens verbunden ist.

Konzentratoren (DAC und SAC) verfügen über einen oder mehrere Typ-M-Ports. Damit ist man in der Lage, eine baumförmige Struktur aufzubauen. Single-Attachment-Knoten (SAS und SAC) verfügen

4 Netzwerkaufbau und Netzwerktopologien

über einen S-Port (Slave Port), der innerhalb eines baumartigen Gebildes mit dem M-Port eines Konzentrators verbunden wird. Abbildung 4.23 stellt dar, wie die einzelnen Stationstypen in einem FDDI-Ring eingebunden werden.

Abbildung 4.23
FDDI-Stationstypen



Da auch schon viel über Fehlertoleranz und Ausfallsicherheit bei FDDI gesprochen und geschrieben worden ist, zeigt Abbildung 4.24, wie die einzelnen Fehlersituationen im FDDI-Ring rekonfiguriert werden können.

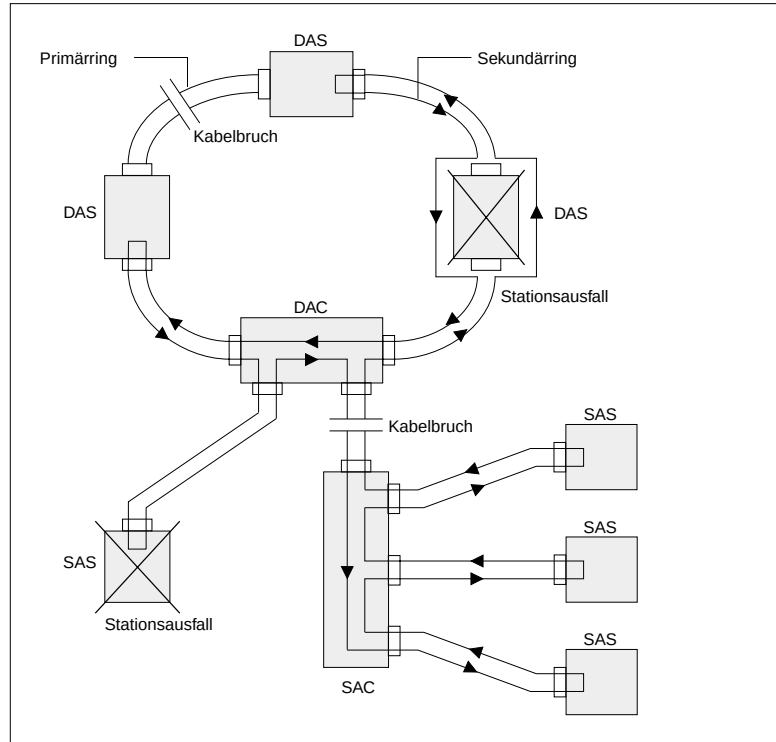
Anschließend sollen die wichtigsten Eigenschaften von FDDI nochmals zusammengefaßt werden.

■ Optische Übertragungstechnologie

- Optische Fasern: Gradientenindexfaser 62,5/125 m, 50/125 m, 85/125 m, 100/140 m
Monomode-Faser 9-10/125 m
- Anschlußtechnik: in FDDI-PMD genormter Duplex-LWL-Stecker
- Passiver optischer Bypass: optional für Dual-Attached-Knoten

4.4 FDDI-LANs

Abbildung 4.24
FDDI-
Rekonfiguration



- **Topologie und Architektur**
 - Doppelter, gegenläufig operierender Ring, Primärring, Sekundärring
 - Inhärente Fehlertoleranz
 - Dual-Attachment-Knoten (Anschluß an Primär- und Sekundärring)
 - Single-Attachment-Knoten (Anschluß an Primärring)
 - FDDI-Stationen und FDDI-Konzentratoren
 - Anzahl anschließbarer Stationen: 500
 - Medienlänge: bis zu 200 Kilometer
 - Abstand zwischen FDDI-Knoten: max. 2 km (Gradientenfaser), 40–60 km (Monomodefaser)
- Nutzbare Datenrate: 100 Mbit/s
- Timer-gesteuertes Multiple-Token-Ring-Protokoll
- Unterstützung von konventionellen (asynchronen) und zeitkritischen (synchronen) Anwendungen

Da FDDI als strategisches Konzept zum Aufbau von Backbone-Verkabelungen genutzt und als Netzwerk in den Abteilungen Ethernet, Token-Ring, ARCNET oder auch wieder FDDI in Betracht gezogen

4 Netzwerkaufbau und Netzwerktopologien

wird, ist die Frage zu stellen, wie eine vernünftige, flexible und zukunftsichere Verkabelungsstrategie entwickelt werden kann. Ich will Ihnen im nächsten Kapitel die grundlegenden Konzepte näherbringen und dabei auch auf die schon erwähnte Hub-Technologie eingehen.

Es sei an dieser Stelle jedoch bereits darauf hingewiesen, daß dies keine vollständige Ausführung sein kann, über dieses Thema könnten ganze Bücher geschrieben werden. Hier soll Ihnen zumindest ein Eindruck über die Mächtigkeit von FDDI vermittelt werden.

Eine weitere Entwicklung im Bereich der High-Speed-LANs bildet ein HP-Produkt, das unter der Bezeichnung 100VG-AnyLAN bekannt ist. Da auch dieses System eine 100-Mbit/s-Übertragungsgeschwindigkeit zur Verfügung stellt, soll es nachfolgend näher beschrieben werden.

4.5 100VG-AnyLAN von HP

Es bemühten sich zwei Hersteller darum, den Standard für das 100-Mbit/s-Ethernet-Netzwerk am Markt zu etablieren. Es waren dies die Firmen HP und Digital Equipment.

Die Konzepte und Lösungsmöglichkeiten sind ziemlich ausgereift, schließlich gibt es FDDI bzw. CDDI bereits seit Jahren auf dem Markt, und entsprechend viele Erfahrungen wurden mit diesen Komponenten und deren Aufbau gemacht.

In diesem Kapitel will ich Ihnen deshalb exemplarisch die Lösungsvorschläge von HP vorstellen. In diesem Zusammenhang werden wir auch auf eine Funktion zu sprechen kommen, die von anderen Herstellern bereits sehr erfolgreich in der Hub-Technologie für Ethernet eingesetzt wird: Es geht um die Funktion der Switching-Technik, die immer interessanter wird, wenn es darum geht, leistungsfähige Netzwerke zu konzipieren.

100VG-AnyLAN basiert auf dem IEEE-802.12-Standard zur Übertragung von IEEE-802.3-Ethernet- und IEEE-802.5-Token-Ring-Daten mit einer Geschwindigkeit von 100 Mbit/s. Mit 100VG-AnyLAN wird der Versuch unternommen, die besten Eigenschaften von Ethernet und Token-Ring zusammenzuführen – d.h. die Kombination des einfachen und schnellen Netzwerkzugriffs, wie bei Ethernet, mit den strengen und deterministischen Eigenschaften der Token-Ring-Technologie.

4.5 100VG-AnyLAN von HP

Die 100VG-AnyLAN-Technologie unterstützt die Netzwerkkonzeptionsregeln und Topologien von Ethernet-10Base-T- und Token-Ring-Netzwerken. Das Konzept von 100VG-AnyLAN ist so aufgebaut, daß es mit einer bestehenden 10Base-T- oder Token-Ring-Verkabelungsstruktur eingesetzt werden kann. Voraussetzung dafür ist, daß die bestehende Verkabelung den 10Base-T-Anforderungen oder Token-Ring-Anforderungen in bezug auf die Kabelspezifikation entspricht.

Eine Kopplung von 100VG-AnyLAN über Bridges und Router mit FDDI-, ATM- oder WAN-Netzen bereitet ebenfalls keine Probleme, sofern die einzelnen Hersteller Unterstützung für 100VG-AnyLAN anbieten können.

Die 100VG-AnyLAN-Topologie verfügt über eine zentral verwaltete Zugriffsmethode, die als Demand Priority Protocol (DPP) bezeichnet wird. Diese Zugriffsmethode ist ein einfaches, deterministisches Request-Verfahren, wodurch die Netzwerkeffizienz so groß wie möglich ist, da Netzwerkkollisionen und Token-Rotation-Zeiten nicht auftreten. Zusätzlich nutzt DPP eine Ebene der Priorität für Daten und eine andere für Multimedia. Damit können auch zeitkritische Anwendungen mit entsprechenden Antwortzeiten bedient werden.

100VG-AnyLAN-Komponenten

Ein 100VG-AnyLAN-Netzwerk wird physikalisch als Stern aufgebaut. Hierzu werden die folgenden Komponenten benötigt:

- Ein oder mehrere 100VG-AnyLAN-Hubs (Repeater)
- Zwei oder mehr 100VG-AnyLAN-Endgeräte
- Optionale Internetworking-Einheiten wie Router, Bridges oder Switches

100VG-AnyLAN-Hub

Die zentrale Komponente ist der 100VG-AnyLAN-Hub, der auch als Repeater bezeichnet wird. Alle 100VG-AnyLAN-Netzwerk-Devices werden an den 100VG-AnyLAN angebunden. Der Hub kann mit zwei unterschiedlichen Arten von Ports ausgestattet sein:

- *Down-Link Port*
An diesen Port werden 100VG-AnyLAN-Devices im Netzwerk eingebunden. Für jedes Endgerät oder Lower Level Hub wird ein Down-Link Port benötigt.
- *Up-Link Port*
Dieser Port ist optional, er ist reserviert für die Kaskadierung von Hubs, d.h. den Anschluß von Lower-Level-Hubs an Upper-Level-Hubs.

4 Netzwerkaufbau und Netzwerktopologien

Zudem sind in einem 100VG-AnyLAN-Hub zusätzliche Sicherheitsfunktionen eingebaut, die optional genutzt werden können:

- *Private Mode*

Ein Endgerät oder ein Port am Hub empfängt nur die Pakete, die direkt an das Endgerät bzw. den Port adressiert sind.

- *Promiscuous Mode*

Ein Endgerät oder ein Port am Hub nimmt alle Pakete im Netzwerk auf, um zu prüfen, ob sie für ihn bestimmt sind.

100VG-AnyLAN-Nodes

Ein 100VG-AnyLAN-Node kann ein Client- oder Server-PC, eine Workstation oder jedes andere 100VG-AnyLAN-Netzwerk-Device, z.B. ein Switch, eine Bridge, ein Router oder ein anderer 100VG-AnyLAN-Hub, sein.

So wie Ethernet-, Token-Ring- oder FDDI-Netzwerke in logische Segmente durch den Einsatz von Bridges oder Router unterteilt werden können, kann auch ein 100VG-AnyLAN-Netzwerk durch Bridges, Router oder Switches logisch getrennt werden. Ein 100VG-AnyLAN kann durch weitere 100VG-AnyLAN-Hubs innerhalb eines Netzwerks kaskadiert werden, ohne zusätzlich Bridges, Router oder andere Verbindungselemente einsetzen zu müssen. Die kaskadierten Hubs werden als Level 2, 3, ... Hubs bezeichnet, in Abhängigkeit davon, auf welcher kaskadierten Ebene sie sich befinden.

100VG-AnyLAN-Network-Link

In einem 100VG-AnyLAN können die folgenden Netzwerkkabel eingesetzt werden:

- 8-adrige CAT 3, Unshielded-Twisted-Pair-Kabel
- 8-adrige CAT 4, Unshielded-Twisted-Pair-Kabel
- 8-adrige CAT 5, Unshielded-Twisted-Pair-Kabel
- 4-adrige Shielded-Twisted-Pair-Kabel
- Glasfaserverbindungen

Regeln für den Aufbau von 100VG-AnyLAN-Netzwerken

Die Anforderungen gleichen denen für den Aufbau von 10Base-T- und Token-Ring-Netzwerken.

Grundsätzlich ist dabei folgendes zu beachten:

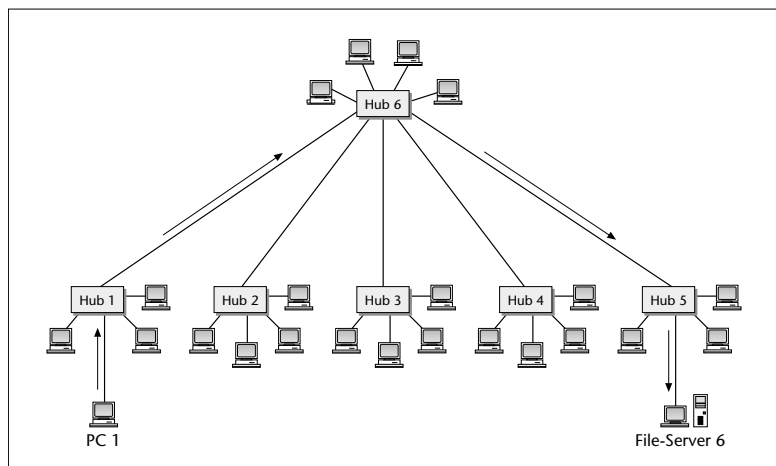
1. Die Netzwerktopologie muß ein physikalischer Stern sein, ohne Verzweigungen und Loops.
2. Bei einem 8adrigen UTP-Netzwerk (4 Paare) werden alle 4 Paare benötigt. Die 4 Paare dürfen in keinsten Weise an einer anderen

4.5 100VG-AnyLAN von HP

- Stelle der Verkabelung gesplittet werden. Bei einer Umstellung von Ethernet 10Base-T oder Token-Ring ist darauf zu achten, daß am Endgerät immer noch alle 4 Paare verfügbar sind. Dies ist vor allem deshalb wichtig, weil 10Base-T nur 2 Paare benötigt.
3. In einem einzigen physikalischen Segment (ohne Bridges und Router) sind nicht mehr als 1024 Nodes (Endgeräte) erlaubt.
 4. In einem 100VG-AnyLAN sollte die Entfernung zwischen zwei Nodes nicht größer als 2,5 Kilometer sein.
 5. Alle Nodes in einem 100VG-AnyLAN müssen das gleiche von 100VG-AnyLAN unterstützte Paketformat verwenden (IEEE-802.3-Ethernet- oder IEEE-802.5-Token-Ring-Format). Auf dem gleichen Netzwerksegment werden keine zwei unterschiedlichen Paketformate unterstützt. Wenn ein Token-Ring-Frame-Format-Netzwerk mit einem Ethernet-Frame-Format-Netzwerk verbunden werden muß, benötigt man eine Bridge oder einen Router zur Kopplung.
 6. Die Kaskadierung von Hubs sollte nicht zu groß sein. Bei einer Ebene von 3 sollte in der Regel aufgehört werden.
 7. Zwischen zwei Endgeräten sollten nicht mehr als 7 Bridges installiert sein.

Ein 100VG-AnyLAN kann in etwa wie folgt aufgebaut werden:

Abbildung 4.25
Aufbau eines
100VG-AnyLAN-
Netzwerks



Ethernet-Switching

Um die Performance im Netzwerk zu erhöhen, kann zusätzlich zu den herkömmlichen Hubs ein 100/10-Ethernet-Switching-Modul eingesetzt werden. Dadurch wird die Leistungsfähigkeit des gesamten Netzwerks erhöht. Die Erklärungen, die Sie an dieser Stelle über den Switching-Mechanismus für Ethernet-LANs erfahren, lassen sich ent-

4 Netzwerkaufbau und Netzwerktopologien

sprechend auf die Technik abbilden, so wie dies in 10-Mbit/s-Ethernet-Switching-Modulen bereits verfügbar ist. So bieten zum Beispiel die Firmen Cabeltron oder Synoptics für ihre Hubs Switching-Einschübe für Ethernet an. Der einzige Unterschied ist, daß diese nicht mit 100 Mbit/s, sondern mit 10 Mbit/s arbeiten.

Cross-Point-Switching verbessert 100 Mbit/s-Ethernet und herkömmliche Ethernet-Netzwerke, indem die gleichzeitige Kommunikation zwischen Segmenten ermöglicht wird. Cross-Point-Switching in einem Fast Ethernet funktioniert genauso wie Cross-Point-Switching in einer herkömmlichen Ethernet-Umgebung. Die nachfolgenden Beispiele orientieren sich am Ethernet-Cross-Point-Switching, da es diese Technik bereits gibt.

Ethernet-Cross-Point-Switching

Ethernet-Netzwerke basieren auf einem einzelnen Segment (sofern keine Bridges/Router eingebaut sind), bei dem zu einem Zeitpunkt nur eine Station den Bus nutzen kann. Mit zunehmender Anzahl der Stationen und zunehmender Last auf dem Segment nimmt die Performance immer mehr ab, und der Durchsatz wird geringer. Beim Einsatz von Cross-Point-Switching kann der Durchsatz wesentlich erhöht werden, da es möglich ist, daß einzelne Stationen parallel Daten übertragen. Wie dies funktioniert, soll im Folgenden näher beschrieben werden.

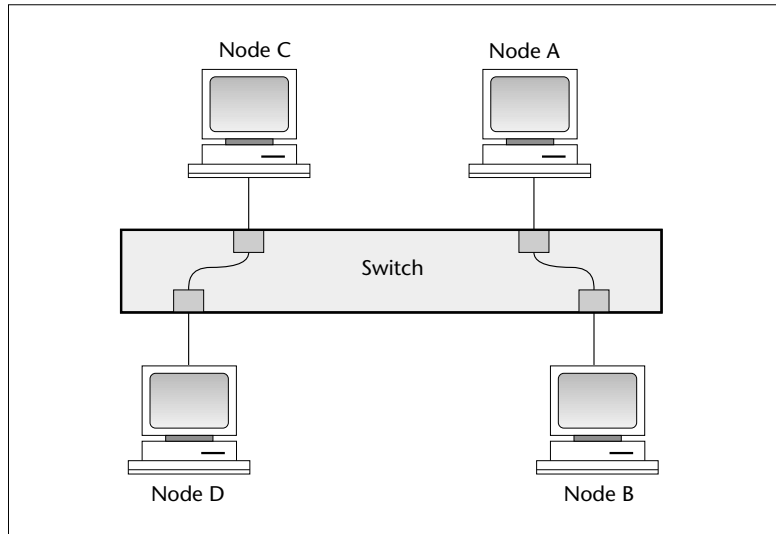
In einer herkömmlichen 10Base-T-Ethernet-Umgebung (ohne Switching-Technik) wird im Halbduplexverfahren gearbeitet, basierend auf einer separaten Transmit-Leitung (Tx) und einer separaten Receive-Leitung (Rx). Nur eine Leitung kann zu einem Zeitpunkt aktiv sein. Sind plötzlich beide Leitungen aktiv, wird eine Kollision erkannt. In diesem Fall zieht sich die kollidierende Station dezent zurück und versucht die Übertragung des Pakets nach einer zufällig erzeugten Zeitspanne von neuem.

Eine Switching-Umgebung ist vergleichbar mit einer Punkt-zu-Punkt-Verbindung. Eine Switched-Point-to-Point-Verbindung zwischen zwei Ethernetsegmenten (Stationen) bleibt nur für die Dauer der Paketübertragung erhalten. Neue Verbindungen werden im laufenden Betrieb durchgeführt, so wie dies in Abbildung 4.26 dargestellt ist.

Wenn die Station A ein Paket mit Station B austauscht, dann verbindet der Ethernet-Cross-Point-Switch nur die Leitung von LAN-Segment A und LAN-Segment B miteinander, da keine Notwendigkeit besteht, Pakete zu irgendeiner anderen Station bzw. irgendeinem anderen Port zu übertragen. Wenn zur gleichen Zeit Station C ein Paket zu Station D übertragen will, dann verbindet der Cross-Point-Ethernet-Switch die LAN-Segmente C und D miteinander.

4.5 100VG-AnyLAN von HP

Abbildung 4.26
Switched-Point-to-
Point-Verbindung



Beide Verbindungen sind parallel aktiv, da beide unabhängig voneinander mit jeweils anderen Segmenten kommunizieren. Der effektive Datendurchsatz des Ethernet-Netzwerks hat sich durch den Einsatz eines Ethernet-Cross-Point-Switch während der Datenübertragung von 10 Mbit/s auf 20 Mbit/s erhöht. Die Erhöhung des Datendurchsatzes hängt davon ab, wie viele LAN-Segmente während der Datenübertragung parallel bedient werden können. Je mehr Ports auf dem Ethernet-Cross-Point-Switch vorhanden sind und parallel Daten übertragen können, desto höher wird der effektive Datendurchsatz werden. Rein rechnerisch kann der Durchsatz wie folgt ermittelt werden, da jede Verbindung zwei Ports benötigt:

So hat zum Beispiel ein 10-Port-10-Mbit/s-Cross-Point-Switch einen theoretischen effektiven Durchsatz von 50 Mbit/s, wenn bei der Datenkommunikation gleichzeitig fünf Datenpakete parallel auf die einzelnen LAN-Segmente übertragen werden können.

Es sei darauf hingewiesen, daß der effektive Durchsatz, der während des Arbeitens mit einem Cross-Point-Switch erzielt werden kann, im wesentlichen vom Netzwerkdesign und vom Netzwerkprotokoll abhängt. Am günstigsten verhält sich die Gesamtsituation, wenn bei der Kommunikation immer parallel Verbindungen aufgebaut werden können. Ein Cross-Point-Switch in einer Client-Server-Umgebung ist ineffektiv, wenn die Clients im gesamten Netzwerk verteilt sind (d.h. in allen LAN-Segmenten existieren) und alle versuchen, miteinander zu kommunizieren, wobei ein paralleles Kommunizieren untereinander unterbunden wird.

4 Netzwerkaufbau und Netzwerktopologien

Der Ethernet-Cross-Point-Switch arbeitet als ein MAC-Layer-Endgerät, das protokollunabhängig ist, d. h., der Switch ist vollkommen unabhängig vom eingesetzten höheren Protokoll (IPX, TCP/IP, AppleTalk etc.).

Klassisches Ethernet-Switching

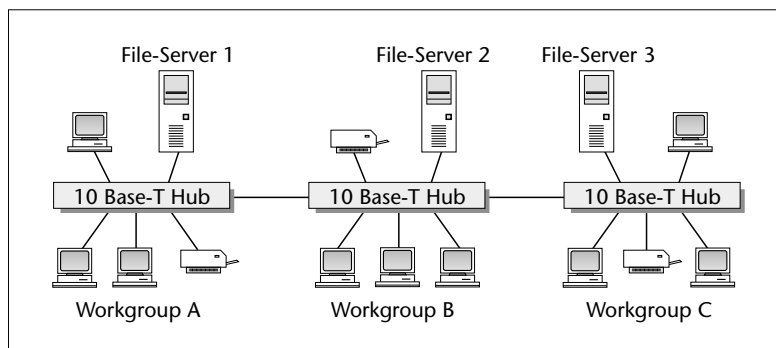
Ein klassischer Cross-Point-Switch besteht aus Prozessoren, die als kleine 2-Port-Bridges fungieren. Jeder Port im Switch ist mit einem eigenen Prozessor ausgestattet. Die Prozessoren filtern Pakete und leiten diese weiter, in Abhängigkeit von der internen Adreßtabelle und dem Inhalt des Datenpakets. So wie bei herkömmlichen Bridges wird die Tabelle verwaltet und gepflegt, inklusive der Verwendung eines Aging-Intervalls, um länger nicht mehr benutzte Einträge zu löschen. Wenn ein Prozessor ein Paket empfängt, dessen Source-Adresse er noch nicht kennt, erlernt der Prozessor (Bridge) die Lokation der neuen Source und schickt das Paket an alle Ports, wenn das Ziel nicht bekannt ist. Wenn ein Antwortpaket zurückkommt, erlernt das Adreßmodul die Lokation und aktualisiert die Adreßtabelle in allen Prozessoren im Switch. Wenn der Eintrag einmal gemacht ist, werden alle nachfolgenden Pakete per Switch-Verbindung direkt zum Ziel transportiert.

Aufbau von Ethernet-Cross-Point-Switch-Netzwerken

In einem typischen Netzwerk sind Server und Workstations im gleichen Segment installiert. Somit müssen sich Server und Workstation die 10 Mbit/s teilen. Es ist klar, daß der Datendurchsatz für jeden einzelnen geringer wird, je mehr Workstations mit dem Server eine Kommunikation aufbauen, d. h. Daten austauschen. In Abbildung 4.27 ist eine solche häufig anzutreffende Konstellation dargestellt.

Um den Datendurchsatz zu erhöhen, könnte man nun versuchen, einen leistungsfähigen Backbone aufzubauen, in diesem die drei Server zu installieren und die Workgroups A bis C über separate Bridges in logische Segmente zu unterteilen und an den Backbone anzubinden.

Abbildung 4.27
Typisches Ethernet-Netzwerk

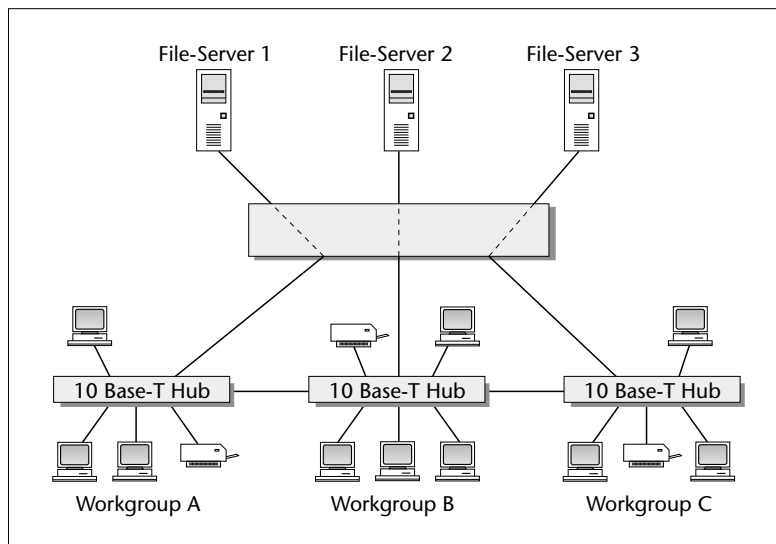


4.5 100VG-AnyLAN von HP

Der Aufbau von drei physikalischen Netzwerken (der eigene Server der Workgroup ist darin jeweils installiert), die über Bridges miteinander verbunden sind, würde nur eine Teillösung bedeuten.

Da in diesem Fall immer noch die Clients der Workgroup x die 10 Mbit/s mit dem Server teilen müssen, ist der Datendurchsatz nur teilweise höher als vorher. Ist ein Netzwerk hingegen mit Hilfe von Switches aufgebaut, erspart man sich unter Umständen den Aufbau eines leistungsfähigen Backbone und die Installation leistungsfähiger Bridges/Router. Kann das Netzwerk, wie in Abbildung 4.27 dargestellt, in Workgroups unterteilt werden, die jeweils einen eigenen Server (oder auch mehrere) haben, so läßt sich ein Netzwerk wie in Abbildung 4.28 aufbauen.

Abbildung 4.28
Netzkonfiguration
mit Cross-Point-
Switches



Jeder Server der Workgroup wird am Cross-Point-Switch an einen eigenen Port angeschlossen. Jedes LAN-Segment (Workgroup A bis C) wird ebenfalls an einen eigenen Port am Cross-Point-Switch angeschlossen. Somit kann jedes LAN-Segment über den Cross-Point-Switch direkt mit dem Server kommunizieren. Auf diese Weise läßt sich die Leistungsfähigkeit sehr schnell und unproblematisch erhöhen.

Wenn man sich die Beschreibungen der Switch-Systeme näher betrachtet, dann stellt man fest, daß hierbei noch unterschieden wird zwischen sogenannten Store-and-Forward-Switches und Cut-Through-Switches. Die Unterschiede liegen zum einen in den Möglichkeiten,

4 Netzwerkaufbau und Netzwerktopologien

unterschiedliche LANs zu koppeln und zum anderen in der Performance, die mit dem jeweiligen Switch-Typ zur Verfügung gestellt werden kann.

Store-and-Forward-Switch

Ein Store-and-Forward-Switch kommt immer dann zum Einsatz, wenn ein Switch von unterschiedlichen LANs durchgeführt werden soll bzw. muß. Bei dieser Variante wird das eingehende Datenpaket erst dann an das Zielsystem weitergeleitet, wenn das Paket vollständig im Switch eingetroffen ist. Das heißt, das Datenpaket wird vollständig empfangen, und erst anschließend wird damit begonnen, die Weiterleitung des Paketes durchzuführen. Dieses Verfahren ist notwendig, da mit einem solchen Switch heterogene Netzwerke miteinander gekoppelt werden. Wenn z.B. Ethernet-Netzwerke mit Token-Ring-Netzwerken verbunden werden, dann unterscheiden sich diese unter anderem im Aufbau der Datenpakete und in der Länge der Datenpakete. Somit ist es verständlich, daß ein Paket aus LAN A erst dann weitertransportiert werden kann, wenn es für LAN B adaptiert worden ist – dies kann eben nur dann erfolgen, wenn das Datenpaket vollständig empfangen ist. Durch diesen Mechanismus kann man zwar unterschiedliche Netzwerke über einen Switch miteinander verbinden, man muß dafür jedoch Geschwindigkeitseinbußen in Kauf nehmen, da der Weitertransport nicht so schnell erfolgen kann wie bei einem Cut-Through-Switch.

Cut-Through-Switch

Der Cut-Through-Switch wird nur für homogene Netzanbindungen angeboten, d.h. nur, wenn man Ethernet mit Ethernet oder Token-Ring mit Token-Ring verbinden will. Der Vorteil eines Cut-Through-Switch ist vor allem in der Performance zu sehen, die auf Grund der zugrundeliegenden Arbeitsweise wesentlich höher ist als bei Store-and-Forward-Switches. Ein Cut-Through-Switch beginnt mit der Weiterleitung des Datenpaketes an den entsprechenden Zielport, sobald die Zieladresse im Datenpaket erkannt wird. Es müssen somit nur die ersten paar Byte eines Pakets empfangen werden, um die physikalische Zieladresse zu erkennen. Näher betrachtet, wird die höhere Performance unter Sicherheitseinbußen bei der Datenübertragung erkauft. Ein Cut-Through-Switch ist aufgrund der Arbeitsweise nicht in der Lage, Fehler im Datenpaket, verursacht durch die Datenübertragung, zu erkennen und entsprechend zu reagieren. Die Fehlererkennung muß deshalb beim Zielsystem durchgeführt werden.

Wenn man sich einen reinen Ethernet-Switch kauft, dann wird es sich fast immer um einen Cut-Through-Switch handeln. Muß der Switch hingegen Ethernet und Token-Ring miteinander verbinden, dann ist dies nur mit Hilfe eines Store-and-Forward-Switches zu realisieren.

4.6 ATM – Asynchronous Transfer Mode

Bislang habe ich nur die Cross-Point-Switch-Technik für Ethernet erläutert. Derzeit sind Entwicklungen im Gang, auch für Token-Ring und FDDI die Switching-Technik zur Verfügung zu stellen. Die führenden Anbieter entsprechender Hub-Systeme sind inzwischen in der Lage, die Switching-Technik auch für Token-Ring und FDDI anzubieten. Es gibt also inzwischen eine Vielzahl von Möglichkeiten, Netzwerke leistungsfähig und effizient aufzubauen.

Grundvoraussetzung ist und bleibt jedoch eine vernünftige Planung, da jedes Unternehmen andere Voraussetzungen hat. Erst eine Analyse der Netzwerkumgebung und der Anforderungen an das Netzwerk erlaubt, eine korrekte Planung für das Netzwerk durchzuführen. Danach kann entschieden werden, welche Technik die sinnvollste ist und wie sich das Netzwerk optimal für die gestellten Anforderungen aufbauen läßt.

Es gibt eine Netzwerktopologie, über die schon viel geredet worden ist und deren zukünftige Bedeutung im Netzwerkbereich immer größer werden wird. Betrachtet man die Konzeption und die damit verbundenen Möglichkeiten, so könnte es langfristig so aussehen, daß sich dieser Netzwerktyp durchsetzen wird. Die Rede ist von ATM – Asynchronous Transfer Mode. Mit ATM ist man in der Lage, über Text, Bilder, Video (bewegte Bilder) bis hin zu Sprache alle notwendigen Datenübertragungen durchzuführen. Wegen seiner großen Bedeutung soll dieser Netzwerktyp näher betrachtet werden.

4.6 ATM – Asynchronous Transfer Mode

ATM ist das Übertragungsverfahren der Zukunft, wenn es darum geht, Datenautobahnen innerhalb und außerhalb eines Unternehmens aufzubauen. Diese Technik wird in allen Bereichen der Kommunikation Einzug halten. Vom CITT wurde sie als die grundlegende Technik für das Breitband-ISDN (B-ISDN) definiert. Der große Durchbruch erfolgt aber erst jetzt im LAN-Bereich. Aufgrund der dort gesammelten Erfahrungen wird sich ATM sukzessive auch im WAN-Bereich etablieren. ATM ist somit der erste Standard, der sowohl für die Kommunikation im lokalen als auch im öffentlichen Bereich Gültigkeit haben wird. Als Übermittlungsverfahren umfaßt ATM die Aspekte der Vermittlung und der Übertragung. Damit wird ATM vom Endgerät über das LAN bis hin zum B-ISDN zukünftig als einheitliche Technologie verwendet.

ATM ist ein Übertragungsverfahren, das auf dem asynchronen Zeit-Multiplexverfahren aufbaut. Dabei werden Daten fester Länge transportiert. Man nennt diese Datenpakete Zellen; jede dieser Zellen ist

4 Netzwerkaufbau und Netzwerktopologien

53 Byte groß. 5 Byte der Zelle sind für den Zellenkopf (ATM Header) reserviert. Im Zellenkopf werden die Angaben über Kanal- und Pfad-Adressierungen gespeichert. Alle Netzknoten werden bei ATM über ein oder mehrere ATM-Schalteinheiten, auch ATM-Switches genannt, miteinander verbunden. Die Aufgabe der ATM-Switches besteht unter anderem darin, die ATM-Zellen an den jeweiligen Bestimmungsort zu transportieren. Aufgrund der Switching-Technik teilen sich die Teilnehmer kein gemeinsames Übertragungsmedium, wie dies im Shared-LAN-Bereich (Ethernet, Token-Ring etc.) der Fall ist, sondern geben die Zellen am ATM-Switch ab, ohne auf Zugriffsverfahren Rücksicht nehmen zu müssen. Die Festlegung auf eine Zellenlänge von 53 Byte ist ein Kompromiß zwischen den Anforderungen von analoger und digitaler Sprachübertragung. Werden analoge Signale über digitale Strecken übertragen, müssen die analogen Sprachsignale 8000mal in der Sekunde abgetastet werden, jeder Meßwert wird dann in 8 Bit kodiert und übertragen.

Daraus ergibt sich, daß pro Sprachkanal 64 Kbit/s übertragen werden müssen – d.h. alle 125 μ Sekunden ein Meßwert bzw. ein Byte. Diese Art der Übertragung von analogen Signalen nennt man auch Puls-Code-Modulation (PCM).

ATM-Netzwerke können generell in einer Vielzahl unterschiedlicher Übertragungsmedien eingesetzt werden. Bei allen bisherigen Netzwerkstrukturen waren die Standards bis zur physikalischen Schicht definiert, z.B. Ethernet, Token-Ring etc. Für ATM ist eine Übertragung von Zellen über SDH-Netzwerke mit Geschwindigkeiten von 155 Mbit/s und 622 Mbit/s angegeben. Es gibt also keine eindeutige Festlegung, über welches physikalische Medium ATM-Zellen, vor allem mit welchen Geschwindigkeiten, übertragen werden sollen. Aufgrund der ATM-Switches können in einem ATM-Netzwerk neue Benutzer eingeschaltet werden, ohne daß für die bislang beteiligten Stationen die zur Verfügung gestellten Bandbreiten eingeschränkt werden. In den ATM-Switches müssen lediglich weitere Anschlußmodule mit den notwendigen Bandbreiten eingebaut werden. Die einzige Begrenzung wird durch den ATM-Switch gestellt. Wenn der nicht mehr in der Lage ist, die angeschlossenen ATM-Endgeräte mit der entsprechenden Übertragungsgeschwindigkeit zu bedienen, kann sich ein Engpaß ergeben. Das bedeutet, daß man bei der Auswahl der ATM-Switches genau darauf achten muß, welche Datenmengen von diesen verarbeitet werden können. Es hat keinen Sinn, viele ATM-Endgeräte anzuschließen, wenn die Datenmengen nicht über den ATM-Backplane im Hub transportiert werden können. Auf jeden Fall kann ATM in allen Bereichen der Datenübertragung genutzt und sowohl für den LAN-Bereich als auch für den WAN-Bereich eingesetzt werden.

4.6.1 ATM-Zellen – Aufbau und Funktion

ATM-Zellen sind Informationseinheiten, die von einem ATM-Switch übertragen und vermittelt werden. Die ATM-Zelle besteht aus einem 5 Byte großen Zellenkopf (Kopffeld) und einem 48 Byte großen Informationsfeld. Alle Nutzdaten, die über ATM übertragen werden, müssen im Informationsfeld einer oder mehrerer ATM-Zellen »verpackt« bzw. umgeformt werden.

ATM-Informationsfeld

Im Informationsfeld mit einer kontinuierlichen Länge von 48 Byte werden alle Nutzinformationen oder auch Signalisierungsinformationen übertragen.

ATM-Kopffeld – ATM Header

Im ATM Header werden alle Informationen gespeichert, die benötigt werden, um die ATM-Zelle durch das ATM-Netzwerk zu transportieren. Der ATM Header hat immer eine Länge von 5 Byte und enthält unter anderem folgende Funktionen:

- *Identifizierung des virtuellen Kanals (16 Bit)*
Dieses Feld dient zur Unterscheidung von unterschiedlichen, gleichzeitigen Verbindungen. Damit werden Zellen identifiziert, die zu einer gleichen virtuellen Verbindung gehören. Die virtuelle Kanalnummer (VCI, Virtual Channel Identifier) ist für eine Verbindung in beiden Richtungen gleich und wird immer für einen Übermittlungsabschnitt vergeben.
- *Identifizierung des Kanalbündels (8 Bit am Teilnehmeranschluß und 12 Bit zwischen ATM-Switches)*
Mit diesem Feld können mehrere Wege der unterschiedlichen Richtungen auseinandergehalten werden, wenn diese jeweils mehrere virtuelle Kanäle beinhalten. Kanäle des gleichen Kanalbündels (VPI, Virtual Path Identifier) können dadurch sehr schnell erkannt und weitergeschaltet werden.
- *Kennzeichnung der Informationsfeldart (3 Bit)*
Mit diesem Feld wird gekennzeichnet, ob es sich um ein Nutzdaten- oder Steuerdatenfeld handelt. Die Nutzdaten werden gemäß dem vorher festgelegten Weg im Netz vermittelt, wohingegen die Steuerdaten von den Netzelementen interpretiert werden müssen.
- *Fehlererkennung und Fehlerbehebung (8 Bit)*
Durch die Prüfsequenz im ATM Header lassen sich Fehler im Header erkennen und können behoben werden.

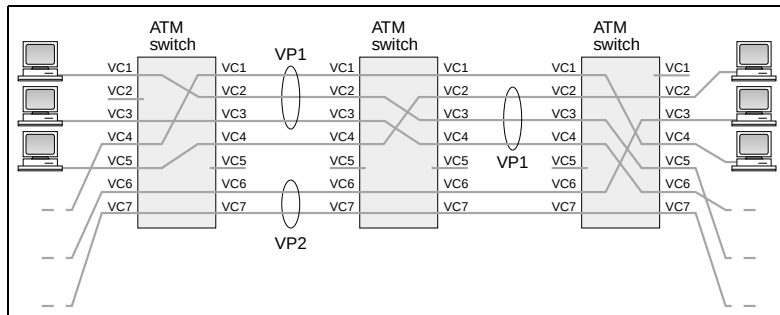
4.6.2 ATM-Netzwerke

Zum Aufbau von ATM-Netzwerken werden unterschiedliche Komponenten benötigt. Hierzu zählen ATM-Switches, ATM-Endknoten oder auch die Anbindung von »herkömmlichen LANs« an ATM-Netzwerke. In Abbildung 4.29 ist dargestellt, wie man sich den grundsätzlichen Aufbau von ATM-Netzwerken vorstellen muß.

4.6 ATM – Asynchronous Transfer Mode

Ein VCC ist eine Verbindung zwischen zwei miteinander kommunizierenden ATM-Endgeräten und kann aus mehreren aufeinanderfolgenden ATM-VC-Links bestehen. Der Virtual Channel Identifier (VCI) im ATM Header wird pro Netzwerk ein Entity-to-Entity-Link zugewiesen. Somit kann sich der VCI beim Durchlaufen des Pakets im Netzwerk innerhalb des gleichen VCC ändern. In Abbildung 4.30 ist zu sehen, wie das Prinzip der Virtual Channels und Virtual Paths in Verbindung mit kaskadierten ATM-Switches zu verstehen ist.

Abbildung 4.30
Virtual Channels
und Virtual Paths



4.6.3 ATM im Referenzmodell

Das ATM-Schichtenmodell beruht im Prinzip auf dem OSI-Referenzmodell. Es lassen sich jedoch nicht alle Funktionen auf die bekannten Schichten im OSI-Referenzmodell abbilden. Neben der Schicht 1 (der physikalischen Schicht) sind im ATM-Schichtenmodell noch zwei spezifische Schichten definiert: ATM-Schicht und ATM-Adaptionsschicht (AAL). Beide Schichten sind speziell für den asynchronen Transfermodus notwendig. Die ATM-Schicht sorgt, einfach gesagt, für den Zellentransportdienst – darin sind die Funktionen des ATM-Headers festgelegt. Die ATM-Adaptionsschicht berücksichtigt das Übertragen von Daten in Form von Zellen, d.h., in dieser Schicht sind alle notwendigen Aspekte zur Anpassung der Nutzdaten an das Zellenformat berücksichtigt. Aufgrund ihrer Bedeutung innerhalb der ATM-Spezifikation sollen diese drei Schichten nachfolgend erläutert werden.

Physical Layer (Bitübertragungsschicht)

Über den Physical Layer wird den darüberliegenden Schichten die Übertragung von Signalen auf einem physikalischen Medium ermöglicht. In der Bitübertragungsschicht werden dabei unter anderem der Zugriff auf das Übertragungsmedium, die Darstellung der Signale auf dem Medium, Synchronisationsmechanismen und Fehlerbehand-

4 Netzwerkaufbau und Netzwerktopologien

lungsfunktionen definiert. Es wurde bereits erwähnt, daß das ATM-Übertragungsverfahren im Prinzip unabhängig von der physikalischen Ebene ist. Deshalb ist für ATM eine Vielzahl von Übertragungsmedien und -formen vorgesehen und möglich. So werden im LAN-Bereich hauptsächlich Lichtleiterkabel und Twisted-Pair-Kabel verwendet.

Zudem besteht die Aufgabe der Physical Layer in der Synchronisation der Zellen, d.h. in der Erkennung des ATM Header und in der Erkennung des Zellenendes. Wenn keine Zellen übertragen werden, müssen Leerzellen übertragen werden. Diese Zellen werden von der Bitübertragungsschicht erzeugt, um einen kontinuierlichen Datenstrom bei der Zellenübertragung zu erreichen. Wenn die Leerzellen durch den Physical Layer erzeugt worden sind, enthalten diese eine besondere Kennung im Header der Zelle.

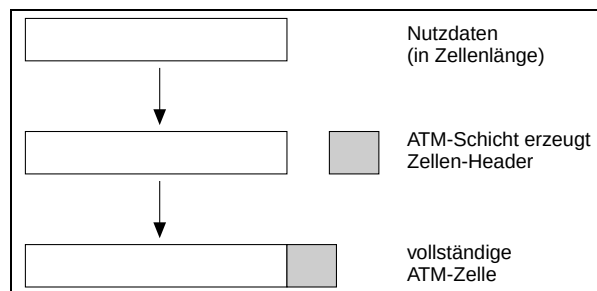
ATM-Schicht

Die Aufgabe der ATM-Schicht besteht im Transport der Zelle. Hierzu zählt auch die Vermittlung von ATM-Zellen in den Netzkomponenten. In der ATM-Schicht werden Funktionen zur Verfügung gestellt, die man im ATM Header wiederfindet:

- Bearbeitung und Identifizierung der virtuellen Kanäle (VC) und virtuellen Kanalbündel bzw. virtual paths (VP)
- Sicherung der Kopfinformationen in der Zelle
- Kennzeichnung von Zellen, wenn diese eine spezielle Bedeutung haben
- Überwachung der maximalen Übertragungsrate, die von höheren Schichten für eine bestimmte Verbindung gefordert worden ist

In der folgenden Abbildung ist dargestellt, wie zum Nutzdatenfeld von 48 Byte der ATM Header von 5 Byte hinzugefügt wird.

Abbildung 4.31
Anfügen des ATM
Header durch die
ATM-Schicht



4.6 ATM – Asynchronous Transfer Mode

Mit Hilfe der ATM-Schicht werden Daten der höheren Schichten auf Basis von ATM-Zellen ausgetauscht. Dabei ist die Aufgabe der ATM-Schicht unabhängig vom gewählten Dienst (Sprache, Daten etc.). Die ATM-Zelle wird transparent durch das gesamte Netzwerk bis zum Zielsystem transportiert.

Die Nutzdaten werden dabei in keiner Weise bearbeitet, bis die Zelle beim Zielsystem angekommen ist. Entsprechend dem beim Verbindungsaufbau festgelegten Weg, werden die Zellen anhand der Kennung VPI+VCI transportiert. Eine Änderung der Kennzeichnungen je Vermittlungsabschnitt ist möglich.

Adaptionsschicht (AAL)

Die notwendigen Informationen für den AAL (ATM Adaptation Layer) befinden sich im Informationsfeld (Nutzdatenfeld) und sind dienstabhängig. Der AAL ist das Bindeglied zwischen den zu übertragenden Nutzdaten und der zellenorientierten Übertragung. Die notwendigen Dienste können eine feste oder eine variable Bitrate haben. Zudem können die Dienste einen kontinuierlichen Bitstrom oder einen sogenannten Burst-Betrieb erfordern. Daneben sind auch noch Nutzdaten- und Signalisierungsdaten zu unterscheiden. Die verschiedenen Anforderungen der Datenübertragung durch den AAL sind auf vier Klassen abgebildet, so wie dies in Abbildung 4.32 dargestellt ist.

Abbildung 4.32
ATM-Datenüber-
tragung und die
vier Dienstklassen

	Klasse A	Klasse B	Klasse C	Klasse D
Zeitbezug:	zeitkontinuierlich		nicht zeitkontinuierlich	
Bitrate:	konstant	variabel		
Verbindungsart:	verbindungsorientiert			verbindungslos
Beispiele:	Sprachübertragung	variable Bitrate Video	verbindungsorient. Datenübertragung (Frame Relay)	verbindungslose Datenübertragung
AAL Typ:	Diensttyp 1	Diensttyp 2	Diensttyp 3/4 und 5	Diensttyp 3/4

4 Netzwerkaufbau und Netzwerktopologien

Die Aufgabe des AAL besteht nun darin, die unterschiedlichen Forderungen auf ATM-Zellen abzubilden bzw. aus den empfangenen Zellen die Nutzdaten der höheren Schicht bereitzustellen. Der AAL stellt den höheren Schichten unter anderem folgende Funktionen zur Verfügung:

- Nutzdaten werden auf ATM-Zellen abgebildet
- Zellenlaufzeiten werden in Abhängigkeit des verwendeten Dienstes ausgeglichen

Für die AAL-Schicht sind folgende Definitionen getroffen worden:

AAL1 Dieser Dienstyp 1 ist zur Übertragung von Nutzdaten mit einem festen Zeitbezug determiniert, wenn es zum Beispiel um die digitale Sprachübertragung nach dem Pulse-Code-Modulationsverfahren geht.

Mit diesem Dienstyp können auch Synchronisationsdaten ausgetauscht werden, die zur Rekonstruktion auf der Empfängerseite erforderlich sind.

AAL2 Dieser Dienstyp 2 wurde für die Übertragung von Nutzdaten vorgesehen, wenn diese eine variable Bitrate verwenden. Das ist zum Beispiel dann der Fall, wenn komprimierte Videoinformationen übertragen werden. Auch mit diesem Dienstyp können Synchronisationsinformationen ausgetauscht werden.

AAL3/4 Der Dienstyp 3/4 wird zur gesicherten Übertragung von Nutzdaten verwendet. Soll z.B. eine LAN-LAN-Kopplung durchgeführt werden, nutzt man diesen Dienstyp. Die aufwendigen Definitionen für die Übertragung von Nutzdaten werden hier festgelegt.

AAL5 Für eine verbindungsorientierte Datenübertragung bietet der Dienstyp 5 eine sehr einfache Übertragungsmethode. Müssen Signisierungsdaten übertragen werden, dann kann auch dieser Dienstyp verwendet werden.

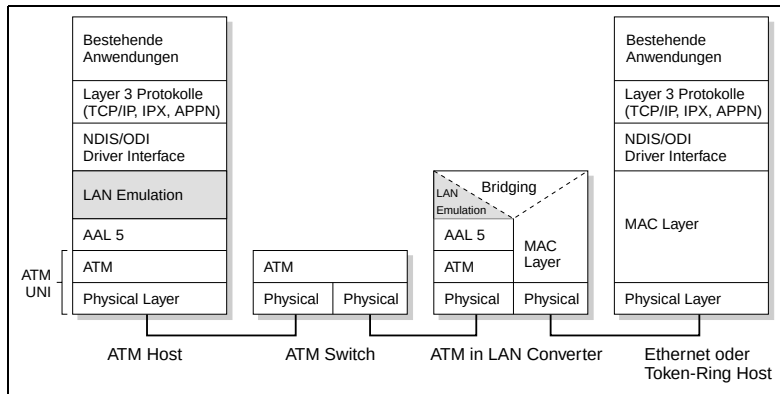
Neben diesen wichtigen Definitionen und Festlegungen existiert eine weitere wichtige Festlegung, um eine nahtlose Integration von ATM in LANs durchführen zu können bzw. um eine Kopplung von Ethernet, Token-Ring etc. mit oder über ATM zu realisieren. Das Schlagwort in diesem Zusammenhang lautet: LAN-Emulation. Die folgenden Ausführungen sollen Ihnen zeigen, wozu dieser Mechanismus benötigt wird.

4.6 ATM – Asynchronous Transfer Mode

4.6.4 ATM-LAN-Emulation

Entsprechend den Spezifikationen, so wie sie vom ATM-Forum für die LAN-Emulation (LANE) definiert worden sind, besteht die Aufgabe vor allem darin, bestehenden Anwendungen die Nutzung von ATM zu ermöglichen, auch wenn sie Protokolle wie APPN, NetBIOS, IP oder IPX einsetzen. Das System soll sich dabei so verhalten, als würde man herkömmliche LANs dafür einsetzen. LAN-Emulation ist sowohl eine Netzkomponentenfunktion als auch eine ATM-Endgerätefunktion. Damit können herkömmliche Netzwerkprotokolle ohne Änderung über ATM transportiert werden. Herkömmliche Endgeräte können LAN-Emulation verwenden, um sowohl mit anderen herkömmlichen Endgeräten zu kommunizieren (die über ATM miteinander gekoppelt sind) als auch mit an ATM angeschlossenen Servern, Router, Hubs oder anderen Netzwerk-Devices. In Abbildung 4.33 ist zu sehen, wie man sich anhand des OSI-Schichtenmodells die Implementierung der LAN-Emulation auf den unterschiedlichen Endgeräten vorstellen muß bzw. welche Elemente dazwischen geschaltet werden müssen.

Abbildung 4.33
Konzeptioneller
Aufbau der LAN-
Emulation



LAN-Emulation stellt zwischen den höheren Protokollen der verbindungslosen Protokolldienste und den niedrigeren verbindungsorientierten ATM-Protokollen einen Translation-Layer zur Verfügung.

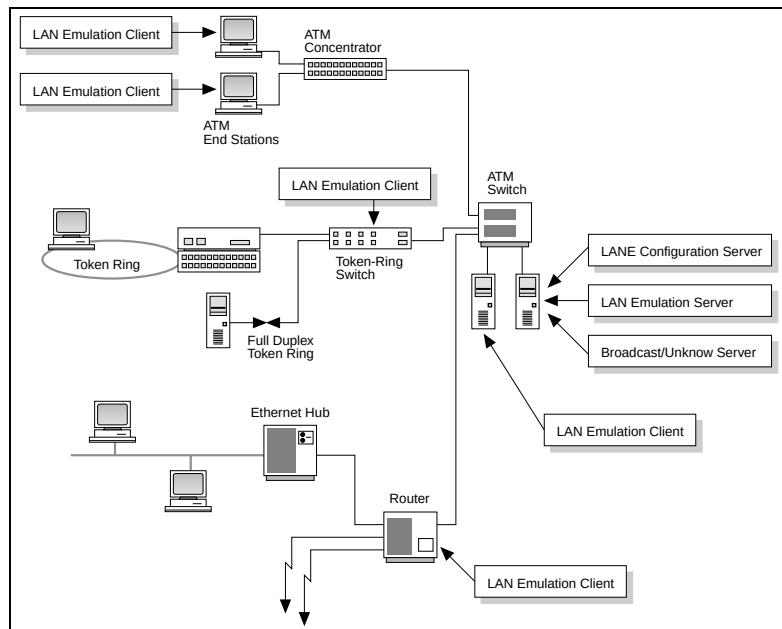
Über diesen Mechanismus ist es möglich, alle notwendigen Netzwerkconfigurationen über ATM aufzubauen. Hätte man die LAN-Emulation nicht eingeführt, könnten nur ATM-Netzwerke mit reinen ATM-Endgeräten aufgebaut werden, d.h. eine Kopplung zwischen ATM-Endgerät und einem ATM-Switch bzw. die Kopplung eines ATM-Switch mit einem anderen ATM-Switch. Neben der bereits erwähnten anderen Arbeitsweise von LANs im Vergleich zu ATM (ver-

4 Netzwerkaufbau und Netzwerktopologien

bindungslos versus verbindungsorientiert) ist auch noch zu beachten, daß LANs Daten als »Broadcast« im Netz transportieren und diese von allen empfangen und geprüft werden, wohingegen ATM nur Point-to-Point- bzw. Point-to-Multipoint-Verbindungen zuläßt.

Um über die LAN-Emulation das gesteckte Ziel zu erreichen, wird das Prinzip der Client- und Server-Mechanismen eingesetzt. LAN-Emulation-Clients (LEC) sind auf Endgeräten mit direktem ATM-Interface, in Ethernet/ATM-Switches und in LAN-to-ATM-Bridge/Router-Systemen implementiert. Die zusätzlich notwendigen LAN-Emulation-Servers (LES), Broadcast and Unknown Servers (BUS) sind Bestandteil des Backbone-Netzwerks. In einigen Implementierungen benötigen LANE-Server (LES und BUS) dedizierte Workstations. In anderen Systemen sind die LANE-Server bereits im Backbone-Switch integriert. Bei der Auswahl der Hub-Systeme zum Aufbau von ATM-Backbones sollte darauf geachtet werden, wie LAN-Emulation implementiert werden muß, d. h., ob diese Mechanismen im Hub-System integriert sind oder dedizierte Server benötigt werden. Abbildung 4.34 stellt dar, wie ein komplexeres Netzwerk auf Basis eines ATM-Backbone (Collapsed Backbone) und daran angeschlossenen LANs bzw. Endgeräten aufgebaut werden kann und wo die jeweiligen LANE-Mechanismen zu finden sind.

Abbildung 4.34
LANE-Prozesse in
einer LAN-ATM-
Umgebung



4.7 Gigabit Ethernet

In den letzten Abschnitten wurden Netzwerke dargestellt, die nicht nur verfügbar, sondern auch zum größten Teil standardisiert sind (sieht man von den kleinen fehlenden Standards bei ATM ab). Wenn man die Fachliteratur konzentriert liest, dann stellt man derzeit fest, daß die großen Artikel nicht mehr unbedingt ATM darstellen, so wie dies in den vergangenen Jahren der Fall gewesen ist, sondern Gigabit Ethernet in den Vordergrund stellen. Gigabit Ethernet wurde in der Anfangszeit von vielen Netzwerkherstellern als Spinnerei belächelt und wird jetzt von allen führenden Herstellern unterstützt. Was verbirgt sich hinter dieser neuen Technik, und wie wird sie sich entwickeln? Diese und eine Vielzahl anderer Fragen sollen im nächsten Kapitel behandelt werden.

4.7 Gigabit Ethernet

Betrachtet man sich die Entwicklung der Netzwerktechnik der letzten Jahre, dann stellt man fest, daß zunächst mit sehr geringen Geschwindigkeiten und geringen Anforderungen im Netzwerk gearbeitet werden konnte. Dies hat sich dramatisch geändert. Nicht nur, daß die Anforderungen an das Netzwerk hinsichtlich der Geschwindigkeit steigen, auch die Sicherheitsanforderungen werden immer höher. Letzteres ist auch damit begründet, daß die technologische Entwicklung immer schneller voranschreitet. Damit ist die Angst verbunden, auf das falsche Pferd zu setzen. Es ist in der heutigen Zeit enorm schwierig geworden, zu garantieren, wie lange die Komponenten eines Netzwerks Bestand haben werden. Wichtig ist daher nur, daß man sich Hersteller sucht, die Beständigkeit nachweisen können.

Die Datenmengen, die zwischen Workstation und Server transportiert werden, werden immer größer. Früher hat man darauf geachtet, daß die Anzahl der Arbeitsplätze in einem Netzwerk nicht zu groß ist, damit der Datendurchsatz pro Station aufgrund der Shared-Media-Technik ausreichend ist, um akzeptable Antwortzeiten zu erhalten. Die immer schneller werdenden PCs, die immer größer werden, den Applikationen führen dazu, daß ein herkömmliches Ethernet-Netzwerk mit 10 Mbit/s bereits mit zwei, drei oder vier Stationen überfordert ist. Deshalb geht man immer mehr in Richtung Switching-Technologie und stellt jedem einzelnen Arbeitsplatz dediziert die LAN-Geschwindigkeit zur Verfügung. So stehen bei einem Switching-Ethernet jedem Anwender 10 Mbit/s zur Verfügung. Nachdem jedoch die LAN-Geschwindigkeit für die Endgeräte mit Hilfe von Fast Ethernet oder ATM 100 Mbit/s und mehr beträgt, wird es für die Server und die Backbones im Netzwerk immer enger, da immer größere

4 Netzwerkaufbau und Netzwerktopologien

Datenmengen transportiert werden müssen, die mit entsprechend höheren Geschwindigkeiten zwischen Workstations und Server zu transportieren sind. Diese Entwicklung ist ein Grund, weshalb sich am Markt Gigabit Ethernet als neue Netzwerktechnik immer mehr etablieren wird. Mit dieser neuen Netzwerktechnik hat man für den Aufbau strukturierter Netze die besten Voraussetzungen, um flächen-deckend und bedarfsgerecht skalierbare Netzwerkgeschwindigkeiten verfügbar machen zu können.

4.7.1 Ethernet – die dominierende LAN-Technik

Untersuchungen haben ergeben, daß weltweit etwa 120 Millionen Ethernet-Knoten installiert sind. Ebenso wurde herausgefunden, daß 83% aller weltweit installierten Netzwerkkomponenten bis 1996 Ethernet-Komponenten waren, und dieser Trend hielt an. Die verbleibenden 17% werden zwischen Token-Ring, FDDI und ATM aufgeteilt. Für das Jahr 1997 hat man festgestellt, daß der Verkauf von Ethernet-Produkten bereits 77% aller Netzwerkprodukte betragen hat. Laut Angaben von IDC sind 1997 42 Millionen Ethernet-Karten und 54 Millionen Ethernet-Ports (Hub und Switch) verkauft worden. Im Vergleich dazu stehen diesen Zahlen 5 Millionen ATM-, FDDI/CDDI- und Token-Ring-Karten und 7 Millionen ATM-, FDDI/CDDI- und Token-Ring-Ports gegenüber. Dieser Trend wird noch sehr lange anhalten. Verantwortlich für diesen Trend ist eine Vielzahl von Faktoren.

Zuverlässigkeit

Zuverlässige und stabile Netzwerke sind wesentlicher Bestandteil für den Erfolg eines Unternehmens. Gefordert sind deren einfache Installation und eine einfache Unterstützung. Seitdem 1986 10Base-T Hubs zum Aufbau einer Sternverkabelung eingeführt worden sind, haben sich die strukturierten Verkabelungen immer mehr durchgesetzt, und die Hub-Systeme bzw. Switches wurden leistungsfähiger. Heutzutage zählt Ethernet immer noch zu den am einfachsten einsetzbaren Netzwerken.

Verfügbarkeit von Management Tools

Management Tools für Ethernet erlauben es den Netzwerkverantwortlichen, den Status aller Endgeräte und Netzwerkkomponenten zu sehen. Dies wird unter anderem auch dadurch erreicht, daß sich Ethernet bei diesen Komponenten an den SNMP-Standard (Simple Network Management Protocol) hält. Die Ethernet Tools zur Fehleranalyse reichen von einer einfachen LED-Anzeige bis hin zu ausge-

4.7 Gigabit Ethernet

reichten Netzwerk-Analysen. Aufgrund der weit verbreiteten Anzahl von Ethernet-Netzwerken gibt es auch eine Vielzahl von Firmen, die sich mit dieser Technik noch auskennen. Für die anderen Netzwerk-techniken werden hingegen wesentlich höhere Anforderungen gestellt.

Skalierbarkeit

Mit der Weiterentwicklung von Fast Ethernet stand ab 1995 die Ethernet-Technik als skalierbare Netzwerktechnik zur Verfügung. Mit der Weiterentwicklung zu Gigabit Ethernet wurde dieser Trend fortgeführt. Unabhängige Marktforscher prophezeien ein sehr großes Interesse an der Ethernet-Technologie. Dies betrifft vor allem die Anbindung von Fast Ethernet Hubs und Switches mit Gigabit Ethernet Uplinks (siehe dazu auch meine späteren Ausführungen), Gigabit Ethernet Switches und Repeatern und der Einsatz von Gigabit Ethernet-Karten in Servern. Es stehen also drei Ethernet-Varianten zur Verfügung: 10 Mbit/s – 100 Mbit/s – 1000 Mbit/s.

Geringe Anschaffungskosten

Im Vergleich zu Token-Ring und ATM zeichnen sich die Ethernet- und Fast-Ethernet-Komponenten durch sehr geringe Kosten aus. Der Preisverfall für diese Produkte hält zudem noch an. Der Schaden ist deshalb auch nicht so hoch, wenn man in einer Netzumgebung die eine oder andere Komponente austauschen oder ersetzen muß. Entscheidend ist, daß man die Verkabelung beibehalten kann.

4.7.2 Ziele und Gründe für Gigabit Ethernet

Es wurde eingangs bereits erwähnt, daß die wachsenden Datenmengen im Endgerätebereich dazu beigetragen haben, ein noch schnelleres Netzwerk als Basis der Datenkommunikation zur Verfügung zu stellen. Bei der Entwicklung von Gigabit Ethernet wurden dabei folgende Ziele verfolgt:

Interoperabilität mit Ethernet und Fast Ethernet

Durch den Einsatz von Gigabit Ethernet kann auf die installierte Basis von NICs zurückgegriffen werden. Zudem werden die Investitionen für bereits installierte Hubs, Switches und Router gesichert. Das bestehende Netzwerkmanagement kann weiterhin verwendet werden.

4 Netzwerkaufbau und Netzwerktopologien

Konform mit dem Ethernet-Standard

Gigabit Ethernet verwendet das gleiche Frame-Format, das bereits für Ethernet und Fast Ethernet zum Einsatz kommt. Dabei wurden auch die Festlegungen für die minimale und maximale Frame-Größe nicht geändert, sondern beibehalten. Als Zugriffsverfahren wird nach wie vor CSMA/CD verwendet, und die 802.2-LLC-Interface-Spezifikationen haben noch Gültigkeit.

Kommunikation für 10, 100 und 1000 Mbit/s

Bei der Kommunikation der verschiedenen Ethernet-Netzwerke untereinander ist, anders als bei Kommunikation mit FDDI- und ATM-Netzwerken, keine Fragmentierung der Frames notwendig. Ebenso besteht keine Notwendigkeit, in irgendeiner Form Encapsulation-Verfahren zu verwenden, so wie man dies aus dem ATM-Verfahren kennt. Eine Translation der Frames, wie man dies von dem FDDI-Bereich kennt, ist auch nicht durchzuführen.

Nicht zu vergessen ist an dieser Stelle, daß Gigabit Ethernet nochmals die zehnfache Geschwindigkeit von Fast Ethernet bietet. Ich möchte auch noch einmal daran erinnern, daß Gigabit Ethernet nicht dazu konzipiert ist, Endgeräte mit 1000 Mbit/s in das Netzwerk einzubinden, sondern dazu, daß zentrale Server und Hub-Systeme untereinander mit diesen hohen Geschwindigkeiten Daten austauschen können. Es ist ein großer Trend festzustellen, der in Richtung 100 Mbit/s bis zum Arbeitsplatz geht. Es ist derzeit auch festzustellen, daß die Euphorie von ATM bis zum Arbeitsplatz auch nicht mehr so groß ist, wie dies anfänglich der Fall war.

Betrachtet man die Anwendungen im Netzwerk, die einen hohen Bandbreitenbedarf aufweisen, dann können die folgenden Unterteilungen vorgenommen werden:

- Wissenschaftliche Modellierung
- CAD/CAM im Ingenieurwesen
- Medizinische Anwendungen
- Internet- und Intranet-Aktivitäten
- Dokumentenverwaltung
- Videokonferenzen
- Backup im Netzwerk
- Interaktives Whiteboard

Zu diesen Faktoren kommt hinzu, daß die CPU-Geschwindigkeiten immer größer werden und damit verbunden auch die Leistungsfähigkeit der Endgeräte. Ein Arbeitsplatz mit 350- oder 400-MHz-CPU-Taktung für einen Intel Pentium II MMX ist inzwischen keine Seltenheit mehr. Die Bildung von Server-Farmen, die alle an einem zentra-

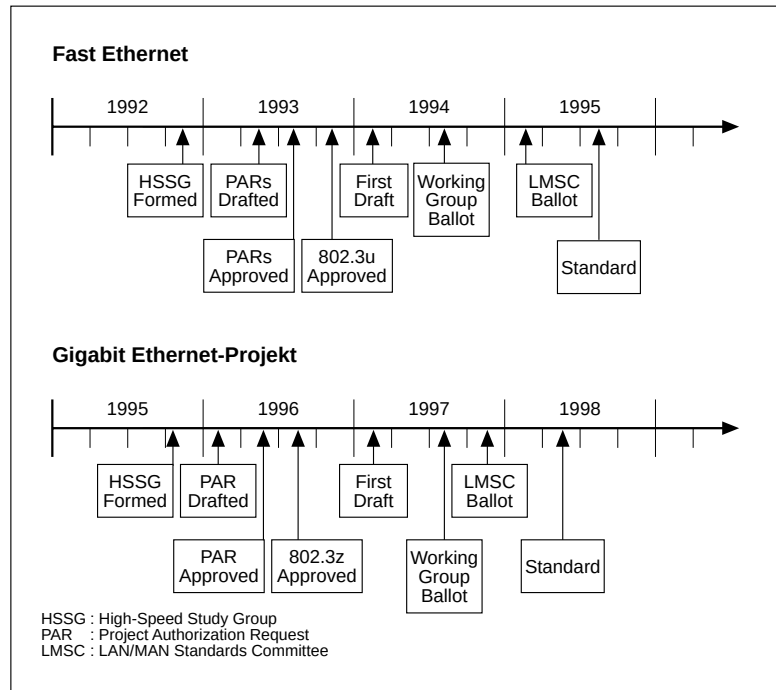
4.7 Gigabit Ethernet

len Hub angeschlossen sind, um konzentrierte Datenzugriffe verfügbar zu machen, wird immer häufiger beim Einsatz und Aufbau von Netzwerkstrukturen eingesetzt. Das Switching-Verfahren im Endgerätebereich mit 10/100-Mbit/s-Ethernet-Karten ist heute bereits ein zwingendes Muß, wenn es um den Aufbau und die Planung von Ethernet-Netzwerken geht. Die Intranet-Anwendungen auf Basis von Java Applets sind ein weiterer Indikator dafür, daß der Bandbreitenbedarf im Endgerätebereich immer größer werden wird.

4.7.3 Technologische Aspekte

Gigabit Ethernet zeichnet sich durch eine Vielzahl von Entwicklungsschritten aus, die bereits aus der herkömmlichen Ethernet-Technik bekannt sind. Am wichtigsten dabei ist, daß die Entwicklung von Gigabit Ethernet auf dem IEEE-802.3z-Standard beruht. 1998 war man kurz vor der Verabschiedung des Standards. In Abbildung 4.35 ist dargestellt, wie sich Fast Ethernet und Gigabit Ethernet entwickelt haben.

Abbildung 4.35
Entwicklung von
Fast Ethernet und
Gigabit Ethernet



4 Netzwerkaufbau und Netzwerktopologien

Um einen vollständigen Überblick zu erhalten, welche Ethernet-Variante zu welchem Standard gehört, ist in der Abbildung 4.36 ein historischer Abriß zu sehen.

Abbildung 4.36
Historischer Überblick der Ethernet-Standards

ETHERNET STANDARD	IEEE 802.3 SPEC SUPPLEMENT	YEAR APPROVED	SPEED
10 BASE5	802.3	1983	10 Mbps
10 BASE2	802.3a	1988	10 Mbps
1 BASE5	802.3c	1988	1 Mbps
10 BASE-T	802.3i	1990	10 Mbps
10 BROAD36	802.3b	1988	10 Mbps
10 BASEF/FOIRL	802.3j	1992	10 Mbps
100 BASE-T	802.3u	1995	100 Mbps
1000 BASE-SX	802.3z	1998	1000 Mbps
1000 BASE-LX			
1000 BASE-T	802.3ab	?	1000 Mbps

Betrachtet man die einzelnen technischen Begebenheiten von Gigabit Ethernet, so stellt man die folgenden Aspekte fest:

Gigabit Ethernet arbeitet Full- und Half-Duplex

Das herkömmliche Ethernet ist für das sogenannte Shared-Media-Verfahren entwickelt. Darunter versteht man, daß sich alle im Ethernet-Netzwerk-Segment angeschlossenen Endgeräte das gemeinsame Übertragungsmedium Kabel teilen müssen. Das heißt, während eine Station gerade dabei ist, Daten zu übertragen, müssen alle anderen Stationen im Segment zuhören. Mit anderen Worten bedeutet dies, daß über das Kabel zu einem Zeitpunkt nur in eine Richtung übertragen werden kann: Entweder werden Daten übertragen oder empfangen, das Endgerät kann zu einem Zeitpunkt entweder Daten versenden oder empfangen. Dieser Vorgang wird auch als Half-Duplex bezeichnet. Die Full-Duplex-Entwicklung war nie Teil einer PHY oder MAC-Ethernet-Spezifikation. Eine Vielzahl von Ereignissen ist jedoch dafür verantwortlich, daß Full-Duplex-Ethernet verwirklicht wurde.

- Die Einführung einer 10Base-T-Verkabelung hat alle Möglichkeiten zur Verfügung gestellt, um getrennte Transmit- und Receive-Kanäle zur Verfügung zu haben. Das ist eine Grundvoraussetzung, die von der ursprünglichen Koaxkabel-Spezifikation für Ethernet nicht geboten werden konnte.

4.7 Gigabit Ethernet

- Die Einführung von Ethernet-Switching hat dazu geführt, daß die Übertragungskanäle nicht mehr mit mehreren Benutzern geteilt, sondern dafür verwendet werden, um zwei Switches oder einen Switch mit einer Netzwerkkarte zu verbinden, und zwar auf Basis einer Punkt-zu-Punkt-Verbindung. Das ist die Grundvoraussetzung für Full-Duplex-Verfahren.

Im Jahre 1992 wurde von der Firma Kalpana zusammen mit einer Vielzahl anderer Hersteller die Möglichkeit geschaffen, einen De-facto-Standard für Full-Duplex-Ethernet über Twisted-Pair-Kabel zu entwickeln. Kalpana ging dabei dazu über, die bestehende MAC-Spezifikation zu nutzen und diese an zwei Stellen anzupassen:

- Ein Paar der Twisted-Pair-Verkabelung (oder ein Glasfaserstrang) wird ausschließlich für die Übertragung und ein Paar ausschließlich für den Empfang von Daten verwendet.
- Es ist kein Carrier-Sense-Verfahren (CRS) notwendig, da der Netzwerkananschluß zur Übertragung und zum Empfang ausschließlich dem Endgerät zugeordnet ist, d.h., der Kabelanschluß ist ausschließlich für die Workstation.
- Collision Detection bzw. Jam-Mechanismen sind nicht notwendig, da Kollisionen nur in einem Shared-Media-Ethernet-Netzwerk auftreten können.

Der Full-Duplex-Mechanismus ist inzwischen für alle Ethernet-Netzwerke verfügbar, die auf Basis einer Twisted-Pair-Verkabelung aufgebaut sind und Switching-Technik verwenden. Das heißt, Full-Duplex ist ohne Switching nicht möglich. An dieser Stelle sei aber auch darauf hingewiesen, daß Ethernet-Switching nicht automatisch Full-Duplex-Möglichkeiten nach sich zieht.

Zur Einführung von Full-Duplex-Mechanismen wurde gegen Ende 1996 der IEEE-802.x-Full-Duplex/Flow-Control-Standard ins Leben gerufen. Hierzu wurden zusätzlich zu den von Kalpana vorgeschlagenen Verfahren weitere Funktionen festgelegt, die im wesentlichen wie folgt festgeschrieben sind:

- Es müssen genau zwei Stationen (DTEs) im LAN auf Basis einer Punkt-zu-Punkt-Verbindung arbeiten. Es kann sich hierbei um eine Switch-Switch-, Switch-Netzwerkkarte- oder Netzwerk-Netzwerk-Verbindung handeln. Das herkömmliche CSMA/CD-Verfahren findet in dieser Form keine Verwendung mehr.
- Beide Endgeräte müssen Full-Duplex-Fähigkeit besitzen. Im Normalfall sollte dies durch Auto-Negotiation von selbst erkannt und eingestellt werden. Manuelle Konfigurationen werden jedoch vom Standard zugelassen.

4 Netzwerkaufbau und Netzwerktopologien

Man sollte sich bei der Auswahl der Netzkomponenten beim Hersteller der Hubs und der Netzwerkkarten danach erkundigen, ob Full-Duplex-Fähigkeit unterstützt wird und wie diese aktiviert werden muß – manuell oder durch Auto-Negotiation.

Flow Control bzw. Flußkontrolle ist in der Kommunikationstechnik immer dann notwendig, wenn zwei Endgeräte mit unterschiedlichen Geschwindigkeiten miteinander kommunizieren müssen. In der Shared-Ethernet-Technologie ist eine eingebaute Flußkontrolle vorhanden. Man muß bei der Kopplung von Ethernet-Netzwerken zwischen Half-Duplex-Flußkontrolle und Full-Duplex-Flußkontrolle unterscheiden.

Ethernet-Netzwerke, die mit Bridges gekoppelt sind oder auf Basis von Switching-Technik aufgebaut werden, besitzen eine eingebaute Methode, um im Half-Duplex-Modus den Datenverkehr zwischen unterschiedlich schnellen Stationen zu kontrollieren. Man nennt dieses eingebaute Konzept »Back Pressure«. Wenn z.B. ein schnell angebundener 1000-Mbit/s-Server Daten zu einer 10-Mbit/s-Station verschickt, dann versucht der Switch, so viele Daten wie möglich zu puffern. Wenn der Switch-Puffer voll ist, dann kann der Switch dem Server signalisieren, daß der Server mit der Datenübertragung aufhören soll. Der Switch kann deshalb eine Kollision mit dem Server verursachen, was den Server dazu veranlaßt aufzuhören. Eine andere Möglichkeit, um die Datenübertragung vorübergehend zu stoppen, besteht darin, daß der Switch den Server-Anschluß-Port als belegt kennzeichnet, was für den Server den Anschein hat, als ob der Switch Daten übertrage.

Für die Full-Duplex-Flußkontrolle wird vom IEEE-802.3x-Standard ein Verfahren für die Flußkontrolle standardisiert. In einer Full-Duplex-Umgebung ist die Verbindung zwischen Server und Switch ein dedizierter Sende- und Empfangskanal. Für den Switch besteht deshalb keine Möglichkeit, eine Kollision zu erzeugen oder den Kanal zu belegen, um den Server von der Datenübertragung abzuhalten. Der Server wird deshalb so lange Daten übertragen, bis der Puffer des Servers überläuft. Ein Switch erzeugt einen sogenannten PAUSE-Frame, der zur datenübertragenden Station geschickt wird. Solange dieser PAUSE-Frame von der empfangenden Station geschickt wird, stoppt der Sender seine Übertragung. Dieser PAUSE-Frame verwendet eine wohldefinierte Multicast-Adresse, die von Bridges und Switches nicht übertragen wird (in Übereinstimmung mit dem 802.1d-Bridging-Standard). Durch den PAUSE-Frame wird somit kein zusätzlicher Datenverkehr verursacht. Betrachtet man sich einen typischen Ablauf, dann sieht dieser in etwa wie folgt aus:

4.7 Gigabit Ethernet

1. Wenn der Server aktiviert wird, dann signalisieren die Server, die Netzwerkkarte und der Switch, daß beide Full-Duplex-fähig sind, und stellen den Übertragungsmodus auf Full-Duplex ein.
2. Die Auto-Negotiation ist ebenfalls dafür verantwortlich, daß beide Endgeräte Flußkontroll-fähig sind.
3. Der Server beginnt die Datenübertragung auf dem Transmit-Kanal, der für den Switch der Receive-Kanal ist.
4. Der Switch empfängt die Datenpakete und übergibt sie an den 10-Mbit/s-Client – jedoch mit einer wesentlich langsameren Geschwindigkeit.
5. Wenn der interne Puffer des Switch fast voll ist, dann überträgt der Switch einen PAUSE-Frame zur Netzwerkkarte des Servers über den Transmit-Kanal (dieser entspricht dem Receive-Kanal des Servers). Dies veranlaßt den Server, mit der Datenübertragung aufzuhören.
6. Der Switch leert daraufhin seinen Puffer durch die Übertragung der Daten zum Client, bis der Puffer wieder genügend Platz bietet, um neue Daten aufnehmen zu können.
7. Wenn der Puffer fast leer ist, hört der Switch mit der Übertragung der PAUSE-Frames auf, damit der Server mit der Übertragung weitermachen kann.

Solange das Gigabit-Ethernet-Netzwerk im Half-Duplex-Modus betrieben wird, bleibt das CSMA/CD-Zugriffsverfahren erhalten. Für die ersten Produkte der Gigabit-Technologie wird derzeit noch die Glasfasertechnik genutzt, zumal hierfür auch die IEEE-802.3z-Standards spezifiziert sind. Die Standardisierung für Cat.-5-Kabel ist abgeschlossen. Diese Standardisierung wird unter der Bezeichnung IEEE 802.3ab geführt. Entsprechende Produkte sind in Entwicklung bzw. von einzelnen Herstellern bereits verfügbar.

Funktionale Elemente der Gigabit-Ethernet-Technologie

- Der IEEE-802.3z-Gigabit-Ethernet-Standard spezifiziert mit 1000Base-SX (Short-Wavelength 850 nm Laser) und 1000Base-LX (Long Wavelength 1300 nm) zwei Varianten, für die Lichtwellenleiter-Übertragung: Während Long-Wavelength sowohl mit Monomode als auch Multimode-Fasern genutzt werden können, beschränkt sich der Einsatz von Short-Wavelength-Laser auf die Multimode-Faser. Aus der nachfolgenden Tabelle ist zu ersehen, welcher Standard welche Spezifikationen unterstützt:

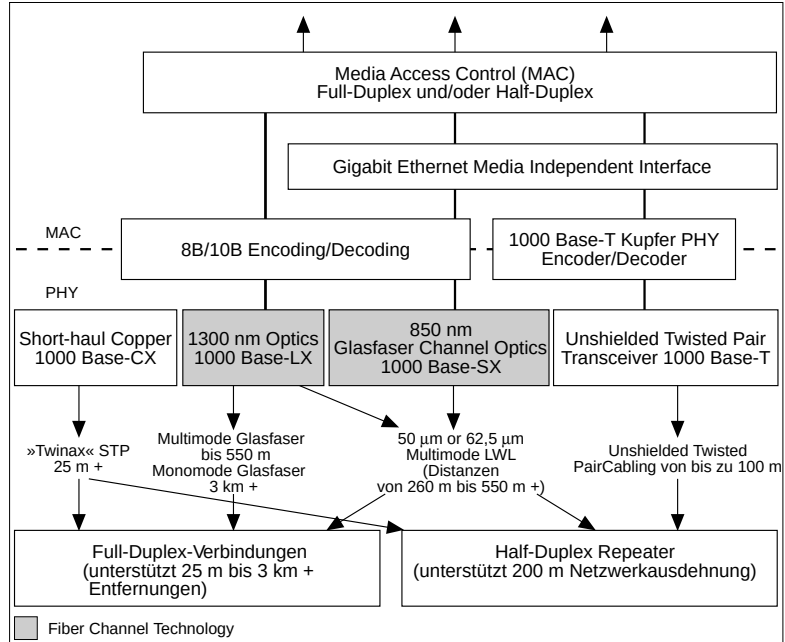
4 Netzwerkaufbau und Netzwerktopologien

Spezifikation	Lasertyp	Fasertyp	Kern	max. Distanz
1000Base-SX	850nm	Multimode	62,5 μm	260 m
1000Base-SX	850nm	Multimode	50 μm	440 m
1000Base-LX	1300nm	Multimode	62,5 μm	550 m
1000Base-LX	1300nm	Multimode	50 μm	550 m
1000Base-LX	1300nm	Monomode	9 μm	3 km

- Aus dieser Tabelle ist zu ersehen, daß Gigabit Ethernet Multi-mode-Gradientenfasern mit einem Kerndurchmesser von 62,5 μm und 50 μm unterstützt, die man bereits in der vertikalen Gebäude- und Campus-Verkabelung vorfinden kann bzw. hierfür benutzt. Zu erwähnen ist dabei auch, daß die 50- μm -Glasfaser eine wesentlich bessere Bandbreiten-Charakteristik besitzt als die 62,5- μm -Glasfaser. Deshalb eignet sich die 50- μm -Glasfaser für größere Entfernungen.

In Abbildung 4.37 sind alle für Gigabit Ethernet notwendigen Definitionen zusammengefaßt und dargestellt.

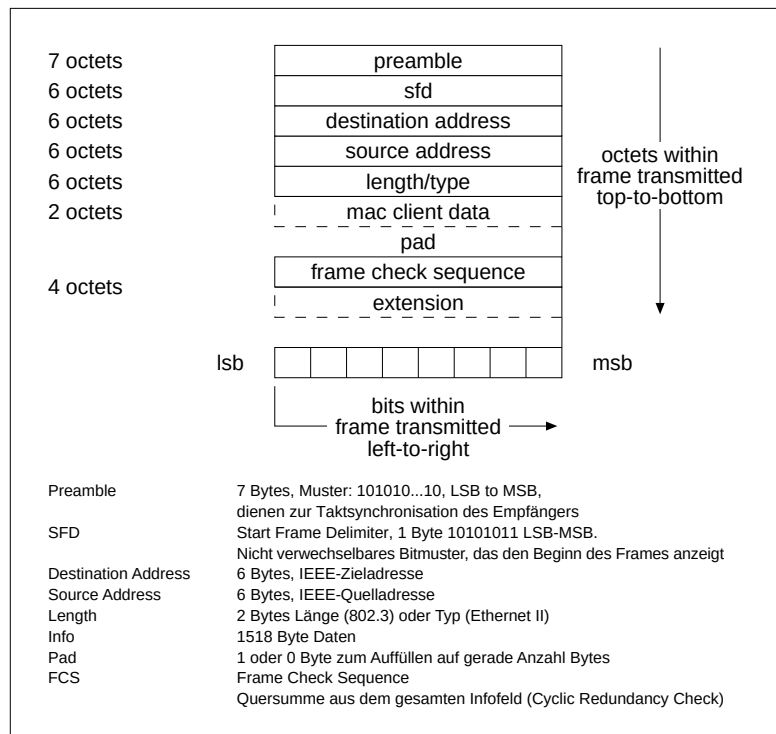
Abbildung 4.37
Die Gigabit-Ethernet-Technologie



4.7 Gigabit Ethernet

Aus Abbildung 4.37 ist auch noch zu erkennen, daß es einen Standard 1000Base-CX gibt, um Gigabit Ethernet über Twinax-(Shielded/Unshielded)-Kabel zu implementieren. Die erlaubten Distanzen sind dabei nicht mehr als 25 Meter, was natürlich für eine herkömmliche Netzwerkumgebung viel zu kurz ist. Für den Anschluß von Endgeräten ist diese Längenbeschränkung nicht akzeptabel. Wie später noch zu sehen sein wird, beträgt die Längenrestriktion beim Einsatz von standardisierter Twisted-Pair-Verkabelung 100 Meter. Der Standard IEEE 802.3ab kümmert sich um die Durchsetzung der notwendigen Spezifikationen, um bei einer herkömmlichen Cat.-5-Verkabelung die 100 Meter Längenbeschränkung einhalten zu können.

Abbildung 4.38
MAC Frame für
Ethernet



Gigabit Ethernet Media Access Frames

Die Struktur der 1000-Mbit/s-Ethernet-Frames sind identisch mit dem Frame-Aufbau, so wie dieser aus der klassischen Ethernet-Technologie bekannt ist und eingesetzt wird. In Abbildung 4.38 ist der Aufbau eines Ethernet-Frame dargestellt.

4 Netzwerkaufbau und Netzwerktopologien

Kollisionsverfahren

In der Abbildung 4.38 ist zu erkennen, daß ein Gigabit Ethernet Frame nicht anders aufgebaut ist als ein 10-Mbit/s- oder 100-Mbit/s-Frame. Betrachtet man sich die Anforderungen für das Kollisionsverfahren, dann sind folgende Aspekte zu berücksichtigen, damit dieses Verfahren funktioniert:

- Jede Station muß eine Kollision beim Aussenden des kleinsten Paketes erkennen.
- Die Zeit, die ein Paket braucht, um von einem Netzwerkkende bis zum anderen Netzwerkkende und zurück zu gelangen, nennt man die Signallaufzeit (Round Trip Delay).
- Die Signallaufzeit ist von der Paketgröße und von der Übertragungsgeschwindigkeit (Mbit/s oder Gbit/s) abhängig.
- Die maximale Signallaufzeit von Gigabit Ethernet schränkt die Ausdehnung des Netzes auf ein paar Meter ein, wenn man sich auch noch die Berechnung der Collision Domain betrachtet:
 - Kleinste Frame-Größe:
 $64 \text{ Byte} = 512 \text{ Bit}$
 - Übertragungsgeschwindigkeit von 10 Mbit/s = $10 \cdot 10^6 \text{ Bit/s}$
 - Wann ist ein Frame vollständig versendet?
 $(512 \text{ Bit} \cdot s) / (10 \cdot 10^6 \text{ Bit}) = 51,2 \cdot 10^{-6} \text{ s}$
 - Ausbreitung mit zwei Drittel der Lichtgeschwindigkeit =
 200.000 km/s
 - Ausbreitungslänge des kleinsten Frame =
 $(200.000 \text{ km} \cdot 51,2 \cdot 10^{-6} \text{ s}) / s = 10,24 \text{ km}$
 - Maximale Collision-Domain-Größe = $10,24 \text{ km} / 2 = 5,12 \text{ km}$

In kollisionsbehafteten Gigabit-Ethernet-Segmenten ist die daraus resultierende Minimallänge eines Ethernet-Pakets viel zu klein, um Kollisionen zu erkennen, es sei denn, man würde die maximale Ausdehnung von Gigabit Ethernet auf 10 Meter beschränken. Dies entspricht aber überhaupt nicht den normalen Vorstellungen vom Aufbau flächendeckender Netzwerke. Man muß sich an dieser Stelle auch noch vor Augen halten, daß sich die elektrischen oder optischen Pulse, die Datenbits auf einem Kupferkabel oder einer Glasfaser repräsentieren, immer konstant abhängig von der Qualität des Kupfer- oder Glasfaserkabels mit Geschwindigkeiten von zwei Drittel bis drei Viertel der Lichtgeschwindigkeit ausbreiten. Diese Geschwindigkeit hat überhaupt nichts mit der Datenrate (Übertragungsgeschwindigkeit) zu tun und hängt ausschließlich vom eingesetzten Material ab. Unter diesem Aspekt ist die Glasfaser nicht wesentlich schneller als Kupfer, da die Laufzeiten pro Meter nur geringfügige Unterschiede aufweisen. Die Glasfaser bietet jedoch den Vorteil, mit sehr hohen Frequenzen zu übertragen.

4.7 Gigabit Ethernet

Überträgt man diese Problematik auf Gigabit Ethernet, dann ist man bei einem Netzwerkdurchmesser von über zehn Metern und einem kleinen Ethernet-Paket bereits in der Situation, daß das Ethernet-Paket schon vollständig den Netzwerk-Kontroller verlassen hat, bevor das erste gesendete Bit überhaupt das Ende der Leitung erreicht. Das klassische Kollisionsmuster kann somit nicht empfangen und deshalb zur Erkennung von Kollisionen nicht eingesetzt werden. Man muß sich deshalb etwas anderes überlegen, um dennoch damit arbeiten zu können, ohne sich an die 10-Meter-Restriktion halten zu müssen. Für Gigabit Ethernet wurden deshalb die Verfahren Frame Extension und Burst Frames eingeführt.

Frame Extension

Das oben geschilderte Problem wird gelöst, indem man jede Station dazu zwingt, eine Mindestzeit zu senden – und zwar so lange wie notwendig, bis an jeder Stelle des Netzwerksegments ausreichend Bits angekommen sind, um eine Kollision erkennen zu können. Da für dieses Verfahren aber nicht immer ausreichend Nutzdaten zur Verfügung stehen, werden für den Rest der dafür erforderlichen Zeit einfach unsinnige Daten übertragen, die bereits nicht mehr zum ursprünglichen Datenpaket gehören. Berechnungen zufolge müssen diese Extensions, besser gesagt Frame Extensions (auch Carrier Extensions genannt), immer dann eingesetzt werden, wenn ein Datenpaket kleiner als 512 Byte ist. Somit wird auch das Kollisionsfenster auf 512 Byte erweitert. Man verwendet für diese Extensions auf alle Fälle spezielle Symbole, die nicht mit Daten oder mit Frame-Informationen verwechselt werden können. Einen kleinen Nachteil hat das Ganze jedoch: Durch die zusätzliche Übertragung von Frame Extensions wird die Nutzdatenübertragung sehr stark beeinträchtigt, sofern immer nur Datenpakete, die kleiner sind als 512 Byte, übertragen werden. Bei größeren Datenpaketen wird dieser Nachteil jedoch wieder ausgeglichen. Um den Verlust der effektiven Datenrate jedoch noch besser in den Griff zu bekommen, hat man das sogenannte Burst-Frame-Verfahren eingeführt.

Burst Frames

Das Burst-Frame-Verfahren erlaubt dem Gigabit-Ethernet-Standard beim Einsatz von 1000 Mbit/s im Half-Duplex-Modus einer Station, mehrere Frames zu verketteten und in einem sogenannten Burst zu verschicken. Hat eine Station bereits Zugriff auf das Netzwerk, dann kann die Station bis zu einer Zeitspanne von 65.000 Bit so viele Pakete hintereinander starten, wie sie will, und anschließend noch das angefangene Paket zu Ende senden. Auf diese Art und Weise ergibt

4 Netzwerkaufbau und Netzwerktopologien

sich eine maximale Burst-Länge von 8192 Byte zuzüglich der 1518 Byte; das entspricht immerhin sechs Ethernet-Paketen mit maximaler Länge. Erst dann muß die Station das Medium wieder freigeben.

Die nachfolgende Tabelle stellt für alle drei Ethernet-Standards die wichtigsten Parameter gegenüber:

	10 Mbit/s	100 Mbit/s	1000 Mbit/s
Slottime (Bit Times)	512	512	4096
Interframe-Gap (µs)	9,6	0,96	0,096
maxFrameSize (Bytes)	1518	1518	1518
minFrameSize (Bytes)	64	64	64
ExtendedSize (Bits)	0	0	448
BurstLength (Bits)	0	0	65.536 (=8192 Byte)

Gigabit Ethernet Independent Interface (GMII)

Der IEEE-802.3z-Standard definiert zwischen dem Media Access Controller (MAC) und dem Physical Layer Controller (PHY) eine neue und erweiterte Schnittstelle, die als GMII (Gigabit Media Independent Interface) bezeichnet wird. Ähnlich wie die MII-Schnittstelle für Fast Ethernet dient die GMII-Schnittstelle nicht nur zum Anschluß unterschiedlicher Ethernet-Medien von 10 bis 1000 Mbit/s, sondern auch zur automatischen Erkennung des Mediums und zum Austausch von Daten über den Zustand und die Eigenschaften der aktuellen Verbindung. Hierzu zählen auch Statistiken über den Datenverkehr zwischen der MAC und PHY.

4.7.4

Einsatzbereich für Gigabit Ethernet

Gigabit Ethernet ist nicht dafür konzipiert worden, um nur noch mit 1000 Mbit/s Datenübertragungen durchführen zu können – nach dem Motto: Je schneller, desto besser. Man sollte sich sehr genau überlegen, ob der Einsatz von Gigabit Ethernet sinnvoll ist oder nicht. Betrachtet man sich die in Frage kommenden Einsatzbereiche (aus heutiger Sichtweise), dann kommt man auf folgende Varianten:

- Verbindung von 10/100-Mbit/s-Switches über einen 1000-Mbit/s-Uplink, um zwischen den Switches sehr hohe Datenraten übertragen zu können.
- Anbindung von mit 10/100 Mbit/s angebundenen Clients an Server, die selbst über einen 1000-Mbit/s-Anschluß verfügen. Auf diese Art und Weise können große Datenmengen zwischen den Servern und den Workstations transportiert werden, ohne daß es sofort zu Engpässen kommt.

4.7 Gigabit Ethernet

- Wenn es die Anforderungen an den Client notwendig machen, können auch diese mit einem 1000-Mbit/s-Anschluß versehen werden. Dies kommt in der Regel dann in Frage, wenn ein sehr hoher Bandbreitenbedarf existiert, da man z.B. CAD/CAM, medizinische Image-Verarbeitung (z.B. Röntgenbilder über das Netz transportieren) oder Publishing-Anwendungen nutzen will bzw. muß.

Vorteile von Gigabit Ethernet

Bei Gigabit Ethernet kann man von einer sehr einfachen und dennoch geradlinigen Entwicklung sprechen, nicht zuletzt, weil man sich viele Anregungen auf dem bereits bekannten und bewährtem Ethernet holen konnte. Die hohen Bandbreiten können genau dort eingesetzt werden, wo diese auch benötigt werden. Es gibt deshalb auch keine Probleme, dieses neue System in existierende Netzwerkstrukturen zu integrieren. Da auf bereits Bekanntes aus dem Ethernet-Bereich zurückgegriffen werden kann, ist der Aufwand für die Ausbildung der Netzwerkadministratoren bzw. Netzanwender minimal. Nicht vergessen werden darf, daß die Anschaffungs- und Unterhaltungskosten für die aktiven Komponenten sehr gering sind. Vergleicht man die derzeit verfügbaren High-Speed-LANs in ihren wichtigsten Funktionen miteinander, dann kommt man zu folgender Tabelle:

Abbildung 4.39
High-Speed-LANs
im Vergleich

Funktionen	Gigabit Ethernet	Fast Ethernet	ATM	FDDI
IP Kompatibel	Ja	Ja	RFC 1577 oder LANE; MPOA	Ja
Ethernet Pakete	Ja	Ja	Benötigte LANE	Ja, 802.1h
Multimediafähig	Ja	Ja	Ja, aber Änderungen in den Applikationen nötig	Ja
Quality of Service	Ja, mit RSVP und 802.1Q/p	Ja, mit RSVP und 802.1Q/p	Zuordnung von 802.1Q/p zu SVC	Ja, mit und 802.1Q/p Synchronous Bandwidth Allocation oder RSVP und 802.1Q/p
VLANs mit 802.1Q/p	Ja	Ja	Benötigte Zuordnung von 802.1Q VLANs zu LANE	Ja

Die Diskussion über High-Speed-LANs wirft die Frage auf, inwieweit die Entscheidung zugunsten von ATM-Netzwerken fallen kann, zumal Gigabit Ethernet sich durchsetzt und dieser Trend auch nicht aufzuhalten ist.

4 Netzwerkaufbau und Netzwerktopologien

Für ATM ergeben sich die nachfolgend aufgeführten Vorteile:

- ATM ist sehr gut für die LAN- und WAN-Integration geeignet.
- Seine Merkmale bei der Prioritätssteuerung und Dienstqualität (Quality of Service – QoS) qualifizieren ATM, um Video, Sprache und Daten gleichzeitig übertragen zu können.
- Die ATM-Funktionalitäten bieten einen sehr großen Nutzen für Anwender, die isochrone und Echtzeit-Kommunikation benötigen und implementieren wollen.

Die Nachteile von ATM sind vor allem in folgenden Punkten zu sehen:

- ATM ist sehr komplex für bestehende Anwendungen und Protokolle.
- Der Schulungsaufwand für Netzwerk-Administratoren und Anwender ist sehr hoch.
- Durch die Notwendigkeit, LANE einzusetzen, wird ATM im Prinzip zu einem »weiteren LAN«.
- ATM nur wegen der hohen Bandbreite zu kaufen, sollte nicht die alleinige Entscheidungsgrundlage sein.
- Für den Einsatz von ATM sollten auch noch weitere wichtige Gründe vorliegen, die nicht von Fast Ethernet bzw. Gigabit Ethernet entkräftet werden können.
- ATM muß sichtbar für die Anwendungen werden.
- Der Einsatz von Sprachübertragung über ATM im LAN stößt derzeit noch auf geringes Interesse.

Wenn man sich schon die Vor- und Nachteile von ATM näher betrachtet, dann sollte man sich auch die Vor- und Nachteile von Gigabit Ethernet etwas näher betrachten.

Die Nachteile von Gigabit Ethernet sind in den folgenden Punkten zu sehen:

- Bei Gigabit Ethernet handelt es sich um eine reine LAN-Technologie.
- Für vehemente Token-Ring-Anwender bietet auch Gigabit Ethernet keine besondere Attraktivität.

Zu den Vorteilen von Gigabit Ethernet zählen unter anderem:

- Gigabit Ethernet ist die optimale Lösung für hohe Leistungen bei geringen Kosten und zugleich kompatibel mit Ethernet und Fast Ethernet.
- Gigabit Ethernet garantiert Investitionsschutz für Komponenten, Betriebssysteme und Anwendungen.
- Gigabit Ethernet bietet Möglichkeiten des IP-Switching.

4.7 Gigabit Ethernet

- Quality of Service / Class of Service
 - Resource Reservation Protocol (RSVP)
 - IEEE 802.1p Priority Functions
 - IEEE-802.3x-Flußkontrolle auf der Verbindungsebene
 - Prioritätssteuerung für IP Datenströme

4.7.5 Gigabit-Ethernet-Migration

Für die Umstellung eines Netzwerks auf Gigabit Ethernet bei bereits vorhandenen Infrastrukturen lassen sich im wesentlichen fünf Szenarien aufführen, nach denen eine Migration sinnvoll ist. Werden hingegen neue Netzwerkinfrastrukturen geplant, dann sollten die Möglichkeiten von Gigabit Ethernet von Anfang an in Betracht gezogen werden.

Für die Migrationspfade kommen in Frage:

- *Upgrade Switch-zu-Switch-Verbindungen*
Damit wird erreicht, daß man 1000 Mbit/s Übertragungskapazität zwischen Switch-Systemen aufbauen kann.
- *Upgrade Switch-zu-Server-Verbindungen*
Hiermit erreicht man die enorm leistungsfähige Anbindung von Servern, um schnellen Zugriff auf Anwendungen und andere Dienste zu erhalten.
- *Upgrade Switched-Fast-Ethernet-Backbone*
Um einen noch schnelleren Backbone zu erhalten, wird die Fast-Ethernet-Backbone-Komponente ersetzt und gegen eine Gigabit-Ethernet-Komponente getauscht.
- *Upgrade Shared-FDDI-Backbone*
Wenn man feststellt, daß der bestehende Shared FDDI-Backbone nicht mehr leistungsfähig genug ist, kann man ebenfalls Überlegungen anstellen, wie man einen Umstieg auf Gigabit Ethernet durchführt.
- *Upgrade High-Performance-Arbeitsplätze*
Wenn die herkömmlichen Übertragungsraten für die Arbeitsplätze nicht mehr ausreichend sind, dann besteht mit Gigabit Ethernet die Möglichkeit, einen sehr schnellen und leistungsfähigen Netzanschluß für die Arbeitsplätze im Netzwerk zu schaffen.

Aufgrund der steigenden Nachfragen für Gigabit-Ethernet-Netzwerke werde ich Ihnen in Kapitel 5 einige Einzelfälle schildern, um zu zeigen, wie in bestimmten Konstellationen Gigabit Ethernet in Verbindung mit anderen Netzwerktechnologien sinnvoll eingesetzt werden kann.

4 Netzwerkaufbau und Netzwerktopologien

Zuvor will ich Ihnen jedoch noch in eine andere technologische Entwicklung Einblick geben. Wenn man sich die letzten Ausführungen etwas genauer betrachtet, dann stellt man fest, daß die älteste Technologie, also Ethernet, stetig und permanent weiterentwickelt wurde, wohingegen auf dem Gebiet der Token-Ring-Technologie keinerlei Fortschritte festgestellt werden können. Es scheint so, als wolle man sich auf der schon etwas in die Jahre gekommenen 16-Mbit/s-Variante ausruhen. Wenn man sich jedoch mit einzelnen Hardware-Herstellern eingehender unterhält, dann erfährt man, daß man auch den Token-Ring in einer 100 Mbit/s- und einer 1000-Mbit/s-Variante zur Verfügung stellen will. Der Nachteil dabei ist nur, daß es die 100 Mbit/s und 1000 Mbit/s für Ethernet bereits gibt und für den Token-Ring diesbezüglich keine genauen Erscheinungstermine bekannt sind. Da man jedoch plant, diese Technik noch vor der Jahrtausendwende verfügbar zu machen, will ich Ihnen im nächsten Abschnitt noch die grundlegenden Aspekte der High-Speed-Token-Ring-Variante aufzeigen, soweit dies zum Zeitpunkt der Erstellung dieses Buches möglich ist. Es sei bereits jetzt erwähnt, daß in allen weiteren Ausführungen HSTR als Abkürzung für High-Speed-Token-Ring steht.

4.8 High-Speed-Token-Ring (HSTR)

Seit der Einführung der Token-Ring-Technologie durch die IBM wurde eine Vielzahl von Token-Ring-Netzwerken installiert. War zu Beginn gerade mal 4-Mbit/s-Datenübertragung möglich, wurde durch die Weiterentwicklung von Token-Ring 16-Mbit/s-Datenübertragung realisierbar. Wie aus den vorherigen Ausführungen zu ersehen ist, steigen die Anforderungen für die Leistungsfähigkeit von Netzwerken immer mehr, so daß auch der Token-Ring davor nicht haltmachen kann. IBM hat zwar etwas länger benötigt, um die Notwendigkeit für einen schnelleren Token-Ring zu erkennen – vor allem unter Berücksichtigung der Weiterentwicklung auf dem Gebiet der Ethernet-Technologie –, aber inzwischen sind alle hierfür notwendigen Spezifikationen und zum Teil auch bereits Produkte verfügbar. Um die Investitionen bestehender Token-Ring-Netzwerke zu schützen und zugleich die notwendigen höheren Übertragungsgeschwindigkeiten bzw. einen besseren Durchsatz im Gesamtnetzwerk gewährleisten zu können, stellt IBM zwei wesentliche Migrationsstrategien vor:

- Durch die Einführung der Switching-Technologie kann bereits eine wesentliche Geschwindigkeitserhöhung bis zum Arbeitsplatz erreicht werden, wenn man eine entsprechende Rekonfiguration des Netzwerks durchführt.

4.8 High-Speed-Token-Ring (HSTR)

- Durch die Einführung von High-Speed-Token-Ring kann eine sehr schnelle Anbindung der Server an das Netzwerk bzw. der Aufbau eines High-Speed-Backbone realisiert werden.

Als Netzwerkverantwortlicher ist man im Prinzip immer gezwungen, ein Auge auf die derzeit im Einsatz befindliche Technologie und die eingesetzten Lösungen zu werfen, wohingegen sich das andere Auge auf zukünftige Probleme und Technologien konzentriert. Es ergeben sich dabei im wesentlichen die immer wiederkehrenden Fragen: Wie wird sich die heutige Netzwerktechnologie ändern? Welche Planungen müssen durchgeführt werden, um eine Umgebung zu erhalten, in der die Netzwerkkapazitäten langsamer anwachsen und dennoch bequem die Unternehmensanforderungen erfüllt werden? Es müssen Pläne erstellt werden, um den Netzwerkanforderungen immer gerecht werden zu können, vor allem dann, wenn Netzwerkanpassungen durchzuführen sind.

In den frühen 80er Jahren hat IBM damit begonnen, mit der Token-Ring-Netzwerk-Technologie ein robustes und effizient arbeitendes Netzwerk einzuführen. Im Vergleich zur damals bereits weit verbreiteten Ethernet-Technologie bot Token-Ring Sicherheitsmechanismen, die anderweitig nicht erfüllt werden konnten. Zu diesen wesentlichen Eigenschaften gehören:

- Endgeräte führen eine Vielzahl von sogenannten Pre-Insertion-Prüfungen durch, bevor diese aktiv in den Token-Ring eingebunden werden. Diese Prüfung betrifft die Elektronik und das Anschlußkabel. Sollten bei diesen Tests Fehler festgestellt werden, wird das Endgerät in der Regel nicht in den Token-Ring eingebunden.
- Jede Station pflegt Informationen über die aktive Vorgängerstation, die sogenannte Upstream-Neighbor-Adresse der Station. Über diese Station wird auch Protokoll darüber geführt, wie viele Pakete von dieser Station geschickt worden, und wie viele davon fehlerhaft gewesen sind. Wenn die Anzahl der fehlerhaften Pakete einen gesetzten Schwellenwert überschreiten, werden entsprechende Nachrichten generiert, die von Netzwerkmanagement-Stationen ausgewertet werden können. Treten sogenannte Hard Errors auf, die von Fehlfunktionen in der Workstation verursacht werden, dann werden spezielle Datenpakete erzeugt, die dazu beitragen, daß sich die Station mit der Fehlfunktion von selbst vom Ring nimmt; der Token-Ring besitzt eine Selbstheilungsfunktion.

Der Zugriff auf den Token-Ring erfolgt mit einem Zugriffsverfahren, das man als »fair« bezeichnet. Dabei sind alle Stationen im Prinzip gleichberechtigt. Ebenso wird durch die Position im Token-Ring kein zusätzlicher Vorteil erreicht. Da der Zugriff auf das Netz sehr

4 Netzwerkaufbau und Netzwerktopologien

kontrolliert erfolgt, treten keine Kollisionen auf, und man kann den Token-Ring mit nahezu 100 % Auslastung betreiben.

- Für spezielle Nachrichtenübermittlungen und/oder Endgeräte (z.B. Bridges) ist es möglich, einen höheren Prioritätszugang zu erzeugen; dadurch kann der Gesamtdurchsatz im Netzwerk erhöht werden.
- Das Source-Routing-Verfahren und die damit verbundenen Source Routing Bridges erlauben den Einsatz mehrerer und parallel gekoppelter Source Routing Bridges, wobei die Zuverlässigkeit und Verfügbarkeit sowie die Performance erhöht werden.
- Der Token-Ring war als Gegenpol zu Ethernet entwickelt worden, um alle negativen Effekte von Ethernet vermeiden zu können. Einzelne Ringe können durch den Einsatz entsprechender Verkabelungskomponenten mehrere Kilometer Ausdehnung haben; es lassen sich aber ebenso kleine Büronetzwerke damit aufbauen. Es gibt auch keine Abhängigkeit zwischen der Ringgröße und der minimalen Paketgröße (vergleiche hierzu die Abhängigkeiten bei Ethernet), so daß das sogenannte Padding von Datenpaketen nicht notwendig ist.

Seit Einführung der Token-Ring-Technologie hat sich für Anwender und Netzbetreiber eine Vielzahl von Änderungen bzw. Neuerungen ergeben, die von allen renommierten Herstellern für Token-Ring-Produkte angeboten wurden bzw. immer noch werden. So haben sich in den letzten fünf Jahren zum Beispiel wichtige Änderungen auf folgenden Gebieten ergeben:

- Von IBM wurde der Token-Ring-Chip in der fünften Generation entwickelt
- Token-Ring für PCMCIA-Karten
- Token-Ring für PCI-Bus
- Token-Ring mit der sogenannten Wake-on-LAN-Technologie
- Token-Ring Switching
- Dedicated Token-Ring (d.h. Token-Ring im Full-Duplex-Modus)
- DMI und SNMP für Token-Ring-Adapter (zum besseren Netzwerkmanagement)
- Zahlreiche Performance-Verbesserungen und Vereinfachungen bei der Installation der Token-Ring-Adapter und Komponenten

Es ist vorstellbar, daß der vollständige Ersatz einer bestehenden LAN-Technologie sehr teuer werden kann, so daß jedes Unternehmen erst einmal untersucht bzw. untersuchen läßt, wie eine Migration des Netzwerks auf eine schnellere Topologie realisiert werden kann und in welchen Phasen dies geschehen soll. Bei erster Betrachtung könnte eine Migrationsstrategie wie folgt aussehen:

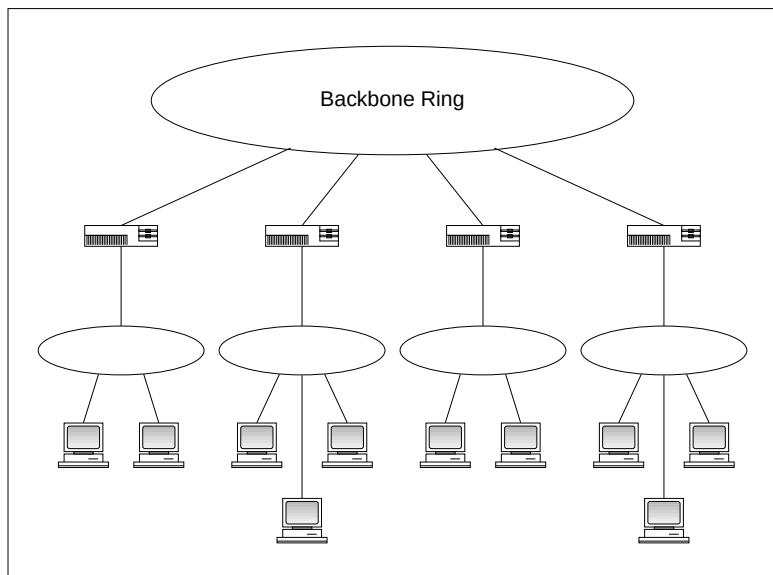
4.8 High-Speed-Token-Ring (HSTR)

- Man verwendet bestehende Technologie und nutzt Switching und Workgroup-Segmentierung.
- Man versucht, Schlüsselemente im Netzwerk über High-Speed-Verbindungen anzuschließen. Zu diesen Anschlußtechniken gehören TokenPipe und Multi-Link.
- Einsatz von High-Speed-Token-Ring auf Basis von 100 Mbit/s (später vielleicht auch 1 Gbit/s).

4.8.1 Switching und Workgroup-Segmentierung

Es wird später noch zu sehen sein, daß ein klassisches Netzwerk auf Basis einer Backbone-Struktur fast immer so aussehen wird, wie dies in Abbildung 4.40 dargestellt ist. Die Kopplung der einzelnen Abteilungsnetze zu einem Gesamtnetzwerk über den Backbone erfolgt über Bridges bzw. Router. Es ist sehr leicht einzusehen, daß eine zentrale Kommunikation über einen herkömmlichen 16-Mbit/s-Token-Ring-Backbone sehr schnell am »Ende« sein kann, da die Anforderungen der Abteilungsnetze derart wachsen, daß diese nicht mehr ausreichend schnell über den Backbone transportiert werden können. Stellt man sich jetzt noch vor, daß der Backbone nicht nur zur Zusammenführung der Etagenetzwerke dient, sondern auch noch die zentralen Server-Systeme im Backbone installiert sind, dann werden die Anforderungen an die Übertragungsgeschwindigkeit noch größer.

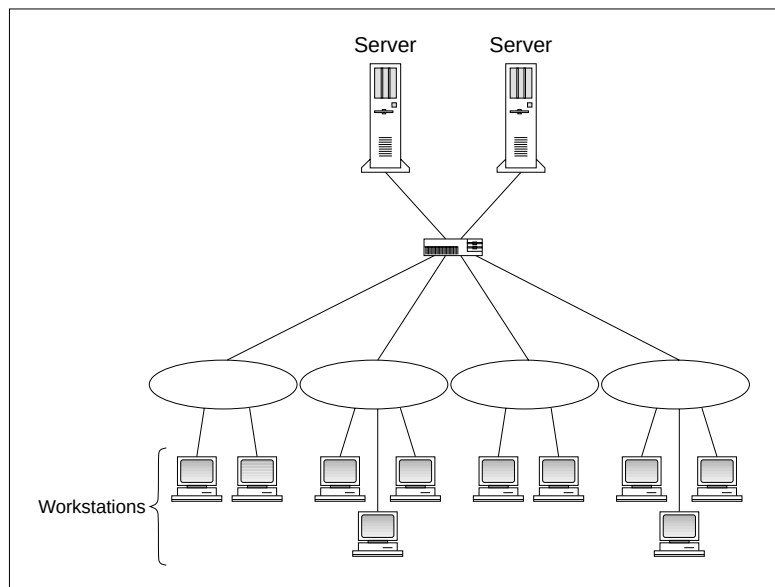
Abbildung 4.40
Klassischer Token-
Ring-Backbone



4 Netzwerkaufbau und Netzwerktopologien

Den ersten Performance-Sprung kann man erzielen, wenn man den zentralen Backbone durch einen Switch ersetzt. Das Netzwerk sieht dann in etwa wie in Abbildung 4.41 aus. Es werden aber nicht nur die einzelnen Netze über jeweils einen eigenen Switch-Port angeschlossen, sondern man erhöht die Leistungsfähigkeit auch noch dadurch, daß man die einzelnen Server an jeweils einen eigenen Switch-Port anschließt. Dadurch stehen für jeden Server jeweils 16 Mbit/s zur Verfügung; wenn zusätzlich im Full-Duplex-Verfahren gearbeitet wird, dann sind dies immerhin schon 32 Mbit/s.

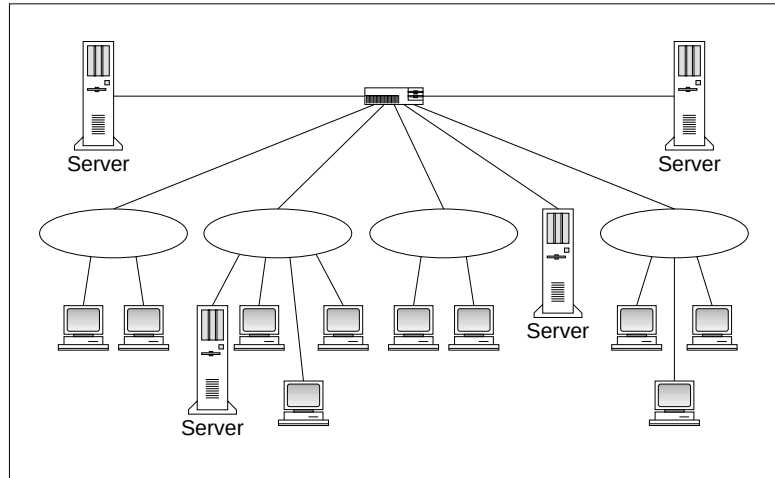
Abbildung 4.41
Switching Backbone im Token-Ring



Eine andere Konstellation tritt auf, wenn sich die zentralen Server-Dienste nicht unbedingt sinnvoll in einen zentralen Backbone integrieren lassen, weil im Vergleich mit einer direkten Integration des oder der Server in den eigenen Etagen-Token-Ring dem Anwender dadurch Performance-Nachteile entstehen würden. Auf diese Art und Weise erfolgt eine Aufteilung des Gesamtnetzwerks in sogenannte Workgroup-Netzwerke, da jedes einzelne Workgroup-Netzwerk ihre eigenen Server-Dienste integriert hat oder auch Peer-to-peer-Netzwerkfunktionen bereitstellen kann. In Abbildung 4.42 ist aufgezeigt, wie man sich eine Mischung aus Backbone und Switch in Verbindung mit einer Workgroup-Segmentierung vorstellen kann.

4.8 High-Speed-Token-Ring (HSTR)

Abbildung 4.42
Backbone Swit-
ching und Work-
group-Segmentie-
rung



Das Ganze kann dann auch noch in Kombination auftreten, so daß man nicht nur einen zentralen Switch einsetzt, sondern aufgrund notwendiger Randbedingungen mehrere Switch-Komponenten einsetzt, die miteinander kaskadiert sind.

4.8.2 TokenPipe und Multi-Link

Es gibt bei den heutigen Netzwerkanforderungen häufig die Situation, daß die oben aufgeführten Mechanismen zur Erhöhung der Performance nicht ausreichend sind. In diesem Fall können das TokenPipe-Prinzip oder das Multi-Link-Verfahren Abhilfe schaffen. Dabei sind die beiden Verfahren hauptsächlich für den folgenden Einsatz geplant:

- TokenPipe für die Switch-Switch-Kopplung
- Multi-Link für die Anbindung leistungsstarker Server

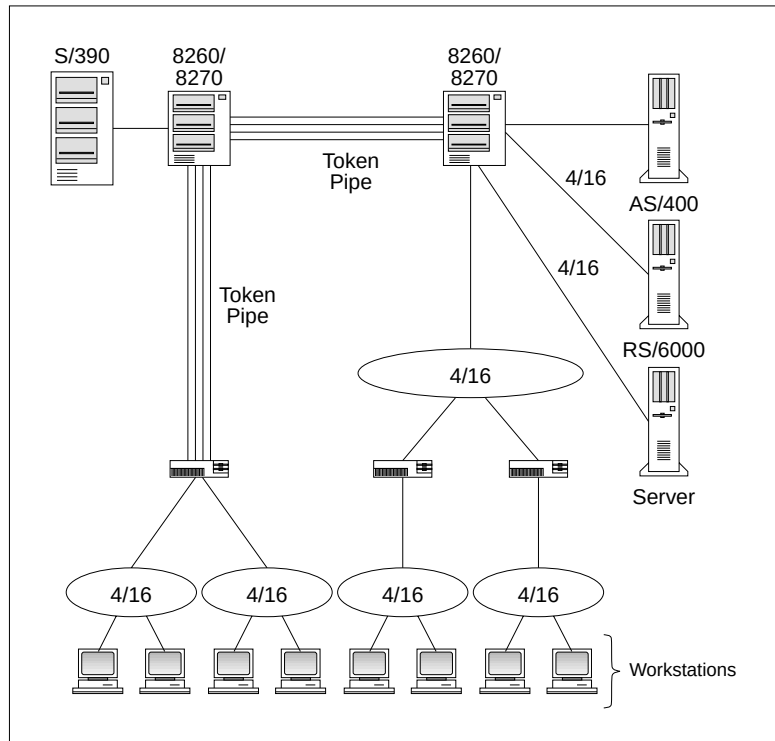
TokenPipe

- Die Mechanismen, die sich hinter dem TokenPipe-Verfahren verbergen, werden vor allem dazu verwendet, um die Bandbreite zwischen zwei Switch-Systemen zu erhöhen. Bei diesem Verfahren ist es erlaubt, mehrere 16-Mbit/s-Ports so zu bündeln, daß diese wie ein Port zur Verfügung gestellt werden bzw. wie ein Port erscheinen. In Abbildung 4.43 ist aufgezeigt, für welche IBM-Komponenten dieses Verfahren unterstützt wird und wie man sich den Einsatz hierfür vorzustellen hat. Zu beachten ist noch, daß TokenPipe die Bündelung von zwei bis vier Token-Ring-Ports erlaubt. Zusätzlich kann die Switch-Port-Kopplung auch noch im Full-

4 Netzwerkaufbau und Netzwerktopologien

Duplex-Verfahren eingesetzt werden, so daß maximal vier mal 32 Mbit/s zur Verfügung gestellt werden, was einer Bruttoübertragungsrate von 128 Mbit/s entspricht. Es werden dabei sowohl Kupfer- als auch Glasfaserverbindungen unterstützt.

Abbildung 4.43
TokenPipe und
Token-Ring



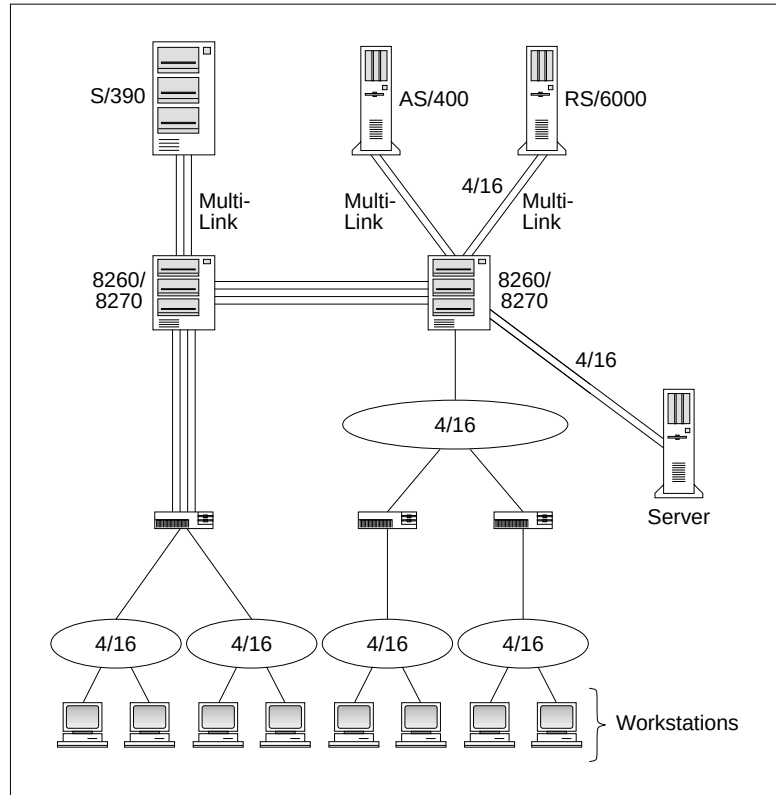
Multi-Link

Dieses Verfahren wird eingesetzt, um die Bandbreite für den Anschluß von Servern zu erhöhen, indem mehrere »Wege« zwischen dem Server und dem Netzwerk zur Verfügung gestellt werden. Wenn z.B. eine RS/6000 mehr Bandbreite benötigt, dann baut man in die RS/6000 mehrere Token-Ring-Netzwerkkarten ein und konfiguriert diese entsprechend.

Da jede Netzwerkkarte die eigene Kartenadresse (MAC-Adresse) nutzt, muß die Server-Anwendung auf jedem Adapter als eigene und unabhängige Verbindung zum Token-Ring-Netzwerk laufen. In Abbildung 4.44 ist dargestellt, wie Multi-Link funktioniert.

4.8 High-Speed-Token-Ring (HSTR)

Abbildung 4.44
Multi-Link und
Token-Ring



Alle diese Ansätze und Lösungen reichen in bestimmten Situationen nicht aus, um den zukünftigen Anforderungen an neue und moderne Netzwerke gerecht werden zu können. Da es bislang im Token-Ring-Bereich nichts Schnelleres gab als 16 Mbit/s, beschreitet eine Vielzahl von Anwendern andere Wege zum Aufbau schnellerer Netzwerke. Dies reicht von einfachem Fast-Ethernet-Netzwerk und Gigabit-Ethernet-Netzwerk bis hin zu vollständigen ATM-Installationen oder einer Kombination aus allen diesen Möglichkeiten. Die nachfolgenden Ausführungen sollen zeigen, wie sich IBM und alle Mitglieder der sogenannten HSTR-Allianz diese technologische Entwicklung vorstellen, was dahinter steckt und zu erwarten ist.

4.8.3

Standards und Status (HSTR)

Die Entwicklung für den High-Speed-Token-Ring hat bereits begonnen, und einzelne Hersteller liefern bereits die ersten Produkte hierfür, auch wenn vielleicht noch nicht alle Fragen bezüglich des Standards geklärt sind. Ein sogenannter Industrie-Round-Table wurde

4 Netzwerkaufbau und Netzwerktopologien

am 26. August 1997 durch die Tolly Group und Network World abgehalten. Als »Gruppe« hat man sich verpflichtet, einen Industrie-Standard für High-Speed-Token-Ring (HSTR) einzuführen. Die Tolly-Group-Round-Table-Teilnehmer haben deshalb die folgende Vereinbarung veröffentlicht, die während der Zusammenkunft getroffen worden war:

»We therefore resolve to pursue an IEEE 802.5 standard for dedicated high speed token ring that scales from 100 Mbps to at least one Gbps. The standard will support key attributes of today's token ring and will be developed in time to allow for multi-vendor demonstrations of high-speed token ring technology at NetWorld & Interop in Las Vegas 1998. The standard will support the use of 802.1q standard for multiple Virtual LANs (VLANs). The goal of this standard's effort is to deliver the most cost effective upgrade path for token ring customers.«

Die Schlüsselfunktionen für die Token-Ring-Eigenschaften in puncto HSTR werden wie folgt gesehen:

- Unterstützung einer sehr großen Token-Ring-Frame-Größe von maximal 18.2 Kbyte
- Volle Unterstützung der Source-Routing-Funktionen mit einem Source-Routing-Information-Field (RI), das in der Lage ist, bis zu 14 Hops (Source Route Bridges) zu speichern
- Prioritätsmechanismen von acht Stufen
- Es soll die gleiche Stufe der Verfügbarkeit und Stabilität erreicht werden, so wie man dies bereits vom 4/16-Mbit/s-Token-Ring kennt.

Am 27. August legten die Teilnehmer eines vorläufigen IEEE-(Institute of Electrical and Electronics Engineers)-802.5-Treffens fest, an das IEEE-802.5-Komitee die folgenden drei Project Authorization Requests (PARs) weiterzuleiten:

- 100-Mbit/s-Token-Ring über Kupfer
- 100-Mbit/s-Token-Ring über Glasfaser
- Gbit/s-Token-Ring

IBM ist dazu verpflichtet, die Entwicklung dieser Standards zu unterstützen. Als Ergebnis des Tolly Round Table und des IEEE-802.5-Interim-Meetings im August 1997 hat sich unter den führenden Netzwerkherstellern eine neue Koalition gebildet, die ab diesem Zeitpunkt als High Speed Token Ring Alliance geführt wird. Die Aufgaben dieser Allianz sollen unter anderem die folgenden Ergebnisse nach sich ziehen:

4.8 High-Speed-Token-Ring (HSTR)

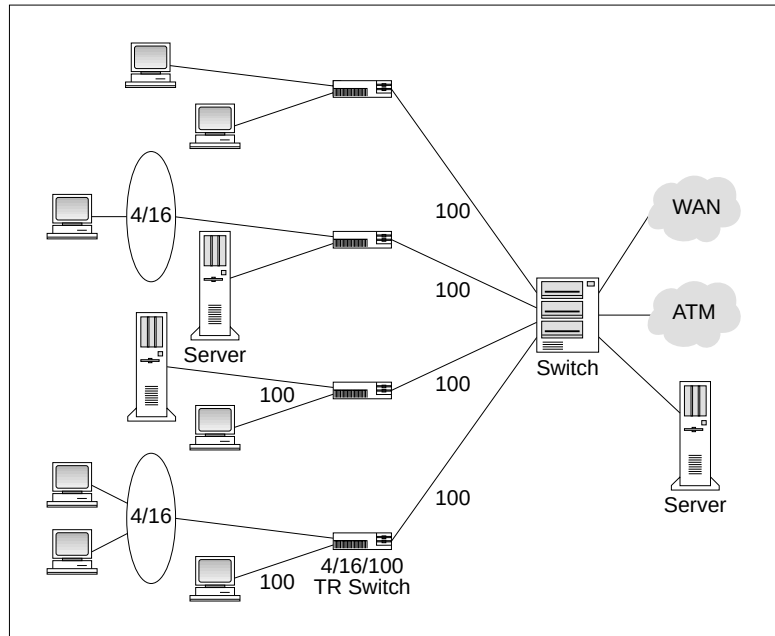
- Die Investitionen der Token-Ring-Kunden sollen durch die High-Speed-Token-Ring-Technik gesichert werden, indem zuerst 100 Mbit/s und später 1 Gbit/s zur Verfügung gestellt werden.
- Die IEEE-802-High-Speed-Token-Ring-Standards und die Interoperabilität soll durch die Zusammenführung der technischen Spezifikationen erleichtert werden.
- Es soll ein Ansprechpartner zur Verfügung stehen, um auf Reaktionen der Kunden bei der Entwicklung von High-Speed-Token-Ring eingehen zu können.
- Durch unabhängige Tests soll die Interoperabilität der Produkte unter Beweis gestellt werden.
- Durch eine frühzeitige Informationsweitergabe soll der High-Speed-Token-Ring als strategisches Produkt am Markt bekanntgemacht werden.

Zu den Allianzpartnern zählen unter anderem: 3Com, Nortel Networks, Cabletron, Cisco Systems (inzwischen aus der Allianz ausgestiegen), TBM, Madge Networks, Novacom, Olicom, The University of New Hampshire Interoperability Laboratory und Xylan.

Ob alle High-Speed-Token-Ring-Hersteller die gleiche Produktphilosophie vertreten, ist nicht bekannt. Hier sollen die »Gedankengänge« von IBM näher betrachtet werden. Laut Aussagen von IBM soll der erste High-Speed-Token-Ring-Adapter ein Autosensing 4/16/100 Mbit/s PCI Adapter sowohl für Server als auch für Clients sein. Somit kann man ähnlich wie bei den Autosensing-Karten aus der Ethernet-Technologie erst mal eine 4/16/100-Mbit/s-Karte kaufen, auch wenn man noch nicht die High-Speed-Token-Ring-Technologie einsetzen will. Bei der Einführung von High-Speed-Token-Ring wird man ähnliche Überlegungen anstellen wie auch bei der Einführung von Fast Ethernet bzw. Gigabit Ethernet. Da jedoch die derzeitige Grenze bei 100 Mbit/s erreicht ist, hat man weniger Skalierbarkeit. Deshalb sieht es meist so aus, als ob man Backbone-Verbindungen und Server-Anschlüsse mit HSTR von 100 Mbit/s realisiere, wohingegen in den Etagen-Netzwerken an 4/16 Mbit/s festgehalten wird (dann sollte man aber zumindest Switching-Technologie einsetzen). Würde man die Etagen-Netzwerke auch noch mit 100 Mbit/s betreiben, dann hätte man das Problem, daß ein Backbone-Netzwerk, das auch nur 100 Mbit/s zur Verfügung stellen kann, bei weitem nicht seine Leistung bringen kann, und somit zum Engpaß werden würde. Man denke an dieser Stelle deshalb immer an die grundsätzliche Randbedingung, daß ein Backbone-Netzwerk zur Zusammenführung von Hochgeschwindigkeitsnetzwerken in der Etage immer wesentlich leistungsfähiger sein muß. Ein entsprechend strukturiertes Token-Ring-Netzwerk könnte deshalb in etwa so aussehen, wie in Abbildung 4.45 dargestellt.

4 Netzwerkaufbau und Netzwerktopologien

Abbildung 4.45
Aufbau von High-Speed-Token-Ring-Netzwerken



Abschließend will ich Ihnen noch die wesentlichen technischen Überlegungen aufzeigen, die bei der Entwicklung der HSTR-Technik berücksichtigt worden sind:

- HSTR-Komponenten sollten mit der Auto-Negotiation-Funktion ausgestattet sein, um automatisch 4-, 16- oder 100-Mbit/s-Token-Ring-Netzwerkanschlüsse erkennen zu können. Zu beachten ist dabei nur, daß die Auto-Negotiation-Funktion nicht zur Standarddefinition für HSTR gehört, so daß dies von den einzelnen Herstellern auf unterschiedliche Art und Weise realisiert werden kann.
- HSTR verwendet die gleiche PHY, so wie diese bereits für Fast Ethernet bekannt und eingeführt worden ist. Deshalb hat die 802.5-Arbeitsgruppe ausführliche Tests durchgeführt, um festzustellen, wie sich ein Ethernet-Netzwerk verhält, wenn eine HSTR Station angeschlossen wird. Grundsätzlich fand die Arbeitsgruppe heraus, daß beim Anschluß einer Token-Ring-Station in ein Ethernet-Netzwerk nichts passiert – die Token-Ring-Station findet nur keinen Zugang zum Netzwerk, ohne jedoch einen störenden Einfluß auf das Ethernet-Netzwerk zu nehmen. Im ungünstigsten Fall kann kurzfristig eine Vielzahl von Kollisionen auftreten, und dies nur, während die Station – aufgrund des Lobe-Tests – das Netzwerk mit einer Vielzahl von Signalen vollschüttet. Anschließend stellt der Selbsttest fest, daß der Lobe-Test fehlgeschlagen ist, und »zieht« sich vom Netzwerk zurück. Nur an der Workstation wird

4.8 High-Speed-Token-Ring (HSTR)

eine entsprechende Meldung ausgegeben, daß das Einfügen in den Token-Ring nicht funktioniert hat – es war schließlich ein Ethernet-Netzwerk, in das man eine Token-Ring-Station einfügen wollte.

Wenn man bedenkt, daß mindestens drei 100-Mbit/s-Netztechnologien existieren, die mit der gleichen Physical-Layer-Kodierung arbeiten (FDDI, 100BaseT und HSTR), dann ist es durchaus von Vorteil, wenn ein Verfahren existiert, das prüft, ob eine Station integriert werden darf oder nicht, ohne dabei das gesamte restliche Netzwerk lahmzulegen.

Zum Zeitpunkt der Erstellung dieses Buches waren die ersten HSTR-Produkte bereits verfügbar, auch wenn der Standard noch nicht ganz und vollständig verabschiedet war. Da die Zeit jedoch inzwischen drängt und um mit anderen High-Speed-Netzwerken Schritt halten zu können, haben sich diese Hersteller bewußt etwas weiter aus dem »Fenster« gelehnt. Wenn es der HSTR nicht schnell gelingt, wichtiges Terrain zurückzugewinnen, dann dürfte dies unter Umständen auf breiter Front das Aus für Token-Ring-Netzwerke gewesen sein. Es zeichnet sich bereits heute zum Beispiel ab, daß die FDDI-Technologie bei weitem nicht mehr die Rolle spielt, wie dies zum Beispiel noch vor zwei Jahren gewesen ist (Betrachtungszeitpunkt Mitte 1999). Eine ursprünglich gute und schnelle Technologie mußte innerhalb kürzester Zeit Fast Ethernet bzw. Gigabit Ethernet weichen, von ATM ganz zu schweigen, selbst wenn deren Verbreitung noch zunehmen sollte. Da jedoch eine Vielzahl von Herstellern in ihren Hubsystemen standardmäßig einen Fast Ethernet Uplink bzw. Gigabit Ethernet Uplink integriert hat, wird dem Entscheidungsträger die Entscheidung für oder gegen »High-Speed«-Ethernet viel leichter gemacht.

Man geht davon aus, daß die Entscheidung für oder gegen HSTR bis spätestens Ende 1999 fallen wird. Sollte dann der große Durchbruch nicht gelungen sein, wird dieser auch nicht mehr kommen. Ein wesentlicher Faktor ist dabei auf alle Fälle der Preis der HSTR-Komponenten. Sollten die ersten Aussagen stimmen, daß HSTR-Komponenten etwa 25% teurer sein werden als die bisherigen Token-Ring-Komponenten, öffnet sich die Preisschere zwischen »High-Speed«-Ethernet und HSTR noch weiter. Um die Akzeptanz am Markt zu erhöhen, müßte auf alle Fälle an der Preisschraube nach unten gedreht werden.

Dieser kurze Überblick sollte Ihnen einen Eindruck vermitteln, mit welchen Möglichkeiten Sie in den nächsten Monaten und Jahren rechnen können. Daß die Anforderungen, die an das LAN gestellt werden, nicht geringer werden, hat man bereits erkannt. Mit diesen

4 Netzwerkaufbau und Netzwerktopologien

höheren Anforderungen muß auch langfristig die Leistungsfähigkeit des LAN und die Leistungsfähigkeit der WAN-Strecken gesteigert werden. Im LAN-Bereich werden bereits Komponenten hierfür angeboten, wohingegen der WAN-Bereich noch nicht so weit ist bzw. dessen gesteigerte Leistungsfähigkeit einen relativ hohen Preis fordert. Dies wird sich jedoch in den nächsten Jahren ändern, wenn die Telekom und deren Konkurrenten (sobald diese auch die technischen Voraussetzungen dazu haben) in der Lage sind, entsprechende ATM-WAN-Strecken zur Verfügung zu stellen. Es ist dann nur noch eine Frage des Preises, ob man sich eine schnelle LAN-WAN-LAN-Kopplung leisten kann oder nicht.

Der aufmerksame Leser hat bereits bemerkt, daß ich immer wieder empfehle, Netzwerke zukünftig auf Basis einer Twisted-Pair-Verkabelung aufzubauen, sofern man nicht Glasfaser bis zum Arbeitsplatz verlegen will. Eine gut ausgebaute Twisted-Pair-Verkabelung erlaubt den Einsatz aller verfügbaren Netzwerktechnologien (Ethernet, Token-Ring, CDDI, Fast Ethernet, Gigabit Ethernet, HSTR oder ATM). Die Investition in die physikalische Infrastruktur bleibt damit für die nächsten zehn (vielleicht auch 15) Jahre gesichert, sofern man sich an bestimmte Regeln hält. Da dies ein wesentlicher Aspekt beim Aufbau von Netzwerken ist, soll im nächsten Abschnitt näher darauf eingegangen werden.

5

Netzwerkkonzeption

In kleineren Netzen ist eine Ebene der Verkabelung durchaus ausreichend. Aufgrund der Gebäudestrukturen ist abzuklären, ob sich die Bus- oder die Sternstruktur besser eignet. Sobald LANs jedoch größere Dimensionen annehmen, ist eine Aufteilung der Verkabelungsstruktur unumgänglich. Man kann das Konzept dann zwei- oder dreistufig aufbauen. Auch das hängt von den baulichen Gegebenheiten ab und bedarf einer erschöpfenden Analyse.

Ich werde versuchen, Ihnen nachfolgend die Möglichkeiten so aufzuzeigen, daß Sie abschätzen können, in welche Kategorie Ihr Verkabelungskonzept eingestuft werden kann. Ein hierarchisch aufgebautes LAN kann aus drei unterschiedlichen Anteilen bestehen:

1. *Primäres LAN (Backbone-Verkabelung)*

Hierbei handelt es sich um eine Gebäude-zu-Gebäude-Verkabelung. Dabei durchläuft die primäre Verkabelung – meist im Keller – alle Gebäude auf einem Gelände oder, wenn es nur eines gibt, ein Gebäude von vorne bis hinten. Auf diese Art und Weise kann vom primären LAN in jeden Gebäudeteil abgezweigt werden. Da es sich meist um längere Strecken handelt, wird eine LWL-Verkabelung empfohlen.

2. *Sekundäres LAN*

Diese Verkabelung wird vom Backbone bis in die letzte Etage des Gebäudes verlegt. Man spricht hier auch von einer sogenannten Steigleitung. Damit ist es möglich, vom Sekundärnetz aus alle Etagen zu erreichen. Je nach Ausdehnung kann auch hier mit LWL verkabelt oder Kupferverkabelung eingesetzt werden.

3. *Tertiäres LAN*

Es handelt sich hier um die Verkabelung der einzelnen Etagen; man spricht deshalb auch von einer Etagenverkabelung. Diese Verkabelung erfolgt in den meisten Fällen mit Kupferkabeln. Sowohl für Ethernet als auch für Token-Ring setzt man hier auf Basis von Twisted-Pair-Kabeln auf die sternförmige Verkabelung.

Welches Netzwerk auf den einzelnen Ebenen verwendet werden soll, hängt von den jeweiligen Anforderungen ab, die an das Gesamtnetz gestellt werden. Eine denkbare Lösung wäre zum Beispiel, das primäre LAN auf ATM-Basis, das sekundäre und tertiäre LAN mit Token-Ring zu vernetzen oder auch Ethernet zu verwenden. Es ist aber auch möglich, Primär-, Sekundär- und Tertiärebenen auf Token-Ring-Basis zu vernetzen. Wie später noch zu sehen sein wird, tendiert man heute dazu, das Primärnetzwerk, also den Backbone, auf einer sehr schnell-

5 Netzwerkkonzeption

len Infrastruktur aufzubauen (ATM oder Gigabit Ethernet) und die anderen Netzbereiche entsprechend zu skalieren. Es ergibt heute keinen allzu großen Sinn mehr, die gesamte Netzinfrastruktur mit nur einer LAN-Technik aufzubauen, da aufgrund der Bandbreitenanforderungen skalierbare Lösungen gefordert und notwendig sind. Dies ist auch ein Grund, warum sich die High-Speed-LANs in den letzten Jahren so rasant entwickelt und durchgesetzt haben.

Eine Frage bleibt jedoch: Wie kann der Übergang vom Primär- auf das Sekundär-LAN und vom Sekundär- auf das Tertiär-LAN erfolgen? Dazu werden Koppelemente benötigt, die man als Bridge, Router, Switch oder Brouter bezeichnet. Worin die Unterschiede dieser Elemente liegen, will ich Ihnen in Kapitel 10 näher erläutern.

Das eben aufgeführte Konzept bietet den Vorteil, daß sich die einzelnen Netzwerkkomponenten logisch sinnvoll installieren lassen. Auf dem Primärnetz werden beispielsweise alle Endgeräte angeschlossen, die den Teilnehmern im Netzwerk zentral zur Verfügung gestellt werden sollen. Im Sekundärnetz können Server und zentrale Drucker installiert werden, die mehreren Abteilungen zur Verfügung gestellt werden sollen, sofern sich diese nicht auf einer Etage befinden. Ein Server für eine Abteilung, die genau auf einer Etage arbeitet, wird in das Tertiärnetz installiert.

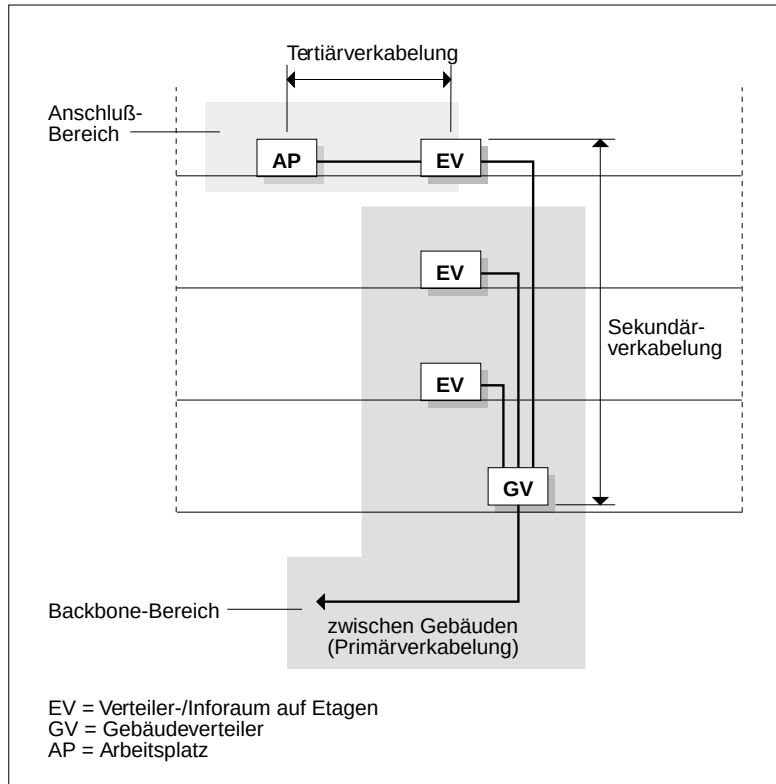
Koppelemente führen eine logische Trennung der Netze durch. Datenpakete werden also immer nur dann in das andere Netzwerk transportiert, wenn sich der Empfänger des Datenpakets im anderen Netzwerk befindet. Somit können große und leistungsfähige Netzwerke aufgebaut werden, wenn man deren logische Struktur sinnvoll plant. In Abbildung 5.1 ist dargestellt, wie eine sinnvolle Werksverkabelung (Gebäudeverkabelung) aussehen könnte.

Beim Aufbau solcher Verkabelungskonzepte und auch zur Strukturierung kleinerer LANs eignen sich besonders gut die Hubs der neuen Generation.

Dabei handelt es sich um Verkabelungskomponenten, die in der Lage sind, nicht nur Ethernet, sondern auch Token-Ring-, Fast Ethernet-, Gigabit Ethernet-, FDDI- und ATM-Komponenten zu integrieren. Da durch Koppelemente die einzelnen LANs miteinander verbunden werden müssen, können in diese Hubs gleich die entsprechenden Bridge- oder Router-(Brouter-)Einschübe eingebaut werden, sofern es sich nicht bereits um entsprechende Switching-Komponenten handelt. Falls es diese Möglichkeit noch nicht gibt, muß man auf externe Verbindungselemente zurückgreifen.

5 Netzwerkkonzeption

Abbildung 5.1
Klassische strukturierte Verkabelung



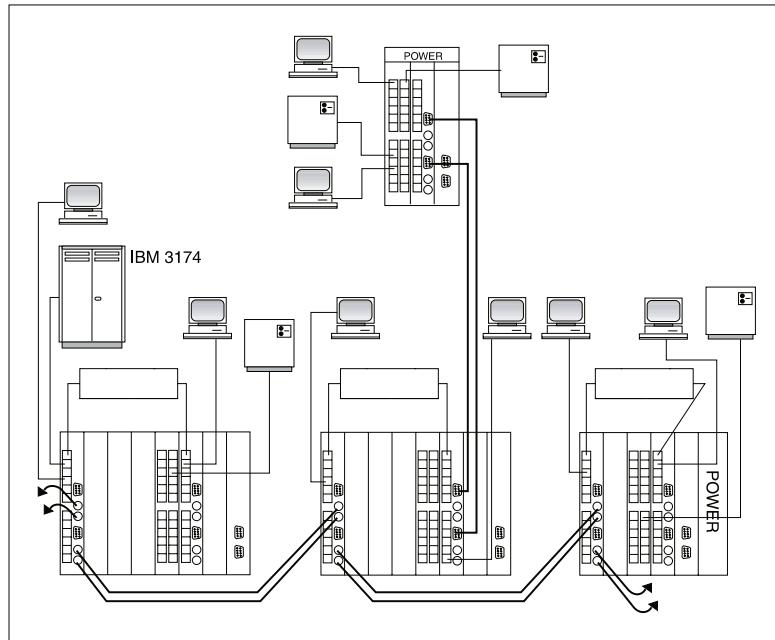
Es ist aber auch möglich, den Hub einheitlich mit den gleichen Einschüben zu bestücken (nur Ethernet, Fast Ethernet, Token-Ring oder FDDI-Module). Auf den einzelnen Einschüben werden meist die unterschiedlichsten Kabeltypen unterstützt. Daneben werden in den Hub noch eigene Managementmodule eingeschoben, damit man in der Lage ist, die Hubs von zentraler Stelle über eine Management-Konsole zu überwachen, zu steuern und zu konfigurieren.

In der Abbildung 5.2 ist dargestellt, wie solche Hubs aufgebaut sind und wie die einzelnen Verteilerräume aussehen können, in denen der Übergang vom Primär- aufs Sekundärnetz bzw. vom Sekundär- aufs Tertiärnetz erfolgt.

Es gibt inzwischen eine so große Anzahl unterschiedlichster Hubs verschiedener Hersteller, daß sie hier nicht im Detail erläutert werden können. Exemplarisch möchte ich Ihnen einige Komponenten näher erläutern. In der jeweiligen konkreten Situation kann aber immer nur entschieden werden, welches System für welchen Einsatz am geeignetsten ist – und hierzu bedarf es einer exakten Planung.

5 Netzwerkkonzeption

Abbildung 5.2
Aufbau von Hubs
in der Praxis



Die Abbildungen 5.3 und 5.4 zeigen einen echten Hub der Firma Bay Networks (Bay Networks ist inzwischen von Nortel aufgekauft worden, dies ändert jedoch nichts an der Funktionalität bzw. dem Prinzip dieses Hub). Die Abbildung 5.3 zeigt den Accelar 1200 mit folgenden wesentlichen Merkmalen:

- Konfigurierbar für bis zu 12-Gigabit-Ethernet-Ports
- Konfigurierbar für bis zu 96 Autosensing-10/100-Mbit/s-Ethernet-Ports
- Erhöhung der Ausfallsicherheit durch redundante Netzteile

Die Centillion-1000-Produktfamilie hingegen ist für sehr spezielle Umgebungen geschaffen. So ermöglicht die Centillion-1000-ATM-Switch-Produktfamilie die Übertragung von Sprachdaten und unterstützt die Verbindung von digitalen Nebenstellenanlagen (PBX). Diese neuen Komponenten eignen sich für den Einsatz in Netzzentren und können mit den ATM-LAN- und WAN-Anwendungen der Kunden betrieben werden. Die Produktfamilie umfasst drei verschiedene modulare Chassis, die entweder mit sechzehn (Centillion 1600), mit acht (Centillion 1400) oder mit vier (Centillion 1200) Steckplätzen ausgestattet sind. Der Centillion 1600 basiert auf einer vollständig redundant ausgelegten, nicht blockierenden 10-Gbit/s-Switch-Architektur. Bis zu 64 Ports unterstützen sie gemäß der Sonet-Hierarchie, und Centillion-1200-Komponenten liegt ebenso eine

5 Netzwerkkonzeption

nichtblockierende Switch-Architektur von 5 Gbit/s beziehungsweise 2,5 Gbit/s zugrunde. Sämtliche neuen Lösungen verfügen sowohl über monomode als auch multimode OC-12- und OC-3-Schnittstellen sowie Unshielded-Twisted-Pair-Schnittstellen.

Abbildung 5.3
Accelar 1200



Die Centillion 1000-Produkte verfügen über einen ATM-Voice-Concentrator (die ersten Geräte, die diese Möglichkeit bieten), der zum Transport von Sprache, Daten oder Bildern über unternehmensweite Intranetze sowie lokale Netze und Weitverkehrsnetze dient.

In vielen Fällen sind Gebäudeverkabelungen und -strukturen vorzufinden, die eine klassische Netzwerkstruktur aufgebaut haben, so wie dies in Abbildung 5.5 dargestellt ist. Aufgrund der neuen Übertragungstechniken (ATM, 100Base-TX, 100Base-T4 etc.) ist es jedoch inzwischen notwendig, Netzwerke in Richtung sternförmiger Verkabelung nicht nur zu planen, sondern auch entsprechend zu implementieren. In diesem Zusammenhang fällt auch immer wieder der Begriff »Collapsed-Backbone«; diese neue Technologie ist im Verbund mit Entwicklungen im Bereich der Switching-Hub-Systeme zu sehen.

Aufgrund bisheriger Erfahrungen kann beim Aufbau neuer Verkabelungsstrukturen bzw. bei der Erweiterung bereits bestehender Gebäudeverkabelungen davon ausgegangen werden, sechs generelle Planungskonzepte zu berücksichtigen.

5 Netzwerkkonzeption

Abbildung 5.4
Centillion 1600

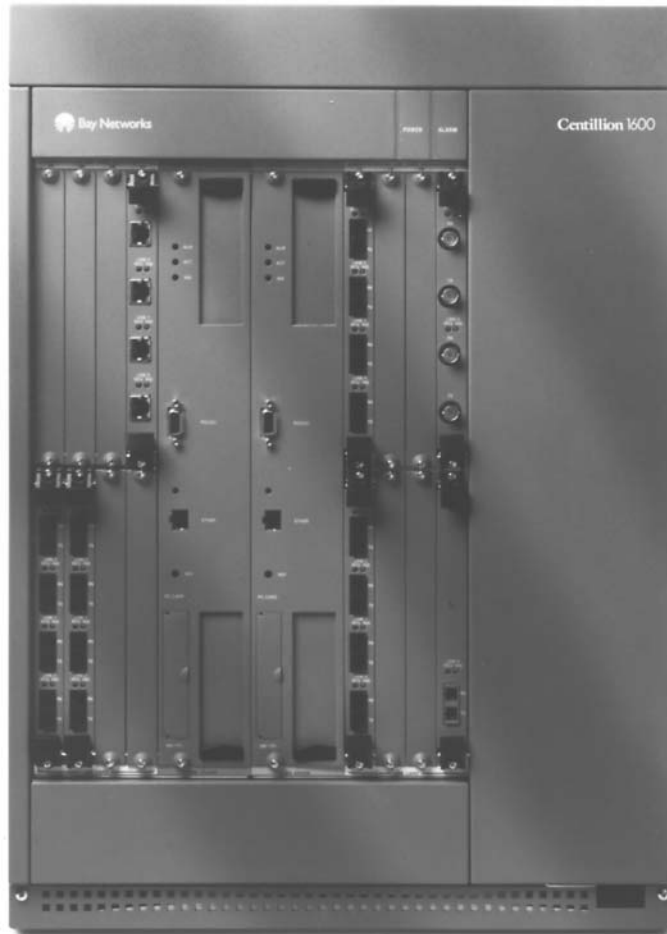
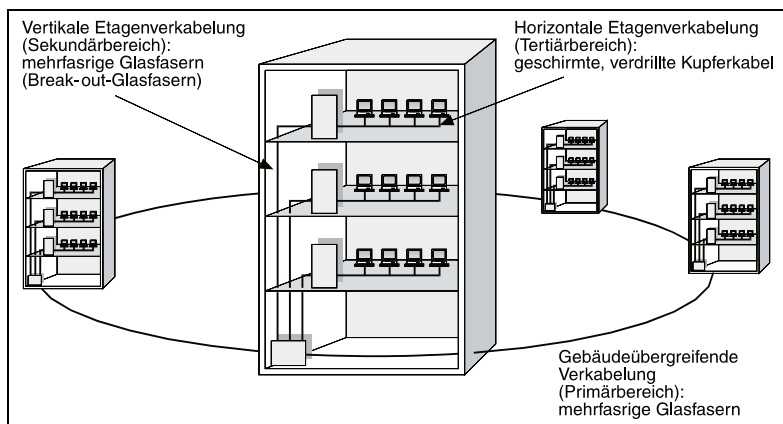


Abbildung 5.5
Klassischer Aufbau
einer flächendeckenden
Gebäude-
verkabelung



5 Netzwerkkonzeption

Sternverkabelung auf Tertiärebene

Betrachtet man die neuen Netzwerkkomponenten auf Basis einer Twisted-Pair-Verkabelung, so stellt man fest, daß diese Komponenten so aufgebaut sind, daß sich alles sternförmig am Hub sammelt. Dies gilt, wie die Ausführungen im Kapitel 4 gezeigt haben, unter anderem für ATM, Fast Ethernet etc. Es ist deshalb bereits aus Gründen der Kompatibilität notwendig, sich an diese Strukturvorgaben zu halten. Die Vorteile einer zentralisierten und sternförmigen Verkabelung sind aber auch darin zu sehen, daß nach dem Aufbau einer vollständigen Verkabelung relativ leicht Änderungen in den Anschlüssen der einzelnen Endgeräte durchgeführt werden können. Benötigt ein Endgerät statt eines 10Base-T-Anschlusses einen ATM-Anschluß, muß nur gewährleistet werden, daß im Verteilerschrank des Etagenverteilers ein entsprechender ATM-Anschluß im Hub zur Verfügung steht. Nach Austausch der Netzwerkkarte im PC gegen eine ATM-Karte und Umlegen im Patchpanel vom 10Base-T-Anschluß auf den ATM-Anschluß kann der PC mit einer wesentlich höheren Geschwindigkeit arbeiten. Somit muß keine neue Verkabelung für die Umstellung vorgenommen werden.

Die Gedankengänge diesbezüglich gehen so weit, daß man bei einem vollständig neuen Aufbau einer Verkabelung auch die Telefonanlagen in das Netzwerkkonzept einbezieht, so daß es möglich ist, im Patchpanel des Verteilerschranks zu entscheiden, ob es sich bei der jeweiligen Anschlußdose im Büro um einen Netzwerkanschluß oder um einen Telefonanschluß handelt. Dies erhöht die Flexibilität insofern man sich nicht mehr festlegen muß, ob es in einem Büro zwei Telefon- und vier Netzwerkanschlüsse geben soll. In Zukunft gibt es dann einfach sechs Anschlußdosen, und im Verteillerraum der Etage wird entschieden, ob daraus vier Telefondosen und zwei Netzwerkanschlüsse oder drei Telefondosen und drei Netzwerkanschlüsse werden.

Die Verkabelung in der Etage ist in der Regel der aufwendigste Bereich, da hiermit doch eine sehr große Anzahl von Endgeräten erreicht werden muß. Deshalb sollte bei der Planung und Ausführung darauf geachtet werden, alle notwendigen Anforderungen auch abzudecken. Es muß nicht nur flexibel geplant werden, sondern auch eine entsprechende Redundanz zur Verfügung stehen, da die Endgeräte mit ziemlicher Sicherheit nicht über einen längeren Zeitraum unverändert bleiben. Es zeigt sich in der Praxis immer wieder, daß Sparsamkeit im Bereich der Endgeräteanschlüsse keineswegs Kostenersparnis bedeutet. Mit ziemlicher Sicherheit werden sehr bald neue Anschlüsse genau an der Stelle benötigt, wo keine freien Netzwerkanschlüsse sind. Der Aufwand, nachträglich zu verkabeln, ist so hoch, daß es effektiver und kostengünstiger gewesen wäre, die in ei-

5 Netzwerkkonzeption

nem Raum eventuell später notwendigen Anschlüsse gleich von Anfang an verkabeln zu lassen. Untersuchungen in diesem Bereich haben ergeben, daß je nach Gebäudeaufbau eine nachträgliche Einzelverkabelung dreimal teurer werden kann, als es die flächen-deckende Verkabelung von Anbeginn ist.

Collapsed Backbone (Sterntopologie im Backbone-Bereich)

Der sternförmige Netzwerkaufbau hat sich inzwischen nicht nur im Etagenbereich durchgesetzt, er wird auch immer mehr beim Aufbau von Backbones verwendet. Das Zauberwort heißt: Collapsed Backbone. Der Aufbau von Ring- oder Busstrukturen im Backbone-Bereich wird nach und nach der Collapsed-Backbone-Technologie weichen. Jedes notwendige Netzwerksegment – in der Regel jeder Etagenbereich – wird dabei über eine Glasfaserstrecke eingebunden. Am anderen Ende der Glasfaser befindet sich dann ein entsprechendes Hub-System, über das auch die einzelnen Netzwerkanschlüsse in den Etagen versorgt werden können. Um künftig auf diese sternförmigen Strukturen aufbauen zu können – falls Umstellungen auf neue schnellere Netzwerktechniken notwendig sind –, konzipiert man auch FDDI-Netzwerke auf Basis dieser Techniken. Damit ist gewährleistet, daß man ohne Änderung der physikalischen Infrastruktur auf neue Netzwerktechniken umstellen kann.

Die Installation eines Collapsed Backbone hat sowohl Vorteile als auch Nachteile. Die wesentlichen Vorteile sind:

- Alle Lichtleiterkabel für die Anbindung der Etagen laufen an einer zentralen Stelle zusammen.
- Es wird nur ein zentraler Raum zum Aufstellen des Hauptverteilers benötigt.
- Die Wartung und Pflege wird vereinfacht, da der Hauptverteiler in einem Raum installiert ist. Man muß also nicht durch das gesamte Gebäude laufen, wenn Wartungsarbeiten durchzuführen sind.

Die Nachteile bei der Realisierung einer Collapsed-Backbone-Struktur sind im wesentlichen:

- Der Einbau erhöhter Redundanz ist notwendig, d.h., man braucht einen doppelten Collapsed Backbone, da sonst beim Ausfall des Collapsed Backbone die Kommunikation der Etagen vollständig gestört ist. Wenn die zentralen Server auch noch im Collapsed Backbone installiert sind, steht das Netzwerk still.
- Die Anbindung der Etagenverteiler sollte im Prinzip auf Basis einer Dual-Homing-Technik erfolgen, so wie dies für FDDI möglich ist.
- Bei ungünstigen, großen Gebäudestrukturen kann sich der Aufbau einer Collapsed-Backbone-Struktur als schwierig erweisen. Man muß nicht alles an einem zentralen Punkt zusammenführen.

5 Netzwerkkonzeption

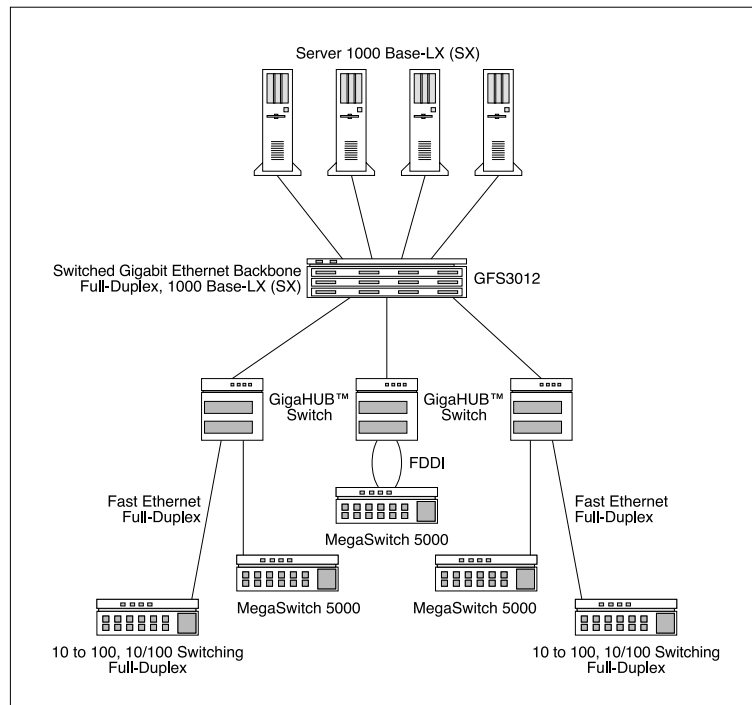
Eine gemischte und verteilte Collapsed-Backbone-Struktur kann von Vorteil sein. Beim Aufbau der Verkabelung ist immer darauf zu achten, daß alles hinsichtlich der ATM-Technik erweiterbar und ausbaufähig ist.

- Im Vergleich zur herkömmlichen Technik wird unter Umständen mehr Lichtleiterkabel benötigt.
- Für die Lichtleiterkabel-Verlegung müssen entsprechende Kabelwege zur Verfügung stehen. Vor allem bei großen Gebäudestrukturen kann es schwierig sein, die richtigen und passenden Wege zum zentralen Hauptverteiler (Collapsed Backbone) zu finden.

Im Zuge der Entwicklungen im Bereich Collapsed Backbone, Fast Ethernet oder auch ATM haben sich die Switching-Techniken immer stärker am Markt durchgesetzt, und es werden ständig neue Systemkomponenten dafür angeboten.

Mit Produkten der Firma Nbase könnte man sich den Aufbau eines Collapsed Backbone unter Einsatz unterschiedlicher Netzstrukturen in den Etagen bzw. Gebäuden wie in Abbildung 5.6 vorstellen. In dieser Abbildung ist auch zu sehen, daß sich die unterschiedlichsten LAN-Strukturen einsetzen lassen.

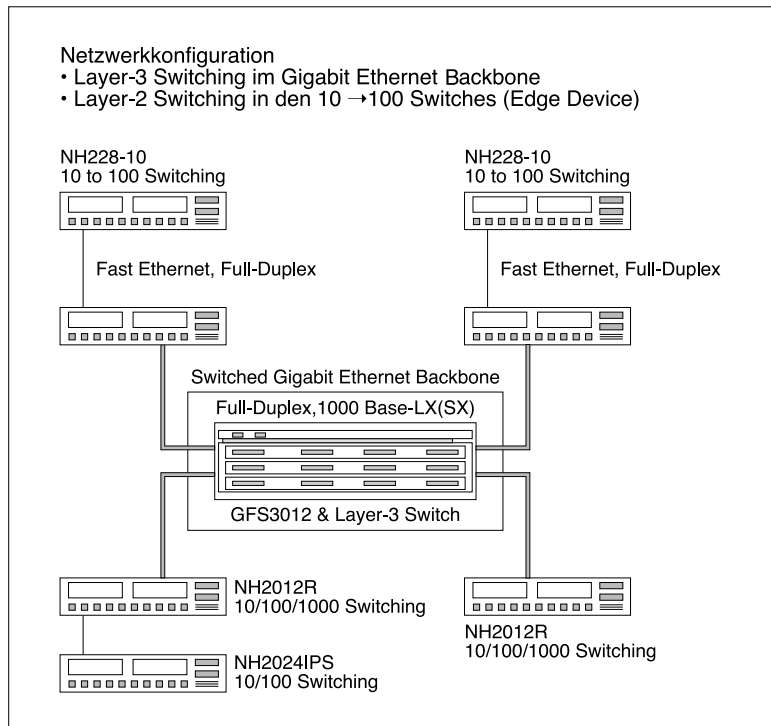
Abbildung 5.6
Collapsed
Backbone
(Quelle: NBase)



5 Netzwerkkonzeption

Es ist aber ebenso möglich, mit Hilfe geeigneter Hubs den Collapsed Backbone auf Basis von Gigabit Ethernet aufzubauen und die Übergänge in den Etagen in einer 10/100/1000-Mbit/s-Ethernet-Variante durchzuführen, so wie dies in Abbildung 5.7 dargestellt ist.

Abbildung 5.7
Collapsed Backbone auf vollständiger Ethernet-Basis (Quelle: Nbase)



Eine weitere Variante ist in Abbildung 5.8 dargestellt. In diesem Falle ist der Collapsed Backbone auf zwei Gebäude verteilt, und beide Hub-Systeme sind miteinander verbunden, da die Server verteilt auf beide Collapsed-Backbone-Hubs angeschlossen sind. Der Nachteil dieser Konstellation fällt sofort auf: Fällt ein Hub-System aus, ist somit ein gesamter Gebäudekomplex lahmgelegt. Um dies zu vermeiden, kann eine Netzinfrastruktur aufgebaut werden, so wie dies in Abbildung 5.9 dargestellt ist.

Diese wenigen Beispiele sollen nur einen kleinen Überblick über das heute technisch Mögliche geben. Es sei nochmals darauf hingewiesen, daß zum Zeitpunkt der Netzplanung die aktuellen technischen Möglichkeiten neu überprüft werden müssen bzw. sollten, da auch die einzelnen Hersteller ständig neue Varianten zur Verfügung stellen.

5 Netzwerkkonzeption

Abbildung 5.8
Collapsed Backbone
auf zwei
Gebäude verteilt
(Quelle: NBase)

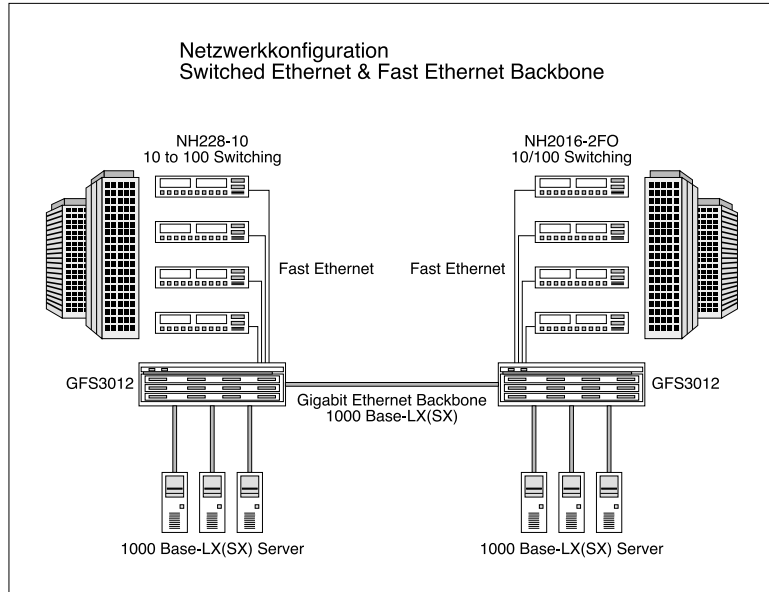
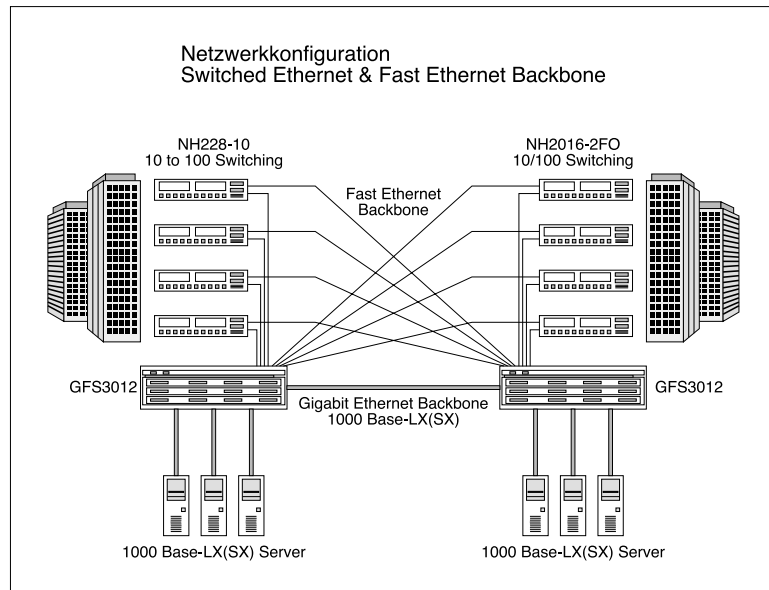


Abbildung 5.9
Redundante Col-
lapsed-Backbone-
Strukturen
(Quelle: NBase)



LAN-Switches

Wenn man sich die Kommunikationsbeziehungen in einem LAN etwas genauer betrachtet, dann stellt man fest, daß die prinzipiell mögliche Kommunikationsbeziehung – jeder kann mit jedem im Netzwerk kommunizieren – nicht erforderlich und auch nicht er-

5 Netzwerkkonzeption

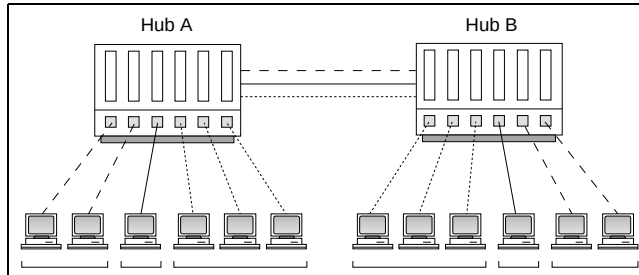
wünscht ist. In der Regel hat man Server und Workstations, wobei die Workstations mit dem Server kommunizieren, aber keine Kommunikation zwischen den Workstations stattfindet. Eine Workstationkommunikation untereinander ist nur dann notwendig, wenn Peer-to-peer-Netzwerkmechanismen aufgebaut werden. Die Client-Server-Anwendungen und die klassischen Server-Anwendungen benötigen immer nur eine Kommunikation zwischen dem Server und der Workstation. Wenn Mailingsysteme aufgebaut werden, steht auch immer ein zentraler Mail-Server im Mittelpunkt, der zur zentralen Kommunikation mit den Mail-Clients zur Verfügung steht. Die Kommunikation läuft also tatsächlich sternförmig ab und wird auch so benötigt. Die ausgereiften Sicherheitsfunktionen der modernen Server-Betriebssysteme widersprechen auch dem Prinzip der Dezentralisierung, d.h. der Möglichkeit, daß jedes Endgerät im LAN auf jedes andere Endgerät zugreifen kann.

Es kommt auch noch hinzu, daß die Hubs in sehr vielen Fällen den Mittelpunkt einer sternförmigen Verkabelung bilden und die Nutzung der auf dem Kabel verfügbaren Übertragungskapazitäten durch das Verfahren und das eingesetzte Netzwerk selbst beschränkt ist. Bei den klassischen Shared-Media-Verfahren (z.B. Ethernet, Token-Ring, FDDI) teilen sich die Endgeräte im LAN die Kabelstruktur und somit die Bandbreite. In einem Ethernet-Netzwerk kann eine Station nur dann Daten übertragen, wenn nicht gerade eine andere Station Daten überträgt. Zudem wird jedes Datenpaket von jeder angeschlossenen Station empfangen. Im Token-Ring durchläuft jedes Datenpaket jede Station. Dies ist auch dann der Fall, wenn die Kommunikation immer nur mit einem Server, der sich im Token-Ring befindet, durchgeführt wird. Günstiger wäre es deshalb, wenn der unnötige Datenverkehr »gefiltert« werden könnte, um die bestehende Infrastruktur optimal zu nutzen.

Aus dieser Situation heraus haben sich die Switching-Techniken entwickelt. Die ersten Switching-Systeme wurden im Bereich der Ethernet-Netzwerke entwickelt und eingesetzt. Inzwischen steht diese Technik aber auch für Token-Ring zur Verfügung. Das ATM-Netzwerk ist generell auf Basis der Switching-Technik aufgebaut. Allerdings sind noch nicht alle Hersteller in der Lage, in allen Bereichen für jedes Netzwerk LAN-Switches anzubieten. Die oben aufgeführten Probleme beim Aufbau klassischer LANs werden durch die Verwendung von LAN-Switches bzw. Switching-Hubs gelöst. Wie in Abbildung 5.10 zu sehen ist, kann durch die Switching-Technik das Netzwerk in Workgroups gegliedert werden, die es ermöglichen, die Kommunikationsbeziehung zwischen Endgeräten und Server gezielt abzubilden.

5 Netzwerkkonzeption

Abbildung 5.10
Bildung von Work-
groups mit Hilfe
von Switching-
Hubs



Bei der Switching-Technologie haben sich zwei Verfahren entwickelt, abhängig auch davon, ob gleichartige oder unterschiedliche LAN-Übergänge notwendig sind. Im Prinzip handelt es sich übrigens bei LAN-Switches um sehr schnelle Bridges, d.h., der Übergang erfolgt – bezogen auf das OSI-Schichtenmodell – auf der Ebene 2. Aufgrund der Bridge-Technik im Switching-Hub kommt man sehr leicht zu einer Multiport Single Station Bridge, über die nur ein Teilnehmer oder eine geringe Anzahl von Teilnehmern bedient werden muß. Man unterscheidet im Bereich der LAN-Switches sogenannte Store-and-Forward-Switches und Cut-Through-Switches. Wo die Vor- und Nachteile liegen und in welchen Netzwerken welche Technik eingesetzt wird, soll in einem späteren Kapitel erläutert werden.

VLANs – Virtuelle LANs

Ein VLAN ist ein Netzwerk auf Basis von Switching-Technologie, das zwar aufgrund der organisatorischen Begebenheiten und aufgrund von Funktionen, Projekt Teams oder Anwendungen in logische Segmente unterteilt wird, aber nicht aufgrund der physikalischen oder geografischen Begebenheiten. So ist es zum Beispiel möglich, daß alle Workstations und Server, die von einer bestimmten Workgroup genutzt werden sollen, zu einem VLAN konfiguriert werden können, ohne daß dabei Rücksicht auf die physikalische Verteilung der Endgeräte genommen werden muß. Eine Rekonfiguration des Netzwerkes kann dann einfach durch Software-Anpassung durchgeführt werden, ohne eine Neuverteilung der Endgeräte oder andere Verpatchung in den Verteilerschränken durchführen zu müssen.

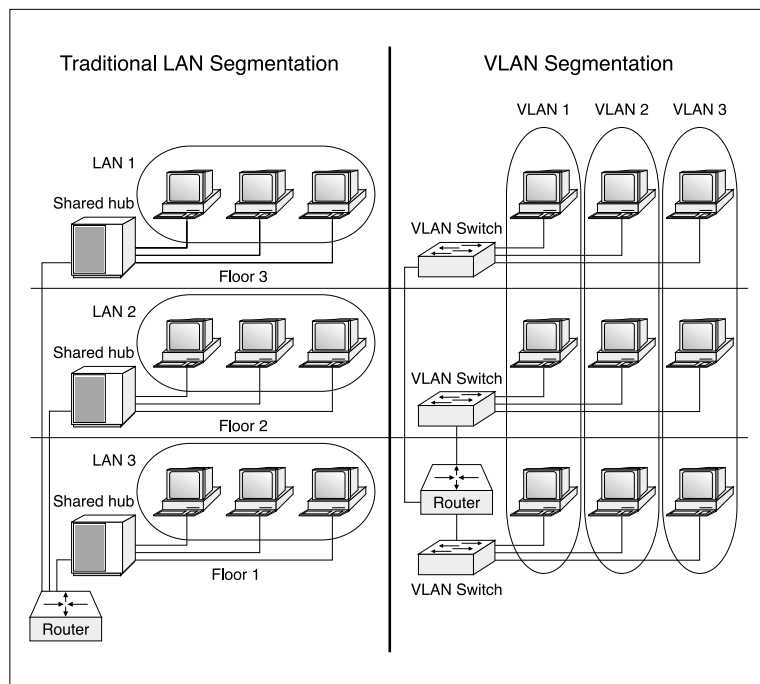
Ein VLAN kann als Broadcast-Domäne betrachtet werden, die innerhalb von Switches aufgebaut wird. Ein VLAN besteht aus einer Anzahl von Endgeräten (z.B. Hosts, Bridges, Router, Workstations, Drucker etc.), die zu dieser Broadcast-Domäne gehören. VLANs werden gebildet, um die Segmentierung so durchführen zu können, wie man dies bislang mit Routern in klassischen LAN-Umgebungen realisiert hat. VLANs bieten Skalierbarkeit, Sicherheit und Netzwerkmanagement. Router in einer VLAN-Umgebung bieten Broadcast-Filter, Sicherheit und Flußkontrolle. Beim Aufbau von VLANs bzw. Switching von LANs sind die folgenden Aspekte zu beachten:

5 Netzwerkkonzeption

■ LAN-Segmentierung

VLANs erlauben es, daß eine logische Netzwerkstruktur über die physikalische Netzwerkinfrastruktur mit Switches gelegt wird, indem LAN-Ports in autonome Benutzergruppen oder Kommunikationseinheiten zusammengefaßt werden. Damit die Kommunikation zwischen den VLANs durchgeführt werden kann, müssen speziell hierfür entwickelte VLAN-Router installiert werden. In Abbildung 5.9 ist ein Vergleich zwischen einem klassischen LAN und einem VLAN dargestellt.

Abbildung 5.11
LAN-Technologie
versus VLAN-
Technologie



■ Sicherheit

Bei Bedarf kann mit Hilfe von VLANs die Sicherheit erhöht werden, indem Arbeitsgruppen isoliert werden. Anwender, die in diesen Sicherheitsbereich gehören, werden in einem VLAN gruppiert. Diese Anwender können sich durchaus mit anderen Endgeräten, die nicht zu diesem VLAN gehören, im gleichen Segment befinden. Durch die spezielle VLAN-Konfiguration kann eingestellt werden, daß Benutzer außerhalb des VLANs nicht mit diesem VLAN kommunizieren können.

5 Netzwerkkonzeption

■ *Broadcast-Kontrolle*

So wie Switches Collision-Domänen für angeschlossene Endgeräte voneinander trennen und nur der notwendige Datenverkehr außerhalb des Ports weitertransportiert wird, bieten VLANs eine vollständige Trennung zwischen den VLANs. Ein VLAN wird deshalb als Bridging Domäne betrachtet, in der Broadcast- und Multicast-Datenverkehr geschehen.

■ *Performance*

Da durch die VLAN-Bildung alle Anwender unabhängig von der physikalischen Lokalisierung zusammengefaßt werden können, stört es im Prinzip auch nicht mehr, wenn plötzlich größere Personalverschiebungen innerhalb bzw. zwischen den Etagen erfolgen und die ursprünglichen Abteilungen nicht mehr auf einer Etage konzentriert sind, sondern auf mehrere Etagen verteilt werden. Dies ist übrigens eines der größten Probleme, wenn es um die Planung von LANs geht, da die zum Zeitpunkt der Planung gemachten Annahmen über den Datenverkehr der einzelnen Abteilungen aufgrund von Umzügen etc. sehr rasch veralten.

■ *Netzwerkmanagement*

Die VLAN-Technik kann erst dann wirkungsvoll eingesetzt werden, wenn auch die Netzwerkmanagementfunktionen hierfür zur Verfügung stehen. Nur so ist es möglich, daß von der Management-Station aus neue VLANs gebildet, erweitert oder verkleinert werden, ohne physikalische Umstellungen im Verteilerraum (Patchungen) durchführen zu müssen.

■ *Kommunikation zwischen VLANs*

Die Kommunikation zwischen VLANs wird durch Router realisiert, wobei nach wie vor die traditionellen Sicherheits- und Filterfunktionen von Routern eingesetzt werden können. So ist es durchaus von Vorteil, wenn das VLAN Router-Funktionen für Sicherheits-Filter, Quality of Services (QoS) und Accounting pro VLAN zur Verfügung stellt.

Anhand dieser Ausführungen dürfte ersichtlich sein, daß der Aufbau von VLANs ebenso sorgfältig geplant werden muß, wie dies für die Netzplanung sonst auch gilt. Ansonsten kann es falsche Zusammenhänge zwischen den VLANs bzw. den Endgeräten innerhalb eines VLAN geben. Die gesamte Kommunikationsinfrastruktur würde dadurch beeinträchtigt.

Twisted-Pair-Kabel im Etagenbereich (Tertiärverkabelung)

Die Verkabelung im Etagenbereich wird auf der Basis einer Twisted-Pair-Verkabelung aufgebaut. Hierzu werden entweder geschirmte oder ungeschirmte Kabel eingesetzt. Die Glasfaserverkabelung bis zum Arbeitsplatz wird bis heute aufgrund des höheren Pro-Port-Preises immer noch nicht durchgeführt, außer »rauhe« Umgebungsbedingungen lassen nichts anderes zu. Bislang ging man auch davon aus,

5 Netzwerkkonzeption

daß die Glasfaserverkabelung auch dann benötigt wird, wenn hohe Übertragungsraten von mehreren Megabit pro Sekunde notwendig sind. Die neue Twisted-Pair-Kabelgeneration, auch als CAT 7 bezeichnet, erlaubt inzwischen Übertragungsraten von mindestens 622 Mbit/s; dies entspricht der ATM-Spezifikation.

Es kann davon ausgegangen werden, daß mit dieser neuen Kabelgeneration auch die Anforderungen der nächsten Jahre erfüllt werden können. Wichtig ist, daß die Kabel den CAT-5- respektive den CAT-7-Anforderungen entsprechen.

Glasfaserkabel für Primär- und Sekundär- bereich

Im Gegensatz zur horizontalen Etagenverkabelung werden in der Regel die vertikale Etagenverkabelung (Sekundärbereich) und die gebäudeübergreifende Verkabelung (Primärbereich) durch mehradrige Glasfaserkabel durchgeführt. In diesen Bereichen muß meist durch »rauhe« Gebäudebereiche verlegt werden, es müssen Kabellängen von mehr als 100 Metern erreicht werden können, und es ist eine erhöhte Sicherheit auf den Übertragungsstrecken gefordert. Diese Bedingungen können nur durch Glasfaserkabel erfüllt werden. Im wesentlichen ergeben sich die folgenden Vorteile:

- Es treten keine störenden elektromagnetischen oder elektrostatischen Einflüsse von außen auf, so daß eine sehr hohe Störsicherheit gewährleistet werden kann.
- Die über Glasfaserstrecken verbundenen Netzwerkkomponenten sind galvanisch getrennt. Dadurch können keine Potentialunterschiede auftreten, d. h., es ist also kein Potentialausgleich durch einen Gleichstromfluß über das Datenkabel möglich. Dies muß auf alle Fälle im Etagenbereich berücksichtigt werden, da nicht selten unterschiedliche Potentiale in Gebäudeteilen vorzufinden sind, ein Problem, das vor allem durch das Auflegen der Schirmung bei den Twisted-Pair-Kabeln auftreten kann. Besitzen nämlich zwei Netzwerksegmente unterschiedliche Erdungen – was häufig vorkommen kann, vor allem, wenn es sich um zwei Gebäude mit unterschiedlichen Erdungsblöcken handelt –, kann es zu einem Gleichstromfluß kommen. Somit kann es im Normalbetrieb durch die leicht unterschiedliche statische Aufladung zu kleinen Gleichstromflüssen auf dem Kabel (über die Schirmung) kommen. Wenn auch noch eine Überspannung wegen Blitzschlags eintritt, können sogar wichtige Netzkomponenten zerstört werden. Der kleine schwarze Haufen war dann einmal ein Hub-System.

Es ist inzwischen mehrfach der Begriff »Hub« gefallen. In Abbildung 5.2 ist dargestellt, wie Netzwerke auf Basis einer Hub-Technologie realisiert werden können. Die nachfolgenden Ausführungen sollen Ihnen zeigen, welche grundsätzlichen Funktionen ein Hub erfüllen

5.1 Funktion und Aufbau von Hubs

muß. Da jeder Hersteller andere Strategien verfolgt, beschränke ich mich hier auf die wesentlichen Funktionen und Mechanismen, sonst würde ein Buch über Strategien von Hub-Herstellern entstehen.

5.1 Funktion und Aufbau von Hubs

Die generelle Aufgabe eines Hub ist darin zu sehen, als aktive, intelligente Komponente sternförmige LAN-Verteilungen und LAN-Konzentrationen unterschiedlicher Topologien aufzubauen. Aufgrund der Komplexität, die mit Hub-Systemen verbunden ist, wird gefordert, daß jeder Hub in der Regel mit Hilfe von Managementkarten von einer zentralen Stelle aus überwacht werden kann. Es muß also eine passende Netzwerkmanagement-Software angeboten werden, um die geforderten Funktionen erfüllen zu können. Dabei kann es sich um eine vollständig eigene Netzwerkmanagement-Software des Hub-Herstellers handeln oder der Hub-Hersteller bietet Add-on-Software für bereits existierende Netzwerkmanagement-Software (z.B. HP OpenView) an.

Technisch betrachtet besteht ein Hub aus einem 19"-Gehäuse, einem entsprechenden Backplane mit einer Vielzahl von Steckplätzen. Die Anzahl der Steckplätze variiert je nach Hubgröße zwischen 3 und 17. Das hängt aber vom jeweiligen Hersteller ab. So gibt es Hersteller von Hubs, die nur große Hubs (mit z.B. 12 Steckplätzen) anbieten, oder auch solche, die einen großen Enterprise-Hub (zum Aufbau des Backbone) und kleinere Workgroup-Hubs (zum Aufbau der Etagenanschlüsse) anbieten.

Die 19"-Technik ist notwendig, damit die Hubs in Standardverteilerschränke eingebaut werden können. Für jeden Hub muß es eine Vielzahl von Einschubmodulen geben, um damit entsprechende LANs und LAN-Funktionen aufbauen zu können. Je nach Hersteller ist die Managementfunktion für den Hub auf einer der Einschubkarten integriert oder muß durch eine explizite Managementkarte realisiert werden.

Zu den wesentlichen Funktionen eines Hub zählen:

- LAN-Hub für Ethernet, Token-Ring, Fast Ethernet, Gigabit Ethernet, 100VG-AnyLAN, FDDI und/oder ATM-Netzwerke
- LAN- und Media-Management
- Hub-Management
- Bridging- und Routing-Funktionen
- Switching-Technik im Hub oder auf den Einschubmodulen
- Bildung von VLANs

5 Netzwerkkonzeption

Mit einem Hub lassen sich in der Regel zentrale und/oder vermischte LANs mit Managementfunktionen für die unterschiedlichsten LAN-Topologien aufbauen. Modularität und flexible Ausbaumöglichkeiten zur Unterstützung unterschiedlicher LAN-Techniken und -Protokolle machen es möglich, sowohl kleine als auch große, sehr komplexe Netzwerke aufzubauen. Durch den modularen Aufbau ist eine Segmentierung von LANs und von LAN-Subnetzwerken möglich, um damit eine übersichtliche Gestaltung und ein gutes Management zu erreichen.

Aufgrund der neuen Anforderungen müssen auch die Switching-Techniken erfüllt werden, um damit nicht nur schnellere Netzwerke aufbauen, sondern auch die Bildung von virtuellen LANs (VLANs) bzw. Workgroup-LANs realisieren zu können. Die gesamten Funktionen zum Aufbau von VLANs können nur über eine geeignete Netzwerkmanagement-Software implementiert werden. Dies bedeutet für die Auswahl von Hub-Systemen, auf alle Fälle darauf zu achten, daß nicht nur die herkömmlichen LAN-Funktionen, sondern auch Switching und VLANs unterstützt werden.

Es darf nicht vergessen werden, daß Hub-Systeme aufgrund der starken Konzentration von Netzwerkfunktionen und -komponenten äußerst kritisch reagieren, wenn ein solches System ausfällt. Daher muß auch darauf geachtet werden, daß Hub-Systeme gegenüber Ausfall von Einzelkomponenten geschützt werden. Dies beginnt unter anderem damit, daß ein Hub-System in der Regel mit einem redundanten Netzteil ausgestattet sein sollte. Damit nicht der Ausfall des gesamten Backplane droht, sollte man auch darauf achten, daß ein Hub-System verwendet wird, das nur mit einem passiven Backplane arbeitet. Somit ist normalerweise gewährleistet, daß nicht der gesamte Hub auf einmal ausfällt. Es sollte auch darauf geachtet werden, daß die Managementfunktionen auch dann noch zur Verfügung stehen, wenn der Hub selbst Probleme macht. Ist das Management nicht mehr über das LAN möglich, weil Netzwerkstörungen auftreten, sollte auf alle Fälle ein Management über Modem als Notfunktion zur Verfügung stehen.

Nachfolgend werden die wichtigsten Funktionsbereiche zusammengefaßt:

■ LAN-Concentrator / LAN-Switch / Hub-System

Im Hub sollten Einschubmodule für alle gängigen Netzwerktopologien zur Verfügung stehen; ebenso sollten die Übergänge von LAN A auf LAN B ermöglicht werden. Ob dabei die Technik von Bridges, Routern oder Switches eingesetzt wird, hängt sehr vom jeweiligen Hersteller ab (und natürlich auch vom Geldbeutel). Für

5.1 Funktion und Aufbau von Hubs

jedes LAN-Modul sollten die unterschiedlichsten Anschlußtypen unterstützt werden. In der Regel ist dies UTP oder STP bzw. Glasfaser. Zusätzlich sollten die einzelnen Module mit einer unterschiedlichen Anzahl von Anschlußports verfügbar sein; nicht selten werden Module mit 12 oder 24 Ports angeboten. Dies hat vor allem Kostengründe, da es ungünstig ist, wenn man ein 12-Port-Modul benötigt, aber nur ein 24-Port-Modul zur Verfügung steht. Wenn es für ein LAN-Modul mehrere Varianten mit einer unterschiedlichen Portzahl und auch noch unterschiedlichen Port-Mediatypen gibt, erhält man für den flexiblen Aufbau von Netzwerken eine wesentlich höhere Granularität.

■ *Hub-Management*

Die Konfiguration eines Hub erfolgt unter anderem durch das Netzwerkmanagement-System. Es geht aber auch darum, neben den Lastinformationen des Gesamtsystems oder eines einzelnen Ports Funktionen zur Verfügung zu stellen, die es erlauben, einzelne Ports ab- oder einzuschalten. Die Konfiguration und das Bilden von Workgroups (VLANs) gehören selbstverständlich auch zu den Aufgaben, die das Hub-Management erfüllen muß. In welcher Form die Mechanismen zur Verfügung gestellt werden und wie groß die Komplexität der damit verbundenen Möglichkeiten ist, hängt vom jeweiligen Hersteller ab.

■ *Interconnection*

Da in einem Hub unterschiedliche LAN-Topologien miteinander gekoppelt werden können, müssen entsprechende Elemente zur Verfügung stehen, die es erlauben, diese unterschiedlichen LANs zu verbinden. Ob man dabei auf Bridges, Router oder die neue Switching-Technik zurückgreift, hängt nicht nur davon ab, ob der Hersteller diese Möglichkeiten zur Verfügung stellt, sondern wird auch durch das gesamte Netzwerkkonzept maßgeblich beeinflusst. Nicht immer ist die Switching-Technik die beste Lösung. So kann durchaus das Routing oder das herkömmliche Bridging Vorteile gegenüber Switching mit sich bringen. Das muß aufgrund der jeweiligen Netzwerkkumgebung und den damit verbundenen Anforderungen entschieden werden. Soweit die wichtigsten Merkmale und Eigenschaften, die bei der Auswahl von Hub-Systemen zu beachten sind. Bevor die Entscheidung für den Hub-Hersteller getroffen werden kann, muß das gesamte Netzwerkdesign konzipiert sein. Erst dann kann näher untersucht werden, welche Möglichkeiten des Hub den gestellten Anforderungen am besten gerecht werden.

5 Netzwerkkonzeption

Wenn man nun weiß, wie das ganze Netzwerk aufgebaut werden soll, geht es darum, die physikalische Infrastruktur zu realisieren. Da es hierbei im Bereich der Twisted-Pair-Verkabelung immer wieder zu nicht kalkulierten Problemen kommt, sollen im nächsten Kapitel die existierenden Vorschriften und Normen dargestellt werden.

5.2 Verkabelung der Zukunft und Vorschriften

Eine zukunftsichere, flexible und leicht erweiterbare Verkabelung gewinnt immer mehr an Bedeutung. Ziel ist, ein System aufzubauen, über das nicht nur ein bestimmtes Netzwerk betrieben werden kann, sondern das es erlaubt, alle am Markt angebotenen Netzwerke einzusetzen. Das beginnt mit Ethernet und hört bei ATM auf. Hierfür ist sowohl eine strukturierte Verkabelung im Unternehmen notwendig als auch die richtige Wahl des Kabels und der damit zusammenhängenden Techniken. Der Trend geht stark in Richtung Twisted-Pair-Verkabelung. Im Rahmen dieser Verkabelungsstrukturen wurden Vorschriften geschaffen, die von Twisted-Pair-Kabeln und den dazu gehörenden Komponenten eingehalten werden müssen. Dieses Kapitel soll Ihnen einen Überblick darüber verschaffen, welche Vorschriften zu berücksichtigen sind und welche Auswirkungen diese Vorschriften in der Zukunft haben werden.

Bevor die Vorschriften einer Verkabelung mit Twisted-Pair näher betrachtet werden, sollen zuerst noch die unterschiedlichen Twisted-Pair-Kabel (geschirmt, nicht geschirmt) vorgestellt werden.

5.2.1 Physikalische Grundlagen der heute verwendeten Datenkabel

Bei ungeschirmten Datenkabeln ist das elektromagnetische Feld nicht auf den Bereich zwischen den beiden Leitern eines Pairs begrenzt. Es ist auch im näheren Umfeld rund um das Paar, also auch im Kabelmantel und außerhalb des Kabels, vorhanden. Dabei nimmt die Feldstärke quadratisch mit der Entfernung ab.

Bei geschirmten Datenkabeln erfährt das elektromagnetische Feld eine natürliche Begrenzung durch den Schirm. Das elektrische Feld wird auf den Bereich zwischen den Leitern eines Pairs begrenzt, und das magnetische Feld dringt bei hohen Frequenzen nicht mehr über den Schirm hinaus.

5.2 Verkabelung der Zukunft und Vorschriften

Abbildung 5.12
Aufbau von unge-
schirmten Kabeln

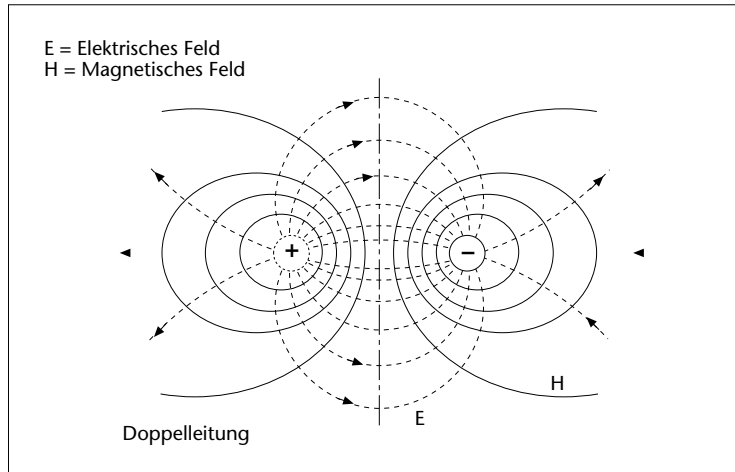
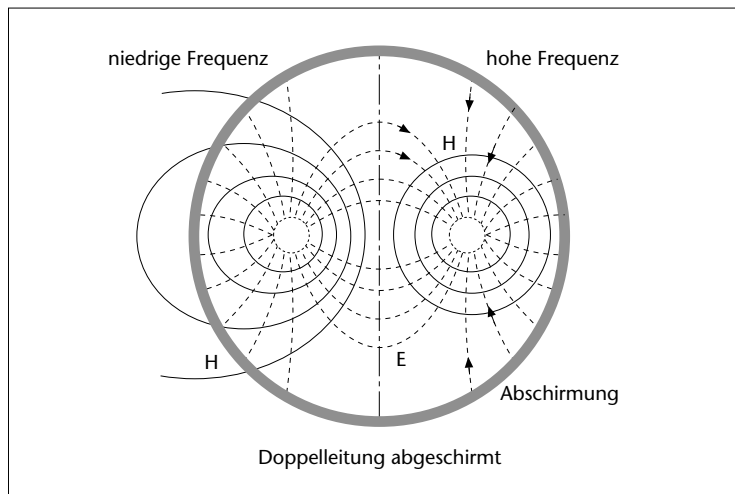


Abbildung 5.13
Aufbau von ge-
schirmten Kabeln



Bei einem installierten Datenkabel ist praktisch in allen Fällen das nähere Umfeld des Kabels weder gleichförmig homogen noch konstant. Die elektrischen Materialien wie Kabelschutzrohre, Kunststoffmäntel anderer Kabel, Brüstungskanäle, aber auch Metalle und insbesondere andere Kabel beeinflussen den für die Übertragungseigenschaften maßgebenden Feldverlauf. Zwangsläufig ergeben sich daher beim Einsatz eines UTP-Kabels zumindest im hohen Frequenzbereich instabile Übertragungsverhältnisse. Dies stellt man nicht erst dann fest, wenn Übertragungsprobleme erkannt werden, sondern auch dann, wenn man im Vorfeld verlegte Kabel mit entsprechenden Meßgeräten analysiert.

5 Netzwerkkonzeption

Nach einer Verlegung der Datenkabel sollte auf alle Fälle die Messung der Kabel erfolgen. Dies sollte auch unter normalen Arbeitsbedingungen durchgeführt werden; u. a. sind alle elektrischen Endgeräte einzuschalten, so daß im Umfeld der Kabel die üblichen »Störeffekte« vorhanden sind. Die Kabel sollten also in dem Zustand gemessen werden, wie er auch im Normalbetrieb vorzufinden ist. Nur so kann festgestellt werden, ob Umgebungsbedingungen einen negativen Einfluß auf die verlegten Kabel ausüben, der Reflexionen und gravierende Systemstörungen zur Folge haben kann.

Die elektrischen Eigenschaften von ungeschirmten Datenkabeln sind also von der Umgebung stark abhängig. Ungeschirmte Datenkabel verändern ihre Eigenschaften, insbesondere wenn sie in die Nähe von elektrisch leitenden Materialien kommen. Dies ist der Fall, wenn die Kabel sich in der Verpackung bzw. auf der Trommel (Nähe zu sich selbst) oder im installierten Zustand (Nähe zu sich selbst oder zu anderen Kabeln, Kabelkanal etc.) befinden. Die Folge sind Impedanzsprünge und Reflexionen sowie bis zu 10% Abweichung bei Dämpfung und Betriebskapazität.

Die elektrischen Eigenschaften von geschirmten Datenkabeln sind dagegen unabhängig vom Umfeld. Das elektrische Feld ist klar auf den Raum innerhalb der Abschirmung begrenzt und unterliegt damit keinen äußeren Einflüssen. Die gleiche Aussage über die Begrenzung des magnetischen Felds durch die Abschirmung kann nicht getroffen werden, da hier sogenannte Skin-Effekte zu berücksichtigen sind. Der Impedanzverlauf wird aber nicht durch die Umgebung beeinflusst; es ergeben sich bei Verwendung von S-Kabeln stabile Übertragungseigenschaften. Der Schirm führt zu definierten und gleichbleibenden Eigenschaften, unabhängig davon, ob sich das Kabel in der Verpackung, auf der Trommel oder im installierten Zustand befindet.

5.2.2 Prüfbedingungen

Aus dem oben genannten Grund werden übrigens ungeschirmte Datenkabel im ausgelegten Zustand, also nicht auf der Trommel und nicht in der Nähe von elektrisch leitenden Materialien, geprüft. Solche Labormessungen unter Idealbedingungen sind in den entsprechenden UTP-Kabelvorschriften TSB 36 und UL 444/13 definiert.

Allerdings ist zu beachten, daß Kabel, die nach diesen Vorschriften geprüft werden, relativ unkritischen Anforderungen bei der Bewertung ihrer Inhomogenitäten unterliegen. Dies gilt insbesondere für UTP-Kabel nordamerikanischer Herkunft. Bei der Ermittlung des Wellenwiderstands ($100 \pm 15 \text{ Ohm}$) darf auf der Basis der gemessenen Eingangsimpedanzen eine Glättungsfunktion angewendet werden, die größere Inhomogenitäten wieder wegbügelt.

5.2 Verkabelung der Zukunft und Vorschriften

Die Inhomogenitäten erfahren lediglich indirekt eine Bewertung durch die Definition der Rückflußdämpfung. Die Anforderungen an die Rückflußdämpfung nehmen allerdings mit wachsender Frequenz ab. Anders verhält es sich bei den geschirmten Datenkabeln. Diese erfüllen in der Regel die Anforderungen an den Wellenwiderstand und an die Eingangsimpedanz ohne Verwendung von Glättungsfunktionen. Die vorhandenen Inhomogenitäten werden ungeschminkt dargestellt.

5.2.3 Übertragungseigenschaften

Beim Einsatz von ungeschirmten Datenkabeln ergeben sich aufgrund des oben beschriebenen Sachverhalts zwangsläufig undefinierte und instabile Übertragungsverhältnisse, insbesondere bei hohen Frequenzen. Dies kann zu Leistungseinbußen oder sogar zu gravierenden Systemstörungen führen. Geschirmte Datenkabel haben dagegen definierte und stabile Übertragungsverhältnisse auch bei hohen Frequenzen.

5.2.4 Elektromagnetische Verträglichkeit

Die Sicherstellung der elektromagnetischen Verträglichkeit (Störausendung, Störfestigkeit) erfolgt zunächst durch Maßnahmen an den Endgeräten bzw. den aktiven Komponenten. Da das Kabel grundsätzlich als Antenne wirkt, muß durch zusätzliche Maßnahmen dafür gesorgt werden, daß möglichst wenig Störungen ausgesendet oder empfangen werden.

Beim Einsatz von ungeschirmten Datenkabeln geschieht das durch eine möglichst symmetrische Auslegung des Kabels (Verdrillung der Adern zum Paar). Durch die bedingte Realisierbarkeit der Symmetrie empfiehlt sich zusätzlich die Verwendung von äußerst symmetrischen Übertragern bzw. Mediafiltern. Diese Maßnahmen greifen allerdings nicht oder nur bedingt bei den häufig auftretenden Gleichtaktstörungen.

Ein Nachweis für die Einhaltung der EMV-Normen konnte bisher nur bei der gutartigen (sehr symmetrischen) Übertragung von 16 Mbit/s (Token-Ring) erbracht werden. Die wesentlich kritischeren Übertragungsarten 10Base-T und TPDDI (100 Mbit/s) sind mit ungeschirmten Datenkabeln kaum zu bewältigen.

Anders ist dies beim Einsatz von geschirmten Datenkabeln. Verkabelungssysteme auf der Basis von symmetrischen geschirmten Kabeln bieten einen doppelten Schutz: die Symmetrie und den Schirm. Dadurch lassen sich auch die kritischen Gleichtaktstörungen wirkungsvoll bekämpfen und die Störfestigkeit der Endgeräte erhöhen.

5 Netzwerkkonzeption

Vor diesem Hintergrund ist laut EMV-Gesetz bei geschirmten Anlagen eine Messung der Störfeldstärke nicht erforderlich, im Gegensatz zu ungeschirmten Anlagen. Dies führt zu einem nicht unerheblichen Mehraufwand bei der Verwendung von ungeschirmten Kabeln.

5.2.5 Level-5-Kabel versus Kategorie-5-Kabel

Im November 1991 wurden von der Electronic Industries Association im EIA/TIA-Bulletin die TSB-36-Spezifikationen vorgeschlagen, in denen Grenzwerte von Wellenwiderstand, Transmissionsdämpfung und Nahnebensprechdämpfung zur Qualifizierung von Kabeln festgelegt worden sind. Zur Veröffentlichung kamen schließlich die TSB-40. In diesem Bulletin existieren fünf sogenannte Kategorien, die sich vorwiegend in der Bandbreite des Frequenzbereichs unterscheiden.

Die Dämpfung bzw. der Dämpfungsfaktor D stellt ganz allgemein das Verhältnis einer Eingangsgröße E zu einer Ausgangsgröße A dar. Diese Größe kann z.B. ein hochfrequentes Signal sein. Die Einheit der Dämpfung ist das dB (Dezibel). Bel (B) ist der Zehnerlogarithmus des Leistungsdämpfungsfaktors, gekennzeichnet mit dem Anhang Bel (B). Meist verwendet man den zehnten Teil des Bels, das Dezibel (dB).

Bei der Transmissionsdämpfung werden ein Sender und ein Empfänger mit dem zu messenden Kabel verbunden. Sie schließen dabei das Kabel mit der entsprechenden Impedanz ab (Abschlußwiderstand). Der Sender speist nun in das Kabel einen definierten Leitungsspegel bei der vorgegebenen Frequenz ein. Im Empfänger wird der ankommende Leitungsspegel vom Sendepiegel abgezogen, und man erhält die Transmissionsdämpfung.

Als weiterer für die Übertragungseigenschaften eines Kabels wichtiger und notwendiger Parameter ist die Nahnebensprechdämpfung zu nennen. So wie ein relativ hohes Umgebungsgeräusch eine Unterhaltung beeinflusst, stört ein starkes Übersprechen im Kabel von einem Adernpaar auf das andere und wirkt sich negativ auf die Datenübertragung aus. Sende- und Empfangsleitung sind während des späteren Datenaustauschs mit der entsprechenden Impedanz abgeschlossen. Durch die über eine bestimmte Länge parallel geführten Leitungen koppelt das Signal mit einem definierten Sendepiegel von einer in die andere Leitung über. Am gleichen Meßort, an dem das Signal eingespeist wird, mißt man auch den Übersprechpegel an der anderen Leitung. Die Differenz von Sendepiegel und Übersprechpegel ergibt die Nahnebensprechdämpfung.

5.2 Verkabelung der Zukunft und Vorschriften

- Kategorie 1 nennt keine Werte für Frequenzbereich und keine Forderungen bezüglich Wellenwiderstand, Transmissions- und Nahnebensprechdämpfung.
- Kategorie 2 legt den Wellenwiderstand und die Transmissionsdämpfung bis 1 MHz fest.
- Kategorie 3 schreibt den Wellenwiderstand, die Transmissions- und Nahnebensprechdämpfung bis 16 MHz vor.
- Kategorie 4 legt diese Größen bis 20 MHz fest.
- Kategorie 5 fordert die Einhaltung dieser Größen bis 100 MHz.
- Eine Diskussion der Kategorie 6 bzw. Kategorie 7 folgt am Ende dieses Kapitels.

In der nachfolgenden Tabelle sind die definierten Werte der ISO/IEC-Norm zusammengefaßt. Diese Tabelle ist wichtig, da die meisten Kabelhersteller die Meßwerte zu diesen Vorgaben in Relation stellen.

*Tabelle 5.1
Vergleich der
erlaubten
Grenzwerte*

Kategorie	1		2		3		4		5	
Bandbreite in MHz	N/A		4		16		20		100	
Frequenz [MHz]	Dämpfung [dB/100m]	NEXT [dB]	Dämpfung [dB/100m]	NEXT [dB]	Dämpfung [dB/100m]	NEXT [dB]	Dämpfung [dB/100m]	NEXT [dB]	Dämpfung [dB/100m]	NEXT [dB]
1	N/A		2.6	N/A	2.6	41	2.1	56	2.1	62
4					5.6	32	4.3	47	4.3	53
8					8.5	28	6.2	42	5.9	48
10					9.9	26	7.2	41	6.6	47
16					13.1	23	8.9	38	8.2	44
20							10.2	36	9.2	42
25									10.5	41
31.25									11.8	40
62.5									17.1	35
100									22.0	32

Neben den Unterteilungen der Kabel in Kategorien gibt es auch die in Level. Auf den ersten Blick scheint hiermit das gleiche gemeint zu sein, da auch hier in fünf unterschiedliche Level unterteilt wird. Die Bezeichnung Level ist offiziell, aber nicht standardisiert, und es gibt keine standardisierten Testprozeduren für diese Kabel. Außerdem gibt es große Unterschiede in den Übertragungseigenschaften der Kabeltypen. Level-Kabel sind im Gegensatz zu Kategorie-Kabeln relativ leicht herzustellen und daher auch im Preis wesentlich günstiger. Bei Level-5-Kabeln ist die Eigenschaft des Kabels nicht kontinuierlich im Bereich von 1 MHz bis 100 MHz garantiert.

Zu berücksichtigen ist dabei, daß nicht nur die Kabel den Vorschriften, sondern auch Stecker, Wanddose, Verteilerfeld etc. den Kategorie-5-Spezifikationen entsprechen müssen – eine Bedingung, die immer wieder vergessen wird.

5.2.6

Aktuelle Normen und deren Aussage

Es gibt entsprechende Vorschriften für das oben Gesagte, die der Hersteller einhalten muß. Bei Gesprächen mit den Herstellern wird man immer wieder mit solchen Angaben konfrontiert. Damit man auch weiß, was sich hinter diesen Zahlenwerten der Normierungsgremien verbirgt, sollten die wichtigsten Aspekte erläutert werden.

EN 55022

Die EN 55022 wird durch nationale Ergänzungsgesetze interpretiert und ist auf nationale Belange zugeschnitten. Die EN 55022 bildet die europaweite Plattform für alle nationalen Einzelgesetze. In der Einleitung der EN 55022 können wir den eigentlichen Sinn der EMV-Richtlinien (Elektromagnetische Verträglichkeit) erkennen:

„Informationstechnische Einrichtungen (ITE), die vorwiegend eine Vielzahl von periodischen, binären, impulsförmigen elektrischen/elektronischen Wellenformen erzeugen, die unbeabsichtigt über den Netzanschluß, Steuer- oder andere Leitungen oder durch direkte Strahlung weitergeleitet werden, können eine potentielle Störquelle für den Funkempfang darstellen.“

Aus dieser Einleitung können alle Aussagen, die in der EN 55022 enthalten sind, abgeleitet werden.

1. Die Schirmung dient primär zur Verhinderung von Störabstrahlung.
2. Störstrahlung kann von den Endgeräten durch Anschlußschnüre und Steuerleitungen (Datenkabel) verursacht werden.
3. Diese Strahlung könnte eine Störquelle für den Funkempfang darstellen.
4. Es wird keine Aussage über den Störeinfluß auf das eigene Datenetz getroffen.

Informationstechnische Einrichtungen werden in zwei Gruppen unterteilt, die als Klasse A bzw. Klasse B bezeichnet werden. Beide Klassen beziehen sich bei der Störspannung auf einen Frequenzbereich von 0,15 MHz bis 30 MHz und bei der Funkstörfeldstärkemessung auf 30 MHz bis 1 GHz.

Die ITE der Klasse A sind Einrichtungen, die nicht den Grenzwerten der Klasse B entsprechen. Die Grenzwerte für Einrichtungen der Klasse A sind unter Verwendung eines Schutzabstands von 30 m gemessen. Diese Grenzwerte sind nach nationaler Einschätzung nicht ausreichend.

5.2 Verkabelung der Zukunft und Vorschriften

In der BRD und auch in den meisten EU-Ländern kommt somit Klasse B zur Anwendung. Die Grenzwerte für solche Einrichtungen sind für typische Heimbetriebe (Industriegebiete) unter Verwendung eines Schutzabstands von 10 m abgeleitet.

Neben der EN 55022, die auf die Störaussendung eingeht, gibt es auch noch die EN 50173. Die EN 50173 befaßt sich mit der Störfestigkeit, also der Stabilität gegen äußere Störeinflüsse. Beide Vorschläge sind in der EMV (Elektromagnetische Verträglichkeit) definiert.

EN 50 173

Im März 1994 wurde der Normentwurf EN 50 173 durch den Beuth Verlag in Berlin veröffentlicht. Für diesen Normenentwurf ist das nationale Arbeitsgremium GUK 715.3 (informationstechnische Verkabelung von Gebäudekomplexen) der deutschen elektrotechnischen Kommission im DIN und VDE zuständig.

Der Entwurf der EN 50 173 ist weitgehend eine 1:1-Übersetzung der ISO/IEC DIS 11 801 (Universelle Verkabelung für Gebäudekomplexe), der von der ISO/IEC JTC 1/SC 25 erstellt worden ist. Er wurde von der CLS/TC 115 überarbeitet und speziell auf die europäischen Anforderungen bezüglich der elektromagnetischen Sicherheit und EMV zugeschnitten.

Die Norm ist in zehn Hauptteile gegliedert:

1. Anwendungsbereich

Die Norm wurde für Standorte mit einer geografischen Ausdehnung von bis zu 3000 Metern, einer Bürofläche von 1 Million Quadratmetern und für 50 bis 50.000 Anwender entworfen. Dies heißt jedoch nicht, daß sich kleinere Unternehmen nicht ebenfalls an diese Vorschriften halten oder an ihnen orientieren sollen. Die Norm berücksichtigt eine breite Palette von Anwendungen, z.B. Sprache und Bewegtbilder.

Die Norm spezifiziert:

- die Struktur und die minimale Ausdehnung eines universellen Gebäudeverkabelungssystems,
- die Errichtungsanforderungen,
- die Leistungsanforderungen an die Kabelstrecke und an die Komponenten und
- die Konformitätsanforderungen und Meßverfahren für die Überprüfung der Verkabelung.

2. Normative Verweise

Um die Funktionalität des Netzes sicherstellen zu können, muß die Konfiguration nach Abschnitt 4, »Struktur des universellen Ver-

5 Netzwerkkonzeption

kabelungssystems», erstellt werden. Bei Einhaltung der Längenrestriktionen in Abschnitt 5, »Ausführungsbeispiele«, und unter Verwendung der spezifizierten symmetrischen Datenleitungen und Anschlußtechniken, die in Abschnitt 7 und 8 näher behandelt werden, kann davon ausgegangen werden, daß das Datennetz ohne zusätzliche Überprüfung funktioniert. Sollten die in Abschnitt 6 spezifizierten Längen nicht eingehalten werden, ist es unbedingt erforderlich, die übertragungstechnischen Eigenschaften der Komponenten (Kabel, Verteiler etc.) auf Konformität mit den aus Abschnitt 6 spezifizierten Mindestwerten nachzukontrollieren. Falls also längere Kabelstrecken als die z.B. festgelegten 90 Meter verwendet werden, müssen die eingesetzten Komponenten (Kabel und Anschlußkomponenten) so ausgelegt sein, daß die Grenzen der Link-to-Link-Performance nicht überschritten werden.

3. *Begriffe und Abkürzungen*

In diesem Abschnitt werden die Definitionen der in der Norm verwendeten Begriffe und Abkürzungen näher erläutert. Es sollen an dieser Stelle nur drei wichtige Definitionen aufgeführt werden:

- *Symmetrisches Kabel*

Ein Kabel, das aus mehreren metallischen und symmetrischen Kabelementen besteht. Kabelemente können Paare oder Vierer sein. Begriffe wie UTP, STP, FTP, SUTP, SSTP wurden absichtlich nicht in der Norm verwendet. Bei solchen Begriffen handelt es sich ausschließlich um herstellerspezifische Angaben.

- *Geschirmte Datenkabel*

Eine Anordnung eines oder mehrerer symmetrischer Kabelemente (Paare oder Vierer), die von einem gemeinsamen Schirm umgeben sind und einen gemeinsamen Mantel haben.

- *Kabel mit geschirmten Kabelementen*

Ein Kabel mit elektrischen Leitern, das aus einem oder mehreren individuell geschirmten Kabelementen besteht. Es kann auch mit einem Außenschirm versehen sein; dann spricht man von einem geschirmten Kabel mit geschirmten Elementen.

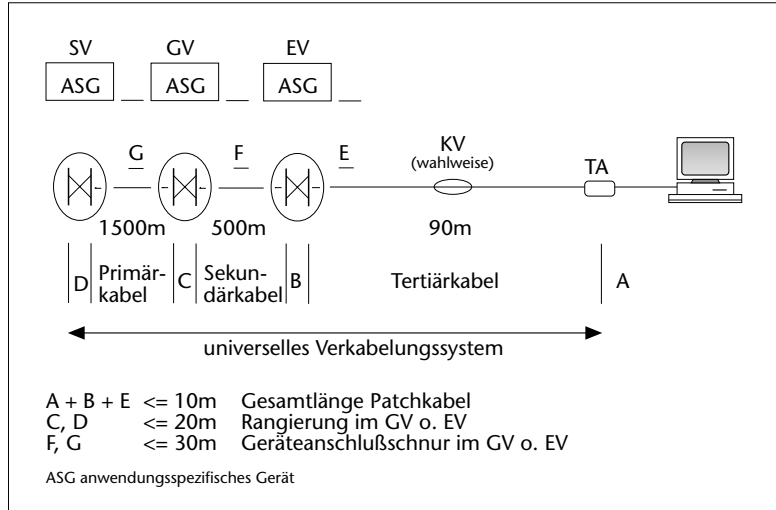
4. *Struktur des universellen Verkabelungssystems*

Beim Aufbau eines universellen Verkabelungssystems werden folgende Komponenten verwendet:

- Standortverteiler (SV) Primärkabel
- Gebäudeverteiler (GV) Sekundärkabel
- Etagenverteiler (EV) Tertiärkabel
- Informationstechnische Anschlußdose (TA)

5.2 Verkabelung der Zukunft und Vorschriften

Abbildung 5.14
Aufbau einer universellen Verkabelung



Die funktionellen Elemente können gemäß Abbildung 5.14 zu einem universellen Gebäudeverkabelungssystem verbunden werden. Wie unschwer zu erkennen ist, ist die Arbeitsplatzverkabelung Bestandteil der Endeinrichtung und nicht der universellen Gebäudeverkabelung. Das bedeutet, daß Anschlußkabel ab TA nur indirekt in die Systemparameter mit eingerechnet werden müssen. Sie sind vielmehr durch die Hersteller der Endeinrichtungen mit zu berücksichtigen. Das ist auch sinnvoll, da es eine Vielzahl von Endgeräten gibt, bei denen bereits die Anschlüsse fest eingebaut sind.

– Primärverkabelung

Das Verkabelungssystem reicht vom Standortverteiler bis zum Gebäudeverteiler. In der Regel wird hierfür eine LWL-Verkabelung verwendet. Der Einsatz von symmetrischen Datenkabeln ist in Ausnahmefällen erlaubt.

– Sekundärverkabelung

Eine Sekundärverkabelung wird verwendet, um Gebäudeverteiler mit Etagenverteilern zu verbinden. In der Sekundärverkabelungsstrecke dürfen keine Kabelverzweiger verwendet werden. Spleiße sollten nach Möglichkeit vermieden werden. In der Regel wird auch hier eine LWL-Verkabelung eingesetzt.

– Tertiärverkabelung

Das Tertiärverkabelungssystem reicht vom Etagenverteiler zu den angeschlossenen Anschlußdosen. Die Tertiärkabel sollten den Etagenverteiler und die Anschlußdosen ohne Unterbrechung verbinden. Wenn nötig, ist ein einziger Kabelverteiler zwischen dem Etagenverteiler und einer beliebigen Anschluß-

5 Netzwerkkonzeption

dose zulässig. Die übertragungstechnischen Eigenschaften dürfen davon aber nicht negativ beeinflusst werden. Im Kabelverzweiger darf nicht rangiert und nur eine 1:1-Zuordnung durchgeführt werden. Die Tertiärverkabelung wird hauptsächlich durch symmetrische Datenkabel realisiert. In Ausnahmefällen können auch LWL-Kabel verwendet werden.

- *Informationstechnischer Anschluß*

Ein informationstechnischer Anschluß kann sich im Boden, in der Wand oder in Kanalsystemen befinden.

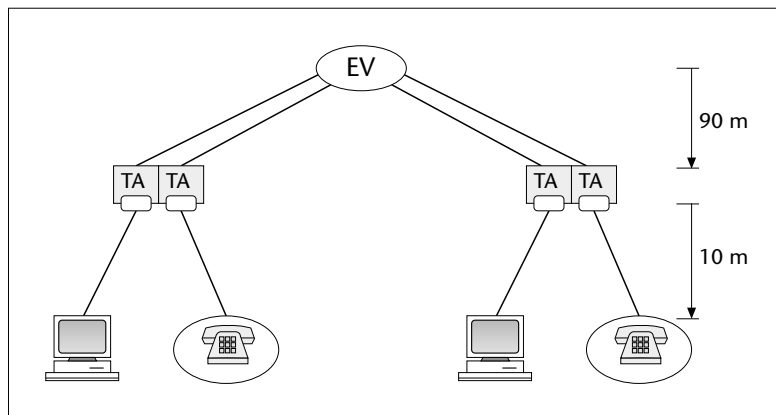
- *Elektromagnetische Verträglichkeit*

Hier müssen europäische Normen für elektromagnetische Störaussendung und Störfestigkeit beachtet werden (z.B. EN 55 022). Die Gebäudeverkabelung ist als passive Einrichtung zu sehen, die für sich allein nicht auf Konformität mit den Regeln der EMV geprüft werden kann. Eine aktive Einrichtung, die für ein bestimmtes Medium entworfen wurde, muß die entsprechende EMV-Norm einhalten.

5. Ausführungsbeispiele

Ein Modell für die Übertragungsstrecke im Tertiärbereich wird in nachfolgender Darstellung veranschaulicht. Die bevorzugten Kabel sind dabei 100-Ohm-Kabel. Alternativ sind das 120-Ohm-, das 150-Ohm-Kabel und LWL erlaubt. Abbildung 5.15 zeigt die Möglichkeit eines Aufbaus der Verkabelung zwischen Etagenverteiler und Endgerät.

Abbildung 5.15
Aufbau einer Verkabelung



6. Klassifizierung von Anwendungen und Übertragungsstrecken

Der internationale bzw. europäische Verkabelungsstandard ISO/IEC 11801 bzw. EN 50173 definiert für symmetrische Verkabelungen vier Anwendungsklassen: A bis D.

5.2 Verkabelung der Zukunft und Vorschriften

- *Klasse A*
Sprach- und Datenverbindungen für niederfrequente Anwendungen bis 100 kHz.
- *Klasse B*
Datenverbindungen für Anwendungen mit mittleren Bitraten, bis 1 MHz spezifiziert.
- *Klasse C*
Datenverbindungen für Anwendungen mit hohen Bitraten, bis 16 MHz spezifiziert (10Base T).
- *Klasse D*
Datenverbindungen für Anwendungen mit sehr hohen Bitraten, bis 100 MHz spezifiziert (TPDDI, ATM).

Häufig verwendete Bezeichnungen für Transmissions- und Nahnebensprechdämpfung sind auch Dämpfung und Next.

7. Anforderungen an das Kabel

Die symmetrischen Datenkabel werden nicht nur durch ihre elektrischen Kenndaten, sondern auch durch mechanische Anforderungen charakterisiert. Dabei wurden die mechanischen Anforderungen an ein in komplizierten Kabeltrassen zu verlegendes Datenkabel mit berücksichtigt. Dies findet seinen Niederschlag in der Angabe von maximalen Zugfestigkeiten, Brennverhalten wie auch in minimalen Biegeradien.

In der folgenden Tabelle sind die Anforderungen an das Kabel noch einmal zusammengefaßt.

Leiterdurchmesser	0,4 mm – 0,65 mm
Leiterzahl	>= 2 Paare / >= 1 Quad
Kabeldurchmesser	<= 20 mm
Temperaturbereich	-20C – 60C 0C – 50C
Biegeradius	4 x Durchmesser

8. Anforderungen an die Anschlußtechnik

In den Verteilern sind alle Arten der Anschlußtechnik erlaubt. Im Enddosenbereich dagegen ist gemäß der EN 60603-7 nur der Einsatz von 8poligen Steckern in geschirmter oder ungeschirmter Ausführung zugelassen.

Bei Verwendung von zweipaarigen Datenkabeln pro Anschlußdose ist die Standardzuordnung von Stift 4 und 5 bzw. 3 und 6 mit der Paarzuordnung zu belegen. Dies ist allerdings nur eine Empfehlung und kann von Fall zu Fall anders entschieden werden. Betrachtet man z.B. die Steckerbelegung bei einer Ethernet-Netzwerkstruktur (1, 2, 3 und 6), wird man feststellen, daß es Abwei-

5 Netzwerkkonzeption

chungen von dieser Empfehlung gibt. Es ist darauf zu achten, daß die Paarverdrillung bis zum Klemmblock der Anschlußdose erhalten bleibt.

9. *Behandlung von Schirmen*

Damit die Schirmung effektiv ausgenützt werden kann, ist es erforderlich, die Anforderungen an den Kopplungswiderstand, wie in den Abschnitten 7 und 8 verlangt, zu erfüllen. Die Schirmung muß vom Sender zum Empfänger durchgehend sein. Diese Anforderungen gelten auch für Arbeitsplatz- und Gebäudeverkabelungen, die nicht zur anwenderneutralen Verkabelung gehören, aber Teil der Übertragungsstätte von Sender und Empfänger sind. Erdungsmaßnahmen sind nach dem Stand der Technik auszuführen.

10. *Verwaltung*

Die gesamte Verkabelungsanlage muß so gekennzeichnet werden, daß eine Verwechslung der einzelnen Anschlüsse, soweit es geht, ausgeschlossen werden kann. Es ist ein geeignetes Verwaltungssystem zu verwenden, das leicht zu ändern und auf den neuesten Stand zu bringen ist. Kabel und Anschlüsselemente sind so zu kennzeichnen, daß es keine Verwechslungen geben kann.

5.2.7

Zukunftssichere Verkabelung

Der momentane Trend geht eindeutig zu den 100-Ohm-Kabeln. Selbst IBM bietet inzwischen die 100-Ohm-Technologie an.

Es sei noch einmal darauf hingewiesen, daß die Begriffe STP, UTP, S-UTP und S-STP nicht genormt bzw. standardisiert sind und lediglich vom Kabelhersteller definiert werden.

Trotzdem haben sich diese vier Begriffe im sprachlichen Gebrauch durchgesetzt, die Übersetzung der Abkürzungen erklärt in der Regel das sich dahinter verbergende Kabel.

■ *UTP*

Unshielded-Twisted-Pair (Kabel ohne Paarschirm, ohne Gesamtschirm)

■ *STP*

Shielded-Twisted-Pair (Kabel mit Paarschirm, ohne Gesamtschirm)

■ *S-UTP*

Screened-Unshielded-Twisted-Pair (Kabel ohne Paarschirm, mit Gesamtschirm)

■ *S-STP*

Screened-Shielded-Twisted-Pair (Kabel mit Paarschirm, mit Gesamtschirm)

5.3 Strukturierte Verkabelung – das ist zu beachten

An dieser Stelle kommt auch immer wieder die Diskussion auf, ob bei einer zukunftsicheren Verkabelung 4adrig (2 Leiterpaare) oder 8adrig (4 Leiterpaare) Kabel verwendet werden sollen. Wenn man eine flexible Verkabelung aufbauen will, die sowohl für Ethernet, Token-Ring, CDDI (FDDI auf Twisted Pair-Basis) oder ATM eingesetzt werden kann, empfiehlt sich der Einsatz von 8adrigen Kabeln. Alle acht Adern werden dabei sowohl im Verteiler als auch an der Dose aufgelegt. Das Patch-Kabel an der Workstation ist dann dafür zuständig, die richtigen Adern bei der Datenübertragung zu verwenden. Da die Pinbelegung bei Ethernet anders aussieht als bei Token-Ring oder ATM, wird damit eine flexible Verkabelung aufgebaut. Man kann aber auch ein einheitliches Patch-Kabel verwenden, da durch die Netzwerkadapterkarte entschieden wird, welche Adernpaare für das jeweilige Netzwerk benötigt werden.

Setzt man hingegen auf 4adrig Kabel, dann müssen in der Regel kodierbare Dosen eingesetzt werden, um die korrekte Pinbelegung für Ethernet und später Token-Ring oder ATM einsetzen zu können. Bei diesen Dosen muß beim Aufbau von Ethernet ein spezieller Adaptereinsatz für Ethernet und bei einer Umstellung auf ATM oder Token-Ring der Einsatz für ATM oder Token-Ring getauscht werden.

Sie sehen, daß Sie beim Einsatz von 8adrigen Kabeln wesentlich besser bedient sind, da Sie sich zukünftig keinerlei Gedanken mehr darüber machen müssen, ob Sie einen anderen Adaptereinsatz oder ein anderes Patch-Kabel benötigen. Die neue Gigabit Ethernet-Spezifikation 802.3ab legt fest, daß zur Datenübertragung über CAT-5-Kabel vier Adernpaare verwendet werden, da über jedes Paar 250 Mbit/s übertragen werden. In diesem Falle haben Sie mit 4adrigen Kabeln keine Chance mehr. Ein 8adriges Kabel öffnet Ihnen den Weg zum Aufbau von erweiterbaren, ausbaufähigen und flexiblen Verkabelungsstrukturen.

5.3 Strukturierte Verkabelung – das ist zu beachten

Bei der Netzwerkplanung, Bauüberwachung und Abnahme von Netzwerkverkabelungen kommt es immer wieder zu Fehlern, die im Zuge der Verkabelung auftreten und dann auch zu Netzwerkfehlern führen, wenn aktive Komponenten (Server, Workstation, Netzdrucker etc.) in Betrieb genommen werden. Oft stellt sich heraus, daß für eine Vielzahl von Netzausfällen oder Netzwerkfehlern Kabel und Steckerverbindungen verantwortlich sind. Es wird häufig unterschätzt, daß beim unsachgemäßen Umgang mit Datenkabeln und

5 Netzwerkkonzeption

der Anschlußtechnik (Dosen, Patchfelder) das elektrische Verhalten der physikalischen Infrastruktur beeinflusst wird und dies der Grund für Netzwerkfehler sein kann. Das beginnt beim nicht eingehaltenen Biegeradius und hört bei der Montage der Stecker auf.

Es sollten nicht erst zum Zeitpunkt der Abnahme die dazugehörigen Kabelmeßprotokolle vorliegen. Wir achten immer darauf, daß die Meßprotokolle bereits vor der Abnahme vorliegen, um zur Prüfung genügend Zeit zu haben. Während der Abnahme kann man dann bereits auf festgestellte Mängel hinweisen bzw. die Behebung dieser Mängel veranlassen.

Bei der Verkabelung kann eine Vielzahl von Fehlern gemacht werden. Auf die wichtigsten Fehlerquellen, die auftreten können und die bei einer Netzwerkabnahme beachtet werden sollten, wird im nächsten Abschnitt eingegangen.

5.3.1 Mögliche Fehlerquellen bei der Verlegung

Um bereits im Vorfeld eine Vielzahl möglicher Fehlerquellen und -ursachen zu vermeiden, sollte darauf geachtet werden, daß zumindest die folgenden Vorschriften, Normen und Richtlinien eingehalten werden:

- Vorschriften und Richtlinien des Hardware-Lieferanten
- Richtlinien des Auftraggebers
- Europäische Verkabelungsnormen (EN)
- VDE-Normenreihe

Offene Verlegung, Mauerdurchbrüche und Kabelkanäle

Wenn Kabel offen verlegt werden, ist es wichtig, daß in diesen Bereichen (Steigtrassen, Verbindungsschächte oder auch andere Verteilerräume) eine Beschädigung des Kabels ausgeschlossen ist. Die Kabel werden in der Regel durch Schellen oder Kabelbinder an einer Profilschiene (Kabeltrasse, Gitterkanäle) befestigt. Es muß unbedingt darauf geachtet werden, daß die Kabel beim Befestigen nicht gequetscht werden, d. h., der Druck auf das Kabel nicht zu groß ist. Vor der Verlegung der Kabel sollte auch untersucht werden, ob die Ecken und Kanten der Mauerdurchbrüche gerundet bzw. gebrochen sind, damit beim Einziehen der Kabel keine Beschädigungen auftreten können. So ist bei scharfen Kanten die Gefahr sehr groß, daß nicht nur der Außenmantel des Kabels kaputtgeht, sondern dadurch auch die Schirmung stark beschädigt werden könnte. Wenn das Kabel verlegt ist, fällt es unter Umständen nicht mehr auf, daß massive Beschädigungen erfolgt sind. Einen Aufschluß über solche Fehlerquellen erhält man in der Regel über die Auswertung der Meßproto-

5.3 Strukturierte Verkabelung – das ist zu beachten

kolle. Ebenso ist darauf zu achten, daß die vom Kabelhersteller vorgegebenen maximalen Biegeradien nicht überschritten werden. Bei Nichtbeachtung ändern sich auch in diesem Fall die physikalischen Eigenschaften eines Kabels, mit dem Effekt, daß bei einem späteren Netzbetrieb Störungen auftreten. Auch solche Situationen können durch gute Meßprotokolle erkannt werden. Bei der Verlegung der Kabelkanäle ist bereits darauf zu achten, daß der Radius der Kabelkanäle bei Richtungsänderungen dem vorgeschriebenen Biegeradius des Kabels entsprechen.

Das Einziehen von Kabeln ist nicht ganz einfach. Man sollte generell vermeiden, fett- und ölhaltige Mittel als Gleitmittel zu verwenden. Beim Einziehen der Kabel dürfen die vom Hersteller spezifizierten maximal erlaubten Zugkräfte nicht überschritten werden.

Biegeradius

Entsprechend den Vorgaben durch die EN 50173 beträgt der maximal erlaubte Biegeradius während des Kabeleinzugs das Achtfache des Kabelaußendurchmessers. Es kann aber durchaus sein, daß der Kabelhersteller dafür andere Angaben macht. Deshalb sollte vor dem Kabeleinzug immer noch geprüft werden, welche spezielle Herstellerangaben gemacht werden.

Druck auf Datenkabel

Man sollte es nicht glauben, aber ein zu großer Druck während oder nach der Verlegung der Datenkabel kann zu einer permanenten Störung führen. Es muß deshalb vermieden werden, daß Druck durch z.B. unsachgemäßes Befestigen mittels Schellen oder Kabelbinder entsteht. Zudem sollten Kabel nicht gekreuzt verlegt werden oder auf Kabeln herumgetreten werden, da in diesem Falle dauerhafte Druckstellen auftreten, die sich negativ auf die Eigenschaften der Adern auswirken können. Da diese Druckstellen eine Änderung der elektrischen Übertragungseigenschaften an den Druckstellen bewirken, sind aussagefähige Meßprotokolle notwendig, um solche Fehlerquellen zu erkennen.

Wärmeeinfluß auf Datenkabel

Das eingesetzte Material zum Aufbau der neuen Datenkabel ist sehr empfindlich gegenüber starker Wärmeentwicklung; es reagiert auf die direkte Wärmeeinwirkung auf das Kabel. Aus diesem Grund ist es zu unterlassen, Datenkabel mit einem Heißluftfön oder einem Gasbrenner zu bearbeiten. Ein Datenkabel ist kein Schrumpfschlauch, und deshalb muß sorgsam damit umgegangen werden.

5 Netzwerkkonzeption

Generell sollte darauf geachtet werden, daß nach Möglichkeit Datenkabel in Kabelschächten von anderen Kabeln getrennt verlegt werden, um mögliche Beeinflussungen zu vermeiden. Aus diesem Grund sollten Trennsteg in den Kabelkanälen vorhanden sein, sofern neben den Datenkabeln auch noch andere Kabel verlegt sind.

Anschluß im Patchpanel und an RJ45-Anschlußdosen

Der wichtige und wesentliche Bestandteil einer ordnungsgemäßen Verkabelung wird nicht nur durch die Verlegung der Kabel selbst gebildet (wie in den vorherigen Abschnitten beschrieben), sondern auch entscheidend durch das richtige Auflegen der Kabel im Patchpanel bzw. an der Endgerätesteckdose beeinflußt. So ist zu beachten, daß der Folienschirm des Kabels nur so weit entfernt wird, wie dies auch tatsächlich notwendig ist. Bei einer Vielzahl von Anschlußsystemen ist es jedoch notwendig und vorgeschrieben, daß die Folien der einzelnen Paare bzw. Vierer ab dem letzten Schirmabgriff nicht weitergeführt werden. Die Vorschriften hierfür hängen vom Hersteller des jeweiligen Anschluß-Systems ab.

Damit bei Twisted-Pair-Kabeln ein gutes Nahnebensprechen (NEXT) garantiert werden kann, wird vorgeschrieben, die einzelnen Paare bzw. Vierer beim Anschließen im Patchpanel bzw. an der Endgerätedose so lange wie möglich in der originalen Adernverdrillung zu belassen. Für ein ordnungsgemäß verlegtes CAT-5-Kabel schreibt die EN 50173 vor, daß die maximale Aderlänge ohne Verdrillung nicht größer als 13 mm sein soll. Es gibt eine Vielzahl von Installationen, bei denen diese Vorschriften nicht beachtet werden. Diese Verkabelungen bereiten in Netzwerken mit niedrigen Übertragungsraten in der Regel keine Schwierigkeiten, sobald jedoch höhere Übertragungsraten zum Einsatz kommen, wirken sich solche Verkabelungsfehler sehr negativ auf das gesamte Netzwerk aus.

Ein ebenso kritischer Punkt beim Verlegen von Twisted-Pair-Kabeln ist der Anschluß des Schirms bei Kabeln mit Folie bzw. mit Geflecht (S/UTP, S/STP). Generell gilt dabei, daß die Schirmung großflächig aufgelegt werden muß. Das Auflegen eines Beilaufdrahts hat bei weitem nicht die notwendige Wirkung. Je nach Anschlußseinheit muß das freiliegende Geflecht am Ende des Kabels ca. 1–2 cm über den Mantel gezogen werden. Anschließend klappt man in der Regel das Geflecht so nach vorne, daß die doppelte Stärke erreicht wird.

Beim Installieren der Kabel und Anschlußsysteme (Datenanschlußdose und Patchpanel) ist darauf zu achten, daß diese kompatibel zueinander sind. So sollte man auf alle Fälle vermeiden, daß man zum Beispiel ein CAT-5-Kabel verlegt und im Patchpanel oder in der Da-

5.3 Strukturierte Verkabelung – das ist zu beachten

tenanschlußdose CAT-4-RJ45-Anschlußtechniken verwendet. Zudem kann es bei RJ45-Buchsen und -Steckern zu Fertigungstoleranzen bei den einzelnen Fabrikaten kommen. Dies kann sich in Leistungseinbußen und schlechteren Übertragungseigenschaften auswirken. Aus diesem Grund wird generell empfohlen, Stecker und Buchsen nach Möglichkeit vom gleichen Hersteller bzw. das gleiche Fabrikat zu verwenden. Da alle im Netzwerk eingesetzten passiven Komponenten der Link Performance standhalten müssen, ist dies nicht nur für das Kabel zu fordern (d. h., die Einhaltung der CAT-5-Spezifikationen muß beachtet werden). Die Link Performance muß deshalb für die gesamten passiven Übertragungseinrichtungen eingehalten und garantiert werden.

5.3.2 Typische Probleme einer strukturierten Verkabelung

Es wurde bereits in den vorherigen Ausführungen mehrfach darauf hingewiesen, daß bei Nichtbeachtung bestimmter Randbedingungen für eine strukturierte Verkabelung mit Störungen zu rechnen ist. In diesem Abschnitt sollen deren häufigsten Ursachen erläutert werden.

Schlecht gecrimpte Stecker

Beim Einsatz symmetrischer Kabel verwendet man in der Regel RJ45-Stecker für die Verbindung zwischen der Netzwerkkarte und dem Hub-System. Diese RJ45-Stecker bestehen aus Kunststoff und einer Zugentlastung am hinteren Ende. Wenn nicht genau darauf geachtet wird, daß die Zugentlastung ordnungsgemäß auf den Kabelmantel gequetscht ist, dann lastet bei jedem Steckvorgang die ganze Kraft auf den Steckkontakten. Nach kürzester Zeit kann damit gerechnet werden, daß erhöhte Übergangswiderstände (Dämpfung) auftreten und es zudem zu zeitweiligen Aussetzern kommen kann. Wenn Anwender über schlechte Datenübertragung klagen und wenn die Datenübertragung durch häufige Wiederholungen langsam wird, kann dies unter Umständen dadurch gelöst werden (wenn alle andere Überprüfungen kein Ergebnis gebracht haben), daß RJ45-Stecker eingesetzt werden, bei denen die Zugentlastung ordnungsgemäß implementiert ist.

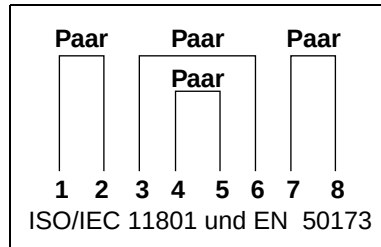
Split-Pair beim Auflegen der Kabeladern

Von einem Split-Pair spricht man dann, wenn Adern einzelner Paare vertauscht werden. Dies resultiert darin, daß in den Meßprotokollen für Split-Pair-Kabel schlechte NEXT-Werte (ca. 20 dB bei 100 MHz) und eine zu hohe Impedanz von ca. 125 Ohm aufgeführt werden.

5 Netzwerkkonzeption

Die Datenübertragung wird dadurch wesentlich schlechter, da es dabei zu häufigen Wiederholungen kommt. Gemäß der ISO/IEC 11801 und der EN 50173 müssen die Paare im RJ45-Stecker wie in Abbildung 5.16 dargestellt belegt sein.

Abbildung 5.16
RJ45-Stecker-
belegung



Patch-Kabel mit schlechten Spezifikationen

Wird ein Kabelsystem der Klasse D für 100-MHz-Übertragungsbandbreite konzipiert und installiert, dann sollten die eingesetzten Produkte (Patchpanel, Kabel, Dose etc.) zumindest den Anforderungen der CAT 5 entsprechen. Nicht selten werden jedoch im Patch- und Anschlußbereich »minderwertige« flexible Patch- und Anschlußkabel eingesetzt, die den geforderten Spezifikationen für CAT 5 nicht entsprechen. Symptome treten erst beim Umstellen auf ein Hochgeschwindigkeits-Netzwerk auf, wenn die Funktion nicht mehr einwandfrei gewährleistet werden kann. Eine Ursache für die Störungen kann im Anschlußbereich gesucht werden. Deswegen sollten nur Patch- und Anschlußkabel verwendet werden, die die geforderten Anwendungen unterstützen bzw. die CAT-5-Spezifikationen für flexible Kabel erfüllen. Bei diesen Anforderungen soll der NEXT-Wert mindestens 32 dB und die Dämpfung maximal 33 dB/100 m betragen.

Keine durchgängige Schirmung

Die Schirmung der Kabel und Komponenten dient in erster Linie dazu, die Erfüllung aller Vorschriften zur Einhaltung der EMV (Elektromagnetische Verträglichkeit) zu gewährleisten. In diesem Zusammenhang gelten unter anderem die Normen EN 55022 und EN 50081. In diesen Normen wird vorgegeben, wie hoch der Strahlungspegel von Hochfrequenzsystemen maximal sein darf, um damit keine Störungen für Drittsysteme zu verursachen. Zudem wird festgelegt, wie störfest eine Hochfrequenzanlage sein muß. Um alle Normen und Vorschriften einhalten zu können, muß für eine durchgängige und breitflächige Schirmweiterleitung gesorgt werden. Nicht selten werden ungeschirmte Patch-Kabel eingesetzt, oder der Schirm der Kabel wird nicht oder nur unzureichend weitergeführt. Auch

5.3 Strukturierte Verkabelung – das ist zu beachten

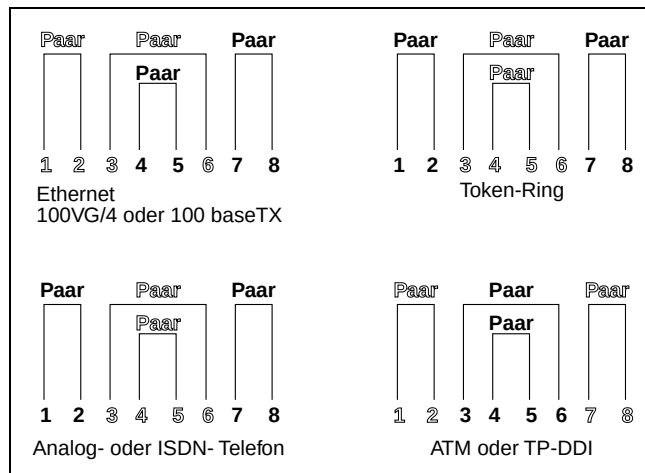
dies kann im ungünstigen Fall zu einer vermehrten Wiederholung der Datenübertragung führen, wodurch das Antwortzeitverhalten schlechter wird.

Verdrillung ist zu weit geöffnet

Beim Auflegen der Twisted-Pair-Kabel im Patch-Feld bzw. den Anschlußdosen muß das symmetrische Kabel abisoliert und für die jeweiligen Komponenten aufgelegt werden. Es ist äußerst wichtig, daß die Verdrillung nicht zu weit geöffnet wird (so weit wie nötig und so wenig wie möglich), da die Spezifikationen an diesen Stellen nicht mehr eingehalten werden können. Die maximal erlaubte Auflösung der Verdrillung beträgt 13 mm, wenn es um die Verlegung von CAT-5-Kabel geht. Es sollte auch nicht der Versuch unternommen werden, eine zu weit geöffnete Verdrillung per Hand nachzudrehen, da dadurch nie die notwendigen Spezifikationen eingehalten werden können. Deshalb muß bereits vor der Kabelauflegung darauf geachtet werden, die Spezifikationen einzuhalten bzw. zu erfüllen.

Abschließend sollen die wichtigsten Datendienste und die dafür notwendigen Pinbelegungen auf dem RJ45-Stecker aufgeführt werden.

Abbildung 5.17
Pinbelegung und
Datendienste



In den letzten Monaten liest und hört man immer mehr über Kategorie-6- und Kategorie-7-Kabel. Es stellt sich die Frage, ob der Aufbau einer Neuverkabelung mit Kategorie-5-Kabeln noch zukunftssicher ist oder ob er bereits mit diesem neuen Kabel erfolgen soll. Im nächsten Kapitel soll deshalb aufgezeigt werden, was es mit den neuen Kategorien auf sich hat.

5.4 Was ist dran an den neuen Kategorien?

Wenn man die Kabelhersteller befragt, dann erhält man über die neuen Kabelstandards die unterschiedlichsten Aussagen: Entweder erachtet man Kategorie-5-Kabel für vollkommen ausreichend, oder man empfiehlt, statt Kategorie 6 bzw. 7 bis zum Arbeitsplatz zu installieren, endlich über LWL bis zum Arbeitsplatz nachzudenken. Alle diese Aussagen verwirren nur, statt einem die Entscheidung zu erleichtern. Ich will deshalb versuchen, den derzeit aktuellen Stand dieser beiden neuen Kabel-Standards etwas näher zu erläutern. Alle diese Informationen basieren auf Informationen, die ich von der Firma Dätwyler, einem der bekanntesten Kabelhersteller, erhalten habe.

Es ist mittlerweile für Netzwerkplaner, Installationsunternehmen und die Betreiber von Netzwerken schwierig, die richtige Entscheidung für das richtige Kabel im Netzwerk bei der Planung eines zukünftigen Netzwerks oder der Erneuerung des Netzwerks zu treffen. Kaum hat man sich daran gewöhnt, daß es ein Kategorie-6-Kabel geben wird, muß man sich bereits mit Kategorie 7 auseinandersetzen. Nicht selten werden dabei Begriffe durcheinandergeworfen, die deshalb immer wieder zu Verwirrungen führen. Für den deutschen Markt muß man sich zum heutigen Zeitpunkt an folgendes halten:

Es gibt derzeit nur eine existierende Norm, nämlich DIN EN 50173 vom November 1995 für die anwendungsneutrale Verkabelung der Kategorie 5, Klasse D und spezifiziert bis 100 MHz. Die bisherige Kategorie 6, Klasse E, war der deutsche Entwurf E DIN 44312-5 für eine europäische Norm, also nur ein Vorschlag und keine Norm. Mittlerweile hat sich weltweit auch die IEC dieser Problematik angenommen. Auf der Sitzung der ISO/IEC JTC/SC 25/WG im September 1997 in München wurde folgendes beschlossen:

1. Ein Entwurf für eine Kategorie 6, Klasse E, die jedoch nur bis 200 MHz spezifiziert ist.
2. Ein Entwurf für eine Kategorie 7, Klasse F, spezifiziert bis 600 MHz.

Für die Kategorie 6 wurden nur die elektrischen Werte für den Link niedergelegt. Die Werte für die Kabel und die Verbindungstechnik müssen noch mit den entsprechenden Working Groups abgestimmt werden. Die Werte hierfür liegen bis heute noch nicht vor. Wichtig ist dabei folgende getroffene Festlegung:

Die Daten der bisherigen Kategorie 6 werden als internationaler Vorschlag unverändert als Kategorie 7 übernommen.

5.4 Was ist dran an den neuen Kategorien?

Wichtig: Kategorie 6 ist jetzt Kategorie 7 – Kategorie 6 wird neu definiert.

In der Tabelle 5.2 sind alle Werte aufgeführt, die eingehalten werden müssen, um Kategorie 5, Klasse D, zu erfüllen, sowie der Vorschlag für Kategorie 7, Klasse F.

*Tabelle 5.2
Mindestanforderungen an Links
der Kategorie 5,
Klasse D und Kategorie 7, Klasse F*

Klasse D (DIN EN 50173)				Klasse F (E DIN 44312-5 und Vorschlag ICE)		
f(MHz)	maximale Dämpf. [dB]	minimaler NEXT [dB]	minimaler ACR [dB]	maximale Dämpf. [dB]	minimaler NEXT [dB]	minimaler ACR [dB]
1	2,5	54	--	2,3	74	60
4	4,8	45	40	4	74	60
10	7,5	39	35	6,2	74	60
16	9,4	36	30	7,7	74	60
20	10,5	35	28	8,6	74	60
31,25	13,1	32	23	10,7	74	60
62,5	18,4	27	13	15,3	69,3	54
100	23,2	24	4	19,2	66,1	46,9
175				25,3	62,3	37
300				33,1	58,7	25,6
600				50	54	4

Erfahrungsgemäß wird es noch eine geraume Zeit dauern, bis man sich auf einheitliche Werte geeinigt hat und entsprechende Standards verabschieden kann.

Bezüglich der einzusetzenden Steckertechnik gibt es ebenso kontroverse Diskussionen, und am Markt werden deshalb aufgrund fehlender Standards von den einzelnen Kabelherstellern auch unterschiedliche Steckervarianten angeboten, die angeblich alle für Kategorie 6 bzw. Kategorie 7 zertifiziert sind. Hierzu liegen mir derzeit die folgenden Informationen vor:

Grundsätzlich bauen diese Normen auf die bestehende, bereits verabschiedete Norm auf, die im Anschlußbereich RJ 45 vorschreibt, und nichts anderes ist derzeit als Basis für Kategorie 6 und Kategorie 7 vorgesehen. Dies ist vor allem unter dem Aspekt zu berücksichtigen, daß einige Hersteller eigene Stecksysteme entwickelt haben. Dabei handelt es sich aber ausschließlich um firmenspezifische Lösungen, wobei man davon ausgehen kann, daß diese mit ziemlicher Sicherheit nicht in den Standard aufgenommen werden.

Im Gegensatz zur Kategorie 5, Klasse D, in der alle Werte bei jeder möglichen Kontaktbelegung (PIN) des Western Plug (RJ 45) gelten und in der bei der zweipaarigen Verkabelung die bevorzugten Kon-

5 Netzwerkkonzeption

takte die PINs 36–45 sind, gelten die Werte in der Kategorie 6, Klasse E, bzw. Kategorie 7, Klasse F, nur bei den Kontakten 12–78. Die Kontakte 36–45 sind noch in Beratung.

Als Beispiel sei erwähnt, daß die Firma Dätwyler von der Gesellschaft für Hochfrequenz-Meßtechnik mbH die Zertifizierung der in Frage kommenden Kabel für bis zu 600-MHz-Links über RJ-45-Stekker durchführen ließ.

Dabei wurde eine Linkprüfung nach der EN 50173 und in Anlehnung an die DIN 44312-5 (Entwurf) der Verkabelungsstrecke mit den hierfür notwendigen Komponenten durchgeführt. Die verwendeten Prüfparameter waren dabei:

- Laufzeit
- Laufzeitdifferenz
- Schleifenwiderstand
- Vierpoldämpfung
- Nahnebenschleifendämpfung
- ACR
- Reflexionsdämpfung
- Erdungssymmetriedämpfung

Als Prüfergebnis wurde ermittelt: Die bei der Durchführung erzielten Ergebnisse beziehen sich auf den beschriebenen und vorgelegten Prüfling. Der Prüfling hält in den genannten Prüfparametern die Grenzwerte der besagten Vorschriften ein.

In Abbildung 5.18 sind alle damit zusammenhängenden Komponenten und Ergebnisse zusammengefaßt dargestellt.

Soll man nun die neuen Kabel, in diesem Falle Kategorie-7-Kabel, einsetzen oder aufgrund fehlender endgültiger Standards besser die standardisierten Kategorie-5-Kabel verwenden? Diese Frage wird kontrovers diskutiert. Obwohl es von allen renommierten Kabelherstellern Kategorie-7-Kabel gibt, erhält man zum Teil selbst von diesen unterschiedliche Aussagen. Auch wenn es noch keine endgültig verabschiedeten Kategorie-7-Spezifikationen gibt, kann man dennoch davon ausgehen, daß alle Vorausangaben in dieser Form verabschiedet werden und sich deshalb auch alle Kabelhersteller daran halten können. Wenn man zukunftsicher investieren will, dann ist prinzipiell anzuraten, die hochwertigsten Twisted-Pair-Kabel einzusetzen, die erhältlich sind und Kategorie-7-Kabeln entsprechen. Da Glasfaser bis zum Arbeitsplatz immer noch teurer als Kupferkabel ist, tendiert man nach wie vor dazu, das Netzwerk in den Etagen auf Basis von Twisted-Pair-Kabeln aufzubauen.

5.4 Was ist dran an den neuen Kategorien?

Abbildung 5.18
Zertifizierter 600-
MHz-Link über RJ
45 für Dätwyler-
Kabel

Linkwerte nach Kategorie 7, Klasse F (E DIN 44312-5 und Vorschlag der IEC)											
Frequenz [MHz]	1	4	10	16	20	31,25	62,5	100	175	300	600
Dämpfung [MHz]	2,3	4	6,2	7,7	8,6	10,7	15,3	19,2	25,3	33,1	50
NEXT [dB]	74	74	74	74	74	74	69,3	66,1	62,3	58,7	54
ACR [dB]	60	60	60	60	60	60	54	46,9	37	25,6	4

Linkwerte aus den GHMT-Zertifikaten für Dätwyler-Kabel und -Komponenten											
Frequenz [MHz]	1	4	10	16	20	31,25	62,5	100	175	300	600
Uninet 3004 4P											
Dämpfung [dB]	1,7	3	5	6,4	7,1	8,9	12,7	16,4	22,8	30	42,7
NEXT [dB]	100	100	97,7	91,8	88,5	83,1	78,5	74,6	70,2	65,8	58,1
ACR [dB]	98,3	97	92,7	85,4	81,4	74,2	65,8	58,2	47,4	35,8	15,4
Uninet 7002 4P											
Dämpfung [dB]	1,9	3,5	5,6	6,9	7,7	10	14	18,3	24,5	32,5	46,6
NEXT [dB]	98,5	96,5	93,5	91,2	90	85,8	79,2	77,7	74	70	60
ACR [dB]	96,6	93	87,9	84,3	82,3	75,8	65,2	59,4	49,5	37,5	13,4
Uninet 8002 4P											
Dämpfung [dB]	1,7	3,1	5	6,3	7,1	9,1	12,7	16,2	22,5	30	41,5
NEXT [dB]	102,3	100	96,9	94	91,5	85,8	81,9	78,9	72	67,7	60
ACR [dB]	100,6	96,9	91,9	87,7	84,4	76,7	69,2	62,7	49,5	37,7	18,5

Die ständigen Verbesserungen und Erweiterungen für Twisted-Pair-Kupferkabel führen dazu, mit Twisted-Pair-Kabeln noch höhere Übertragungsgeschwindigkeiten zu erreichen. Deshalb ist es auch nicht notwendig, im Etagenetzwerk nur Glasfaser einzusetzen. Nach der Verlegung von Kupferkabeln und/oder Glasfaserkabeln darf eines nicht vergessen werden: die Erstellung von Meßprotokollen – das ist unabdingbar für jede physikalische Netzwerkinfrastruktur. Da für Kategorie-7-Kabel die notwendigen Meßinstrumente fehlen, können diese nicht bis 200 MHz bzw. bis 600 MHz gemessen werden, sondern nur bis 100 MHz, entsprechend den Werten, die für Kategorie-5-Kabel in der Norm definiert sind. Dies sollte einen aber nicht davon abhalten, bereits jetzt die besseren Kabel einzusetzen, auch wenn man noch nicht in der Lage ist, bis hin zu 600 MHz zu prüfen bzw. zu messen. Physikalisch ist man jedoch bei 600 MHz noch nicht am Ende des technisch Möglichen. Nach Aussagen einzelner Hersteller ist man durchaus in der Lage, auf Twisted-Pair-Kabeln Übertragungsraten von bis zu 1 GHz zu erreichen. Man kann deshalb davon ausgehen, daß wir in den nächsten Jahren immer noch »Überraschungen« auf dem Gebiet der Twisted-Pair-Kabel erwarten können. Erst wenn auch für das Twisted-Pair-Kabel das physikalisch Mögliche erreicht ist, wird es keine Diskussion mehr über Glasfaser bis zum Arbeitsplatz geben. Solange es noch Preisunterschiede von Glasfaser bis zum Arbeitsplatz zur Twisted-Pair-Verkabelung gibt und solange es noch

5 Netzwerkkonzeption

nicht die gleiche Portdichte für die Einschubmodule im Hub-System gibt, wird Glasfaserverkabelung hauptsächlich im Primär- und Sekundärbereich eingesetzt werden. Glasfaser bis zum Arbeitsplatz wird derzeit vor allem dann eingesetzt, wenn die Umgebungsbedingungen dies erfordern, d.h. wenn die Störeinflüsse bei Kupferkabel so hoch sind, daß eine störungsfreie Datenübertragung nur noch auf Basis einer Glasfaserverkabelung gewährleistet werden kann. Es wird deshalb noch einige Jahre dauern, bis Glasfaser bis zum Arbeitsplatz tatsächlich realisiert sein wird.

Sie haben in diesem Kapitel erfahren, welche Vorschriften und Normen existieren, wenn eine strukturierte Verkabelung aufgebaut werden soll, und welche Spezifikationen für Twisted-Pair-Kabel existieren bzw. in Vorbereitung sind. Nicht weniger wichtig ist in diesem Zusammenhang die Möglichkeit, auf Ereignisse im Netzwerk schnell und flexibel zu reagieren.

Aus diesem Grund will ich im nächsten Kapitel auf einige wichtige Aspekte des Netzwerkmanagements – Einsatz und Funktionsweise – eingehen.

6

Netzwerkmanagement

Ein Netzwerk mit nur wenigen PCs und einem Server zu verwalten ist eigentlich kein Problem. Anders sieht die Sache aus, wenn das Netzwerk aus sehr vielen unterschiedlichen Workstations (DOS, Unix, Macintosh, OS/2, Windows 95 oder NT) und einer Vielzahl von Servern, Gateways, Bridges, Routern und Hub-Systemen besteht. Erschwerend kommt oft noch hinzu, daß das Netzwerk nicht nur aus einer Topologie besteht, sondern aus Ethernet, Token-Ring, FDDI und auch schon ATM aufgebaut ist. Unterschiedliche Topologien, Server, Host-Systeme etc. bedeuten auch, daß im Netzwerk nicht nur ein Protokoll zum Einsatz kommt, sondern eine Vielzahl unterschiedlicher Protokolle genutzt werden muß, um eine Kommunikation untereinander zu ermöglichen.

Es ist schon schwierig, auftretende Fehler überhaupt zu lokalisieren, bevor man sich an ihre Behebung machen kann, wenn es sich um heterogene Netzwerke der oben beschriebenen Form handelt. Um Netzwerkadministratoren das Leben zu erleichtern, wird am Markt eine Vielzahl unterschiedlicher Netzwerkmanagement-Systeme angeboten.

Die Entwicklung auf dem Gebiet der Netzwerktechnik und Netzwerkmanagement-Technik hat uns in den letzten Jahren eine fast unüberschaubare Vielfalt an Techniken und Komponenten (Hard- und Software) beschert. Die richtige Auswahl zu treffen ist nicht leicht, da die »eierlegende Wollmilchsau« bis heute noch nicht erfunden worden ist. Sie werden also kein System finden, mit dem alle Anforderungen erfüllt werden können, und immer gezwungen sein, mehr als eine Lösung zu implementieren.

Die wichtigsten Fragen, die bei der Auswahl von Netzwerkmanagement-Systemen zu treffen sind, lauten: Welche Anforderungen werden an das gesuchte System gestellt, und was soll damit erreicht werden? Es ist zu unterscheiden, ob man klassische Systeme zur Überwachung der installierten aktiven und passiven Komponenten sucht (Hub-Systeme und Verkabelung) oder ob mit dem System auch Endgeräte wie Server, Workstations, Router oder Bridges überwacht werden sollen. Von diesen Anforderungen hängt es ab, welche Systeme in Frage kommen werden. Die Entscheidung ist dabei zwischen den herstellereigenen und herstellerunabhängigen Systemen zu treffen. Ein genauer Vergleich ist durchaus sinnvoll, da in der Regel die herstellereigenen Systeme in der Lage sind, alle Funktionen

6 Netzwerkmanagement

vollständig zu unterstützen. Bei herstellerunabhängigen Systemen kann es durchaus vorkommen, daß nicht alle Funktionen vollständig zur Verfügung stehen.

Wenn an das Netzwerkmanagement-System zudem noch die Anforderungen gestellt werden, Lizenzüberwachung, Software-Metering, Remote Control und dergleichen mehr zur Verfügung zu stellen, so kann dies unter keinen Umständen von nur einer Hard- und Software erfüllt werden, da sich die einzelnen Hersteller auf einzelne Aspekte konzentrieren. So liegt das Hauptaugenmerk für Cisco oder Cabletron vor allem darin, die Hardware-Komponenten im Hub zu überwachen und zu steuern. Das Software-Metering oder die Lizenzüberwachung hängt in dieser Situation vom jeweiligen Netzwerk ab, so daß hier auf zusätzliche Produkte zurückgegriffen werden muß. Die Komplettlösung aus einer Hand wäre zwar schön, aber die Einzelanforderungen sind so komplex, daß es wahrscheinlich immer darauf hinauslaufen wird, eine Lösung, die aus Einzelkomponenten zusammengesetzt ist, zu implementieren. Von Vorteil ist es in jedem Fall, wenn ein Daten- und Informationsaustausch zwischen den Produkten möglich ist.

Kennzeichnend für eine heterogene Netzwerklandschaft ist nicht nur der Einsatz der unterschiedlichsten Hardware-Komponenten, sondern meist auch eine heterogene Protokollandschaft. Wenn es nur ein Protokoll zur Kommunikation in Netzwerken geben würde, wäre das zwar wünschenswert – das wird aber für die nächsten Jahre Wunschdenken bleiben. Man wird sich damit abfinden müssen, daß unterschiedliche Rechnerwelten auch unterschiedliche Protokolle einsetzen. Die Idee von OSI als Einheitsprotokoll hat sich inzwischen als Traum erwiesen, da die etablierten Protokolle bereits so weit verbreitet sind, daß eine Umstellung auf OSI mit enormen Kosten und Aufwendungen verbunden wäre (immer unter dem Gesichtspunkt, daß auch jeder Hersteller OSI verfügbar hätte – was noch nicht der Fall ist).

Die eingesetzten Protokolle sind stark abhängig vom jeweiligen Hersteller des Systems. So wird man in der IBM-Großrechnerwelt immer noch auf SNA stoßen, obwohl es inzwischen auch möglich ist, Terminalemulationen über TCP/IP zu realisieren. IBM ist inzwischen, wie andere Hersteller auch, in der Lage, TCP/IP als Protokoll zu unterstützen. Zu beachten ist dabei nur, daß die TCP/IP-Implementierung auf Host-Seite sehr kostspielig ist. In einem Netzwerk mit NetWare als Serversystem kommen die Protokolle IPX/SPX zum Einsatz. Auch hier ist man inzwischen in der Lage, durch NetWare IP und Native-IP im Netzwerk, TCP/IP als Transportprotokoll einzusetzen. Beim Einsatz von Apple wird man auf das Protokoll ATP stoßen. Auch hier soll

6 Netzwerkmanagement

es demnächst möglich sein, statt ATP als Transportprotokoll TCP/IP einzusetzen. Betrachtet man jetzt noch den NT Server 3.5, so verwendet auch Microsoft sein eigenes Protokoll, läßt jedoch die Wahl bei der Installation offen, TCP/IP als Transportprotokoll einzusetzen.

TCP/IP nimmt offensichtlich eine zentrale Stellung im Bereich der Protokolle ein. TCP/IP, ursprünglich aus der Unix-Welt kommend, zeichnet sich immer mehr als das universelle Protokoll aus, das so ziemlich von allen führenden Herstellern unterstützt wird. Auch im Bereich Netzwerkmanagement wird man oft auf diese Umgebung stoßen; dazu jedoch später mehr.

Hat man TCP/IP vor Jahren noch keine Chancen am Markt gegeben, wird dieses Protokoll gerade in den letzten Jahren in großer Zahl installiert, vor allem wenn es um den Aufbau von heterogenen Welten geht. Dies ist auch der Grund, warum TCP/IP zum De-facto-Standard zählt. TCP/IP bietet auf den Schichten 3 und 4 einfache anwendungsorientierte Grunddienste wie Dateitransfer, E-Mail und Virtual-Terminal-Emulation. Da auch Unix in den letzten Jahren immer mehr an Bedeutung gewonnen hat und TCP/IP sehr stark mit Unix verbunden ist, wurde und wird der zukünftige Einsatz von TCP/IP noch gefördert; der verstärkte Einsatz von Internet und Intranet-Anwendungen trägt wesentlich zum erhöhten Einsatz von TCP/IP bei.

Mit TCP/IP kann man in einfacher Weise heute das tun, was man eigentlich mit den Protokollen und Standards nach OSI hätte machen wollen. Geht es jedoch darum, hier und jetzt eine heterogene Welt aufzubauen, kommt man um den Einsatz von TCP/IP nicht herum. Das vor allem auch deswegen, weil man für dieses Protokoll schneller und einfacher Lösungen findet, als dies für OSI der Fall ist. Das hat auch Auswirkungen auf den Bereich Netzwerkmanagement, wenn es um die Entscheidung geht: Netzwerkmanagement nach SNMP (kommt aus der TCP/IP-Welt) oder nach OSI. Allerdings hat sich SNMP im Vergleich zu OSI so viel stärker am Markt etabliert, daß selbst Hersteller wie IBM, die ursprünglich ganz auf OSI-Netzwerkmanagement gesetzt haben, diese Entwicklungsrichtung nicht mehr unbedingt forcieren und sich lieber in Richtung SNMP-Netzwerkmanagement orientieren.

Jeder renommierte Hersteller bietet heute Implementierungen für TCP/IP an, um heterogene Welten erschließen zu können. In Zusammenhang damit werden auch Komponenten angeboten, die sich angeblich mit einem SNMP-Netzwerkmanagement-System überwachen lassen. Was von solchen Aussagen zu halten ist, werde ich an anderer Stelle behandeln. SNMP-Netzwerkmanagement bedeutet nicht

6 Netzwerkmanagement

immer, daß damit auch alle Informationen von einer beliebigen Netzwerkmanagement-Konsole abgerufen werden können. Nur soviel: Vorsicht ist geboten.

Mit TCP/IP als Protokoll für die Erschließung heterogener Welten hat man in der Regel auch die Gewißheit, daß Implementierungen unterschiedlicher Hersteller auch untereinander kommunizieren können und deren Dienste miteinander kompatibel sind. Dabei sollte es vollkommen gleichgültig sein, ob es sich um Installationen auf einem IBM-Host, einer Unix-Anlage, einer Siemens-Anlage oder einem PC mit TCP/IP-Protokoll-Stack handelt. Die Grundfunktionen FTP, SMTP und Telnet sollten auf alle Fälle problemlos einsetzbar sein und untereinander funktionieren.

Im Zuge der TCP/IP-Entwicklung wurde auch ein einfaches und leicht zu implementierendes Netzwerkmanagement-Protokoll entwickelt – SNMP (Simple Network Management Protocol) –, auf das später noch näher eingegangen wird. Wegen seiner Einfachheit und leicht zu realisierenden Implementierung unterstützt SNMP auch die Netzwerkkomponenten fast jedes Herstellers und erfreut sich bei Netzwerkadministratoren großer Beliebtheit. Das OSI-Netzwerkmanagement ist dagegen ins Hintertreffen geraten, auch wenn führende Hersteller versucht haben, OSI-Netzwerkmanagement am Markt zu etablieren. Im Gegenteil, um den gestiegenen Anforderungen gerecht zu werden, hat man SNMP weiterentwickelt und SNMPv2 verfügbar gemacht.

Das Netzwerkmanagement-Protokoll SNMP ist zwar meist mit TCP/IP als Protokoll verbunden, das muß aber nicht sein. So hat zum Beispiel die Firma Novell ein Netzwerkmanagement-System entwickelt (NMS), das, wie könnte es anders sein, für SNMP IPX als Transportprotokoll verwendet.

Aufgrund der Anforderungen am Markt ist SNMP-Unterstützung für jeden renommierten Hersteller zwingend geworden. So werden inzwischen bereits kleine Hub-Systeme angeboten, denen die SNMP-Funktionalität eingebaut worden ist. Für diese Systeme gibt es dann auch entsprechende Software-Lösungen, um das Netzwerkmanagement damit realisieren zu können. Eine Integration in andere Netzwerkmanagement-Lösungen ist in den meisten Fällen machbar (wenn auch zum Teil mit eingeschränkter Funktionalität und weniger komfortablen grafischen Darstellungen).

Anders sieht die Situation beim OSI-Netzwerkmanagement aus. Das liegt zum Teil daran, daß die Funktionalität der Kommunikationskomponenten vorhanden ist, das Netzwerkmanagement jedoch noch nicht eindeutig für OSI formuliert wurde. Eine Begründung hierfür

6 Netzwerkmanagement

ist unter anderem auch darin zu sehen, daß die OSI-Gremien das Netzwerkmanagement in der Vergangenheit eher stiefmütterlich behandelt haben, so daß jetzt zum entscheidenden Zeitpunkt die notwendigen Standards und Produkte fehlen. Mittlerweile werden verstärkt Anstrengungen unternommen, um an diesem Zustand etwas zu ändern, aber es werden noch ein paar Jahre vergehen, bis die Arbeit daran abgeschlossen ist. In den kommenden Jahren werden immer mehr SNMP-basierende Systeme eingesetzt werden, und eine Verdrängung bereits etablierter und gefestigter Komponenten und Softwareprodukte dürfte schwer fallen. Man hat anscheinend die Notwendigkeit und die rasante Entwicklung und die Bedarfsanforderungen unterschätzt. Dem SNMP-Management wird nachgesagt, es sei in seiner Funktion weniger flexibel und leistungsfähig als der OSI-Standard. Zudem wird das OSI-Netzwerkmanagement nur von einigen großen Herstellern unterstützt (und die unterstützen auch parallel dazu SNMP).

Das Netzwerkmanagement beschränkt sich jedoch nicht nur auf die Überwachung von aktiven und passiven Komponenten (Hubs, Verkabelung, Dosenanschlüsse). Das langfristige Ziel ist, von einer zentralen Stelle im Netzwerk das gesamte Netzwerk zu steuern.

Deshalb steigen bei der Auswahl von Netzwerkmanagement-Lösungen auch die Anforderungen, die Arbeitsplätze im Netzwerk zu überwachen und zum Teil auch steuern zu können. Da in großen Netzwerken die unterschiedlichsten Rechnerwelten vorzufinden sind, ist dies eine Aufgabe, die noch nicht von allen Netzwerkmanagement-Systemen erfüllt wird. Ich werde am Schluß dieses Kapitels zwei Produkte vorstellen, die darauf abzielen, ein Netzwerkmanagement-System verfügbar zu machen, mit dem der größte Teil dieser Anforderungen erfüllt werden kann. Das sind zwar keine hundertprozentigen Lösungen, aber man hat damit ein leistungsfähiges System zur Hand und erkennt an ihnen auch den Trend, den Netzwerkmanagement-Systeme in den nächsten Jahren einschlagen werden.

Netzwerkmanagement bedeutet auf der anderen Seite aber auch, den ständig wachsenden Anforderungen und Möglichkeiten gerecht zu werden. Zumindest lassen sich folgende Tendenzen vorhersagen:

- Die Anzahl der Stationen im Netzwerk und die damit verbundenen Komponenten werden ständig steigen.
- Die logische Komplexität eines Netzwerks bzw. die physikalische Infrastruktur wird weiterhin wachsen.
- Es wird kein Netzwerk geben (zumindest kenne ich bis heute keines), das auf einem bestimmten Status eingefroren werden könnte (auch wenn man dies ab und zu gern tun würde).

Um den gestellten Anforderungen an das Netzwerkmanagement besser gerecht zu werden und deren Leistungsfähigkeit besser einordnen zu können, wurden im Zuge der OSI-Entwicklung bestimmte Prämissen aufgestellt, die ein Netzwerkmanagement-System erfüllen muß. Auf sie soll im nächsten Abschnitt näher eingegangen werden.

6.1 Anforderungen an das Netzwerkmanagement

Alle Anforderungen an ein Netzwerkmanagement lassen sich mit Sicherheit nicht erfüllen. Von daher ist es sehr angenehm, daß im Zuge der OSI-Standardisierung für das Netzwerkmanagement fünf wichtige Aspekte definiert worden sind, die von einem Netzwerkmanagement-System erfüllt werden müssen (oder besser gesagt: erfüllt werden sollten). Auch wenn es sich dabei um eine Spezifikation der OSI-Umgebung handelt, orientieren sich doch fast alle Hersteller daran. Um einen generellen Überblick über Netzwerkmanagement-Aufgaben zu erhalten, sollen diese Aspekte anschließend näher betrachtet werden.

OSI hat die folgenden fünf Bereiche definiert, die von einem Netzwerkmanagement-System erfüllt werden müssen:

Fault- Management

Darunter sind Aufgaben zu verstehen, die es ermöglichen, Fehler zu lokalisieren, zu erkennen und zu beheben.

Configuration- Management

Darunter versteht man Aufgaben, die es ermöglichen, Konfigurationsdaten zu sammeln, auszuwerten und zu ändern, also die zu überwachenden Systeme nicht nur überwachen, sondern auch steuern zu können.

Performance- Management

Ist auch dieser Bereich abgedeckt, so dient das Netzwerkmanagement-System dazu, den Zustand der zu überwachenden Systeme bezüglich Durchsatz, Effizienz und Effektivität (d.h. die Leistung aller einzelnen Systeme) zu kontrollieren.

Accounting- Management

Wenn es darum geht, die Nutzung bestimmter Komponenten zu verrechnen, weil diese gleichzeitig von mehreren Abteilungen genutzt, aber von einer zentralen EDV-Abteilung bereitgestellt werden, muß es die Möglichkeit geben, Einzelauswertungen durchzuführen. Auf diese Weise kann ermittelt werden, welche Komponenten wie stark »belastet« worden sind. Nur so kann eine interne Kostenverrechnung effektiv gestaltet werden.

Security- Management

Damit nicht jeder die oben aufgeführten Bereiche (Fault-Management etc.) ändern und manipulieren kann, müssen bestimmte Sicherheitsvorkehrungen vorhanden sein, um nur berechtigten Personen deren Möglichkeiten verfügbar zu machen.

6.1 Anforderungen an das Netzwerk-management

Bei dieser Aufzählung handelt es sich um Standards, die von OSI definiert worden sind. Nicht jedes Managementsystem wird alle diese Punkte vollständig abdecken können. Andere Systeme werden auch noch andere Funktionen enthalten, die nicht exakt in diese Bereiche eingestuft werden können. Hierbei geht es um Zusätze, die vor allem im LAN-Bereich durch den Einsatz von Servern notwendig werden. Erwähnt sei nur die Notwendigkeit der Lizenzkontrolle, das Software-Metering, der Remote Control, die Software-Distribution oder auch die Virenschutzproblematik. Je nach Hersteller werden solche Möglichkeiten auch noch zusätzlich angeboten. Um uns jedoch erst mal wieder den Standards zu widmen, seien hier die oben aufgeführten fünf Netzwerkmanagement-Aufgaben etwas näher erläutert.

6.1.1 Fault-Management

Ab einer bestimmten Netzwerkgröße wird die Aufgabe immer schwieriger, das System im Ganzen zu überwachen und zu kontrollieren, vor allem wenn es darum geht, nicht mehr funktionierende Komponenten nicht nur schnell zu erkennen, sondern auch auszuwechseln. Für den Fall, daß Fehler auftreten, geht es vor allem darum, so schnell wie möglich

- festzustellen, wo genau der Defekt aufgetreten ist,
- den Rest des Netzwerks von der fehlerhaften Komponente abzuschotten, so daß es immer noch funktionsfähig zur Verfügung steht,
- das Netzwerk so zu rekonfigurieren oder anzupassen, daß der Einfluß der fehlerhaften Komponente auf das Netzwerk so gering wie möglich ist,
- die fehlerhafte Komponente auszutauschen oder zu reparieren, um das Netzwerk in den ursprünglichen Zustand versetzen zu können.

Ausschlaggebend hierbei ist, welche Komponenten in einem Netzwerk ausfallen. So verursacht der physikalische Ausfall einer Verkabelung, daß keine Signale mehr transportiert werden können und somit die Kommunikation zwischen Workstation und Server gestört ist. Zu ähnlichen Effekten kann ein schlecht montiertes Kabel führen. Treten bei einer Netzwerkkarte Fehlfunktionen auf, kann das ebenso zu Störungen im Netzwerk führen. Diese Probleme müssen erkannt und behoben werden, um anschließend wieder ein funktionsfähiges Netzwerk zu haben.

6 Netzwerkmanagement

In der Regel erwartet jeder Anwender eine schnelle und zuverlässige Lösung seiner Probleme. Die Praxis zeigt, daß das kaum zu erfüllen ist, wenn den Verantwortlichen solche kleinen Hilfsmittel wie Cable Scanner (zum Prüfen der physikalischen Kabel im Netzwerk) verwehrt werden, mit deren Hilfe es möglich ist, einfache Kabelfehler zu erkennen bzw. zu finden. Nur die geeigneten Werkzeuge können dabei helfen, schnell zu reagieren und auftretende Fehlfunktionen zu finden und zu beheben.

Nur vage Vermutungen, warum ein Kabel oder das Netzwerk (oder ein Teil davon) nicht funktioniert, sind hier nicht angebracht, da ein Fehler im Netzwerk unter Umständen durch eine Vielzahl von Randbedingungen beeinflußt werden kann. Allein durch geeignete Fehlererkennungs- und Diagnosemanagementfunktionen kann dem Netzwerkverwalter Unterstützung und Hilfestellung gegeben werden.

Als Netzwerkverwalter will man aber nicht immer nur reagieren, sondern auch agieren können. Das Netzwerkmanagement soll Unterstützung bieten, um die sich anbahnenden Ausfälle frühzeitig erkennen zu können, so daß bereits im Vorfeld entsprechende Maßnahmen eingeleitet werden können. Daher müssen auch Möglichkeiten zur Verfügung stehen, den aktuellen Zustand des Netzwerks ständig überwachen und kontrollieren zu können. Dazu zählen unter anderem auch Tests, die für bestimmte Komponenten durchgeführt werden können, Fehlermeldungen in entsprechenden Alert-Dateien oder auch Statistiken, die ausgewertet werden können. Nach einer erfolgreichen Behebung des oder der Ausfälle ist zu prüfen, ob nicht auch noch an anderer Stelle Fehlfunktionen zu erwarten sind. Dieser Vorgang wird auch als Problem Tracking und Control bezeichnet.

6.1.2 Configuration-Management

Heutige Netzwerke bestehen aus einer Vielzahl von Einzelkomponenten und logischen Subsystemen (Device Driver, Protocol Stacks etc.), die zur Erfüllung der einzelnen Aufgaben konfiguriert und modifiziert werden können. Da ein Netzwerk nicht statisch ist, sondern sich durch seine Dynamik auszeichnet, ist die ständige Anpassung von bestehenden Konfigurationen gefordert.

So kann es durchaus notwendig werden, einen seit langem in Betrieb befindlichen Router bezüglich der zu übertragenden Protokolle zu erweitern oder einzuschränken; die Konfiguration des Routers muß also geändert werden. Es könnte auch sein, daß interne Kommunikationsmechanismen des Routers (Timer, Pufferbereiche, Routing-Tabellen etc.) im Router anzupassen sind.

6.1 Anforderungen an das Netzwerk-management

Das Configuration-Management bezieht sich auf die Möglichkeiten, ein Netzwerk neu zu initialisieren oder teilweise abzuschalten, ohne daß davon andere wesentliche Teile des restlichen Netzwerks in Mitleidenschaft gezogen werden. Damit verbunden sind auch die Mechanismen, Teile des Netzwerks zu pflegen, neue Komponenten hinzuzufügen, anzupassen oder gar zu entfernen – und dies alles im laufenden Betrieb –, um anschließend allen davon betroffenen Stellen im Netzwerk die neuen Funktionen verfügbar zu machen.

Bei der Durchführung solcher Anpassungen kommt es nicht selten vor, daß eine neu konfigurierte Komponente regulär beendet (Shut Down) und anschließend neu gestartet werden muß. Es wäre wünschenswert, solche Operationen »unbeaufsichtigt« durchführen zu können. Dies bedeutet zum Beispiel, daß man einen Router in Berlin von München aus konfiguriert und anschließend neu hochfährt. Nach einer gewissen Zeit müßte der neu konfigurierte Router in Berlin im Managementsystem wieder erscheinen und mit den neuen Werten im Netzwerk arbeiten.

Der Netzwerkverwalter muß die Möglichkeit haben, alle Komponenten im Netzwerk automatisch zu erkennen und deren aktuellen Zustand und deren Konfiguration abzubilden. Wenn bestimmte Komponenten öfters installiert werden oder einer ähnlichen Konfiguration unterliegen, wäre es gut, bestehende Konfigurationen für andere, ähnliche Komponenten nutzen zu können, d.h. diese Einstellungen und Attribute per Download auf die Komponenten zu übertragen. Es geht in diesen Fällen aber nicht nur um die Rekonfiguration der einzelnen Komponenten, sondern auch um die Möglichkeit, über aktuelle Änderungen sofort informiert zu werden, Konfigurationslisten zu erzeugen oder auch bestehende Konfigurationen abzuspeichern, um diese später an anderer Stelle nutzen zu können. Netzwerkverwalter wollen zudem die Sicherheit, daß nur berechtigte Personen die Komponenten ändern und anpassen dürfen (Software-Distribution und Software-Updates).

6.1.3 Performance-Management

Ein Netzwerk größeren Ausmaßes besteht aus einer Vielzahl von Komponenten: physikalische Verkabelung, Netzwerkadapter in den Workstations und Servern, Router, Bridges, Brouter, Gateways, Fax-Server und vieles mehr. Alle Komponenten stehen dabei in einer bestimmten Wechselwirkung, die unter anderem auch für die Leistungsfähigkeit und den Durchsatz im Netzwerk verantwortlich ist. So kann es durchaus sein, daß in einem Netzwerksegment viele Stationen mit weniger Durchsatz angeschlossen sind, wohingegen in einem anderen Segment Stationen eingebunden sind, die eine Menge

6 Netzwerkmanagement

Datenverkehr im Netzwerk verursachen. Durch eine einfache Verteilung der Workstations auf die einzelnen Segmente könnte zum Beispiel der Gesamtdurchsatz im Netzwerk gesteigert werden. Ähnlich sieht die Situation aus, wenn ein Server im Netzwerk falsch platziert ist und dadurch die Koppelemente (Bridge, Router oder Brouter) ständig mit Datenpaketen belastet werden, die in das andere Segment transportiert werden müssen.

Aufgabe für das Performance-Management ist dabei im wesentlichen das Monitoring und Controlling im Netzwerk. Unter Monitoring versteht man die Aufgabe, den Datenverkehr im Netzwerk sichtbar zu machen, um zum Beispiel oben aufgeführte Situationen zu erkennen und eventuell Konfigurationsänderungen durchführen zu können. Unter die Kategorie »Controlling« fallen Aktivitäten, die es ermöglichen, Anpassungen durchzuführen, um die Leistungsfähigkeit im Netzwerk zu verbessern.

Für den Netzwerkverwalter sind dabei die folgenden Fragen von Bedeutung:

- Wie groß ist die Auslastung im Netzwerk?
- Kann intensiver Datenverkehr einzelner Stationen festgestellt werden?
- Ist der Gesamtdurchsatz auf ein nicht akzeptables Maß gesunken?
- Sind generelle Engpässe festzustellen?
- Hat sich die Antwortzeit verschlechtert?

Diese Aufgaben können vom Netzwerkverwalter nur dann vernünftig überwacht und kontrolliert werden, wenn Mechanismen zur Verfügung stehen, die es ermöglichen, entsprechend aussagefähige Informationen zu erhalten. Hierzu zählen unter anderem Mechanismen, um Schwellenwerte zu definieren, ab deren Erreichen Meldungen erzeugt werden, die den Netzwerkverwalter darüber informieren, daß Leistungsengpässe aufgetreten sind. So ist es zum Beispiel ausschlaggebend, wie oft im Netzwerk Retransmissions (Wiederholung der Übertragung von Datenpaketen durch Fehlersituation) auftreten, bis ein Datenpaket korrekt vom Sender zum Empfänger transportiert ist. Das Performance-Management muß daher in der Lage sein, eine Vielzahl von Ressourcen im Netzwerk zu überwachen und entsprechend aussagefähige Werte zu liefern. Auf diese Weise kann genau kontrolliert werden, wie sich die Leistungsfähigkeit mit einer zunehmenden Anzahl von Endgeräten im Netzwerk verschlechtert bzw. durch Ergreifen von Gegenmaßnahmen wieder verbessert.

Damit der Netzwerkverwalter auf die Beschwerden der Anwender über ein zu langsames Netzwerk angemessen reagieren kann, müssen über die aktuellen Zustände bezüglich Durchsatz und Leistungs-

6.1 Anforderungen an das Netzwerk-management

fähigkeit der Einzelkomponenten genaue Informationen vorliegen. Ohne solche Informationen wäre es nicht mehr als ein »Stochern im Heuhaufen«, wenn der Netzwerkverwalter nach Gefühl an der einen oder anderen Stelle Anpassungen durchführte. Erst wenn ein Gesamtüberblick über alle Komponenten vorliegt, kann am Router, an der Workstation oder der physikalischen Verteilung der einzelnen Stationen etwas geändert werden, um gezielt mehr Leistung zu erhalten. Zu beachten ist auf jeden Fall, daß Aussagen über das Antwortzeitverhalten im Netzwerk auch auf subjektiven Eindrücken der Anwender beruhen.

6.1.4 Accounting-Management

In einem flächendeckenden Netzwerk müssen oft einzelne Abteilungen oder Profit Center, teilweise sogar vielleicht einzelne Projektgruppen, für die Inanspruchnahme von Netzwerkleistungen Gebühren bezahlen. Hier geht es vor allem um die interne Kostenverrechnung. Dies gilt insbesondere, wenn das Netzwerk im Zuge von Outsourcing durch externe Firmen betrieben wird und die Kosten der Firma das Netzwerk entsprechend den benötigten Leistungen verrechnet werden. Auch wenn keine interne Kostenverrechnung durchgeführt wird, ist es für den Netzwerkverwalter aus folgenden Gründen von Vorteil, sich über die einzelnen verursachten Kosten einen Überblick zu verschaffen:

- Benutzer geben Berechtigungen an andere Benutzer weiter, ohne dafür die Erlaubnis zu haben. Somit arbeiten einige Teilnehmer auf Kosten anderer im Netzwerk.
- Die Anwender nutzen das Netzwerk auf ineffiziente Weise, und der Netzwerkverwalter kann in geeigneter Form den Anwender unterstützen, um eine effizientere Nutzung zu erreichen.
- Für den Netzwerkverwalter ist es einfacher, den zukünftigen Ausbau des Netzwerks zu planen, wenn die einzelnen Aktivitäten der Anwender genau bekannt sind (eine Aufgabe, bei der auch das Performance-Management von Bedeutung ist).

Für den Netzwerkverwalter bedeutet Accounting-Management die Möglichkeit, die Accounting-Informationen festzulegen, die überwacht werden sollen und für die Gebühren verrechnet werden müssen. Zudem sind die Zeitintervalle zu definieren, in denen entsprechende Accounting-Daten generiert werden müssen. Das Erstellen von Accounting-Auswertungen ist zudem nur von entsprechend autorisierten Personen durchzuführen, da es sich hierbei um sehr sensible Daten handelt.

6 Netzwerkmanagement

Das Accounting-Management ist mit äußerster Vorsicht einzusetzen, da es durchaus sein kann, daß die damit erzeugten Daten und Auswertungen unter die Kategorie der Mitarbeiterkontrolle fallen. Gegebenenfalls ist in größeren Unternehmen die Zustimmung des Betriebsrats erforderlich. Das Netzwerkmanagement-System muß die Möglichkeit besitzen, notwendige Benutzerkennungen einzurichten, die das Accounting nicht nur konfigurieren, sondern auch auswerten dürfen.

6.1.5 Security-Management

Das Security-Management ist unter anderem verbunden mit der Erzeugung, der Verteilung und dem Speichern von Verschlüsselungsinformationen. Paßwörter, andere Autorisierungen und Zugangskontrollinformationen müssen gewartet werden. Das Security-Management betrifft aber auch die Überwachung und das Monitoring für den Zugang im Netzwerk bzw. aller Informationen, die über das Netzwerkmanagement-System erhalten werden. Dies bezieht sich auf sämtliche Komponenten im Netzwerk. Log-Files sind ausschlaggebend für die damit verbundenen Sicherheits-Tools. Daher ist das Security-Management sowohl mit dem Sammeln und Speichern von Auditing-Informationen und Sicherheitsmechanismen als auch mit dem Aktivieren und Deaktivieren dieser Mechanismen verbunden.

Durch das Security-Management wird die Nutzung einzelner Ressourcen im Netzwerk sicherer gemacht. Dies betrifft auch das Sammeln und Auswerten spezieller benutzerspezifischer Informationen (s. Accounting-Management). Von daher sollten die Möglichkeiten auch nur für autorisierte Benutzer verfügbar sein, also nur von solchen aktiviert und deaktiviert werden können.

Dabei ist zu beachten, daß alle Netzwerkbetriebssysteme in der Regel eigene Sicherheitsmechanismen implementiert haben, so daß das Security-Management nur für ausgewählte Funktionsbereiche eingesetzt werden muß (bzw. kann). So kann man hierüber zum Beispiel definieren, daß ein bestimmter Port im Hub nur dann freigeschaltet wird, wenn die Workstation mit der richtigen Node-Adresse angeschlossen ist. Andererseits kann man jeden nicht belegten Port im Hub generell abschalten, so daß es nicht vorkommen kann, daß plötzlich jemand einen weiteren Rechner im Netzwerk in Betrieb nimmt, weil gerade noch eine Anschlußdose im Büro frei ist (d.h., der Netzzugang wird dann also verhindert). Andere Sicherheitsfunktionen betreffen aber auch das Netzwerkmanagement-System selbst, um nur berechtigten Personen die Konfiguration und das Auswerten von Managementinformationen zu ermöglichen. Auf diese Weise

6.2 Aufbau von Netzwerkmanagement-Systemen

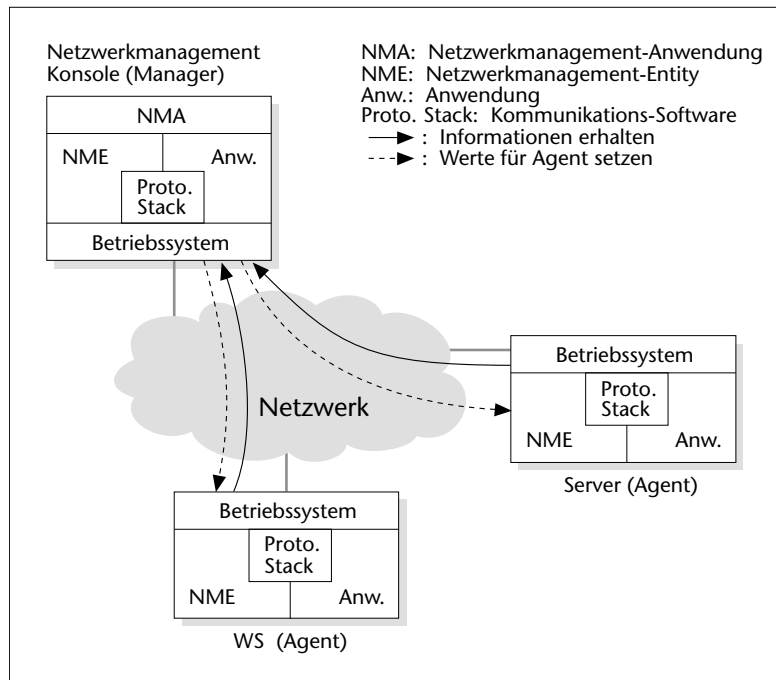
kann keine unberechtigte Person einfach an der Hub-Einstellung oder am Router Änderungen vornehmen und so das gesamte Netzwerk in Unordnung bringen.

6.2 Aufbau von Netzwerkmanagement-Systemen

Bei der Betrachtung unterschiedlicher Netzwerkmanagement-Systeme stellt man fest, daß der prinzipielle Aufbau in der Regel immer gleich ist. Man benötigt eine bestimmte Anzahl von Hard- und Software-Komponenten, die in einer bestimmten Beziehung zueinander stehen. In Abbildung 6.1 ist dargestellt, aus welchen Komponenten ein Netzwerkmanagement-System besteht.

Es fällt auf, daß auf jedem zu überwachenden System ein sogenannter Agent eingesetzt wird. Der Agent ist dafür zuständig, alle notwendigen Informationen zu sammeln, um vom Fault-Management bis hin zum Security-Management allen Anforderungen gerecht werden zu können.

Abbildung 6.1
Elemente eines
Netzwerkmanagement-Systems



6 Netzwerkmanagement

Das Sammeln der Informationen hilft nichts, wenn sie nicht an einer zentralen Stelle abgeliefert werden. An dieser Netzwerkmanagement-Konsole werden die gesammelten Informationen der Agents nicht nur abgeliefert, sondern auch für den Benutzer anwendungsfreundlich zur Verfügung gestellt. Ein Netzwerkmanagement-System besteht aus folgenden Komponenten:

Grafische Benutzer- oberfläche

Diese Software-Schnittstelle ermöglicht es dem Netzwerkverwalter, das Netzwerk zu überwachen und zu steuern. Alle Informationen, die von den Agents in den einzelnen Netzwerkkomponenten gesammelt und abgeliefert werden, bereitet die Software als aussagefähige grafische Oberflächen auf. Die Gestaltung dieser Oberfläche ist ausschlaggebend für die gesamten administrativen Möglichkeiten. Je nach Software-Hersteller werden verschiedene generelle Möglichkeiten zur Verfügung gestellt.

Netzwerk- management- Software

Die grafische Benutzeroberfläche funktioniert nur dann als Netzwerkmanagement-Software, wenn im Hintergrund auch die korrekte Netzwerkmanagement-Anwendung läuft. Diese notwendige Anwendung kann so einfach aufgebaut sein wie bei SNMP oder relativ komplex wie bei OSI.

Netzwerk- management- Support- Software

Damit eine Netzwerkmanagement-Software überhaupt in der Lage ist, alle notwendigen Aufgaben zu erfüllen, benötigt sie Zugriff auf eine lokale Management Information Base (MIB) und Zugriff auf remote Agents (mit MIB) und Manager. Die lokale MIB eines Agent beinhaltet unter anderem Informationen über die Konfiguration und den Zustand des zu überwachenden Systems. Zudem sind Parameter enthalten, die die Arbeitsweise dieses Systems überwachen und steuern helfen. Die lokale MIB eines Managers (Netzwerkmanagement-System) beinhaltet die Informationen aller zu überwachenden Systeme (d.h. die Summe aller MIBs). Die Kommunikation mit den zu überwachenden Systemen (Agents) wird durch einen Protocol Stack realisiert. Dabei kann es sich um das OSI-Protokoll oder das TCP/IP-Protokoll handeln. Es sind aber auch Systeme verfügbar, die IPX als Kommunikationsprotokoll unterstützen. Der Austausch der Informationen erfolgt dabei über ein notwendiges Netzwerkmanagement-Protokoll. Da ich mich hier auf das einfachere Protokoll beschränken will, behandle ich SNMP.

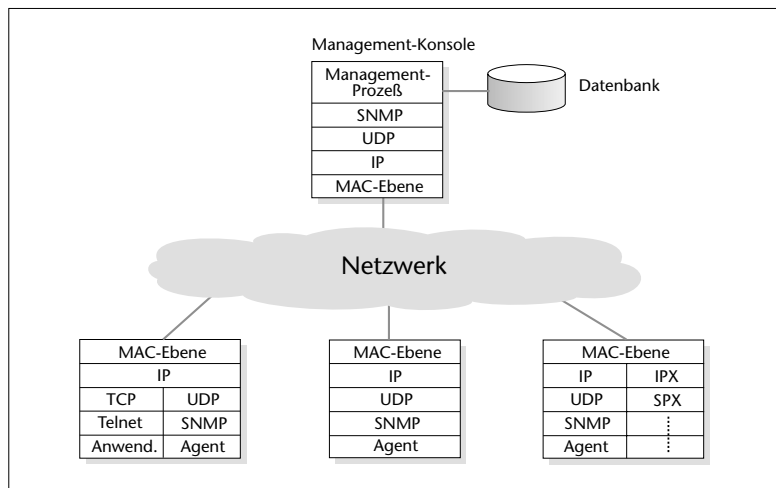
6.3 SNMP-Netzwerkmanagement

SNMP wurde im Rahmen der TCP/IP-Protokollumgebung konzipiert und entwickelt. Standardgemäß wird das UDP-Protokoll verwendet. In Abbildung 6.2 ist dargestellt, wie das SNMP-Protokoll in die Netzwerkmanagement-Landschaft eingebettet wird.

Auf der Netzwerkmanagement-Station überwacht der Managerprozeß die zentrale MIB auf der Managementstation und stellt eine Schnittstelle zum Netzwerkverwalter zur Verfügung. Der Manager realisiert seine Aufgabe über SNMP, das auf UDP (eingebettet in IP) aufsetzt. Transportiert werden die Informationen dann über Ethernet, Token-Ring, FDDI, ATM oder andere Netzwerkprotokolle. Jedes zu überwachende System benötigt einen Netzwerkmanagement-Agent, um über den Managerprozeß bearbeitet werden zu können.

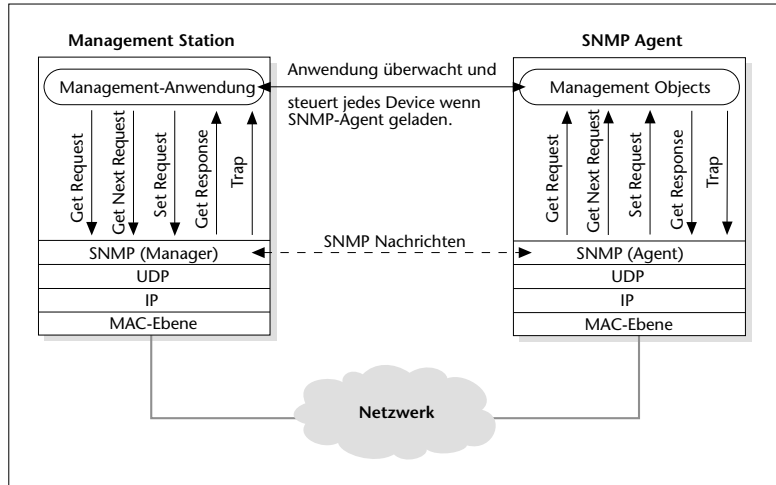
Jeder Netzwerkmanagement-Agent auf der zu überwachenden Einheit besitzt ebenfalls SNMP-, UDP- und IP-Implementierung. Zusätzlich ist ein Agent-Prozeß aktiv, der die SNMP-Nachrichten interpretiert und die MIB des Agent überwacht. In Abbildung 6.3 ist dargestellt, welche Aufgaben der SNMP-Manager und der SNMP-Agent hierzu erfüllen müssen.

Abbildung 6.2
SNMP-Netzwerk-
management



6 Netzwerkmanagement

Abbildung 6.3
Die SNMP-Management-Station
und der SNMP-Agent in einer
Netzwerkmanagement-Umgebung



6.3.1

SNMP-Management-Information-Base

So wie für jedes andere Netzwerkmanagement-System bildet eine Datenbank die Grundlage für das SNMP-Netzwerkmanagement, in der alle Elemente definiert sind, die durch das Netzwerkmanagement-System überwacht werden können. Sowohl für SNMP- als auch für OSI-Netzwerkmanagement wird diese Datenbank als Management Information Base (MIB) bezeichnet. Der Aufbau der MIB wird zudem über die Structure of Management Information (SMI) festgelegt. Die SMI definiert die Datentypen, die in der MIB verwendet werden können. Außerdem legt sie fest, wie Ressourcen innerhalb der MIB dargestellt und benannt werden. Die MIB selbst wird in der ASN.1-Notation definiert. Die Variablen der MIB werden in einem sogenannten RFC (Request for Comment) festgelegt. MIB-Variablen enthalten Angaben über Systemnamen, TCP-Verbindungen, Routing-Tabellen usw. Neben den Standard-MIBs können Hersteller auch private, sogenannte Enterprise-MIBs definieren, damit auf diesem Weg die herstellereigenen (nichtstandardisierten) Geräte und Ressourcen verwaltet werden können. Die Definition einer Private-MIB ist ebenfalls über einen RFC festgelegt. Sofern das Netzwerkmanagement-System einen MIB-Compiler besitzt, kann eine Private-MIB eingelesen und verarbeitet werden.

Ein Netzwerkmanagement-System wird immer die Standard-MIB unterstützen (MIB I und MIB II). Die Standard-MIB enthält nur herstellernunabhängige Definitionen. Sie können also auf alle Fälle mit jedem Netzwerkmanagement-System Informationen abfragen, die innerhalb der Standard-MIB abgedeckt werden. Die Standard-MIB-II ist

6.3 SNMP-Netzwerkmanagement

eine Erweiterung der Standard-MIB-I, und man sollte darauf achten, daß vom Netzwerkmanagement-System die Standard-MIB-II unterstützt wird (somit wird auch MIB I unterstützt).

Jedes Netzwerkmanagement-System hat in der Regel einen MIB-Browser. Mit diesem MIB-Browser können zumindest alle MIB-Informationen in textlicher (tabellarischer) Form abgefragt werden. Handelt es sich um eine Komponente, die mit einer Private-MIB ausgestattet ist, dann muß die Netzwerkmanagement-Software so angepaßt werden, daß die Informationen der Private-MIB eingebunden werden können. Hierzu bieten eine Vielzahl von Netzwerkmanagement-Herstellern einen sogenannten MIB-Compiler an. Da es sich bei der MIB um eine ASCII-Datei im ASN.1-Format handelt, kann sie über den MIB-Compiler ganz einfach in ein bestehendes Netzwerkmanagement-System eingebunden werden. Sobald die Private-MIB auf diese Weise integriert ist, können mit dem MIB-Browser auch die Private-MIB-Informationen abgefragt werden.

Vorsicht ist geboten, wenn Sie bei der Auswahl der Netzwerkmanagement-Software den Hersteller fragen, ob die Managementsoftware auch in der Lage ist, den Hub vom Hersteller XY zu überwachen. Die Standard-MIB-Informationen werden Sie immer erhalten, sofern die Managementsoftware einen MIB-Browser erhält. Aber die Private-MIB können Sie nur dann abfragen, wenn der Hub-Hersteller die Private-MIB als ASCII-Datei zur Verfügung stellt und die Managementsoftware einen MIB-Compiler enthält.

Die tabellarische Abfrage der Private-MIB-Informationen wird jedoch nicht ausreichen, zumindest nicht auf Dauer. Man möchte mit Sicherheit bei einer grafischen Managementsoftware auch die Komponenten anderer Hersteller in grafischer Form darstellen können. Solange der Hersteller der Managementsoftware die Integration in die grafische Oberfläche programmtechnisch nicht vorsieht, können die Werte nur über den MIB-Browser abgefragt werden. Es ist somit bei der Auswahl der Managementsoftware und der Netzwerkkomponenten darauf zu achten, daß diese auch zusammenpassen. Renommierete Hardware-Hersteller für Netzwerkkomponenten (z.B. CISCO, CABLETRON etc.) bieten standardmäßig für die eigenen Komponenten eine passende Netzwerkmanagement-Software an. Zu prüfen ist dann allerdings, wie in dieses Netzwerkmanagement-System Komponenten von anderen Herstellern integriert werden können (über MIB-Browser oder durch Anpassung der grafischen Oberfläche).

Da auf dem Markt eine Vielzahl von Herstellern existiert, die Netzwerkmanagement-Software anbieten, soll anschließend exemplarisch eine Software vorgestellt werden, die eine offene Plattform auf

6 Netzwerkmanagement

Basis von SNMP zur Verfügung stellt. Es handelt sich dabei um das Netzwerkmanagement-System von Novell (siehe Kap. 6.4).

6.3.2 Remote Network Monitoring (RMON)

Der wichtigste Zusatz für den SNMP-Standard (SMI, MIB und SNMP) ist der RMON-Standard. Dabei handelt es sich um einen weiteren Schritt in Richtung Internetwork-Management. Mit der üblichen Standard-MIB-II kann der Netzwerkverwalter Informationen für das lokale Netzwerk sammeln und erhalten. Man kann sehr leicht sehen, wie viele Datenpakete von einem Netzwerkknoten empfangen bzw. ausgesandt werden. Es ist jedoch nicht möglich, den Datenverkehr als Ganzes im Netzwerk zu überwachen. Endgeräte, die solche Vorgänge im Netzwerk aufzeichnen und zur Verfügung stellen, werden als Netzwerkmonitore bezeichnet, andere Bezeichnungen sind Netzwerk-Analyzer oder Probes. Der Netzwerkmonitor kann zusammengefaßte Informationen erstellen (einschließlich Fehlerstatistiken über zu kleine oder zu große Pakete, Anzahl der Kollisionen etc.) oder Pakete für spätere Analysen speichern. Zudem lassen sich Filter setzen, um nur bestimmte Informationen zu sammeln. In einem Internetwork benötigt man in der Regel einen Netzwerkmonitor pro LAN-Segment (d.h. pro Netz, das über Bridges oder Router von einem anderen getrennt ist).

Der Netzwerkmonitor kann entweder als eigenes Gerät im Netzwerksegment installiert sein oder als Zusatzsoftware (evtl. mit zusätzlicher Hardware) auf einer Workstation, einem Server, einer Bridge oder einem Router laufen. Um somit Netzwerkmanagement effizient gestalten zu können, müssen die Netzwerkmonitore mit der zentralen Netzwerkmanagement-Console Informationen austauschen.

6.4 ManageWise

In einem komplexen Netzwerk wird es immer Situationen geben, in denen der Anwender über langsame Druckerausgaben, schlechte Antwortzeiten, unvollständige Backups, nicht erklärbare Änderungen auf den Workstations und dergleichen mehr klagt. Für den Netzwerkadministrator müssen deshalb Möglichkeiten zur Verfügung stehen, solche Vorfälle rechtzeitig zu erkennen und darauf zu reagieren. Novell bietet dafür bereits seit längerer Zeit entsprechende Lösungen an.

6.4 ManageWise

ManageWise stellt eine leistungsfähige Managementplattform zur Verfügung, mit dem das gesamte Netzwerk erfolgreich überwacht und gesteuert werden kann; hierzu zählen Workstations, Server, Router, Gateways und die Netzwerkinfrastruktur. Novell ist immer noch Marktführer im Netzwerkbereich und bietet seit langem Netzwerkmanagement-Technologie auf Basis von SNMP an.

Zusammen mit den sogenannten Agents überwacht und sammelt ManageWise die Performance von NetWare-Servern, Ethernet-, Token-Ring- und FDDI-Netzwerksegmenten. Ebenso ist es möglich, in diese Überwachungsfunktionen Windows-NT-Server zu integrieren.

ManageWise besteht aus den folgenden Komponenten:

- *ManageWise-Software*
 - ManageWise-Console-Software
 - NetExplorer-System
- *ManageWise-Agents (separat verfügbar)*
 - NetWare Management Agent
 - NetWare LANalyzer Agent

Hinzu kommt, daß ManageWise eine umfangreiche Lösung für das Desktop-Management zur Verfügung stellen kann, inklusive der Installation einer zentralen Virenüberwachung. In der jetzigen Version besteht noch keine hundertprozentige Integration von bzw. mit Z.E.N.works, jedoch ist Novell im Begriff, eine solche Integration herzustellen. Z.E.N.works wird dann auch alle Mechanismen beinhalten, um Software-Distribution und erweiterte Workstation-Management-Funktionen durchführen zu können.

Auf diese Weise erhält man eine optimale Netzwerkmanagement-Umgebung. Auch wenn ich an dieser Stelle ManageWise von Novell exemplarisch als Netzwerkmanagement-Plattform beschreibe, so soll dies auch dazu dienen, einen Gesamtüberblick darüber zu geben, worauf Sie bei der Auswahl von Netzwerkmanagement-Systemen achten sollten. Es ist mir bewußt, daß es noch eine Vielzahl anderer Systeme gibt, jedoch muß man sich irgendwann auf ein Produkt beschränken, um dies etwas ausführlicher zu beschreiben – dabei ist die Entscheidung für ManageWise gefallen.

Die Bezeichnung NMS (NetWare Management System) stammt übrigens aus den Zeiten, als Novell ein eigenständiges Produkt für das Netzwerkmanagement zur Verfügung gestellt hat. Erst durch den Zusammenschluß der NMS-Komponente und der Desktop-Management-Komponenten zu ManageWise, wurde diese Bezeichnung aufgegeben. In der Dokumentation und Beschreibung von ManageWise wird jedoch ebenfalls noch zwischen NMS und Desktop-Management unterschieden.

6 Netzwerkmanagement

An dieser Stelle sei bereits auf einen wesentlichen Aspekt von ManageWise hingewiesen: ManageWise kann durch Dritthersteller über sogenannte Snap-in-Module ergänzt und erweitert werden. Derzeit werden weit mehr als 100 Snap-in-Module zur Verfügung gestellt und ständig neue Module entwickelt. Durch die entsprechenden Erweiterungen wird das Netzwerkmanagement unter ManageWise erweitert für:

- Router
AVM stellt zum Beispiel ein Snap-in-Modul für den MPR-ISDN-Router zur Verfügung, um darüber nicht nur die Konfiguration durchführen, sondern auch notwendige Performance- und Statistikdaten erhalten zu können.
- Hubs
Um die aktiven Hub-Komponenten in einem Netzwerk überwachen und steuern zu können, stellt zum Beispiel Cabletron Snap-in-Module zur Verfügung.
- Drucker
Die Firma HP bietet hierfür zum Beispiel Komponenten an, um JetDirect-Karten über die Management-Console steuern zu können.
- Alarmbehandlung
- Trouble Ticketing
- Reporting
- NetWare for SAA Services Manager
- Connect View für NetWare Connect
- Z.E.N.works

ManageWise stellt somit ein integriertes Management für das gesamte Netzwerk zur Verfügung. Hierzu zählen im wesentlichen:

- Asset Management (Hard- und Software-Inventarisierung)
- Management der NetWare-Server
- Management der Netzwerkkomponenten
- Desktopmanagement
- Netzwerkanalyse
- Virenschutz für Server und Workstation
- SNMP-Netzwerkmanagement-Konsole
ManageWise besteht aus den folgenden Komponenten:
- ManageWise-Console-Software (läuft am besten auf einer Windows-95/98- oder Windows-NT-Workstation-Plattform)
- ManageWise-Server-Software (sie kann auf NetWare-3.x-, NetWare-4.1x-, NetWare-5-, Netware-IP- und NetWare-4.1-SFT-III-Servern installiert werden)

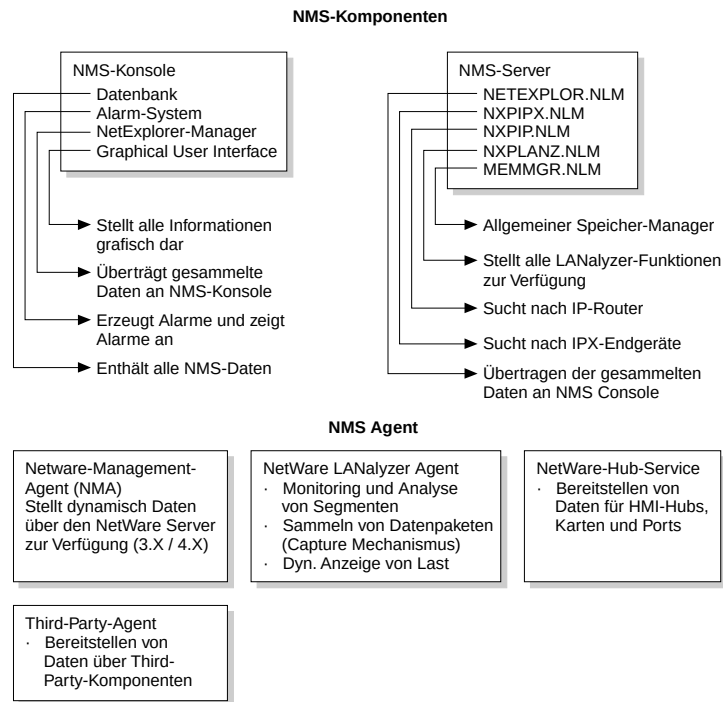
6.4 ManageWise

Zusätzlich stehen unterschiedliche Agents zur Verfügung, mit denen weitere Informationen einzelner Komponenten im Netzwerk erhalten werden. Zu diesen standardmäßig verfügbaren Agents zählen:

- NetWare Management Agent (sollte auf jedem Server installiert werden)
- NetWare LANalyzer Agent (sollte pro Netzwerksegment installiert werden)
- NetWare Hub Service Agent (für alle Hub-Systeme, wenn die HMI-Spezifikation unterstützt wird)

In Abbildung 6.4 wird gezeigt, aus welchen Komponenten die NMS-Umgebung von ManageWise zusammengesetzt ist, und auf welchen Hardware-Komponenten die einzelnen Komponenten installiert werden müssen.

Abbildung 6.4
NMS-Aufbau



Die wichtigsten Komponenten sollen aufgrund der damit verbundenen Funktionen, die immer in einem direkten Zusammenhang untereinanderstehen, näher beschrieben werden.

6 Netzwerkmanagement

NMS-Console-Software

Bei der NMS-Console-Software handelt es sich um eine Windows-Anwendung, mit der eine vollständige grafische Oberfläche zur Verfügung gestellt wird, um damit alle Netzwerkmanagement-Funktionen für das gesamte Netzwerk ausführen zu können. Zusätzlich wird auf der NMS-Console-Station eine Datenbank gepflegt, in der alle gesammelten Informationen (über den Netexplorer) gespeichert werden. Daneben wird ein Alarmmanagementsystem zur Verfügung gestellt, um auftretende Alarmer zu behandeln zu können. Neben diesen grundsätzlichen Funktionen bietet die NMS-Console auch Management-Tools für die wichtigsten Netzwerkfunktionen.

Hierzu zählen Netzwerkmanagement-Funktionen für NetWare Server, Clients, Netzwerksegmente, Hubs, Router und andere SNMP-basierende Endgeräte. Werden die Funktionen nicht direkt von Novell zur Verfügung gestellt, bietet eine Vielzahl von Herstellern bereits Snap-in-Module an.

Die NMS-Console-Software stellt auch den Netexplorer-Manager zur Verfügung. Dieses Modul hat eine besondere Bedeutung, da die Anwendung mit dem Netexplorer NLM des Explorer-Servers kommuniziert, um darüber alle gesammelten Informationen des Explorer-Servers zu erhalten. Diese Daten werden in der lokalen Explorer-Datenbank abgespeichert und anschließend von der NMS-Console-Software grafisch aufbereitet und dargestellt. Über das NMS-Alarmsystem wird in der grafischen Darstellung bereits optisch darauf hingewiesen, wenn in ein oder mehreren Komponenten Fehler auftreten, die es zu analysieren und zu beheben gilt.

Ein Server, auf dem SNMP installiert ist, bietet Zugriff auf entsprechende SNMP-Funktionen und kann sogenannte Traps über IP und IPX empfangen. Zusätzlich besitzt die NMS-Console einen MIB-Browser, der es ermöglicht, wichtige und notwendige MIB-Daten von Endgeräten anzufragen, die sich nicht direkt grafisch in die NMS-Console integrieren lassen. Über den MIB-Compiler lassen sich sogar die Private-MIBs integrieren, sofern diese vom jeweiligen Hersteller in der ASN.1-Notation zur Verfügung gestellt werden.

Alle Informationen, die über die NMS-Console am Bildschirm dargestellt werden, stammen von der lokalen Datenbank, die ständig über die Netexplorer-Komponenten aktualisiert wird. In der Datenbank werden das logische Modell des Netzwerks, die Konfigurationen über das Netzwerk und die Endgeräte, eigene angepasste »Netzwerkpläne«, Alarmmeldungen und NMS-Konfigurationen selbst gespeichert. Die NMS-Console-Software bietet nicht nur die Möglichkeiten für das Netzmanagement sondern auch für das Desktop-Management.

6.4 ManageWise

Auf die Möglichkeiten, die NMS-Console-Software durch die Integration von Snap-in-Modulen bietet, soll später eingegangen werden.

6.4.1 Netzwerkmanagement

In den nachfolgenden Ausführungen soll gezeigt werden, welche Komponenten für das Netzwerkmanagement zur Verfügung gestellt werden und wie deren Zusammenspiel aussieht. Diese Ausführungen sind wichtig, um die Arbeitsweise des Gesamtsystems besser verstehen zu können.

Netexplorer-NLM-Software

Auch wenn NMS installiert ist, sind deswegen noch keinerlei Informationen über das Netzwerk bekannt. Bevor also mit der Verwaltung des Netzwerks über die NMS-Console begonnen werden kann, müssen hierfür alle notwendigen Informationen gesammelt und aufbereitet werden. Dieser Discovery-Prozeß schließt die folgenden Komponenten ein: Netzwerksegmente, Router, Endgeräte im Netzwerk, Server und alle anderen Devices, die über eigene Agents verfügen.

Die wichtigste Basiskomponente von NMS ist die Autodiscovery-Funktion, damit kann das gesamte Netzwerk automatisch durchsucht werden. Anschließend stehen alle gesammelten Informationen in einer Internetwork Map zur Verfügung.

Da die Autodiscovery-Funktion ständig aktiv ist, werden neu installierte Komponenten im Netzwerk sehr schnell erkannt und sofort in der Internetwork Map abgebildet. Die Internetwork Map zeigt alle installierten Router und die damit aufgebauten einzelnen Netzwerksegmente. Da standardmäßig nur IPX-Devices erkannt werden, müssen zum Abbilden von IP-basierenden Routern notwendige Konfigurationsparameter aktiviert werden, um auch solche Router-Systeme erkennen und abbilden zu können.

Für jedes abgebildete Segment werden alle erkannten Workstations und NetWare-Server dargestellt. Damit das Netzwerk nicht nur quasi nackt am Bildschirm dargestellt wird, kann man sich über die eingebaute Locational-Map-Funktion die eigenen Gebäude- und Raumpläne einscannen und sich damit die Darstellung einer hierarchischen Netzwerkstruktur aufbauen. Dies könnte dann in etwa so aussehen, daß man zuerst eine Deutschlandkarte abbilden läßt, auf der alle Standorte der Städte gekennzeichnet sind, in denen sich Netzwerke des Unternehmens befinden. Aktiviert man den Standort einer Stadt, kann sich eine Karte dieser Stadt öffnen, um das Netz-

6 Netzwerkmanagement

werk dort zu lokalisieren. Irgendwo in der Stadt wird sich dann ein Firmengebäude befinden, auf das mit der Maus geklickt werden muß. Schritt für Schritt läßt sich das Netzwerk soweit öffnen, bis man sich auf der Etage oder in dem Büroraum befindet, wo das zu überwachende System tatsächlich installiert ist. Auf diese Weise läßt sich sehr schnell eine übersichtliche Darstellung des Netzwerks konfigurieren. Sollte eine Komponente im Netzwerk Fehler aufweisen, wird dies mit Hilfe einer Alarmglocke über dem jeweiligen Objekt dargestellt. Öffnet man zum Beispiel die Locational Map für Deutschland, und im Netzwerk, z.B. im Standort München, ist ein Fehler aufgetaucht, dann wird dies durch eine Alarmglocke über dem Standort München dargestellt. So weiß man, daß man die Locational Map für diesen Standort genauer ansehen muß. So wird die Locational Map Ebene für Ebene durchgeblättert, bis die fehleraufweisende Komponente gefunden ist. Die Fehlersuche und -erkennung ist damit wesentlich einfacher und komfortabler geworden.

Der Autodiscovery-Mechanismus erkennt alle Stationen im Netzwerk unabhängig vom eingesetzten Protokoll (sofern dieser Mechanismus entsprechend konfiguriert ist). Alle gesammelten Informationen der Netzwerkstruktur werden von NMS in einer Datenbank gespeichert. Diese Datenbank liegt in der Regel lokal auf der Netzwerkmanagement-Station. Da es sich bei dieser Datenbank um eine Btrieve-Datenbank handelt, kann diese auch mit anderen SQL-Front-Ends ausgewertet werden, sofern die Standardmöglichkeiten von NMS nicht ausreichen sollten.

Ein wichtiger Bestandteil von ManageWise bzw. der NMS-Console ist der eingebaute MIB-Browser und MIB-Compiler. Über den MIB-Browser können alle SNMP-basierenden Agents im Netzwerk angesprochen und notwendige Informationen zumindest in textlicher Darstellung abgebildet werden. Um die SNMP-Informationen zu erhalten, erfolgt dabei die Kommunikation mit dem Agent entweder auf Basis von TCP/IP oder IPX. In Abhängigkeit davon können die abgefragten Werte in Tabellenform oder als Diagramm dargestellt werden. Dies hängt von der jeweiligen Implementierung der MIB im NMS ab. Ein aktives Management ist nur dann möglich, wenn dies vom Agent unterstützt wird. Für die entsprechende Unterstützung beim Bearbeiten und Auswerten von Informationen sind in der Regel Module erforderlich, die für die jeweilige Komponente zugeschnitten sein müssen.

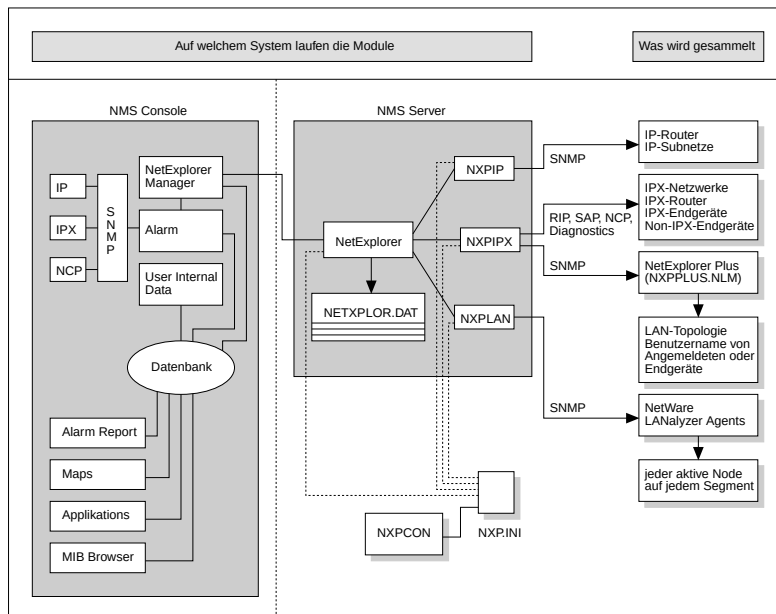
Das ist zum Beispiel für Cabletron-Komponenten der Fall oder für das Snap-in-Modul zur Überwachung und Steuerung von UPS-Systemen von APC. In diesem Zusammenhang ist es auch notwendig, die MIB-Informationen der Managementstation zu erweitern. Hierzu

6.4 ManageWise

wird der MIB-Compiler benötigt. Die vom Hersteller gelieferte MIB wird auf die lokale Management-Station kopiert und durch den MIB-Compiler eingebunden. Ab diesem Zeitpunkt können die Informationen der neuen Agents abgefragt werden.

In Abbildung 6.5 ist dargestellt, wie die einzelnen Module des Netexplorer-Discovery-Systems zusammenarbeiten.

Abbildung 6.5
Netexplorer-
Discovery-System



NMS Agents

Unter den NMS Agents sind Komponenten zu verstehen, deren Aufgabe darin besteht, für spezielle Komponenten Informationen zu sammeln und über den Netexplorer der NMS-Console verfügbar zu machen. Novell selbst stellt drei wichtige Agents zur Verfügung.

NetWare Management Agent (Server Management)

Diese Funktion steht nur dann in vollem Umfang zur Verfügung, wenn auf dem Server ein entsprechender NetWare Management Agent installiert ist. Ab diesem Zeitpunkt erhält man durch ein einfaches Doppelklicken auf das Serversymbol in der Internetwork Map alle notwendigen Informationen des Servers. In dem daraufhin geöffneten Fenster erscheinen z.B. die Symbole für CPU, Speicher, NLMs, Volumes, Platten-Controller, Netzwerkadapter und Print-Server. So kann man sich über das CPU-Symbol die aktuelle CPU-Auslastung des Servers anzeigen lassen. Über das Symbol *Memory* erhält man die aktuelle Auslastung des Hauptspeichers unter NetWare, um

6 Netzwerkmanagement

schnell feststellen zu können, ob die Speicherbelegung optimal ist oder mehr Speicher unter Umständen für eine bessere Performance sorgt. Über das Symbol *Volume* kann festgestellt werden, auf welcher Platte dieses Volume eingerichtet ist. Mit *Zusatzoptionen* können zudem für jeden Server Leistungsdaten über Schreib- und Lesevorgänge auf den Platten oder auch Protokollinformationen der installierten Netzwerkadapter überwacht und analysiert werden. Für eine Vielzahl der zu überwachenden Objekte lassen sich Schwellwerte definieren, um bei Über- oder Unterschreitung entsprechende Fehlermeldungen zu erhalten. Alle zeitabhängigen Informationen (CPU-Last, Protokollverkehr etc.) werden in grafischer Form online abgebildet. Insgesamt kann der Server Agent über 370 unterschiedliche SNMP-Alarme erzeugen und bekanntgeben. Sehr wichtig und informativ ist die Anzeige aller derzeit am Server geladenen NLMs. Hiermit werden schnell und übersichtlich nicht nur alle aktiven NLMs angezeigt, sondern auch deren Versionsnummer und Größe. Wenn verglichen werden muß, ob auf allen Servern die gleichen Versionen laufen, ist die Funktion sehr hilfreich und aussagefähig.

NetWare LANalyzer Agent (Netzwerkanalyse)

Zu einer der interessantesten Funktionen von NMS gehört die Möglichkeit von NMS, Segmente über den integrierten LANalyzer überwachen zu können. Das hier verfügbare Produkt gibt es bereits seit Jahren als Einzelprodukt unter der Bezeichnung LANalyzer for Windows.

Um mit dem integrierten LANalyzer als Administrator das gesamte Netzwerk überwachen zu können, muß in jedem Segment ein entsprechender LANalyzer Agent installiert werden. Dieses entsprechende NLM auf dem NetWare-Server hat dann die Aufgabe, alle notwendigen Informationen zu sammeln und an die Netzwerkmanagement-Station abzugeben. LANalyzer Agents sind entsprechend den notwendigen zu überwachenden Segmenten einzeln zu erwerben. Im Lieferumfang eines jeden LANalyzer Agent befindet sich eine Runtime-Version von NetWare, um sie dann auch in Nicht-NetWare-Segmenten einsetzen zu können. Die mit dem LANalyzer Agent gesammelten Informationen werden in einer Datenbank zusammengefaßt, die den für die Netzwerkanalyse festgelegten RMON-Standard unterstützt. Für den LANalyzer Agent ist zu unterscheiden: Single Segment (1-Adapter-Version), mit der nur ein Segment überwacht werden kann, Multiple-Segment-Version für NetWare-Server, die als interne Router fungieren und mehrere Netzwerksegmente koppeln. Somit kann der LANalyzer Agent alle von diesem Server bedienten Segmente überwachen.

Über die LANalyzer-Console im NMS kann der Netzwerkverwalter jederzeit alle verfügbaren Informationen über die Auslastung der

6.4 ManageWise

überwachten Segmente abfragen. Sie erhalten dann Informationen über das gesamte Datenvolumen pro Sekunde die prozentuale Auslastung, die Anzahl der Broadcasts und die fehlerhaften Pakete, die pro Sekunde ermittelt worden sind. Neben bloßen Zahlenkolonnen lassen sich diese Werte auch in Form einer Grafik am Bildschirm darstellen, um einen noch schnelleren und besseren Überblick zu erhalten. Über den Station-Monitor lassen sich Einzelinformationen über die Anzahl der über das Netzwerk transportierten Daten, die empfangenen und fehlerhaften Daten für die jeweils ausgewählte Station, anzeigen.

Auf diese Weise ist es für den Netzwerkverwalter sehr einfach, schnell die Station zu ermitteln, die den größten Datenverkehr im Netzwerk verursacht. Falls notwendig, lassen sich über einen bestimmten Zeitraum Datenpakete über den Capture-Mechanismus sammeln. Damit läßt sich eine gezielte Analyse durchführen, welche Datenpakete im Netzwerk transportiert werden – um zum Beispiel feststellen zu können, warum eine bestimmte Funktion nicht ausgeführt werden kann. Derzeit können damit nur Ethernet- und Token-Ring-Netzwerke analysiert werden.

Der NetWare LANalyzer Agent überwacht somit ständig den gesamten Verkehr auf den angeschlossenen Ethernet- und Token-Ring-Segmenten, speichert die gesammelten statistischen Daten und Trendinformationen über jede Workstation auf dem Netzwerk und liefert dafür Echtzeitinformationen über den Netzwerkstatus. Durch die Möglichkeit, die Netzwerkfunktionalität über einen längeren Zeitraum zu überwachen, lassen sich Netzwerkerweiterungen besser planen. Über die Auslastungsstatistik wird aufgezeigt, ob bzw. welche Geräte überlastet sind, welche Anwender für die Überlastung verantwortlich sind und über welche Anwendungen die Überlastung verursacht wird. Die Möglichkeit der Trendstatistik gibt an, wann die Überlastungen auftreten.

Ein aktivierter LANalyzer Agent warnt auch rechtzeitig davor, wenn zum Beispiel IP-Adressen doppelt vergeben worden sind. Somit kann bereits rechtzeitig ein Fehler erkannt werden, bevor man lange nach den Ursachen des Fehlers suchen muß.

Die wesentlichen Merkmale für den LANalyzer Agent sind:

- Erfassung und Speicherung von Netzwerkstatistiken
- Verbesserung der automatischen Erkennungsfunktion des NMS-Explorers
- Überwachung des Verkehrs auf Ethernet- oder Token-Ring-Segmenten

6 Netzwerkmanagement

- Ausgabe von Alarmmeldungen bei übergroßen Paketen, Überlastung und einem zu großen Multicast-Aufkommen
- Alarmmeldung bei Erkennen von doppelten IP-Adressen
- Vollständige Unterstützung von SNMP und allen neun Ethernet-RMON-Gruppen
- Informationsaustausch über die NMS-Console
- Speicherung von Paketen zur Analyse und Auswertung
- Zusammenarbeit mit dem Modul NetWare Expert, um schnell und einfach Vorschläge zur Behebung aufgetretener Fehler zu erhalten
- Ausführliche Statistiken
- Möglichkeit zur Analyse des gesamten Netzwerks, einer einzelnen Workstation oder eines gezielten Datenaustauschs zwischen zwei Endgeräten
- Identifizierung überlasteter Endgeräte oder überlasteter Netzwerksegmente
- Identifizierung des Benutzers, der am meisten Datenverkehr verursacht
- Konzeptunterstützung, wenn es darum geht, neue Endgeräte zu integrieren, ohne bestehende Segmente zu überlasten.

NetWare-Hub-Services (Hub-Management)

Zum Lieferumfang von NMS gehört auch das Hub-Management, um damit HMI-fähige Hubs verwalten zu können.

Unter HMI-fähigen Hubs sind Komponenten zu verstehen, die meist als Steckkarte konzipiert und in einem NetWare-Server eingebaut sind. Dies muß jedoch nicht so sein. So haben die Hersteller Networth und UB Networks die Unterstützung von HMI (Hub-Management-Interface) bereits für die externen Hubs realisiert. Die hierfür notwendige Software NetWare Hub Services enthält bereits die notwendige SNMP-Unterstützung, die einen separaten Hub-Agent nicht mehr notwendig werden läßt. Wenn der Hersteller diesen Mechanismus unterstützt, erhält man in einer grafischen Darstellung eine genaue Übersicht des Hub-Aufbaus und der Konfiguration des Hub. Für jeden Port, den gesamten Hub oder eine einzelne Hub-Karte werden Statistiken, Konfigurationsdaten oder auch Performance-Analysen ausgegeben. Sollte ein Port irgendwelche Fehler aufweisen, kann er abgeschaltet werden.

Neben diesen Möglichkeiten der Netzwerkerkennung und -darstellung bietet NMS noch eine Vielzahl von Standardfunktionen. Hierzu zählt unter anderem auch das Monitoring von Routern bzw. die Handhabung des Alarms.

6.4 ManageWise

Router-Management

Mit dem Router-Management ist es möglich, jeden MIB-II-kompatiblen Router zu administrieren. Dabei ist es egal, ob es sich um einen MPR von Novell oder einen Router von CISCO oder Wellfleet handelt. Beim Aktivieren des Router-Managements können Sie zum Beispiel die Informationen über die Netzwerkadapter im Router und die dazugehörige Konfiguration auf diesen Karten abfragen. Damit erhält man einen umfassenden Überblick über alle im Netzwerk installierten Router, den aktuellen Status, die installierten routbaren Protokolle, die empfangenen, gesendeten, gefilterten und fehlerhaften Pakete des jeweiligen Routers.

Somit ist der NMS-Explorer in der Lage, sowohl IPX-Router als auch IP-Router zu erkennen. Nach Auswahl eines erkannten IPX-Routers lassen sich unter anderem die folgenden Informationen anzeigen:

- *Interfaces*
Man erhält eine Übersicht über alle im Router eingebauten Netzwerkkarten.
- *IPX-Konfiguration*
Alle relevanten IPX-Parameter werden übersichtlich dargestellt. Hierzu zählen auch die Parameter für NLSP, wenn dies am Router aktiviert ist.
- *IPX-Statistiken*
Der ein- und ausgehende Datenverkehr wird – bezogen auf die Zeit – dargestellt.
- *NLSP-Topologie*
Es wird die Netzwerktopologie dargestellt, die zwischen einer Gruppe miteinander verbundener NLSP-Router aufgebaut wird.

Neben diesen wichtigen Informationen erhält man an der NMS-Console auch die Möglichkeit, Informationen über vergebene Netzwerkadressen aufzulisten. Entsprechend den erkannten Netzwerkadressen durch den Netexplorer wird dabei zwischen IPX-Adressen-Tabellen und IP-Adressen-Tabellen unterschieden. In dieser Auflistung sind auch die Adressen für NetWare/IP-Domains aufgenommen.

Wenn im entsprechenden Fenster per Doppelklick auf eine Netzwerkadresse gegangen wird, dann erhält man zusätzlich folgende Informationen:

- Alle IPX-Endgeräte, die sich auf diesem Segment befinden, wenn es sich beim ausgewählten Segment um ein physikalisches Netzwerk handelt.

6 Netzwerkmanagement

- Alle Protokolladressen, die einem internalen Network zugewiesen sind, wenn es sich bei der Auswahl um einen NetWare-Server handelt.
- Alle NetWare/IP-Endgeräte in der Domain, wenn es sich bei der ausgewählten Einheit um eine NetWare/IP-Domain handelt.

In der IP-Netzwerk-Tabelle werden alle IP-Netzwerke und die dazugehörigen Subnetzmasken aufgelistet. Wenn eine IP-Adresse per Doppelklick ausgewählt wird, werden alle erkannten IP-Router in diesem Segment aufgelistet. Wenn in diesem Segment auch der LANalyzer Agent aktiv ist, werden zusätzlich alle erkannten IP-Endgeräte dargestellt.

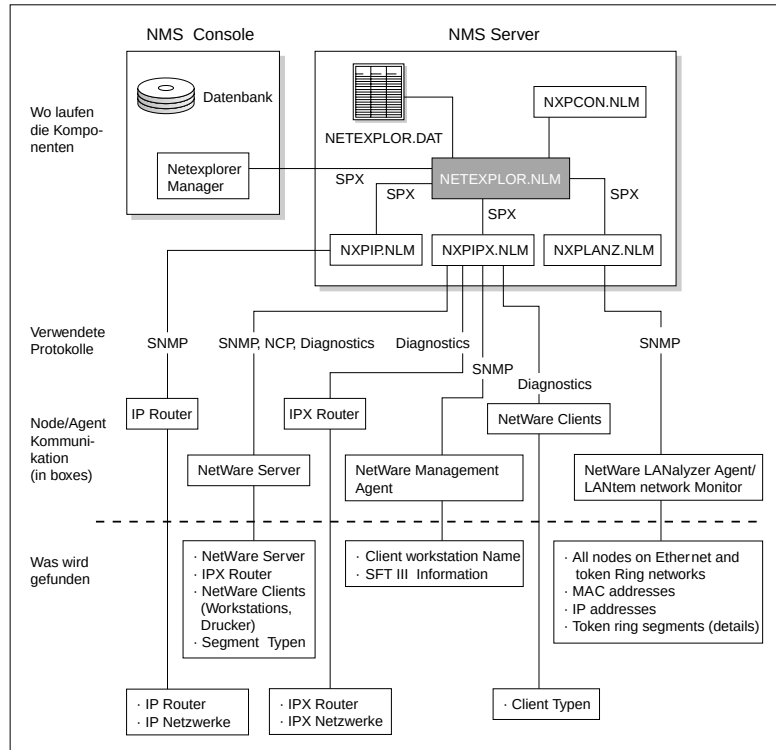
Aus der TCP/IP-Welt ist der Ping-Befehl bekannt, mit dem festgestellt wird, ob ein Endgerät im Netzwerk funktionsfähig ist und auch erreicht werden kann. Dies ist vor allem dann wichtig, wenn zu testen ist, ob die Router im Netzwerk richtig konfiguriert sind und damit auch ordnungsgemäß Daten ausgetauscht werden können. Über die Connectivity-Funktion von NMS kann ein Netzwerkadministrator prüfen, ob einzelne Devices aktiv im Netzwerk vorhanden sind und erreicht werden können. Der Connectivity-Test kann dabei entweder über IPX-Protokoll oder IP-Protokoll durchgeführt werden. Bei Bedarf kann man diesen Test periodisch einstellen, um bestimmte Devices in regelmäßigen Abständen prüfen zu lassen.

Das NMS-Alarmsystem informiert die NMS-Console über alle auftretenden Probleme und andere Fehlersituationen im Netzwerk. Alarmer können von jedem Endgerät kommen, wenn es in der Lage ist, einen SNMP-Trap an die NMS-Console zu schicken. So erzeugt der NetWare Management Agent bestimmte Alarmmeldungen, wenn bestimmte Thresholds überschritten worden sind. Aufgetretene Alarmer sind in der Internetwork Map bzw. der Custom Map bereits optisch zu erkennen, da über dem jeweiligen Device in der Map ein Glockensymbol auf einen Alarm hinweist. Die unterschiedliche Farbgebung des Glockensymbols kennzeichnet den Alarm als Hinweis oder als dringlich (rotes Glockensymbol).

Einen Überblick der gesamten NMS-Funktionalitäten und Arbeitsweisen sowie der Mechanismen, die in Zusammenarbeit mit dem NMS-Netexplorer und der NMS-Console zur Verfügung gestellt werden, gibt die Abbildung 6.6.

6.4 ManageWise

Abbildung 6.6
NMS-Discovery-
Architektur



ManageWise Maps

Wenn alle notwendigen Komponenten für ManageWise installiert worden sind, erfolgt die Überwachung des Systems über die NMS-Consolen-Software. Hierbei arbeitet ManageWise mit den sogenannten Maps, um das Netzwerk am Bildschirm darstellen zu können. Zu unterscheiden sind dabei:

- Logical Maps, diese werden automatisch durch die gesammelten Daten erstellt,
- Custom Maps, individuell erstellte Maps.

Zusätzlich können in ManageWise eigene Objekte erstellt und in die Maps integriert werden, sofern Objekte nicht automatisch vom Explorer-Mechanismus erkannt werden.

Logical Maps

Wenn Netzwerkdaten vom Explorer an die NMS-Consolen-Software übermittelt und in die ManageWise Datenbank eingetragen werden, beginnt die NMS-Consolen-Software damit, ein Abbild (Map) des

6 Netzwerkmanagement

Netzwerks aufzubauen. Nach »kurzer« Zeit, in Abhängigkeit von der Netzwerkgröße, findet man in dieser Map das ganze Netzwerk in Form von Segmenten, Connections und Endgeräten. Per Default bietet ManageWise für Logical Maps zwei Arten von Maps:

- *Internetwork Map*

Hierin werden alle erkannten Netzwerksegmente, Router und die logischen Verbindungen zwischen diesen Segmenten aufgezeigt.

- *Segment Map*

Pro erkanntes Netzwerksegment kann eine eigene Map geöffnet werden, die dessen Server, Workstations, Router und andere Endgeräte aufzeigt.

Zu beachten ist dabei, daß die Maps auch dazu dienen, um sich durch das Netzwerk zu navigieren. Wenn z.B. ein Alarm für einen Server erkannt wird, dann erscheint eine Alarmglocke über dem jeweiligen Objekt. Durch Markieren und Öffnen des Alarm-Managers kann nachgelesen werden, welcher bzw. welche Fehler aufgetreten sind, um dann die notwendigen Gegenmaßnahmen ergreifen zu können.

Custom Maps

Neben den standardmäßigen Logical Maps stellt ManageWise auch noch einen Map-Editor zur Verfügung, mit dem man in der Lage ist, seine eigenen, angepaßten Maps darzustellen. Auf diese Art und Weise kann man zum Beispiel mit gescannten Bildern des Firmengeländes, der Gebäude, der Raumpläne etc. das Netzwerk Schicht für Schicht in Bildform darstellen, um dann zum Beispiel in den Raumplänen den Server bzw. die Workstation an die korrekten Stellen platzieren zu können. Somit erhält man eine Navigationshilfe, die vom Übersichtsplan immer mehr ins Detail geht.

Alarmsystem

Über das ManageWise-Alarmsystem wird man rechtzeitig über Fehler und andere Bedingungen im Netzwerk informiert. Die Alarme können dabei von einer Vielzahl von Quellen stammen:

- Von jedem Endgerät, das SNMP unterstützt und in der Lage ist, SNMP-Traps an die ManageWise-Console abzusetzen
- Vom NetExplorer, wenn der Discovery-Mechanismus durchgeführt wird
- Von Programmen, die auf der ManageWise-Console laufen
- Von einem Fehler, der beim Connectivity-Test erkannt wird

6.4 ManageWise

Allen Alarmen sind standardmäßig Wichtigkeit, Status und Reaktionen zugewiesen, die jedoch bei Bedarf modifiziert werden können. Man sollte sich dabei genau überlegen, wie diese Anpassung der Alarm-Disposition aussehen soll.

Alarmtabellen

Über die aufgetretenen Alarme kann man sich im Detail entweder über den Alarm-Report oder den Alarm-Monitor informieren. Die Aufgaben dieser beiden Möglichkeiten sind folgende:

- *Alarm-Report*

Es werden Alarme angezeigt, die in der Datenbank gespeichert sind. Es können alle Alarme oder nur Alarme für ein bestimmtes Objekt angezeigt werden. Über den Alarm-Report lassen sich auch Alarme löschen, akzeptieren und Kommentare hinzufügen. Für den Alarm lässt sich auch ein Experten-System aufrufen, das Vorschläge unterbreitet, wie auf den Alarm zu reagieren ist.

- *Alarm-Monitor*

Dieser wird standardmäßig beim Aufruf der ManageWise-Console gestartet und zeigt eine Tabelle, in der sich die letzten 400 Alarme befinden, die empfangen worden sind.

ManageWise-Datenbank

Der wesentliche Bestandteil von ManageWise ist die installierte Datenbank, in der alle notwendigen Informationen gesammelt und anschließend grafisch am Bildschirm dargestellt werden. Die wesentlichen Informationen sind dabei:

- *Netzwerk-Topologie*

Darin enthalten sind Informationen über Netzwerke, Segmente, Endgeräte im Segment, Adapterkarten, die am Segment angeschlossen sind, Adressen, die Endgeräten zugewiesen sind, Dienste wie Routing, Files Services, Print Services etc.

- *Daten über die Custom Map*

Diese Informationen werden nicht automatisch erkannt, sondern individuell eingegeben und konfiguriert.

- *Konfiguration*

Für jedes Objekt können zusätzliche Informationen in Form von Attributen eingegeben werden. So können zum Beispiel Informationen über die Betriebssystem-Version, Plattengröße, Hauptspeicher etc. eingegeben werden.

- *Alarm-System-Konfiguration*

Wenn unterschiedliche Dispositionen für das Alarmsystem eingegeben werden, dann werden auch diese in der Datenbank gespeichert.

6 Netzwerkmanagement

■ *Logged Alarme*

Ausgewählte Alarme können ebenfalls in der Datenbank gespeichert werden.

■ *Class-Informationen*

Die Datenbank enthält auch Informationen über sich selbst und die Objekttypen, die der Datenbank bekannt sind. Third-Party-Entwickler können weitere Objekte in der Datenbank erstellen und abspeichern.

Netzwerkadressen und Verbindungen

ManageWise stellt Werkzeuge zur Verfügung, die eingesetzt werden können, um damit Netzwerkadressen zu verwalten und die Verbindungen mit anderen Systemen zu testen. Die ManageWise-Console bietet drei Netzwerktabellen, die eingesetzt werden können, um eine bessere Planung für die Vergabe von IPX-, IP- und NetWare/IP-Adressen durchführen zu können. Hierzu zählen:

■ *IPX-Netzwerk-Tabelle*

Hierin werden alle IPX-Netzwerkadressen aufgelistet, die im gesamten Netzwerk erkannt worden sind.

■ *IP-Netzwerk-Tabelle*

Hierin werden alle vergebenen IP-Netzwerkadressen und die dazugehörigen IP-Subnet-Masks aufgelistet.

■ *NetWare/IP-Tabelle*

Hierin werden alle NetWare/IP-Nodes aufgelistet, die zu einer Domäne gehören.

Netzwerk-Segment-Management

Mit ManageWise ist man in der Lage, jedes Ethernet-, Token-Ring- oder FDDI-Netzwerk zu verwalten, wenn es mit Hilfe des NetWare LANalyzer Agent überwacht wird. Dieser Agent überwacht ständig die folgenden Werte:

- Sammlung von Statistiken anhand sogenannter Verkehrsmuster
- Suchen von Alarmbedingungen
- Aufsammlen von Datenpaketen (Capture von Datenpaketen) entsprechend selbst gesetzter Werte und Parameter

Der bzw. die LANalyzer Agents können alle Datenpakete im Netzwerk überwachen und aufnehmen, egal ob diese von Servern oder anderen Endgeräten erzeugt werden. Durch die Analyse der gesamten Datenpakete können Fehlersituationen noch besser eingegrenzt und ausgewertet werden. Wenn der LANalyzer Agent in einem anderen Segment läuft, bezogen auf das Segment, in dem sich

6.4 ManageWise

die ManageWise-Console befindet, dann kann man von jeder beliebigen ManageWise-Station aus mit Hilfe des LANalyzer Agent die Netzwerksegmente problemlos überwachen und auswerten.

ManageWise wird durch den LANalyzer Agent zusätzlich um die folgenden Funktionen erweitert:

- Es werden alle Endgeräte auf dem Segment erkannt, die vom LANalyzer Agent überwacht werden, unabhängig davon, welches Protokoll eingesetzt wird.
- Überwachung der Performance aller Segemente, die überwacht werden, so daß an die ManageWise-Console dynamisch Informationen gegeben werden.
- Es wird leichter, Schwellenwerte für eine Vielzahl nützlicher Alarmer zu setzen, um damit proaktives Netzwerkmanagement durchführen zu können.

SNMP-Objekt-Management

Mit ManageWise lassen sich alle Endgeräte im Netzwerk überwachen, wenn diese SNMP-fähig sind. Im besonderen kann man damit

- Alarmer empfangen (SNMP-Traps an die ManageWise-Console übertragen) und
- den SNMP-MIB-Browser einsetzen, um SNMP Werte anzeigen zu lassen oder zu ändern (sofern es sich nicht um Objekte handelt, die bereits von ManageWise vollständig integriert worden sind).

Mit dem SNMP-MIB-Browser kann die Verbindung zu jedem SNMP-fähigen Endgerät aufgebaut werden, entweder IP- oder IPX-Protokoll, um Werte anzuzeigen oder Werte zu ändern.

Neben diesen NMS-Funktionalitäten, die sich noch erheblich ergänzen lassen, werden die gesamten Netzwerkmanagement-Funktionen von ManageWise um die Komponenten der Desktop-Management-Komponenten erweitert.

Das Management der Workstations im Netzwerk ist mit ManageWise im Vergleich zum ursprünglichen NMS wesentlich erweitert worden. Mußte man früher bei NMS alle Informationen für die Workstations selbst pflegen, übernimmt diese Aufgabe im ManageWise die integrierte Desktop-Komponente, deren wesentlichen Aufgaben bereits automatisch beim Anmelden durchgeführt werden.

6.4.2 Management von Workstations

Durch die Integration der Desktop-Management-Funktionen bietet ManageWise hervorragende Möglichkeiten, Workstations im Netzwerk zu verwalten. Mit einem einfachen Mausklick auf das entsprechende Workstation-Symbol in der Internetwork Map werden die Desktop-Manager-Systemfunktionen automatisch aktiviert. Zu diesen Funktionen gehören:

- Desktop Access** Mit dieser Funktion steht Ihnen der Remote Access auf andere Workstations sowohl unter DOS als auch unter Windows zur Verfügung. Somit kann bei Problemen sofort überprüft werden, ob Eingabefehler gemacht wurden oder aufgrund von falschen Konfigurationen bestimmte Mechanismen nicht funktionieren. Zudem ist der Netzwerkverwalter in der Lage, Informationen über die Konfiguration und Netzwerkaktivitäten einzelner Workstations abzurufen. Bei Bedarf können notwendige Aktivitäten auch auf der remoten Workstation gestartet werden. Ist es notwendig, dann kann auch ein Warmstart dieser Workstation durchgeführt werden. Der Remote Access wird nur dann aktiviert, wenn der Anwender auch die Genehmigung hierfür erteilt. Somit kann es nicht vorkommen, daß Anwender unberechtigt in ihrer Tätigkeit überwacht werden.
- Chat** Bei dieser Funktion öffnet sich eine Dialogbox, um mit dem Remote-Anwender eine »schriftliche« Kommunikation durchzuführen. Der Bildschirm wird dabei in zwei Teile gesplittet. In den oberen Teil werden die Nachrichten geschrieben, die der Anwender auf seinem Bildschirm empfängt, wohingegen im unteren Teil des Bildschirms die Nachrichten gezeigt werden, die der Anwender als Antwort schreibt.
- File-Transfer** Mit dieser Funktion können Dateien von und zu einer Zielstation übertragen werden. Auf diese Weise kann der Netzwerkverwalter zum Beispiel Korrekturen an der AUTOEXEC.BAT durchführen oder neue Treiber übertragen, ohne seinen Arbeitsplatz verlassen zu müssen.
- Desktop Remote** Die Funktion ermöglicht es dem Netzwerkverwalter, auf ein Remote-Netzwerk über eine Remote-Verbindung (z. B. per Modem) zuzugreifen.
- Inventory Manager** Mit dem Inventory Manager werden sämtliche Hard- und Software-Komponenten der Workstations und Server durchgeführt. Diese Informationen werden in einer Datenbank gesammelt und können über umfangreiche Abfragefunktionen ausgewertet werden. Durch die Kombination der Abfragen mit logischen Verknüpfungen können so ziemlich alle Abfragetypen realisiert werden, um genau die benötigten Informationen zu erhalten.

6.4 ManageWise

Queue Monitor

Dieser Mechanismus stellt alle im Netzwerk eingerichteten Print-Queues zur Verfügung. Mit den gesammelten Informationen ist es dem Administrator möglich, den Status der Print-Queues auszuwerten, Druckaufträge zu löschen oder die Reihenfolge der Druckaufträge zu ändern.

In Tabelle 6.1 ist aufgezeigt, welche Desktop-Management-Funktionen für die jeweiligen Workstations zur Verfügung stehen.

Tabelle 6.1

Desktop-Management-Funktionen

	IPX	Microsoft NetBIOS, IPX, TCP/IP, NetBEUI	Winsock TCP/IP
Windows 98 Windows 95 Windows for workgroups, Windows 3.1x	Remote Control Chat File Transfer Diagnostics Reboot Inventory Anti-virus	Remote Control Chat File Transfer Diagnostics Reboot Inventory	Remote Control Chat File Transfer Diagnostics Reboot Inventory
Windows NT workstations and Server	Remote Control Chat File Transfer Reboot Inventory		Remote Control Chat File Transfer Reboot Inventory
NetWare Server	Remote Control Inventory		
DOS	Remote Control Chat File Transfer Reboot Inventory	Remote Control Chat File Transfer Reboot Inventory	
OS/2	Remote Control Inventory		
Macintosh	Inventory		

Eine wesentliche Funktion, die mit ManageWise zur Verfügung gestellt wird, sind die Möglichkeiten zur Überwachung des gesamten Netzwerks und dessen Schutz gegen Virenbefall. Es stehen dazu mehrere Möglichkeiten zur Verfügung:

Netzwerkweiter Virus Protect

Das Risiko, einen Virus im Netzwerk oder auf einer Workstation einzuschleusen, nimmt immer mehr zu. Dabei muß das inzwischen nicht mehr durch den Austausch von Disketten passieren. Aufgrund der immer beliebter werdenden Online-Dienste können Viren inzwischen auch über diesen Weg eingeschleust werden. Vergessen werden darf auch nicht das Internet, zu dem inzwischen immer mehr Unternehmen Zugang haben. Im Lieferumfang von ManageWise sind deshalb entsprechende Komponenten enthalten, die eine auto-

6 Netzwerkmanagement

matische Virenprüfung auf dem NetWare-Server und/oder auf den Workstations im Netzwerk zulassen. Mit ManageWise setzt Novell inzwischen auf die Virus-Protect-Komponente InocuLAN von CA (früher Cheyenne). Hierbei handelt es sich um ein inzwischen sehr leistungsfähiges und relativ einfach zu konfigurierendes System.

InocuLAN setzt vier Techniken ein, um Viren zu erkennen:

- *Integrity Checking*
Hiermit wird festgestellt, ob sich der Inhalt eines Programms geändert hat, weil eine Infizierung mit einem Virus erfolgte.
- *Regelbasierend bzw. polymorphe Analyse-Erkennung*
Das ist die Festlegung des Verhaltens von Programmen, so daß ein ungewöhnliches Verhalten von Programmen erkannt wird.
- *Interrupt Monitoring*
Es werden hierbei alle Programmsystemaufrufe beobachtet, um zu erkennen, ob die Sequenz von Aufrufen geändert ist, so daß Virus-Aktivitäten erkannt werden.
- *Signatur Scanning*
Bei dieser Methode wird eine Virus-Signaturliste verwendet, um zu erkennen, ob ein Virus die Hex-Kennung in der Datei zurückgelassen hat. Dadurch ist man in der Lage, bekannte Viren zu erkennen und daraufhin entsprechende Aktionen einzuleiten. Für diesen Teil der Virenerkennung muß in regelmäßigen Abständen eine neue Signaturliste aus dem Internet besorgt werden.

Zu den wichtigsten unterstützten Funktionen zur Virenerkennung und zum Virenschutz zählen unter anderem:

- *Realtime Scanning Mode*
Alle ein- und ausgehenden Dateien vom und zum Server werden automatisch auf Viren geprüft.
- *Virus Wall*
Ähnlich wie Realtime Scanning wird versucht, eine infizierte Datei auf den Server zu kopieren; dann wird diese »bereinigt« auf dem Server abgelegt.
- *Virus Quarantine*
Benutzer, die versuchen, eine infizierte Datei auf den Server zu kopieren, werden automatisch suspendiert, so daß eine Infektion isoliert wird, bevor größerer Schaden entstehen kann.
- *Floppy-Laufwerk-Schutz*
Disketten sind immer noch die größte Gefahr (neben Internet und anderen Online-Diensten), um sich mit Viren zu infizieren. Mit diesem Schutzmechanismus wird beim Zugriff auf die Diskette sofort der Boot-Sektor und beim Zugriff auf eine Datei auch diese sofort auf Viren geprüft. Somit ist im Prinzip die größtmögliche Sicherheit für das Arbeiten mit Disketten gegeben.

6.4 ManageWise

■ *CD-ROM-Schutz*

Nicht alle Virenprüfprogramme sind in der Lage, auch CD-ROMs in den Schutzmechanismus aufzunehmen. InocuLAN kann auch CD-ROMs auf Viren prüfen.

■ *Internet-enabled*

Durch das Internet verbreiten sich Viren noch schneller als zuvor, so daß man auch hier vorsichtig sein muß. Durch den Einsatz von InocuLAN werden automatisch alle Dateien, die man aus dem Internet holt, auf Viren geprüft, bevor der Rechner damit infiziert werden kann. Darin enthalten ist auch die Unterstützung für Compressed Files und der Einsatz für NetScape Navigator und Microsoft Internet Explorer.

■ *GroupWare Messaging AntiVirus*

Durch den Austausch von Mailing, vor allem durch sogenannte Attachments, steigt die Gefahr, sich Viren zu holen. Um auch dieser Gefahr aus dem Weg zu gehen, ist InocuLAN in der Lage, Lotus Notes und Microsoft Exchange Mailing Systeme abzusichern. Zum Zeitpunkt der Erstellung dieses Buches war CA dabei, auch eine Unterstützung für GroupWise zu entwickeln.

Dies ist nur ein kleiner Ausschnitt der Möglichkeiten, die mit InocuLAN als Virus-Protect-System zur Verfügung stehen. Diese Auflistung soll auch dazu dienen, einen groben Überblick darüber zu erhalten, was beim Einsatz solcher Systeme zu berücksichtigen ist. Auf alle Fälle gilt, daß man sich vor einer endgültigen Entscheidung die in Frage kommenden Systeme genau ansehen sollte.

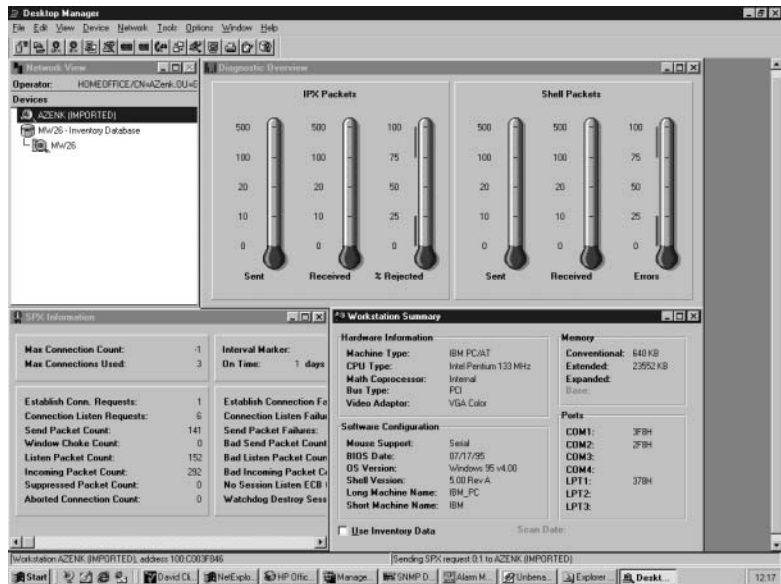
Beachtet werden sollte dabei auch, daß die Installation der Workstation-Komponenten für das Viren-Protect-System automatisch abgewickelt werden kann, ohne als Administrator weitere Eingriffe durchführen zu müssen. Hierzu sind in der Regel nur entsprechende Einträge in den Anmeldeskripten durchzuführen.

Dieser Überblick soll Ihnen aufzeigen, welche Möglichkeiten heute bereits zur Verfügung stehen und auch verfügbar sein sollten, um ein effizientes Netzwerkmanagement durchzuführen bzw. durchführen zu können. Die nachfolgenden Abbildungen zeigen auf, wie sich die entsprechenden Informationen am Bildschirm darstellen und welche Informationen damit erhalten werden. Es sei nochmals darauf hingewiesen, daß es sich hierbei nur um einen kleinen Überblick dessen handelt, was Ihnen in der Praxis damit zur Verfügung gestellt wird.

Abbildung 6.7 zeigt, wie ManageWise unter anderem die Informationen über den SPX-Datenverkehr einer ausgewählten Station am Bildschirm darstellt. Ebenso kann man ein Workstation Summary erkennen und ein Diagnose-Fenster, über das ein- und ausgehende Pakete der Station gemessen werden.

6 Netzwerkmanagement

Abbildung 6.7
Desktop-Access-
Funktion



In dieser Abbildung ist auch zu sehen, welche einzelnen Funktionen im Fenster »Desktop Access« für die ausgewählte Station zur Verfügung stehen.

In Abbildung 6.8 sehen Sie im oberen Bildschirmfenster einen Auszug von gesammelten Datenpaketen über den eingebauten LAN-analyzer. Das untere Bildschirmfenster zeigt das sogenannte Dashboard, eine schnelle Übersicht über Pakete/s, Broadcast, Utilization und Errors.

Zudem wird Ihnen für jede Station im Netzwerk die momentan davon erzeugte Netzwerklast angezeigt. Der aktuelle Balken ist die momentane Last, wohingegen der abgesetzte Strich im Balken den letzten Peak-Wert angibt.

In Abbildung 6.9 sehen Sie für das ausgewählte Netzwerksegment die Speicheraufteilung eines ausgewählten Dateiservers, die CPU-Auslastung für einen ausgewählten File-Server und die bislang aufgetretenen Alarme für das ausgewählte Netzwerk.

An dieser Stelle sei auch darauf hingewiesen, daß für ein effektives Netzwerkmanagement der Administrator unbedingt mit einem 20-Zoll-Bildschirm arbeiten sollte. Nur so werden genügend Informationen übersichtlich auf einer Bildschirmseite dargestellt.

6.4 ManageWise

Abbildung 6.8
LANalyzer-Funktion von NMS

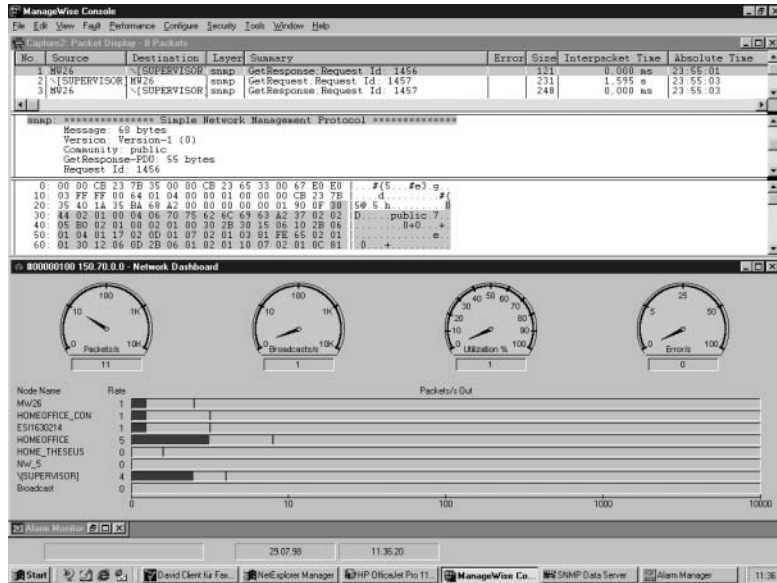
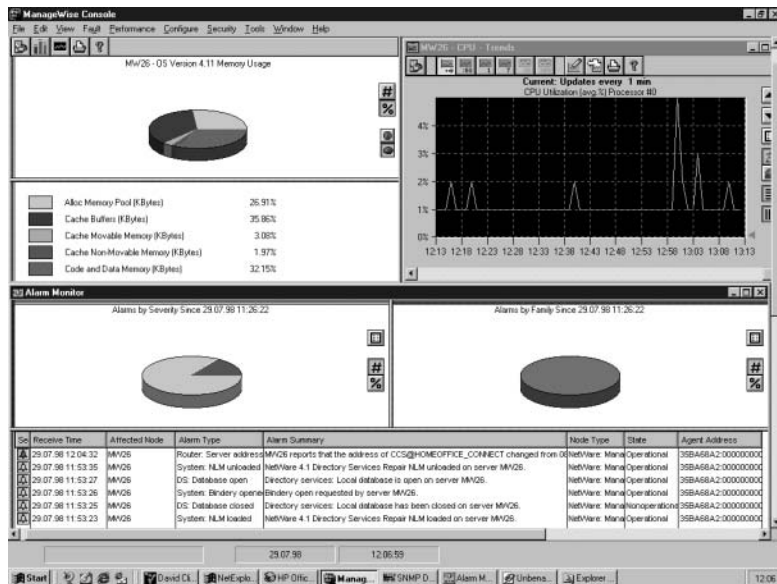


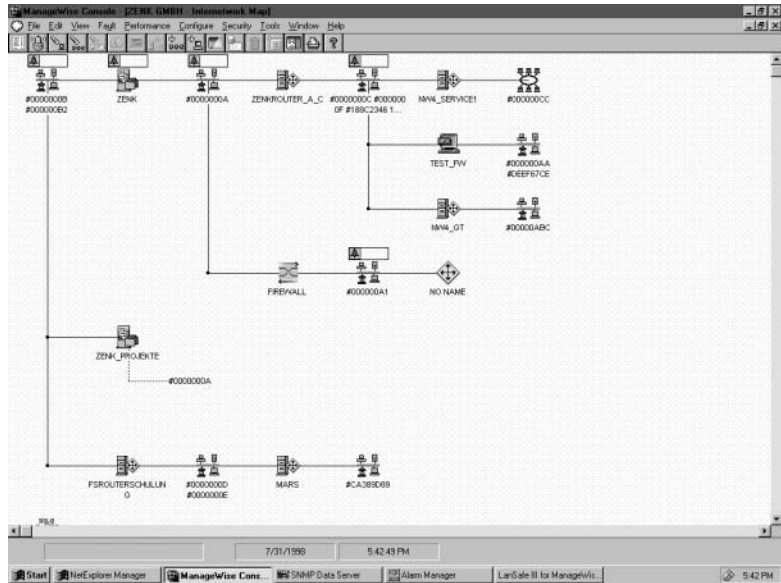
Abbildung 6.9
Unterschiedliche
Informationen in
einzelnen Fenstern
dargestellt



In Abbildung 6.10 ist dargestellt, wie eine Internetwork Map aussehen kann, wenn es sich um ein größeres Netzwerk handelt. Von dieser Map aus kann durch das gesamte Netzwerk traversiert werden.

6 Netzwerkmanagement

Abbildung 6.10
Internetwork Map



Abschließend soll Ihnen noch ein Überblick gegeben werden, welche Hersteller derzeit Snap-in-Module zur Verfügung stellen, um den Funktionsumfang von ManageWise zu erweitern bzw. Netzwerkmanagement-Funktionen eines anderen Herstellers in ManageWise zu integrieren, wobei nur die wichtigsten Hersteller aufgeführt sind und die Liste somit noch um eine Vielzahl anderer Hersteller erweitert werden könnte.

6.5 Snap-in-Module anderer Hersteller

Allied Telesyn

Für die Verwaltung von Standalone, Stackable oder Chassis Mounted Hubs stellt Allied Telesyn ein passendes Snap-in-Modul zur Verfügung.

APC (American Power Conver- sion)

Eine weitverbreitete USV-Anlage stammt von der Firma APC. Durch die optimale Integration in eine NetWare-Umgebung und den für ManageWise verfügbaren PowerNet-SNMP-Manager lässt sich die Verwaltung der USV-Systeme sehr schön in die Netzwerkmanagement-Umgebung integrieren. So sammelt der PowerNet-Manager den aktuellen Zustand der USV und stellt alle Informationen in grafischer Form dar. Hierzu ist es nur notwendig, daß auf dem Server der PowerNet SNMP Agent installiert ist.

6.5 Snap-in-Module anderer Hersteller

Nortel Networks Zur Überwachung und Steuerung der Nortel-Networks-Komponenten, also für das Router- und Hub-Management, steht ein entsprechendes Snap-in-Modul zur Verfügung. Optivity for ManageWise unterstützt unter anderem Funktionen wie Error und Status Thresholds, Management Tools und automatische Früherkennung sich abzeichnender Fehler.

Cabletron Zur Überwachung der Ethernet-, Token-Ring- und FDDI-Komponenten stellt Cabletron einen Teil der Spectrum-Funktionen als Snap-in-Modul für ManageWise zur Verfügung. Hierbei werden unter anderem Managementfunktionen für die Komponenten EMME, EMME-E6, MRXI, TRMM, TRXI oder auch die FDMMIM geboten.

AVM Die Firma AVM stellt für den AVM MPR for ISDN ein sehr gutes Snap-in-Modul zur Verfügung, um einen vollständigen Überblick über alle Aktivitäten des Routers zu erhalten. Mit diesem Modul lässt sich eine Vielzahl von Statistiken und Auswertungen erstellen, mit denen man nicht nur die Funktionsfähigkeit genauer überwachen kann, sondern auch die Leitungskosten in den Griff bekommt.

Weitere bekannte Hersteller mit Snap-in-Modul-Unterstützung sind: Blue Lance, Cheyenne, Compaq, Conner, Eicon, IBM, Intel, Lexmark, Madge, NetWorth, Storage Dimensions, SunSoft und viele andere mehr.

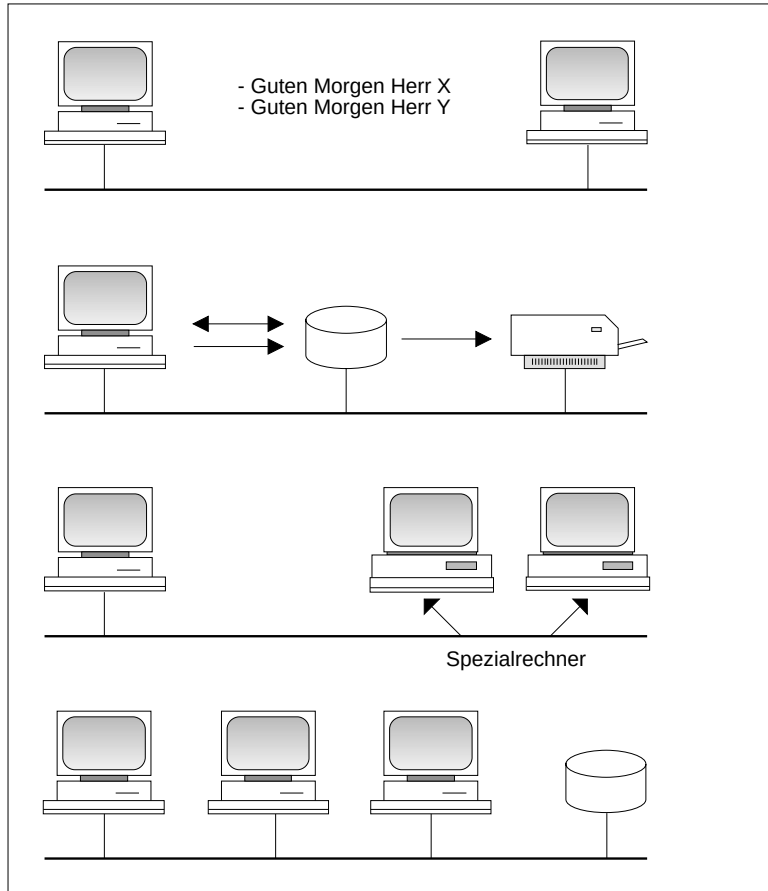
Um sich einen Überblick über die Snap-in-Module für ManageWise zu verschaffen, sei auf den Solutions Guide verwiesen. Darin sind alle bekannten und noch in Entwicklung befindlichen Produkte aufgeführt.

7

Aufgaben

Lokaler Netzwerke

Abbildung 7.1
Die vier Aufgaben
eines LANs



Nachdem bisher viele der grundlegenden Voraussetzungen für den Betrieb und den Aufbau von LANs erläutert worden sind, sollen in diesem Kapitel die Aufgaben eines LAN näher untersucht werden. Übrigens: Wenn hier von LANs gesprochen wird, sind ganz allgemein Lokale Netzwerke gemeint. Es kann sich dabei um Netzwerke handeln, die aus beliebigen Rechnertypen bestehen. Tatsache ist, daß sich das LAN generell nur auf die eigene Grundstücksfläche beschränkt. Später werde ich mich dann den speziellen LANs – PC-

7 Aufgaben Lokaler Netzwerke

LANs – widmen. Hierbei handelt es sich um Netzwerke, die nur aus Personalcomputern bestehen. Die Aufgaben eines LAN kann man, wie in Abbildung 7.1 zu sehen ist, in folgende Bereiche einteilen:

- Nachrichtenaustausch
- Zugriff auf zentrale Betriebsmittel
- Zugriff auf die Verarbeitungskapazität anderer Rechner
- Zugriff auf zentrale Datenbestände

7.1 Nachrichtenaustausch

Unter Nachrichtenaustausch ist zum einen die einzelilige Nachrichtenübermittlung an andere Stationen zu verstehen (Einblendung dieser in der Statuszeile), zum anderen der Einsatz von Electronic-Mail-Systemen, um ganze Dokumente oder Dateien an Mitarbeiter zu versenden. (Das papierlose Büro der Zukunft läßt grüßen.) Die verschickten Texte und Dokumente sind so lange in einem elektronischen Briefkasten beim Empfänger gespeichert, bis sie vom Empfänger gelesen, anderweitig gespeichert oder gelöscht werden.

Grundsätzlich kann mit einem E-Mail-System jede Art von Datei übertragen werden. Es handelt sich dabei im Prinzip um einen Dateitransfer.

7.2 Zugriff auf zentrale Betriebsmittel

In einem LAN ist es nicht unbedingt notwendig, daß alle Stationen mit einer kompletten Peripherie ausgestattet werden. Es muß zum Beispiel nicht jeder Arbeitsplatz einen eigenen Drucker oder hochwertigen Plotter zur Verfügung haben. Eine geforderte Aufgabe eines LAN besteht deshalb darin, allen im Netz befindlichen Stationen eine festgelegte Peripherie zur Verfügung zu stellen. Dies gilt vor allem für zentrale Plattenspeicher, Drucker oder spezielle Peripheriegeräte. Die Aufgabe, die ein LAN erfüllen sollte, wird auch als Ressourcen-Sharing bezeichnet, d.h. gemeinsamer Zugriff auf zentrale Betriebsmittel.

Zu diesen Aufgaben zählen auch sämtliche Gateway-Funktionen, um zum Beispiel den Zugriff auf zentrale Host-Systeme zu ermöglichen. Die Nutzung von Online-Diensten wie CompuServe, AOL oder T-Online wird in einem Unternehmen immer wichtiger. Aus diesem Grund werden immer häufiger Komponenten installiert, die es erlauben, Modems oder ISDN-Anschlüsse als Pool im Netz zur Verfügung zu stellen. Auf diese Weise kann von jedem Arbeitsplatz aus auf diese Komponenten zugegriffen werden. Eine zweite Forderung in

7.3 Zugriff auf die Verarbeitungskapazität anderer Rechner

diesem Kontext besteht darin, einen Remote-Zugriff zu ermöglichen. Das bedeutet, es sollen Mechanismen installiert werden, die es ermöglichen, daß Mitarbeiter oder Wartungspersonal von außerhalb über Modems oder ISDN-Anschlüsse Zugriff im Netz erhalten.

Am Markt wird inzwischen eine Vielzahl von Produkten angeboten. Ausschlaggebend bei der Auswahl einer solchen Lösung ist die unterstützte Netzwerkumgebung (vor allem Protokoll- und Zugangsunterstützung), wobei es hauptsächlich um NetWare, NT Server oder auch Unix geht. Da Remote-Zugänge von außen immer mit Sicherheitsrisiken verbunden sind, muß besonderer Wert auf die Schutzfunktionen gelegt werden, die mit einem solchen Produkt implementiert werden können. Es bedarf also einer genauen Untersuchung, welche Anforderungen einerseits vom Unternehmen gestellt werden und welche Produkte diese Anforderungen erfüllen. Am Markt werden diese Produkte allgemein als RAS-Systeme bezeichnet, wobei die Abkürzung RAS für Remote Access Service steht.

7.3 Zugriff auf die Verarbeitungskapazität anderer Rechner

Allgemeine LANs bieten in der Regel die Möglichkeit, Verarbeitungsaufträge (Stapeljobs) auf Rechner innerhalb eines Netzwerks zu verteilen. Diese Art der Netzwerkausnutzung ist auch unter dem Begriff des Lastverbundes bekannt. Um Aufträge nicht nur auf einer Maschine abarbeiten zu lassen, was zuweilen zu Engpässen auf den Verarbeitungsmaschinen führen kann, wird gefordert, Aufgaben auf verschiedene Rechner aufteilen zu können. Damit kann die Belastung und Geschwindigkeit des LAN optimal genutzt werden.

Denkbar ist es jedoch auch, Rechenoperationen oder ähnliches an Spezialprozessoren vergeben zu können. Es wäre somit möglich, daß ein Rechner zur Verarbeitung von Bilddaten (rechenintensiv und teuer) in einem Bildverarbeitungssystem eingesetzt wird und im LAN allen Benutzern zur Verfügung steht.

7.4 Zugriff auf zentrale Datenbestände

Neben dem Ressourcen-Sharing ist der Zugriff auf zentrale Datenbestände mit eine der wichtigsten Aufgaben eines Lokalen Netzes. Datenbestände sollen von allen Mitarbeitern, die diese benötigen, auch benutzt werden können, sei es nur lesend oder lesend und ändernd. Für diese Art der Aufgabenstellung reicht es nicht aus, daß das Netzbetriebssystem dies zuläßt, vielmehr muß die Anwendungssoft-

7 Aufgaben Lokaler Netzwerke

ware für einen gemeinsamen Zugriff auf die zentralen Datenbestände konzipiert sein. Stichwort dafür ist die Multi-User-Fähigkeit. Das heißt, mehrere Personen können zum Beispiel zu ein und demselben Zeitpunkt mit der gleichen Datenbank arbeiten. Die Applikations-Software muß hierfür geeignete Synchronisationsmechanismen, in Zusammenarbeit mit dem Netzwerkbetriebssystem, zur Verfügung stellen, damit der Datenbestand zu jedem Zeitpunkt konsistent und die Integrität der Daten erhalten bleibt.

Eine generelle Aufgabe, die im Laufe der Zeit in fast jedem LAN installiert ist, betrifft entweder die Kopplung mit anderen LANs, d.h. dem Übergang vom LAN zum WAN, oder die Anbindung des LAN an das Internet. Kein Thema wurde in den letzten Monaten so häufig diskutiert wie die Frage: Wie kann das Unternehmensnetzwerk sicher und bequem an das Internet angebunden werden? Das Internet wurde vor Jahren noch als reines »Forschungsnetzwerk« betrachtet. Mittlerweile wuchs die Zahl der Anbieter im Internet aber so stark an, daß immer mehr Firmen dazu übergingen, sich einen Internet-Anschluß anzuschaffen.

Nicht weniger wird darüber diskutiert, ob ein Unternehmen nicht einen eigenen Web-Server implementieren soll, um Informationen bereitstellen zu können. So wäre es zum Beispiel durchaus überlegenswert, ob die Zenk Gesellschaft für Systemberatung mbH nicht auch einen eigenen Web-Server anbieten soll, um damit das Schulungsangebot und die Dienstleistungen des Unternehmens verfügbar zu machen. Damit könnte man die jährlichen Kosten für den Versand von Schulungskatalogen reduzieren, die Informationen wären 24 Stunden am Tag abrufbar, und man könnte auch noch Web-Seiten einrichten, die es ermöglichen, Anfragen zu hinterlegen oder sogar das Buchen von Schulungen darüber abzuwickeln. (Der Web-Server ist natürlich längst realisiert.)

Ein weiterer wesentlicher Aspekt für den Internet-Anschluß ist die damit verbundene E-Mail-Funktionalität. Es fällt immer mehr auf, daß bei Gesprächen mit Kunden oder Hard- und Software-Herstellern die Frage gestellt wird, ob man per E-Mail im Internet erreichbar ist. Das Internet kann als »Transportmedium« genutzt werden, um E-Mails über das Internet in das unternehmenseigene E-Mail-System zu transportieren und umgekehrt. Aus diesem Grund gibt es für jedes »gute« E-Mail-System ein SMTP-Gateway, da genau dieser Übergang für den Transport von E-Mail über und in das Internet benötigt wird.

Ein Internet-Zugang birgt jedoch auch die Gefahr, daß das unternehmenseigene Netzwerk nach außen geöffnet wird. Jeder Internet-Nutzer hätte somit die Möglichkeit, über das TCP/IP-Protokoll in Ihr

7.4 Zugriff auf zentrale Datenbestände

Netzwerk einzudringen. Das eingesetzte Protokoll im Internet basiert auf TCP/IP, die dafür bereitgestellten Schutzfunktionen sind bei diesem Protokoll jedoch sehr gering.

Um das eigene Netzwerk durch den Internet-Anschluß aber nicht in Gefahr zu bringen, werden in diesen Fällen sogenannte FireWall-Systeme installiert. Sie dienen dazu, das unternehmenseigene Netzwerk vom Internet abzuschotten, um unberechtigten Anwendern aus dem Internet einen Zugang zum unternehmenseigenen Netzwerk zu verwehren. Da es inzwischen unterschiedliche FireWall-System-Konzepte gibt, sollen deren grundsätzliche Aspekte in einem späteren Kapitel behandelt werden.

Bevor ich Ihnen einen Kriterienkatalog für die Auswahl von LANs aufzeige und wir uns näher mit den Möglichkeiten der Netzwerkbetriebssysteme von Novell NetWare bzw. Microsoft auseinandersetzen wollen, sollen die wichtigsten Grundlagen der Kommunikation und der Kopplung von Netzwerken betrachtet werden.

8

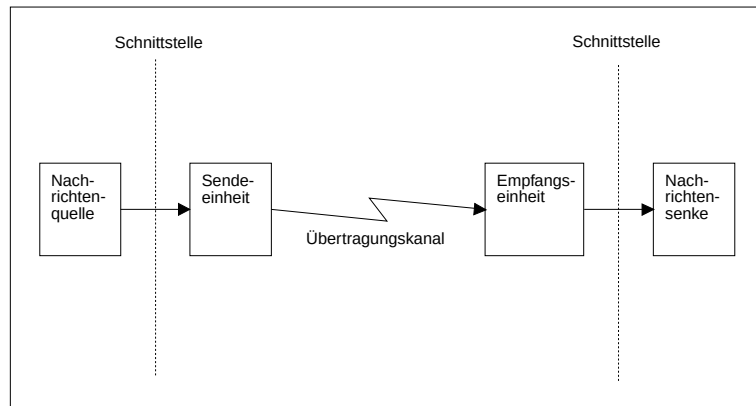
Kommunikations- grundlagen

Unter Kommunikation ist allgemein die Übertragung einer Nachricht zwischen einem Punkt als Sender und einem anderen Punkt als Empfänger zu verstehen. Ein Kommunikationssystem stellt eine Infrastruktur dar, die durch Kommunikationseinrichtungen und ein Wegenetz (Übertragungseinrichtungen) die Verteilung von Nachrichten ermöglicht. Ein Kommunikationssystem besteht im Prinzip aus folgenden Komponenten:

- Nachrichtenquelle
- Sendeeinheit
- Übertragungskanal
- Empfangseinheit
- Nachrichtensenke

In Abbildung 8.1 ist das dargestellt.

Abbildung 8.1
Komponenten
einer Kommuni-
kationseinheit



Die Verarbeitung von Nachrichten erfolgt dabei in drei Phasen:

1. Aufbereitung der Nachricht und Umsetzung in übertragungskonforme Signale (Modulation der Nachricht)
2. Signaltransport der Nachricht über das Übertragungsmedium
3. Aufnahme der Nachricht und Umsetzung in empfangskonforme Signale (Demodulation)

Die *Nachrichtenquelle* ist die Einheit, die aus der Menge aller möglichen Nachrichten die zu übermittelnde auswählt.

8 Kommunikationsgrundlagen

Die *Sendeeinheit* wandelt die Nachricht in eine adäquate Signalfolge um, um diese über den Übertragungskanal zu transferieren (Signal-konverter).

Der *Übertragungskanal* ist das Medium zur Übertragung der Signale vom Sender zum Empfänger. Maßzahlen zur Beurteilung des Übertragungskanals sind:

- Übertragungsdistanz
- Kanalkapazität
- Durchlaufzeit
- Zuverlässigkeit
- Wirtschaftlichkeit
- Flexibilität

Der Informationsfluß kann dabei entweder

- in eine Richtung (Simplexbetrieb) oder
- abwechselnd in die eine oder andere Richtung (Halbduplexbetrieb) oder
- gleichzeitig in beide Richtungen (Duplexbetrieb) erfolgen.

In der *Empfangseinheit* erfolgt die Rekonstruktion der Nachricht in einer für die Schnittstelle zur Nachrichtensenke adäquaten Form.

Die *Nachrichtensenke* ist die Einheit, für welche die zu übermittelnde Nachricht bestimmt ist.

Die *Schnittstelle* ist die Gesamtheit der Festlegungen über

- die physikalischen Eigenschaften der Schnittstellenleitungen,
- die auf den Schnittstellen ausgetauschten Signale und
- die Bedeutung der ausgetauschten Signale.

8.1 Synchronisationsverfahren

In der Datenfernübertragung erfolgt die Datenübertragung über größere Entfernungen immer seriell. Bei der seriellen Übertragung ist eine Synchronisation, d.h. ein Gleichlauf von Sender und Empfänger, erforderlich, um die korrekte Interpretation der Wechsel zwischen den binären Zuständen »0« und »1« zu gewährleisten.

Die Signalwechsel werden deshalb in einen sogenannten »Rahmen« verpackt, um die Unterscheidung von Nutzinformation, Steuerinformation und Pausen zu ermöglichen. Innerhalb dieses Rahmens müssen Sender und Empfänger zeitsynchron laufen, damit der Empfänger genau weiß, wie lang ein Bit ist und wann das nächste Bit abgetastet werden muß.

8.1 Synchronisationsverfahren

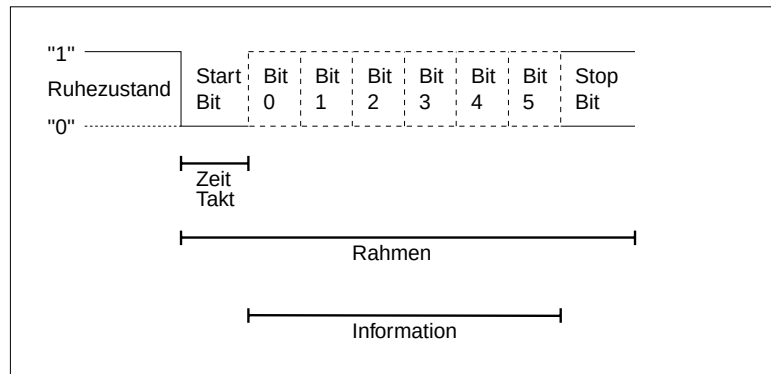
In der Praxis werden zwei Synchronisationsmechanismen angewandt:

- asynchrone Datenübertragung und
- synchrone Datenübertragung.

8.1.1 Asynchrone Datenübertragung

Die asynchrone Datenübertragung erfolgt zwischen Sender und Empfänger immer zeichenweise (Byte für Byte). Dabei wird vor jedem Zeichen, das übertragen werden soll, ein Startbit und nach jedem Zeichen ein Stopbit gesendet. Das heißt, die Synchronisation zwischen Sender und Empfänger wird immer für kurze Zeit (ein Zeichen) vorgenommen. Sender und Empfänger weisen deshalb eine relativ große Toleranz für die Gleichlaufgenauigkeit auf. Die asynchrone Datenübertragung wird allerdings nur bei ziemlich niedrigen Übertragungsgeschwindigkeiten eingesetzt. Es wird beispielsweise für die Übertragung von Terminals oder Druckern und bei der Übertragung in Fernmeldenetzen mit Hilfe von Akustikkopplern meist mit Übertragungsgeschwindigkeiten von ca. 1200 Bit/s gearbeitet.

Abbildung 8.2
Der Rahmenaufbau für asynchrone Übertragung



Der Vorteil beim Einsatz der asynchronen Datenübertragung liegt unter anderem darin, daß die notwendige Hardware einfach und billig ist. Nachteilig hingegen ist die Empfindlichkeit gegen Signalverzerrungen, die vor allem bei höheren Übertragungsgeschwindigkeiten und längeren Bitfolgen auftreten.

Zudem ist eine große Redundanz durch den erhöhten Synchronisationsaufwand je Zeichen zu verzeichnen. Dadurch steigen auch die Kosten für die Datenübertragung.

In Abbildung 8.2 ist die Rahmenbildung für die asynchrone Datenübertragung dargestellt.

8.1.2 Synchroner Datenübertragung

Bei der synchronen Datenübertragung wird der Empfangstakt aus dem Leitungssignal wiedergewonnen. Dieses Verfahren ist somit frei von Start- und Stopbits. Es werden immer ganze Datenblöcke übertragen, meistens mehrere hundert Zeichen, bevor eine neue Synchronisation zwischen Sender und Empfänger durchgeführt wird. Die Erkennung des Rahmenbeginns und des Rahmenendes muß dennoch immer durchgeführt werden. Man unterscheidet hierbei zwischen:

- Bytesynchronisation (Oktettsynchronisation) und
- Bitsynchronisation.

Der Unterschied zwischen diesen beiden Verfahren soll im folgenden Abschnitt erläutert werden.

Bytesynchronisation

Zusätzlich zur Bytesynchronisation muß der Empfänger noch einen Oktettgleichlauf aufbauen. Um dies zu erreichen, wird vor der Übertragung des Rahmens ein für diesen Zweck reserviertes Zeichen zwei- bis viermal übertragen. Hierfür läßt sich zum Beispiel das ASCII-Zeichen <SYN> (Synchronisation) verwenden. Damit stellt sich der Empfänger auf die weiteren nachfolgenden Oktettsequenzen ein. Die eigentliche Rahmenbildung erfolgt dann, je nach eingesetztem Protokoll, mit weiteren Zeichen.

Im ASCII-Code sind dies die folgenden Zeichen:

<SOH>:	Start of Header
<STX>:	Start of Text
<ETX>:	End of Text
<EOT>:	End of Transmission

Diese Zeichen können generell nicht mehr als Informationseinheit verwendet werden, sondern dienen nur noch zur Synchronisation. Sollen nun im Datenpaket trotzdem beliebige Zeichen (inklusive der eigentlichen Synchronisationszeichen) übertragen werden, also auch die Zeichen, die zur Rahmenbildung verwendet werden, müssen Vorkehrungen getroffen werden, damit der Rahmenaufbau klar erkennbar bleibt. Diese notwendige Vorkehrung wird als Transparenz bezeichnet. Wie wird das erreicht?

8.1 Synchronisationsverfahren

Realisierung der Transparenz

- Vor einem transparent zu übermittelnden Zeichen wird ein sogenanntes Ausweichzeichen (bei ASCII-Code das Zeichen <DLE>) eingefügt, das beim Empfänger anschließend wieder entfernt wird.
- Bei der anderen Methode wird der Rahmenteil mit einem Ausweichzeichen (ASCII-Code <DLE>) gekennzeichnet. Im Informationsteil muß dann nur noch das Zeichen <DLE> bei der Übertragung mit Hilfe eines Ausweichzeichens gekennzeichnet werden. Auch dieses wird beim Empfänger anschließend wieder entfernt.

In den Abbildungen 8.3 und 8.4 ist die Transparenz durch Ausweichzeichen und die Rahmenbildung und Transparenz mit Hilfe von Ausweichzeichen dargestellt.

Abbildung 8.3
Transparenz
durch Einfügen
von Ausweich-
zeichen

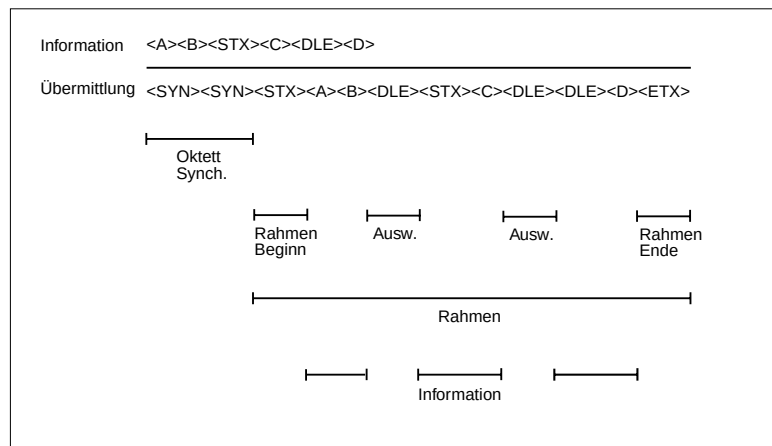
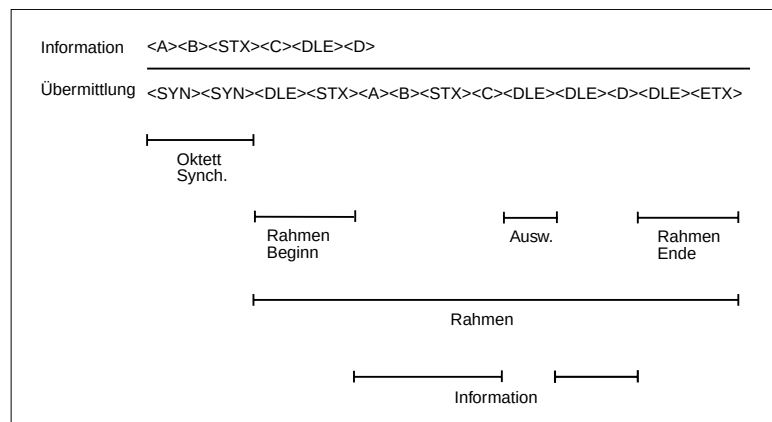


Abbildung 8.4
Rahmenaufbau
und Transparenz
durch Ausweich-
zeichen



8 Kommunikationsgrundlagen

Bitsynchronisation

Bei der bitsynchronen Datenübertragung wird der Takt ebenfalls aus dem Leitungssignal wiedergewonnen. Im Gegensatz zur Bytesynchronisation muß der Empfänger die ankommenden Signale nicht mehr als Oktettsequenz interpretieren, da zur Rahmenbildung eindeutige, einfache Bitsequenzen an beliebiger Stelle verwendet werden.

Beispiel: Übertragungsprozedur HDLC (High Level Data Link Control)

Beim HDLC-Format kennzeichnet die Bitsequenz »0111 1110« (als Flag) den Beginn und das Ende eines Rahmens. Damit das besprochene Transparenzproblem umgangen werden kann, muß sichergestellt sein, daß keine Bitfolge von sechs Bit mit »1« zwischen den Flags auftritt. Die bei dieser Prozedur verwendete Methode wird allgemein als »Stopfen« (bit stuffing) bezeichnet. Das heißt, nach jeweils fünf aufeinanderfolgenden »1«-Bits wird ein zusätzliches Bit »0« eingefügt. Dieses Bit gehört somit nicht zur ursprünglichen Information und wird beim Empfänger wieder automatisch entfernt.

Wenn übertragen wird:

Information: ...01111111001101011111000110110...,

dann erzeugt die HDLC Prozedur die Bitfolge:

Übertragung: ...0**11111**101100110101**11111**0000110110...

8.2 Verbindungslose und verbindungsorientierte Kommunikation

Die Kommunikation zwischen Sender und Empfänger kann entweder verbindungslos oder verbindungsorientiert durchgeführt werden. In diesem Abschnitt will ich Ihnen zeigen, worin der Unterschied dieser beiden Methoden liegt und wie sie funktionieren.

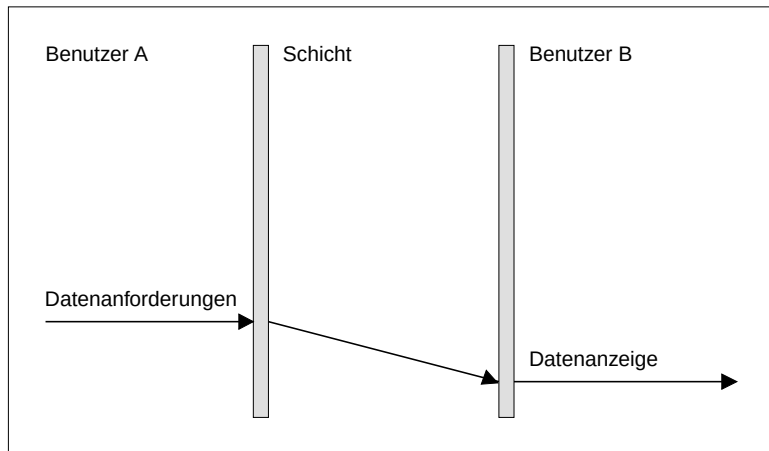
Ein Kommunikationsdienst ist verbindungslos, wenn jede Nachrichtentransaktion unabhängig von der vorangehenden oder nachfolgenden Nachricht ist. Im Gegensatz hierzu muß bei der verbindungsorientierten Kommunikation vor der Übertragung einer Nachricht eine logische Verbindung zwischen den beiden Kommunikationspartnern aufgebaut werden.

8.2 Verbindungslose und verbindungsorientierte Kommunikation

8.2.1 Verbindungslose Kommunikation

Bei dieser Kommunikationsart können die beiden Kommunikationspartner ihre Kommunikation im Prinzip spontan durchführen. Das heißt, vor dem Austausch von Daten muß keine Verbindung zwischen Sender und Empfänger aufgebaut werden. Die Nutzdaten werden dem Transportsystem unmittelbar übergeben.

Abbildung 8.5
Prinzip der
verbindungslosen
Kommunikation



Die zu übertragenden Blöcke von Daten werden als Datagramme bezeichnet. Da keine Verbindung aufgebaut wird und aufeinanderfolgende Datagramme von einer Quelle zum gleichen Ziel über unterschiedliche Wege geleitet werden können, muß jedes Datagramm mit der Absender- und Empfängeradresse versehen sein. In Abbildung 8.5 ist diese Kommunikationsart schematisch dargestellt.

8.2.2 Verbindungsorientierte Kommunikation

Die verbindungsorientierte Kommunikation ist in ihrer Realisation wesentlich komplexer als die verbindungslose Kommunikation. Charakteristisch für diese Kommunikationsart ist, daß jede Kommunikation aus drei Operationsphasen besteht:

- Verbindungsphase,
- Datentransferphase und
- Verbindungsabbauphase.

Die Verbindung zwischen Sender und Empfänger muß aufgebaut werden, bevor ein Datentransfer zwischen beiden Partnern durchgeführt werden kann. Nach erfolgreicher Datenübertragung muß die Verbindung wieder abgebaut werden. Für den Verbindungsaufbau

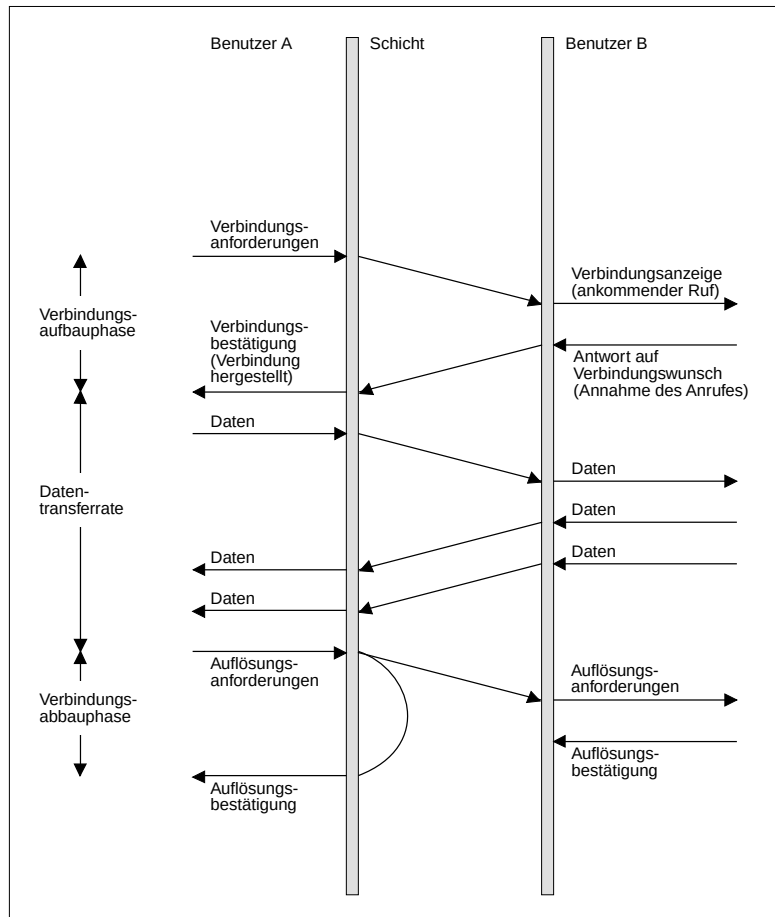
8 Kommunikationsgrundlagen

ist die Angabe der vollständigen Netzadresse des Empfängers notwendig. In der Datentransferphase wird anschließend ein »kurzer« Verbindungsidentifizierer eingesetzt, um den Benutzer zu identifizieren. Die Verbindungsaufbauphase kann dazu verwendet werden, die Dienstgüte oder bestimmte Optionen »abzusprechen«.

Die Dienstleistungen des analogen Fernsprechnetzes, des Telexnetzes, aber auch die Dienstleistungen der im kommerziellen Bereich eingesetzten Herstellernetze sind verbindungsorientiert.

In Abbildung 8.6 ist die verbindungsorientierte Kommunikation schematisch dargestellt.

Abbildung 8.6
Prinzip der verbindungsorientierten Kommunikation



8.3 Kommunikationsprotokolle

Ein Protokoll (Prozedur) beinhaltet Regeln, die genau festlegen, wie die Kommunikation zwischen einem Sender und einem Empfänger durchzuführen ist. Zur erfolgreichen Datenübertragung reicht die Festlegung von physikalischen Schnittstellenparametern bei weitem nicht aus. Es bedarf hierfür noch weiterer wichtiger Funktionalitäten.

Festgelegt werden müssen unter anderem:

- Übertragungsgeschwindigkeit
- Gleichlaufverfahren
- Datenformat
- Kodierung
- Sicherungsverfahren
- Betriebsarten
- algorithmischer Ablauf der Übertragung mit allen (Ausnahme-)Situationen

Folgende Funktionen können einzeln im Protokoll definiert sein:

- *Synchronisation*
Hier handelt es sich um die Einrichtung zum Erkennen des ersten Bit eines Byte.
- *Initialisierung, Terminierung*
Dies ist ein Prozeß zum Starten bzw. zum Beenden der Datenübertragung. Es dient somit dem Verbindungsaufbau und -abbau.
- *Blockbildung*
Regeln zur Kennzeichnung von Blockbeginn und Blockende.
- *Steuerung der Datenverbindung*
Überwachung des Ablaufs der Datenübertragung.
- *Fehlererkennung*
Das Erkennen von Übertragungsfehlern durch Blocksicherungskennzeichen nach den unterschiedlichsten Verfahren (VRC, LRC oder CRC). Empfangene Blöcke müssen unter Umständen quittiert werden.
- *Blocknumerierung*
Die Verwendung einer fortlaufenden Numerierung der Übertragungsblöcke verhindert die Duplizierung von Nachrichten und ermöglicht somit die Feststellung, ob Blöcke bei der Datenübertragung verlorengegangen sind.
- *Flußkontrolle*
Dieser Mechanismus regelt die Weiterleitung von Datenblöcken über unterschiedliche Übertragungswege, sofern diese zur Verfügung stehen.
- *Transparenz*
Möglichkeit, beliebige Datenströme zu übertragen.

8 Kommunikationsgrundlagen

■ *Wiederherstellungsverfahren*

Tritt ein abnormer Zustand ein, muß es möglich sein, auf einen definierten Zustand aufsetzen zu können (z.B. Timeout, Sequenzfehler, Kollision).

■ *Zugangskontrolle*

Hier wird festgelegt, wann eine Dateneneinheit (DEE) den Zugang zum Netzwerk erhält, um Daten senden oder empfangen zu können.

Im Bereich der Netzwerktechnologie existieren die unterschiedlichsten Protokolle. Damit der Wildwuchs auf diesem Gebiet eingeschränkt werden kann, wird versucht, diese Protokolle durch internationale Gremien normieren zu lassen.

Gängige und häufig eingesetzte Leitungsprotokolle (Kommunikationsprotokolle) sind:

- Basis-Mode-Protokolle LSV, MSV oder BSC
- DLC-Protokoll
- SDLC-Protokoll

Die oben aufgeführten Protokolle unterscheiden sich hinsichtlich der Konzeption:

- Die Basis-Mode-Protokolle sind zeichenorientiert, d.h., es sind nur definierte Übertragungssteuerzeichen zulässig. Als Übertragungscode kann zum Beispiel EBCDIC oder CCITT IA5 eingesetzt werden.
- Die HDLC/SDLC-Protokolle sind bitorientiert, d.h., die Steuerfunktion für die Datenübertragung ist bitverschlüsselt. Somit ist es möglich, eine codeunabhängige Datenübertragung durchzuführen.

9

Das ISO-Schichtenmodell der offenen Kommunikation

Die Netzwerkarchitekturen der einzelnen Hersteller verfolgen unter anderem das Ziel, den gemischten Einsatz von Hardware verschiedener Hersteller in Netzen unter Sicherstellung der Funktionsfähigkeit zu ermöglichen. Einzelne Architekturen haben sich im Laufe der Zeit zu De-facto-Standards entwickelt, so zum Beispiel SNA von IBM, DECnet von DEC oder Transdata von Siemens. Dritthersteller erhalten so die Möglichkeit, eigene Hard- und Software zu entwickeln, die dann auch auf Systemen anderer Hersteller lauffähig sind. Für die Kopplung der verschiedensten Rechnersysteme und Netzwerke ist dies jedoch keine befriedigende Lösung. Dieser Mißstand wird durch die Aktivitäten verschiedener Großanwender, eigene, herstellereunabhängige Architekturen zur Vernetzung heterogener Systeme zu entwickeln, noch gefördert.

9.1

Prinzip des Schichtenmodells

Normalerweise reicht es nicht aus, daß zwei oder mehr Rechner, die miteinander kommunizieren sollen, mit etwas Draht verbunden werden, und dann hat sich die Sache. Im Gegenteil, neben den Hardwarevoraussetzungen müssen auch noch eine große Menge softwaremäßige Probleme bewältigt werden.

Solange es sich um die Kommunikation von homogenen Systemen handelt (Geräte ein und desselben Herstellers), läßt sich dies mit gewissen Einschränkungen meist auch realisieren. Schwieriger wird die Sache jedoch, wenn unterschiedliche Systeme untereinander und miteinander vernetzt werden sollen, um einen Datenaustausch gewährleisten zu können.

Da jeder Hersteller unterschiedliche Konventionen benutzt und herstellereigene Netze und Protokolle verwendet, wurde versucht, dieses Problem durch die Festlegung von Richtlinien in den Griff zu bekommen.

Die herstellerabhängigen Systeme, die mit bestimmten Protokollen, Zeichensätzen und Übertragungssequenzen arbeiten, werden oft auch als geschlossene Systeme bezeichnet, da bei der Festlegung

9 Das ISO-Schichtenmodell der offenen Kommunikation

dieser Konventionen an die Einbindung von Fremdsystemen nicht gedacht worden ist. Zum Zeitpunkt der Entwicklung dieser Architekturen sah man sich auch nicht gezwungen, die Schnittstellen von diesen Systemen offenzulegen.

Im Gegensatz zu den geschlossenen Systemen werden bei offenen Systemen bestimmte Richtlinien eingehalten, die es anderen Herstellern erlauben, entweder kompatible Geräte zu bauen, die in das andere System ohne Probleme zu integrieren sind, oder Schnittstellenprogramme zu schaffen, die eine nachträgliche Eingliederung möglich erscheinen lassen.

Um eben dieses Durcheinander der einzelnen Hersteller nicht noch größer werden zu lassen, wurde 1978 ein »Referenzmodell für die Kommunikation offener Systeme« definiert. OSI ist die Abkürzung für Open Systems Interconnection, und ISO steht für International Standardisation Organization. In der Literatur finden Sie für dieses Modell zuweilen unterschiedliche Bezeichnungen, alle meinen jedoch das gleiche. Die Bezeichnungen reichen von ISO/OSI-Modell bis Sieben-Schichten-Modell.

Wie die zuletzt genannte Bezeichnung bereits errahnen läßt, besteht das Modell aus insgesamt sieben Ebenen (Schichten oder auch Layers genannt).

Mit Hilfe dieser sieben Schichten wird versucht, die Struktur der Kommunikation innerhalb eines Netzwerks und von Netzwerken untereinander hardware- und softwaremäßig genau festzulegen und zu standardisieren. Ziel ist es, eine Definitionsgrundlage zu schaffen, mit der es gelingt, Systeme zu entwickeln (Hardware und Software), die, wenn sie sich streng an diesem Schichtenmodell orientieren, untereinander kommunizieren bzw. miteinander verbunden sein können.

Aus der Erfahrung heraus ist festzustellen, daß die Wirkungsweise dieses Modells immer wieder auf große Mißverständnisse stößt. Entweder wird der Sinn dieses Modells nicht verstanden, oder die Arbeitsweisen der Ebenen werden falsch gedeutet.

Mit einem kleinen Beispiel aus dem Alltag will ich versuchen, die Funktion des Schichtenmodells zu erläutern. Es hat zwar mit Netzwerken nichts zu tun, beinhaltet jedoch einige Grundzüge der Informationsübertragung.

Ein deutscher Tourist (Hans) lernt im Urlaub in Frankreich eine Französin kennen (Marlene). Da er diese Bekanntschaft auch nach seinem Urlaub aufrechterhalten will, beschließt er, mit ihr brieflich in Kontakt zu bleiben. Er kann jedoch kein Französisch und sie kein Deutsch. Da sie sonst auch keine weitere gemeinsame Fremdspra-

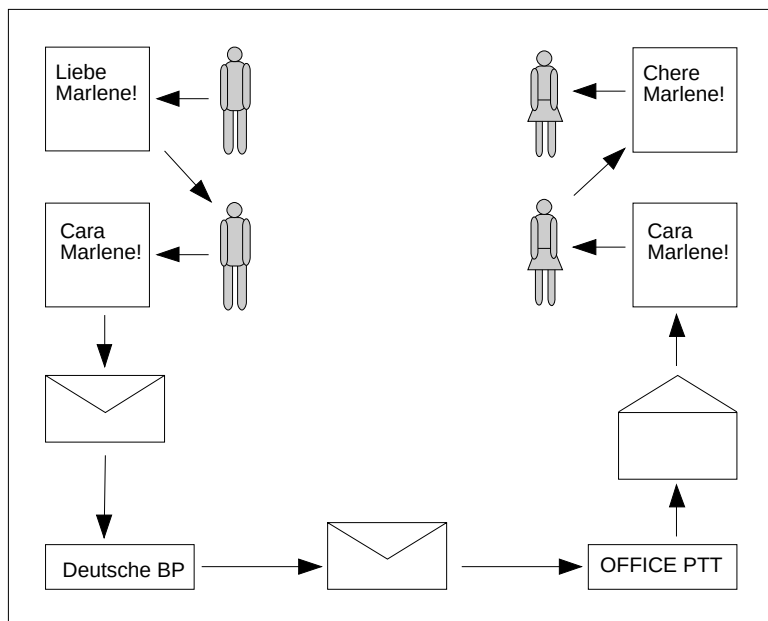
9.1 Prinzip des Schichtenmodells

che zur Verständigung benutzen können, müssen sie einen Dolmetscher einschalten. In Abbildung 9.1 ist der Ablauf dieses Vorgangs illustriert.

Hans verfaßt seinen Brief an Marlene in Deutsch und gibt diesen an seinen Dolmetscher weiter. Der übersetzt ihn, hoffentlich unverfälscht, ins Italienische (gemeinsam festgelegte Sprache der Kommunikation), steckt den Brief in ein Kuvert, adressiert dieses und übergibt es der Deutschen Bundespost. Durch die Post wird der Brief nun per Flugzeug oder Bahn nach Frankreich zum Office PTT transportiert. Der Dolmetscher von Marlene erhält den Brief, nimmt ihn aus dem Kuvert und übersetzt ihn ins Französische. Der übersetzte Brief wird vom Dolmetscher an Marlene weitergereicht, die ihn dann lesen kann.

An diesem Beispiel wird klar, daß auf beiden Seiten der Kommunikationspartner bestimmte Regeln eingehalten werden müssen. Hans muß den Brief in Deutsch schreiben (es sei unterstellt, daß der Dolmetscher nur vom Deutschen ins Italienische übersetzen kann). Der Dolmetscher dagegen darf den Brief von Hans nur in die italienische Sprache übersetzen, da sonst der Dolmetscher von Marlene den Brief nicht übersetzen könnte.

Abbildung 9.1
Schichtenmodell
für den
Briefverkehr



9 Das ISO-Schichtenmodell der offenen Kommunikation

Würde Hans einen neuen Dolmetscher beauftragen, seine Briefe zu übersetzen, der nur vom Deutschen ins Arabische übersetzen kann, müßte diese Änderung der Gegenseite mitgeteilt werden, da Marlene dann einen Dolmetscher bräuchte, der vom Arabischen ins Französische übersetzt.

Der Dolmetscher von Hans darf den Brief auch nicht in irgendeinen Briefkasten einwerfen oder an irgendeine Adresse verschicken, sondern muß sich daran halten, einen Briefkasten der Deutschen Bundespost zu verwenden und die Adresse von Marlene auf das Briefkuvert zu schreiben.

Desgleichen muß der Brief in lateinischen Buchstaben geschrieben werden, wenn man sich auf diese Art der »Kodierung« geeinigt hat, und darf nicht etwa in kyrillischen Buchstaben verfaßt werden.

An diesem Beispiel sehen Sie, daß exakte Regeln existieren, die es zu befolgen gilt. Genauso verhält es sich bei der Festlegung von Vorschriften zur Datenkommunikation.

Im OSI-Modell zur Kommunikation offener Systeme wird auf jeder Ebene genau festgelegt, was in dieser Schicht getan bzw. eingehalten werden muß. Die Ebenen erfüllen ganz bestimmte Aufgaben, und zwar nur die Aufgaben, die man ihnen aufgetragen hat.

Im nächsten Abschnitt soll das Sieben-Schichten-Modell näher erläutert werden.

9.2 Die Schichten des ISO-OSI-Modells

Wie bereits erwähnt, ist das Modell in sieben hierarchische Schichten aufgeteilt. Jeder Schicht oder Ebene ist eine klar umrissene Aufgabe zur Durchführung der Kommunikation zugewiesen. Die Formen der Schichtdefinitionen sind dabei willkürlich festgelegt worden. Es wären durchaus andere Einteilungen denkbar, aber irgendwann mußte man sich auf eine einheitliche Einteilung einigen. Das komplexe Problem der Datenkommunikation innerhalb eines Netzwerks und im Verbund von Netzwerken wird durch dieses Modell in kleinere Teilprobleme gegliedert. Es ist durchaus zulässig, eine Schicht selbst wieder in kleinere Teilschichten aufzuteilen, wie dies zum Beispiel in der Schicht 2 erfolgt. Die Schicht 2 wird in sich noch mal in eine MAC-Layer (Media Access Control) und LLC-Layer (Logical Link Control) aufgeteilt.

Dies ist dann durchaus sinnvoll, wenn die Protokolle einer Schicht bei einem speziellen Netzkonzent zu umfangreich sind, um noch übersichtlich gestaltet zu werden.

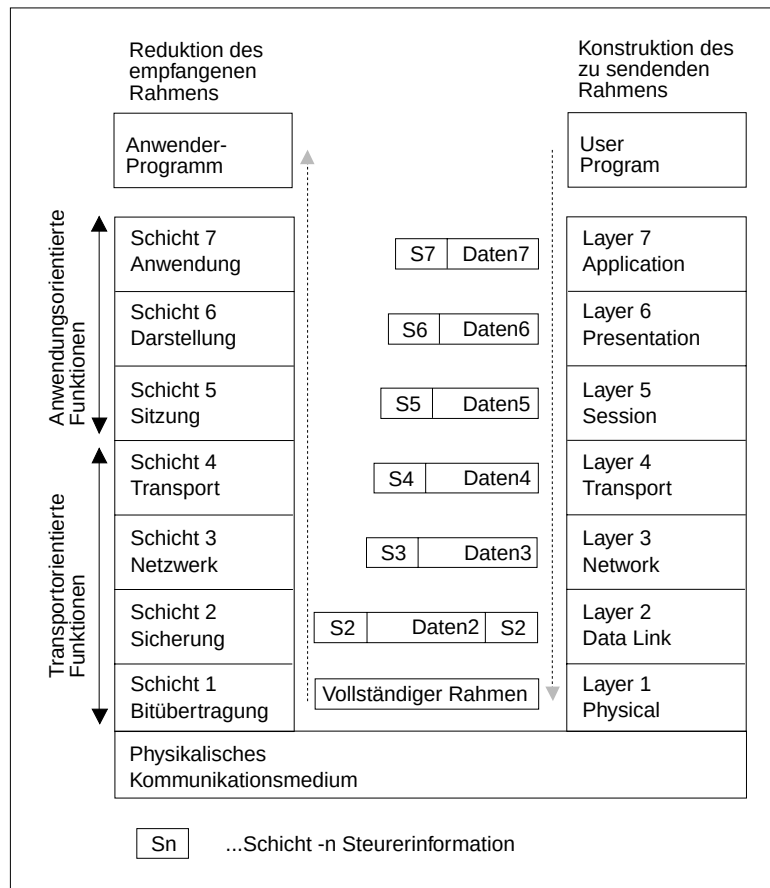
9.2 Die Schichten des ISO-OSI-Modells

Umgekehrt ist es nicht zwingend notwendig, daß jede Schicht eines Protokolls Verwendung findet. Es ist durchaus gestattet, daß einzelne Schichten (oder Teilschichten) leer bleiben, wenn sie für die Funktion nicht benötigt werden.

Für jede Schicht wird eine Beschreibung des Funktionsumfangs gegeben und das notwendige Verhalten an den Schnittstellen zu den darunter- oder darüberliegenden Schichten bestimmt. Wie diese Schichten zu implementieren sind, wird nicht festgelegt. Es wird nur gefordert, daß die notwendigen Funktionen abgedeckt werden.

In Abbildung 9.2 sind das ISO-Referenzmodell und der Ablauf einer Kommunikation zweier Partner schematisch dargestellt.

Abbildung 9.2
Aufbau und Ablauf des Schichtenmodells



9 Das ISO-Schichtenmodell der offenen Kommunikation

Der vorher etwas einfach dargestellte Mechanismus zur Arbeitsweise einer Kommunikation zwischen zwei Partnern soll jetzt etwas näher betrachtet werden, um darzustellen, wie die einzelnen Abläufe im Schichtenmodell zu sehen sind.

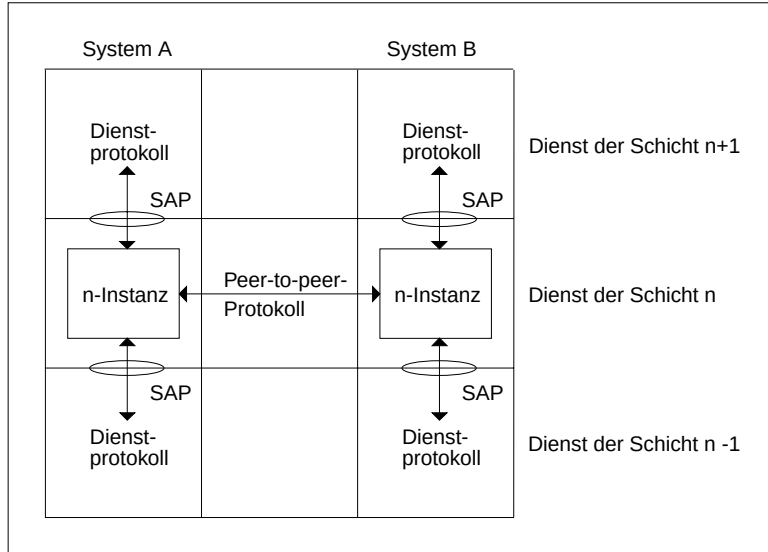
Beim Ablauf einer Kommunikation zwischen Sender und Empfänger wird vom Sender das zu übertragende Datenpaket erzeugt, durchläuft von Schicht 7 bis Schicht 1 das OSI-Modell und wird über die physikalische Leitung übertragen. Auf Seite des Empfängers durchläuft das Datenpaket Schicht 1 bis Schicht 7. Es liegt ein tieferer Sinn darin, daß man sich für diese sieben Schichten und deren Funktionalität entschieden hat. Den will ich nachfolgend aufdecken.

Der Kommunikationsprozeß zwischen zwei Partnern im Netz hat immer eine vertikale und eine horizontale Komponente, die es zu erläutern gilt. Jede Schicht N ($N = [1..7]$) in einem System S (Sender) kommuniziert mit Schicht N im System E (Empfänger) auf gleicher Ebene. Diese vorhandene horizontale Kommunikation wird auch als Peer-to-peer-Kommunikation bezeichnet. Der Ausdruck »Peer« stammt aus dem Englischen und bedeutet soviel wie »gleichgestellter Partner«. Die gültigen Regeln und Formate zur Kommunikation zwischen Schicht N im System S und Schicht N im System E werden in einem Protokoll festgelegt. Man spricht bei Ebene N vom N -Layer-Protokoll, bei allen Ebenen im OSI-Referenzmodell, außer Ebene 1, handelt es sich ausschließlich um logische Kommunikation bzw. Verbindung. Nur auf Ebene 1 (physikalische Ebene) erfolgt die tatsächliche physikalische Verbindung und Übertragung der Daten. Die Dateneinheiten, die zwischen zwei Peer-Ebenen ausgetauscht werden, heißen PDU (Protocol Data Unit), also z.B. DPDU für die Data Link Protocol Data Unit oder SPDU für Session Protocol Data Unit.

Damit die Daten von der Anwendung auf System S bis zum physikalischen Kabel und von diesem Kabel wieder bis zur Anwendung auf System E übertragen werden können, sind vertikale Kommunikationsmechanismen festgelegt. Jede Schicht im OSI-Referenzmodell erfüllt ganz bestimmte Dienstleistungen, die sogenannten Services. Diese Dienstleistungen stellt die jeweilige Schicht der nächsthöheren zur Verfügung. Dabei greift sie auf die Dienste der nächstniedrigeren Schicht zu, die sie zur Realisierung der eigenen zu erbringenden Funktionen nutzt. Dazu sind im Rahmen der Standardprotokolle Schnittstellen zwischen zwei Schichten definiert, an denen ganz bestimmte Dienste über Dienstzugangspunkte zur Verfügung gestellt werden. Diese Dienstzugangspunkte werden als *Service Access Point* (SAP) bezeichnet. Die Dienste einer Schicht sind wiederum in Instanzen angeordnet, wobei eine Instanz der Schicht N als N -Instanz bezeichnet wird. Dieser Zusammenhang ist in Abbildung 9.3 dargestellt.

9.2 Die Schichten des ISO-OSI-Modells

Abbildung 9.3
Prinzip der vertikalen und horizontalen Kommunikation im OSI-Referenzmodell



Beim Kommunikationsablauf bettet jede Schicht die Nutzdaten in Protokollinformationen ein, damit sie von der Peer-Schicht entsprechend verarbeitet und weitergeleitet werden können. Die Protokollinformationen bezeichnet man auch als Header, da sie sich am Paketanfang befinden. Informationen, die an das Paketende gefügt werden, bezeichnet man als Trailer. Die hinzugefügten Protokollinformationen sind in Relation zu den Nutzdaten zusätzlicher Overhead, der übertragen werden muß, da sie beim Empfänger in allen Schichten wieder entfernt werden müssen, bis das eigentliche Nutzdatenpaket, wie dies vom Sender aufgebaut worden ist, in seiner ursprünglichen Form wieder vorliegt.

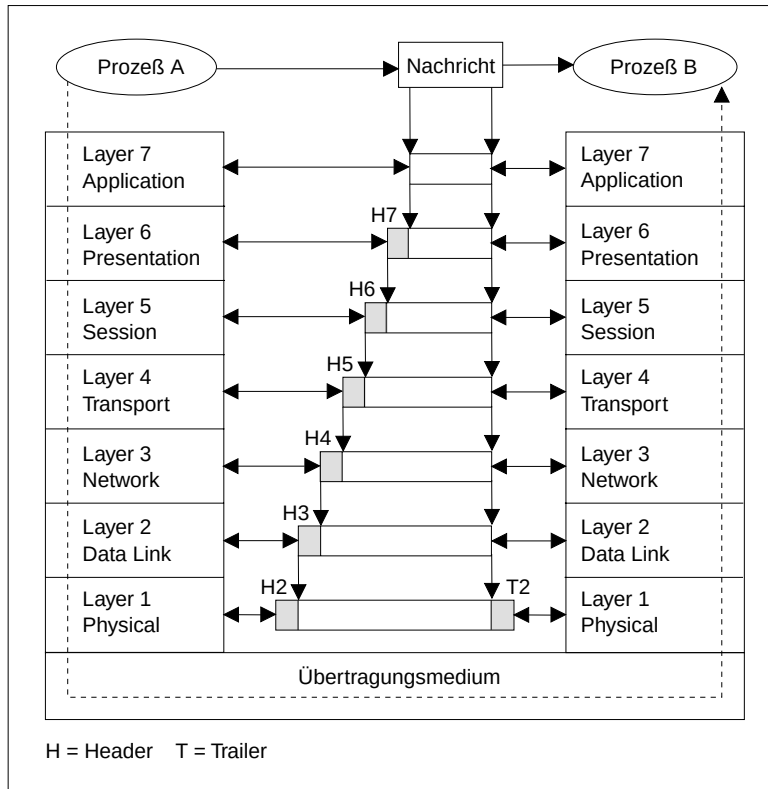
Wichtige und wesentliche Elemente des Protokoll-Overhead sind vor allem die physikalische Sender- und Empfängeradresse sowie die logische Sender- und Empfängeradresse und bei bestimmten Protokollen Routing-Informationen zum Weitertransport des Pakets in einem mit Routern gekoppelten Internet-Netzwerk. Außerdem zählen dazu auch Informationen zur Eintragung des Protokolltyps, um verschiedene Protokolle unterscheiden zu können.

Wenn man sich den Protokollablauf genau ansieht, stellt man fest, daß die Nutzdaten von der Anwendung bis zur Übertragung sechsmal mit Protokollinformationen angereichert werden, d.h., auf jeder Schicht wird zusätzlicher Protokoll-Overhead erzeugt. Die Protokollinformationen einer höheren Schicht werden von der niedrigeren Schicht als Nutzdaten betrachtet und somit vollkommen transparent behandelt. Auf der untersten Schicht wird das Nutzdatenpaket, so

9 Das ISO-Schichtenmodell der offenen Kommunikation

wie dies vom Sender über die Anwendung erzeugt wurde, inklusive aller Protokollinformationen in einen Bitstrom umgewandelt und über das physikalische Medium (Kupferkabel, Lichtwellenleiter, Funk, Laser etc.) übertragen. In Abbildung 9.4 sehen Sie auf der linken Seite den schichtweisen Aufbau und das Hinzufügen der einzelnen Protokollinformationen an das Datenpaket. Dabei ist festzustellen, daß auf Ebene 2 ein Trailer (zusätzlich zum Header) an das Datenpaket angehängt wird. Es handelt sich dabei um das sogenannte CRC-Feld (Cyclic Redundancy Check), das, wie später noch zu sehen ist, der erste Mechanismus ist, um die Korrektheit der Datenübertragung zu prüfen.

Abbildung 9.4
Peer-to-peer-Kommunikation zwischen Sender und Empfänger



Auf der Seite des Empfängers erfolgt mit dem übertragenen Datenpaket der umgekehrte Vorgang. Auf Empfängerseite werden auf jeder Schicht die Protokollinformationen der Peer-Schicht, die auf Senderseite hinzugefügt worden sind, interpretiert und nach erfolgreicher Durchführung der entsprechenden Dienste entfernt. Die verbleibende Nachricht mit eventuell weiteren Protokollinformationen,

9.2 Die Schichten des ISO-OSI-Modells

die für höhere Schichten bestimmt sind, wird an die nächsthöhere Schicht weitergereicht, die den gleichen Vorgang durchführt, wie er vorher beschrieben wurde. Trifft die Nachricht bei der Anwendung des Empfängers ein, sind bis dahin alle Protokollinformationen entfernt. Nur das ursprüngliche Nutzdatenpaket wird empfangen. In Abbildung 9.4 ist das auf der rechten Seite dargestellt.

Wie später noch zu sehen ist, können bei der Kommunikation zwischen zwei Endsystemen auch Zwischenknoten vorhanden sein. Diese werden auch als Relay-Systeme bezeichnet, die nur bestimmte Funktionalitäten zu erfüllen haben. Deshalb sind dabei nicht alle Schichten implementiert. Solche Relay-Systeme können Brücken, Router, Brouter oder Gateways sein.

Nachdem Sie jetzt wissen, wie der Kommunikationsablauf zwischen zwei Endsystemen stattfindet, will ich nachfolgend die Funktionen der sieben Schichten erläutern.

Wie bereits bekannt, ist das OSI-Referenzmodell in sieben Schichten aufgeteilt, wobei die ersten vier Schichten unter der Bezeichnung »Transportsystem« und die Schichten 5 bis 7 als »Anwendersystem« festgelegt worden sind. Im Normungsgremium für die Schichten des Transportsystems hat sich eine Unterscheidung zwischen LANs und WANs ergeben. Für die Definition von WANs wurde auf die Festlegungen von CCITT und EIA zurückgegriffen. Bei den Festlegungen für LANs hingegen orientierte man sich an IEEE (Dokumente der IEEE 802), die von der ISO als Serie ISO 8802 übernommen worden sind.

9.2.1

Physical Layer

(Bitübertragungsschicht, physikalische Schicht)

Aufgabe der Schicht 1 ist die Übertragung von Bitströmen über die Datenleitung zwischen den an dieser Leitung angeschlossenen Systemen. Es hängt von der gewählten Topologie ab, ob über diese Leitungen zwei oder mehrere Rechner miteinander verbunden werden. Dabei sind vor allem folgende Aspekte zu unterscheiden:

- *Mechanische Definition*

Es handelt sich dabei um die Festlegung der Kabelspezifikation, der Spezifikation des Steckers und der entsprechenden Pinbelegungen des Steckers.

- *Elektrische Definitionen*

Hierbei geht es um die Zuordnung der physikalischen Meßgrößen bezüglich der logischen Werte 0 und 1 zur Darstellung von Bits. Ebenso werden Festlegungen für Widerstandswerte, Impedanz etc. getroffen.

9 Das ISO-Schichtenmodell der offenen Kommunikation

■ Funktionale Definitionen

Es werden Aussagen darüber gemacht, wie die Funktionen der einzelnen Leitungen und die Zeitabläufe auszusehen haben. Bei den Leitungen muß zwischen Datenleitungen, Steuerleitungen und Erdungsleitungen unterschieden werden.

Ebenso muß festgelegt werden, wie die Datenflußrichtung und die Bedeutung der Steuerleitungen auszusehen haben. In welcher Betriebsart die Übertragung stattzufinden hat, ist auch Bestandteil der Schicht 1. Man unterscheidet hierbei zwischen paralleler und serieller Datenübertragung.

Bei der Festlegung der Übertragungsrichtung ist zu unterscheiden, ob die Datenübertragung in beiden Richtungen gleichzeitig möglich ist. In diesem Fall spricht man von Vollduplexübertragung. Kann die Datenübertragung hingegen nur abwechselnd für die eine und dann für die andere Richtung durchgeführt werden, wird dies als Halbduplexverfahren bezeichnet. Ist die Übertragung dagegen nur in einer Richtung möglich, spricht man von einer Simplexübertragung.

9.2.2

Link Layer

(Sicherungsschicht, Verbindungsschicht)

Die Ebene 2 im OSI-Referenzmodell ist für den zuverlässigen Austausch von Datenpaketen zwischen Systemen, die durch die Schicht 1 miteinander gekoppelt sind, zuständig.

Sie ist unter anderem für den logischen Auf- und Abbau von Verbindungen (nur von Bedeutung bei verbindungsorientierten Übertragungen, z.B. HDLC), für die Erkennung und Beseitigung von Übertragungsfehlern und die Synchronisation der darunterliegenden Schicht verantwortlich.

Die grundlegenden Aufgaben der Schicht 2:

- Aktivierung, Überwachung und Deaktivierung einer Verbindung.
- Aufteilung der zu übertragenden Informationen in Datenpakete. Diese werden auch als *Frames* bezeichnet.
- Erkennung und Beseitigung von Übertragungsfehlern, die von der Schicht 1 kommen. Hierzu werden in Standard-LANs über alle Bits eines Pakets Prüfsummen nach dem CRC-Verfahren gebildet und als Protokollinformation angefügt (Trailer).
- Synchronisation der verbundenen Einheiten.
- Steuerung der Reihenfolge von Datenpaketen.

9.2 Die Schichten des ISO-OSI-Modells

Für Lokale Netze ist die Schicht 2 in zwei Subebenen aufgeteilt. Es handelt sich um die Media-Access-Control- (MAC, Zugangsverfahren) und die Logical-Link-Control-Ebene (LLC). Auf diese beiden Ebenen wird im Kapitel, das die Standards für LANs behandelt, näher eingegangen.

9.2.3 Network Layer (Netzwerkschicht)

Die Aufgabe dieser Schicht besteht darin, den Austausch von Binärdatenpaketen zwischen nicht direkt miteinander verbundenen Stationen zu steuern. Sie ist für den reibungslosen Ablauf der logischen Verknüpfung von an physikalische Leitungen gebundenen Schicht-2-Verbindungen zuständig. Dabei erfolgt der Datentransport über einzelne Zwischenknoten. In dieser Schicht wird vor allem die Vermittlungsfunktion der Zwischenknoten im Netz behandelt.

Der Network Layer unterstützt im einzelnen:

- Die Identifizierung der Knoten (Netzwerkadressen)
- Den Auf- und Abbau logischer Verbindungskanäle:
 - Wegsteuerung (Routing)
 - Flußsteuerung

Die Netzwerkknotenadressen sind notwendig, um Zielknoten von Nachrichten eindeutig identifizieren zu können.

Die Hauptaufgabe der Netzwerkschicht ist darin zu sehen, daß logische Knoten-zu-Knoten-Wege zwischen beliebigen Knoten des Netzwerks aufgebaut werden können. Die notwendigen Verbindungen können dabei auf verschiedene Art und Weise hergestellt werden.

Generell denkbar wären:

- Leitungsdurchschaltung
- Virtuelle Kanäle (Virtual Circuit)
- Datagramme

Im Rahmen der Realisierung von OSI sind jedoch nur virtuelle Kanäle und Datagramme vorgesehen. Beiden Prinzipien ist gemeinsam, daß die Verbindung nicht über die elektrische Durchschaltung von Leitungen, sondern durch das Store-and-Forward-Prinzip von Datenpaketen realisiert ist. Dabei wird ein Datenpaket von einer Station zur nächsten übertragen und dort zwischengespeichert. Anschließend verschickt diese Station die Pakete wieder weiter. Im Rahmen dieser Datenübertragung werden über eine Schicht-2-Verbindung logischerweise Pakete aus verschiedenen Schicht-3-Verbindungen übertragen, d.h., es ist eine Mehrfachnutzung der Schicht-2-Verbindungen (Multiplex) möglich. Wird vor Beginn der eigentli-

9 Das ISO-Schichtenmodell der offenen Kommunikation

chen Datenübertragung ein expliziter Verbindungsaufbau durchgeführt, in dessen Rahmen für die folgende Datenübertragung die Wegsteuerung vorgenommen werden muß, so spricht man von *virtuellen Kanälen* oder einer *virtuellen Verbindung*. Über diese virtuelle Verbindung werden sodann die Datenpakete vom Absender zum Empfänger übertragen. Die Datenpakete benötigen dabei keine Informationen mehr darüber, wer der Empfänger ist, da der Kanal, sprich der Weg zum Empfänger, virtuell durchgeschaltet worden ist. Ist die Datenübertragung beendet, wird der virtuelle Kanal, die virtuelle Verbindung, explizit wieder abgebaut (z. B. X.25-Verbindung).

Im Gegensatz dazu wird bei der Datagrammtechnik kein virtueller Kanal zwischen Sender und Empfänger geschaltet. Jedes zu übertragende Paket muß gesondert übertragen werden und erhält jeweils die Adresse des Empfängers mit dazu. Für jedes Paket, das übertragen wird, wird die Wegsteuerung (Routing) neu vorgenommen, so daß die Pakete auf verschiedenen Wegen zum Empfänger gelangen können. Bei dieser Technik ist es möglich, daß bei Überlastung eines Weges eine alternative Wegwahl durchgeführt wird. Im Gegensatz dazu muß bei der virtuellen Verbindung die Nachricht komplett über den für die Übertragung aufgebauten virtuellen Kanal transportiert werden. Bei der Datagrammtechnik hingegen können die einzelnen Pakete wegen ihrer unterschiedlichen Wegwahl in verschiedener Reihenfolge beim Empfänger eintreffen. Es müssen also Maßnahmen ergriffen werden, die die richtige Reihenfolge der übertragenen Pakete wieder herstellen.

Je nachdem, welche Topologie in einem Netzwerk eingesetzt wird, können Nachrichtenpakete auf verschiedenen Wegen vom Sender zum Empfänger gelangen. Die Aufgabe der *Wegsteuerung* liegt vor allem darin, solche Übertragungsstrecken zu finden, die für die Übermittlung der Daten am geeignetsten sind, und bei mehreren Alternativen den optimalsten auszuwählen. Bezüglich der Optimierungsentscheidung sind der maximale Durchsatz und die minimale Transportzeit für die einzelne Nachricht, die übertragen werden soll, zu nennen. Die am häufigsten eingesetzten *Routing-Algorithmen* verwenden Tabellen, die in den einzelnen Netzknoten geführt und aktualisiert werden. In Zusammenarbeit mit der Adressierungstechnik wird mit Hilfe dieser Tabellen entschieden, auf welchem Weg, d. h., über welche Leitung, die Nachricht durch das Netzwerk transportiert wird. Die Tabelleneinträge können dabei statisch sein oder dynamisch dem Verkehrsaufkommen auf den einzelnen Leitungsabschnitten angepaßt werden. Im letzteren Fall wird auch von einer *adaptiven Routing-Methode* gesprochen. Mit dieser Art der Anpassung werden unter anderem Überlastsituationen auf einzelnen Leitungsabschnitten vermieden. Die adaptive Routing-Methode er-

9.2 Die Schichten des ISO-OSI-Modells

fordert jedoch einen selbständigen Informationsaustausch aller Netzwerkknoten untereinander, um die Routing-Tabellen dementsprechend anpassen zu können. Das ist vor allem dann der Fall, wenn ein kompletter Netzwerkknoten ausgefallen ist und die Nachrichten nicht mehr über diesen geschickt werden können.

In Zusammenhang mit diesen Routing-Mechanismen ist auch die Flußsteuerung zu sehen. Sie hat dafür Sorge zu tragen, daß durch gute Routing-Methoden Überlastungen einzelner Leitungsabschnitte im Vorfeld vermieden werden. Dennoch kann es passieren, daß durch enorm hohes Datenvolumen eine Überlastung nicht mehr zu vermeiden ist. Die Komplexität der Methoden und Mechanismen zur dynamischen Verwaltung und Steuerung eines Netzwerks nimmt dabei rasch zu.

Zusammengefaßt werden von der Schicht 3 folgende grundlegenden Aufgaben erfüllt:

- Wegwahl (Routing)
- Multiplexen von Schicht-2-Verbindungen
- Sequenzbildung von Paketen (Aufteilung in angepaßte Längen)
- Flußkontrolle
- Acknowledgements
- Fehlerbehandlung
- priorisierte Übertragung

9.2.4 Transport Layer (Transportschicht)

Die Aufgabe der Transportschicht ist, den höheren Schichten die Möglichkeit zu bieten, Nachrichten zwischen logischen Benutzern des Netzwerks zu übertragen. Unter logischen Benutzern sind dabei kommunikationsfähige Einheiten der höheren Schichten zu verstehen. Im praktischen Einsatz sind das Menschen, die Prozesse auf Knotenrechnern ablaufen lassen. Vor den Benutzern sollen dabei die Details der Übertragung auf den unteren Schichten verborgen und zudem verschiedene Transportqualitäten angeboten werden. Die Transportschicht ist die oberste Ebene des Transportsystems und stellt seine Dienste dem Anwendungssystem zur Verfügung. Es bildet praktisch eine Schnittstelle zwischen Transport- und Anwendungssystem. Zwischen einem Paar logischer Benutzer können mehrere Transportverbindungen gleichzeitig bestehen.

In der Transportschicht werden die logischen Benutzer durch Transportadressen gekennzeichnet. Dabei werden bei zu übertragenden Informationen die Transportadressen in die Netzwerkadressen jener Knoten umgesetzt, in denen die logischen Benutzer zu finden sind. Die Nachrichten werden durch die Transportschicht in Datenpakete

für die Netzwerkschicht verpackt. Eine Nachricht kann dabei in mehrere Pakete zerfallen, oder ein Paket kann mehrere Nachrichten enthalten. Eingehende Pakete hingegen werden in der richtigen Reihenfolge wieder zu den entsprechenden Nachrichten zusammengesetzt. Auf der Transportschicht werden aber auch Maßnahmen zur Steuerung des Datenflusses unternommen.

9.2.5 Session Layer (Sitzungsschicht)

Wenn es sich bei dem Transport Layer um die oberste Schicht des Transportsystems handelt, so ist der Session Layer die unterste Schicht des Anwendungssystems. Seine Aufgabe besteht darin, den Dialog auch bei vorübergehendem Ausfall des Transportsystems aufrechtzuerhalten. Auf dieser Ebene können logische Benutzer gleichzeitig über mehrere Verbindungen kommunizieren. Session-Layer-Verbindungen werden unter Verwendung von Transportverbindungen realisiert. Bricht dabei eine Transportverbindung zusammen, so ist es die Aufgabe der Sitzungsschicht, die Verbindung aufrechtzuerhalten, im Notfall auch durch den Aufbau einer neuen Transportverbindung.

Analog zu den Betriebsweisen von Datenleitungen kann man die Kommunikationsform der Session-Schicht wie folgt einteilen:

- *Two-way Simultaneous Interaction*
Sie entspricht der Vollduplex-Betriebsart. Hierbei können beide Kommunikationspartner gleichzeitig senden und empfangen.
- *Two-way Alternate Interaction*
Sie ist vergleichbar mit der Halbduplex-Betriebsart. Der Dialog wird durch wechselseitiges Senden und Empfangen der Kommunikationspartner realisiert.
- *One-way Interaction*
Genauso wie bei der Simplexmethode ist hier nur ein Monolog möglich. Nachrichten können nur von einem Benutzer gesendet und vom anderen empfangen werden.

Zusammengefaßt ermöglicht also die Sessionschicht den höheren Ebenen den Aufbau, Betrieb und Abbau von Sitzungsschichtverbindungen. Zudem stellt diese Schicht Elemente zur Verfügung, die den Dialog steuern und synchronisieren.

9.2.6 Presentation Layer (Präsentationsschicht)

Auf dieser Ebene werden die Darstellungsformate der übertragenen Nachrichten behandelt. Dabei ist es notwendig, daß eine gemeinsam bekannte Darstellungsart zwischen den entsprechenden Systemen

9.2 Die Schichten des ISO-OSI-Modells

zur Verfügung steht. Man könnte die Dienstleistung dieser Ebene auch als Dolmetscherdienst bezeichnen. Typische Funktionen der Ebene 6 sind Remote-Job-Entry-Funktion, Terminalemulation oder Datenübertragung zwischen unterschiedlichen Systemen.

Die wesentliche Aufgabe liegt in der Umwandlung von Codes und Formaten. Die Ebene 6 erzeugt eine neutrale Form der Daten, so daß sie auch für Systeme von verschiedenen Herstellern interpretiert werden können. Es muß eine Transformation der Datendarstellung und des Datentyps erfolgen, d.h. eine Umsetzung der Syntax und der Semantik. Numerische Werte zum Beispiel werden auf verschiedenen Rechnern, die nicht miteinander kompatibel sind, unterschiedlich dargestellt. Sie müssen daher an das jeweilige Zielsystem angepaßt werden.

9.2.7 Application Layer (Anwendungsschicht)

Die Anwendungsschicht bildet das Bindeglied zur eigentlichen Benutzeranwendung. Sie ist aus einer Reihe von Protokollen zusammengesetzt, die sich ständig erweitern, entsprechend den wachsenden Anforderungen der Anwender. Die Ebene 7 kann dabei unterteilt werden in »Association Control Service Elements (ACSE)« und in »Specific Application Service Elements (SASE)«. Zur SASE-Gruppe gehören folgende Netzwerkanwendungen:

- *FTAM (File Transfer Access and Management)*
Hierbei handelt es sich um die Möglichkeit, einem Anwenderprogramm den Zugriff auf ein entferntes Dateisystem zu gewährleisten und die Dateiattribute zu ändern (Lesen, Schreiben etc.), und um den damit verbundenen Dateitransfer.
- *JTM (Job Transfer and Manipulation)*
Erlaubt das Abschicken eines Programms an einen anderen Rechner und die ständige Kontrolle des Programms während seiner Ausführung.
- *VT (Virtual Terminal)*
Erlaubt den Dialogzugriff von einem Endgerät auf einen entfernten Rechner in einer vom Hersteller des Terminals und des Rechners unabhängigen Form.
- *MHS (Message Handling System) – X.400*
Der Datenaustausch für E-Mail-Systeme gemäß X.400-Standardisierung wird durch MHS gewährleistet. Diesem Standard kommt im Zuge der rasanten E-Mail-Implementierungen immer mehr Bedeutung zu. Das MHS ist somit eine Sammlung von Message-Handling-Funktionalitäten, die es Benutzern ermöglichen, Nachrichten zu senden und zu empfangen. Dieser MHS-Standard darf nicht mit dem Novell-MHS-System (Message Handling Services)

9 Das ISO-Schichtenmodell der offenen Kommunikation

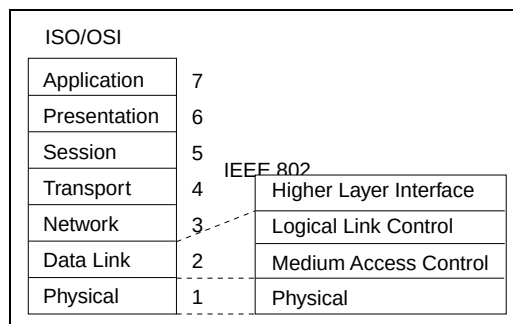
verwechselt werden. Wenn man sich mit X.400 etwas näher auseinandersetzt, stellt man fest, daß es sich dabei um mehr als nur einen Standard handelt. X.400 bezeichnet im Prinzip nur das Systemmodell und die damit verbundenen Serviceelemente. Daneben gibt es noch die Standards X.401, X.408, X.409, X.410, X.411, X.420 und X.430. 1988 wurde der X.400-Standard aus dem Jahre 1984 nochmals erweitert. Weitere Erweiterungen erfolgten 1992. Eine sehr enge Integration erfolgt mit dem X.500-Standard, um damit auch die Funktionen der Directory-Services nutzen zu können. Im Kapitel über E-Mail wird auf diese Zusammenhänge noch näher eingegangen.

■ DS (Directory Services) – X.500

Das sind Netzerkanwendungen, die Informationen über die Teilnehmer eines Netzwerks verwalten und verfügbar machen. Die Standards werden im Rahmen des X.400-Projekts erarbeitet und als X.500 bezeichnet. Der X.500-Standard beschreibt das Konzept, die Modelle und Dienste, die darüber definiert werden sollen. Ebenso wie X.400 setzt sich der X.500-Standard aus einer Vielzahl von Einzelstandards zusammen, das sind X.501, X.509, X.511, X.518, X.519, X.520, X.521, X.525, X.581 und X.582. Erweiterungen für den X.500-Standard wurden 1993 durchgeführt.

Der Protokollstandard X.500 wird für NetWare 4 eine besondere Bedeutung haben, da auf diesem Standard die Netware 5 Directory Services aufbauen. Das fällt zum Beispiel dann auf, wenn man die Festlegungen für X.525 liest und feststellt, daß es hierbei um die Replizierung von Partitionen geht, ein Mechanismus, der im X.500-Standard definiert ist und auch von NetWare 4 unterstützt wird.

Abbildung 9.5
Das ISO/OSI-
Modell und das
IEEE-802-Modell
im Vergleich



Zum Aufbau von Kommunikationssystemen sind inzwischen fest etablierte Standards am Markt vorhanden. Das ISO/OSI-Referenzmodell läßt sich als Kommunikationsarchitektur auch für LANs heranziehen.

9.2 Die Schichten des ISO-OSI-Modells

Aufgrund der speziellen Eigenschaften von LANs (zum Beispiel entfällt die Vermittlung in Lokalen Netzen, da andere Zugangsverfahren eingesetzt werden) wurde vom IEEE Standards Committee 802 wie auch von der ECMA eine von den unteren drei Schichten des ISO/OSI-Modells abgeleitete LAN-Architektur entwickelt. In Abbildung 9.5 ist das IEEE-802-Modell dem ISO/OSI-Schichtenmodell gegenübergestellt. Abbildung 9.6 hingegen zeigt die einzelnen Komponenten im Detail.

Wir werden uns im Folgenden mit diesen einzelnen Komponenten etwas näher befassen.

Abbildung 9.6
Die einzelnen
Funktionalitäten
des IEEE-802-
Modells

Higher Layer Interface	IEEE802.1 Higher Layer Interface Standard	Internet	3b
		Routing	3a
Logical Link Control	IEEE802.2 Logical Link Control Standard		2b
Medium Access Control	IEEE802.3 CSMA/CD	IEEE802.4 Token-Bus	2a
	IEEE802.5 Token-Ring	IEEE802.6 Metropolitan Area NetWork	
Physical	Physical Media		1

■ IEEE 802.1 – Higher Layer Interface Standard (Schicht 3)

In dieser Beschreibung wird zum einen eine Einführung in die Struktur des IEEE-802-Berichts gegeben und zum anderen die Problematik des Internetworking behandelt. Unter Internetworking ist als Teil der Kommunikation zu verstehen, der notwendig ist, um Informationen zwischen Lokalen Netzwerken austauschen zu können. Darunter fällt auch die Kommunikation zwischen heterogenen Lokalen Netzwerken über Gateways. Der IEEE-802.1-Bericht enthält auch Beschreibungen über Funktionen für noch zu spezifizierende höhere Schichten. Neben der Behandlung der Gateway-Funktion werden vor allem auch die Funktionen von Bridges festgelegt; es sind die Definition des Spanning Tree und das Management zu nennen.

■ IEEE 802.2 – Logical Link Control

Dieser Standard beschreibt das für alle Netztechnologien gleiche Protokoll der Data-Link-Ebene und die Schnittstelle zur Netzwerkebene und zum Medium Access Control Sublayer sowie zu den dazu notwendigen Managementfunktionen.

Im IEEE 802.2 werden zwei Servicetypen spezifiziert, die der Netzwerkebene angeboten werden:

- *Typ 1: datagramorientierte (verbindungslose) Dienste*
Beim Typ-1-Dienst werden Dateneinheiten unabhängig voneinander gesendet, eine bestimmte Reihenfolge muß nicht eingehalten werden. Die Daten können zu einem (Punkt-zu-Punkt), zu mehreren (Multi-Cast) oder an alle (Broad-Cast)

9 Das ISO-Schichtenmodell der offenen Kommunikation

angeschlossenen Empfänger gesendet werden. Der Empfang von Dateneinheiten wird nicht bestätigt. Überlegungen werden jedoch inzwischen dahingehend angestellt, einen Datagrammdienst mit Quittungen einzuführen.

– *Typ 2: verbindungsorientierte Dienste*

Im Gegensatz dazu muß beim Typ-2-Dienst, bevor Daten gesendet werden können, eine Verbindung zwischen Sender und Empfänger aufgebaut werden. Dabei ist es möglich, daß bestimmte Merkmale für die Verbindung festgelegt werden. Nach Beendigung des Datenaustauschs wird die Verbindung wieder abgebaut. Die Dateneinheiten werden unter Beachtung der Reihenfolge über diese aufgebaute Verbindung gesendet. Der Empfang von Dateneinheiten wird bei dieser Art der Verbindung quittiert. Dies gilt vor allem für WAN-Verbindungen und die hierfür eingesetzten Protokolle, z. B. HDLC.

■ *IEEE 802.3 bis IEEE 802.12 – Media Access Control*

In diesem Standard wurden die Netzzugangsverfahren festgelegt, wer also wann übertragen darf. Da im LAN für alle Stationen nur ein Übertragungsmedium zur Verfügung steht, muß auf irgendeine Art und Weise geregelt werden, wer zu welchem Zeitpunkt dieses Medium zum Senden seiner Daten verwenden darf.

Da es für die verschiedenen LAN-Topologien auch unterschiedliche Zugangsverfahren gibt, wurden diesbezüglich von IEEE verschiedene Standards festgelegt, die auch als IEEE-802-Standards bezeichnet werden.

Die folgenden IEEE-Standards sind zu unterscheiden:

IEEE 802.3	CSMA/CD-Zugriffsverfahren
IEEE 802.4	Token-Bus-Zugriffsverfahren
IEEE 802.5	Token-Ring-Zugriffsverfahren
IEEE 802.6	Metropolitan Area Network
IEEE 802.7	Broadband Technology Advisory Group
IEEE 802.8	Optical Fiber Technology Advisory Group
IEEE 802.9	Sprach-/Daten-Integration in LANs
IEEE 802.10	Standard für LAN Security
IEEE 802.12	100BaseVGAnyLAN Standard
IEEE 802.30	100BaseT, Standard für ein CSMA/CD-basierendes Ethernet mit 100 Mbit/s Übertragungsgeschwindigkeit

9.3 TCP/IP – ein universelles Protokoll

TCP/IP ist zwar kein standardisiertes Protokoll, aber es wird aufgrund seiner sehr weiten Verbreitung als De-facto-Standard anerkannt. Durch die weite Verbreitung von Internet-Zugängen und -anschlüssen wurde die Akzeptanz und die Verbreitung von TCP/IP immer größer. Betrachtet man die Entwicklungen der renommierten Netzwerkbetriebssystem-Hersteller, so stellt man fest, daß die Bedeutung von TCP/IP nicht von der Hand zu weisen ist.

Bislang war die Protokolldomäne von Novell IPX/SPX. Seit einigen Jahren jedoch gibt es einen Zusatz für NetWare, der als NetWare/IP bezeichnet wird. Mit diesen Modulen ist man in der Lage, die IPX/SPX-Umgebung von Novell gegen eine TCP/IP-Umgebung auszutauschen. Mit Einführung von NetWare 5 wird standardmäßig das IP-Protokoll für die Kommunikation in einem NetWare-Netzwerk eingesetzt werden. Aus Kompatibilitätsgründen wird jedoch auch IPX/SPX optional weiterhin unterstützt.

Das Microsoft-Produkt NT Server wird außer mit den Standardprotokollen NETBeui, NWLink (IPX/SPX) ebenfalls mit TCP/IP ausgeliefert. So kann man bei der Installation von NT-Servern entscheiden, welches Protokoll eingesetzt werden soll. Zu beachten ist jedoch, daß die TCP/IP-Umgebung von Windows NT keine Native-IP-Umgebung ist. Dies fällt zum Beispiel dann auf, wenn zwei NT-Netzwerke über Router miteinander verbunden sind, IP als Protokoll eingesetzt wird und der Server in dem einen Netzwerk und die Workstations in dem anderen Netzwerk installiert sind. In diesem Fall können die Windows-NT-Workstations nicht auf den Windows-NT-Server zugreifen, da NT hierfür NetBios-Mechanismen nutzt, die man lediglich in ein IP-Paket verpackt. Da es sich in diesem speziellen Fall auch noch um einen NetBios-Broadcast handelt, wird dieser nicht über den Router transportiert. Um diese Problematik in den Griff zu bekommen, hat Microsoft den Mechanismus WINS eingeführt. Bei der Beschreibung von Windows-NT-Servern wird auf dieses Problem nochmals näher eingegangen. An dieser Stelle sei nur nochmals bemerkt, daß in einem Router-Netzwerk und dem Einsatz von TCP/IP als Protokoll die Kommunikation zwischen NT-Workstation und NT-Server nur dann stattfinden kann, wenn sich entweder alle NT-Systeme in einem Segment befinden oder bei routerübergreifenden Datenverkehr WINS eingesetzt wird.

9 Das ISO-Schichtenmodell der offenen Kommunikation

Mit Einführung von Windows 2000 (der genaue Zeitpunkt steht immer noch nicht fest) wird auch Microsoft in der Lage sein, Native-IP zu verwenden. Aus Gründen der Kompatibilität mit Windows NT 4.0 werden jedoch auch die alten Protokollmechanismen (NetBEUI, WINS etc.) unterstützt.

Es ist festzustellen, daß sich immer mehr Hersteller von den proprietären Protokollen abwenden und auf das Universal-Protokoll TCP/IP setzen. Sobald alle Hersteller Native-IP-Implementierungen unterstützen, wird zumindest die kommunikationstechnische Integration heterogener Systeme wesentlich einfacher und bequemer.

Hinter TCP/IP (Transmission Control Protocol/Internet Protocol) verbirgt sich eine ganze Familie von Protokollen und Funktionen, die in den siebziger Jahren im Auftrag vom DoD (Department of Defense der USA) entwickelt und implementiert wurde. Das Ziel war eine möglichst gesicherte Verbindung zwischen heterogenen Systemen über Wide Area Networks.

Die TCP/IP-Protokolle entwickelten sich zu einem Kommunikationspaket, das sowohl in lokalen als auch in öffentlichen Netzen eingesetzt wird. Durch die Offenheit von TCP/IP und als Bestandteil der Berkeley-Unix-Version-4.2 wurde TCP/IP zum »Industriestandard« zur Vernetzung von unterschiedlichen Systemen.

Langfristiges Ziel aller Bemühungen um die Kommunikationsstandards ist die universelle Open Systems Interconnection auf der Basis von ISO-Standards. Doch diese Standards sind trotz aller Euphorie noch nicht vollständig definiert, und es wird sicher noch einige Zeit dauern, bis sie verfügbar sein werden. Alle bereits verfügbaren ISO-Protokolle zeigen aber auch, daß die Performance aufgrund der Komplexität, die diesen Protokollen zugrunde liegen, im Vergleich zu bereits existierenden Protokollen wie IPX/SPX oder TCP/IP wesentlich schlechter ist. Dagegen stellt heutzutage TCP/IP die einzige definierte Architektur für herstellerübergreifende Datenkommunikation dar. TCP/IP hat sich inzwischen im professionellen Einsatz vielfach bewährt und gilt als Zwischenlösung, bis entsprechende ISO-Standards verfügbar sind – so war zumindest der bisherige Ansatz. So wie die Entwicklung jedoch derzeit aussieht, läßt sich TCP/IP als universelles Protokoll, das von allen renommierten Herstellern unterstützt wird, nicht mehr verdrängen. Die Anzahl der TCP/IP-Implementierungen ist inzwischen so groß, daß eine Umstellung auf ein neues Protokoll einen zu großen Aufwand bedeuten würde.

In Abbildung 9.7 ist die Eingliederung des TCP/IP-Protokolls in das ISO/OSI-Referenzmodell dargestellt. Die Bedeutung der wichtigsten Protokolle von TCP/IP sind hier ebenfalls zu sehen.

9.3 TCP/IP – ein universelles Protokoll

Bild 9.7:
TCP/IP im ISO/OSI-
Modell

OSI	TCP/IP		
Application	Anwendungen		
	Standard:	Erweiterte Anwendungen:	System-meldungen
Presentation	TELNET	NFS	Fehlerbehandlung
Session	FTP	Name Server	
	SMTP	Drucker Server	
		Remote Execution	
		Terminal Server	
Transport	TRANSMISSION CONTROL PROTOCOL (TCP) USER DATAGRAM DELIVERY PROTOCOL (UDP)		
Network	INTERNET PROTOCOL (IP) ADDRESS RESOLUTION PROTOCOL (ARP) INTERNET CONTROL MESSAGE PROTOCOL (ICMP)		
Data Link	Übertragungsmedium		
Physical	802.3 Ethernet, 802.5 TRN, ProNET 4/10/80 Synchron, X.25/T1		

Internet Protocol (IP)

Das Internet Protocol deckt Schicht 3 (Network) ab. In Schicht 1 und 2 sind keine speziellen Protokolle vorgesehen (in Abbildung 9.7 sind die gebräuchlichsten aufgelistet). Die Aufgabe des IP besteht darin, Datenpakete von einem Sender über mehrere Netze hinweg zu einem Empfänger zu transportieren. Diese Datenpakete sind sogenannte Datagramme. Das IP gewährleistet weder die Einhaltung einer bestimmten Datagramm-Reihenfolge noch die Ablieferung beim Empfänger.

Um Sender und Empfänger eindeutig adressieren zu können, verwendet IP 32-Bit-Adressen, die normalerweise in vier Oktetts geschrieben werden, welche wiederum dezimal dargestellt werden, z. B. 128.5.9.16. Die Bezeichnung Oktett statt Byte hat seinen guten Grund. Bei verschiedenen Computern, die TCP/IP unterstützen, hat ein Byte nicht die Länge von 8 Bit. Diese Internet-Adressen werden vom DDN-Network Information Center weltweit eindeutig vergeben, so daß jeder Anwender von TCP/IP mit allen anderen TCP/IP-Benutzern kommunizieren kann.

Ein Teil dieser Adressen spezifiziert das Netzwerk, der Rest die Rechneradresse innerhalb eines Netzes. Die Grenze zwischen Netzwerkanteil und Host-Anteil an der Gesamtadresse ist fließend und hängt maßgeblich von der Größe des Netzwerks ab. Da diese Adresse be-

9 Das ISO-Schichtenmodell der offenen Kommunikation

liebig vergeben werden kann, ist sie auch unabhängig von der zur Datenübertragung eingesetzten Hardware. Sobald man jedoch den Anschluß zum Internet plant, sollte man sich um offizielle IP-Adressen kümmern. Nur so kann gewährleistet werden, daß eine Einbindung des Firmennetzwerks in das Internet keine Adressierungsprobleme nach sich zieht. Die Vergabe der offiziellen IP-Adressen wird von ISP durchgeführt. Im internen Netz sollten die privat reservierten IP-Adressen eingesetzt werden. Die Verbindung vom privatem Netz mit dem Internet wird dann über ein Firewall-System abgesichert.

Transmission Control Protocol (TCP)

Das Transmission Control Protocol setzt direkt auf dem Internet Protocol auf; das bedeutet, daß TCP auf Ebene 4 des OSI-Modells arbeitet. Somit ist es für den Aufbau von logischen Verbindungen zwischen zwei Kommunikationspartnern verantwortlich.

TCP ist ein verbindungsorientiertes End-to-end-Protokoll, das eine folgerichtige und zuverlässige Datenübertragung gewährleistet. Zur Absicherung der Datenübertragung ist ein relativ großer Protokoll-Overhead notwendig, der die Übertragung aber auch langsamer werden läßt. Die Sicherung der Datenübertragung war bei der Entwicklung dieses Protokolls allerdings ein sehr wichtiger Aspekt, und somit wird dieser kleine Nachteil in Kauf genommen. Jedes Datagramm wird mit einem Header, der eine Mindestlänge von 20 Oktetts hat, versehen. In diesem Header befindet sich auch eine Folgenummer (Sequence Number), mit der jedes Datagramm so durchnummeriert wird, daß die richtige Reihenfolge der Pakete erkannt werden kann. Bei einem Netzwerkverbund können die einzelnen Datagramme so auch auf unterschiedlichen Wegen zum Ziel gelangen.

User Datagram Protocol (UDP)

Das UDP-Protokoll ist ein verbindungsloses Transportprotokoll. Es wurde im RFC 768 (Request for Comment) definiert. Im Vergleich zu TCP hat es wesentlich weniger Merkmale:

- verbindungslos
- Adressierung durch Portnummern
- sehr einfach aufgebaut

UDP liefert über die Leistungen von IP hinaus nur noch eine Portnummer und eine Prüfsumme der Daten. Im Gegensatz zu TCP gibt es bei UDP keine Transportquittung oder gar andere Sicherheitsmaßnahmen. Das Fehlen dieser Mechanismen macht UDP jedoch zu ei-

9.3 TCP/IP – ein universelles Protokoll

nem sehr schnellen Protokoll, und es wird deshalb immer dann eingesetzt, wenn Hochgeschwindigkeitsanwendungen zum Einsatz kommen (z.B. NFS).

Die Schichten 5 bis 7 des OSI-Referenzmodells werden von den verschiedenen TCP/IP-Anwendungen abgedeckt. Auf keinen Fall dürfen bei einer TCP/IP-Anwendung die drei Standardprotokolle Datei-Transfer, Terminalemulation und Mail-Transfer fehlen.

TCP/IP ist grundsätzlich unter Ethernet, Token-Ring oder anderen gängigen Netzwerktopologien einsetzbar. Da TCP/IP jedoch meist zusammen mit Unix eingesetzt wird und beim Einsatz von Unix-Rechnern fast ausschließlich Ethernet zum Einsatz kommt, findet man TCP/IP-Protokolle oft zusammen mit der Ethernet-Topologie.

Da bei TCP/IP einige Anwendungen fest definiert sind, sollen diese kurz dargestellt werden. Bei keiner Installation von TCP/IP fehlen die Anwendungen Telnet, FTP oder SMTP.

File Transfer Protocol (FTP)

Dieses Protokoll erlaubt die gemeinsame Benutzung von Dateien auf unterschiedlichen Systemen, den Transfer von Dateien zwischen den Systemen und eine vereinfachte Dateihandhabung. Das heißt, der Benutzer kann zum Beispiel Dateien auf seinen Rechner kopieren oder seine Dateien auf einem anderen Computer ablegen.

Trivial File Transfer Protocol (TFTP)

TFTP ist eine sehr einfache Variante, um Daten zwischen Computern zu transferieren. Im Gegensatz zu FTP arbeitet TFTP auf Basis von UDP. Aus diesem Grund muß TFTP über eigene Mechanismen zur Fehlerkorrektur verfügen. Herkömmliche Anwender werden nur sehr selten mit diesem Dienst arbeiten, sondern in der Regel das komfortablere FTP-Programm nutzen.

Terminalemulation (TELNET)

Mit Telnet ist es für einen Benutzer möglich, sich auf einem beliebigen anderen Rechner anzumelden. Bekannt muß der Name des Rechners sein sowie der entsprechende Benutzername inklusive Paßwort. Jede Eingabe wird dann direkt an den anderen Rechner weitergegeben, falls nötig, wird eine Zeichensatzumwandlung durchgeführt. Für den Host bedeutet dies nur, daß ein zusätzliches Terminal angeschlossen ist. Nach dem Abmelden vom Host wird die Terminalemulation beendet, und man kann auf dem eigenen Rechner wieder lokal weiterarbeiten. Im Normalfall werden standardmä-

9 Das ISO-Schichtenmodell der offenen Kommunikation

ßig die Teminal emulationen für VT100- und VT220-Terminals angeboten. Über entsprechende Treiber lassen sich aber auch andere Emulationen einbinden.

Mail Transfer (SMTP)

Mit dem E-Mail-Protokoll SMTP (Simple Mail Transfer Protocol) ist es möglich, daß zwei Mail-Systeme auf unterschiedlichen Computern miteinander kommunizieren. Aus dem Namen läßt sich bereits erkennen, daß es sich dabei um ein sehr einfaches Protokoll handelt. Die Funktionsweise ist vergleichbar mit FTP. Der Client sendet einen ASCII-Befehl an den Mail-Server, der Mail-Server hingegen antwortet mit Ziffernfolgen und Text.

Zusätzlich zu diesen drei Standardanwendungen stehen noch weitere Anwendungen zur Verfügung, die nachfolgend kurz erläutert werden sollen.

Network File System (NFS)

Mit Hilfe des Network File System können die Dateien direkt auf fremden Computern im TCP/IP-Netzwerk bearbeitet werden. Man verwendet dabei virtuelle Festplatten. Der Anwender hat dann den Eindruck, als sei die Datei auf der eigenen Festplatte abgespeichert. Somit können große Festplattenkapazitäten dem gesamten Netzwerk zur Verfügung gestellt werden.

Name-Server

Um bei großen Netzwerken die gesamten Definitionen wie Benutzernamen, Paßwörter, Netzwerkadressen etc. nicht auf jedem Host pflegen zu müssen, können sogenannte Name-Server eingerichtet werden. Auf diesem Name-Server werden also alle Benutzerdefinitionen etc. zentral gespeichert und zur Verfügung gestellt. Im Zuge der Internet-Anbindung gewinnt dieser Dienst immer mehr an Bedeutung. Die zu installierende Komponente wird dabei als DNS Server (Domain Name Server) bezeichnet.

Remote Execution

Mit dieser Applikation können Programme auf anderen Rechnern aufgerufen und ausgeführt werden. Anwendungen, die beispielsweise ganz bestimmte Ressourcen benötigen, können dann auf dem Rechner gestartet werden, der diese Ressourcen besitzt. Die hierfür verfügbaren Befehle werden auch als R-Befehle bezeichnet. Die gebräuchlichsten R-Befehle sind:

9.3 TCP/IP – ein universelles Protokoll

- *rlogin*
Wie bei Telnet wird dadurch die Verbindung mit einem Remote-Computer ermöglicht.
- *rsh*
Auf einem Remote-Computer wird die Ausführung eines Befehls vorgenommen.
- *rexec*
Auf einem Remote-Computer wird die Ausführung eines Befehls vorgenommen.
- *rcp*
Zwischen zwei Remote-Computern können Dateien kopiert werden.

Für die Behandlung der Frage, wie Netzwerke miteinander verbunden werden können bzw. sollen, egal ob es sich um eine LAN-LAN- oder LAN-WAN-LAN-Kopplung handelt, ist die Kenntnis des ISO-Schichtenmodells von entscheidender Bedeutung. Da in diesem Kapitel der Grundstock gelegt worden ist, kann im nächsten Abschnitt darauf eingegangen werden, wie Netzwerke gekoppelt werden können.

10 Internetworking

In diesem Kapitel will ich zeigen, wie Netzwerke durch Repeater, Bridges oder Router erweitert werden können. Wenn es um den Einsatz kleiner Netze geht, muß man sich in der Regel keine Gedanken über diese Dinge machen, bei größeren Netzen sieht die Situation jedoch wieder ganz anders aus.

Durch den Einsatz solcher Koppellemente wird unter anderem die Anzahl der anschließbaren Stationen vergrößert, eine bessere Lastkontrolle und vor allem die Entlastung des gesamten Netzwerks erreicht, Übergänge von einem Netzwerk zu einem anderen Netzwerk (Aufbau heterogener Netze) und auch die Anbindung an öffentliche Netze ermöglicht.

Folgende Koppellemente stehen zur Verfügung:

- *Repeater*

Repeater arbeiten auf Ebene 1 des ISO/OSI-Schichtenmodells. Ein Repeater nimmt Datensignale auf, verstärkt sie und gibt sie auf das andere Kabelsegment wieder aus.

- *Bridge*

Die Bridge dient zum Verbinden von zwei oder mehreren LANs und transportiert Datenpakete zwischen diesen LANs.

- *Router*

Router haben die gleiche Funktion wie Bridges (das Koppeln von LANs), arbeiten jedoch auf anderen Ebenen im Schichtenmodell und unterscheiden sich deshalb grundlegend in ihrer Arbeitsweise.

- *Brouter*

Der Brouter ist eine Kombination aus der Arbeitsweise einer Bridge und eines Routers. Je nach Anwendungsfall geht der Brouter mit zu transportierenden Datenpaketen um wie eine Bridge oder ein Router.

- *Gateway*

Ein Gateway arbeitet auf der höchsten Ebene im ISO/OSI-Schichtenmodell und erlaubt es dadurch, daß Netze mit unterschiedlichsten Protokollen und Zeichensätzen miteinander verbunden werden.

- *Switch*

Die Anforderungen an den Datendurchsatz werden immer größer. Die zu transportierenden Datenmengen nehmen immer mehr zu, so daß inzwischen sehr schnelle Koppellemente benötigt werden. Mit dieser neuen Technik wird versucht, den Anforderungen

10 Internetworking

hierfür gerecht zu werden. Wurden zu Beginn der Entwicklung nur Layer-2-Switches eingesetzt, so ist man heute auch in der Lage, Layer-3-Switches einzusetzen.

Die Arbeitsweise und der Einsatz dieser Koppellemente sollen in den nächsten Kapiteln näher ausgeführt werden.

10.1 Repeater

Beim Repeater handelt es sich um das einfachste Koppellement. Es dient ausschließlich der Verstärkung von Signalen und den Kabellängen eines LAN zur Vergrößerung. Mit Repeatern der neuen Generation ist es auch möglich, die Umsetzung auf unterschiedliche Kabeltypen durchzuführen, z.B. Kupfer auf LWL oder Koaxialkabel auf Twisted-Pair und dergleichen mehr. Im Prinzip besteht der Repeater aus einer reinen Hardware-Schaltung, d.h. zum Betreiben eines Repeaters werden keinerlei Software-Komponenten benötigt. Dies macht seinen Einsatz auch sehr einfach – eine typische Plug&Play-Lösung.

Mit neuen Repeatern können nicht nur zwei Kabelsegmente miteinander gekoppelt werden, sondern es besteht die Möglichkeit, mehrere Segmente miteinander zu verbinden. Bei diesen Systemen handelt es sich dann um sogenannte Multiport-Repeater. Aus Sicherheitsgründen sind gute Repeater auch in der Lage, defekte Segmente automatisch abzuschalten, um nicht den Betrieb der anderen Segmente in Mitleidenschaft zu ziehen. Daneben sind Repeater auch in der Lage, »Rauschen« aus der Leitung zu filtern.

Repeater haben folgende Charakteristika:

- Sie sind vor allem aus dem Bereich der Ethernet-Verkabelung bekannt. Hierfür gibt es auch eine Vielzahl unterschiedlicher Varianten, da Ethernet mit den unterschiedlichsten Kabeltypen aufgebaut werden kann und entsprechende Übergänge mit Hilfe von Repeatern realisierbar sein sollen und müssen. Token-Ring verstärkt die Signale in jeder Adapterkarte. Daneben kann über RI bzw. RO ein Repeater eingesetzt werden, um die Entfernungen zwischen zwei Ringleitungsverteilern zu erhöhen. Bei ARCNET fungiert jeder Active Hub bereits als Verstärker, sofern diese Techniken noch eingesetzt werden.
- Repeater arbeiten gemäß dem ISO/OSI-Schichtenmodell auf der untersten Ebene 1, der physikalischen Ebene. Protokolle und Zugriffsmethoden sind für Repeater uninteressant, da eine reine Signalverstärkung der einzelnen Bitströme durchgeführt wird. Die zu koppelnden Segmente müssen jedoch das gleiche Zugriffsver-

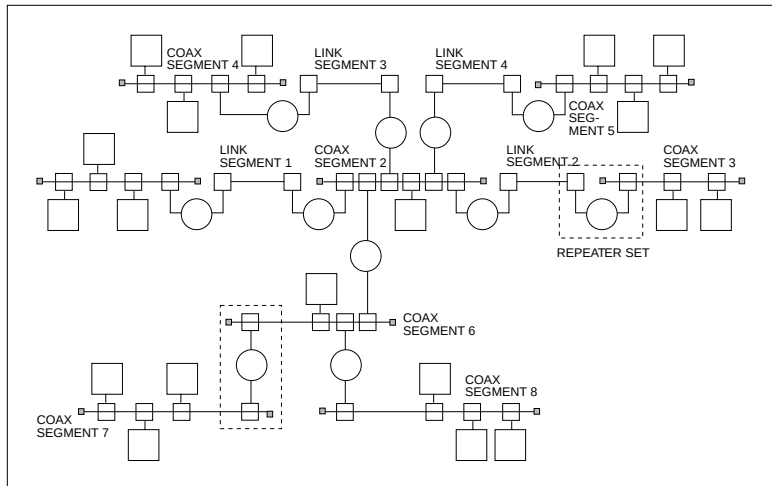
10.2 Bridge

fahren haben (Ethernet, Token-Ring oder ARCNET-Topologie). Eine Kopplung von Ethernet und Token-Ring zum Beispiel ist mit Repeatern nicht möglich. Hierfür werden andere Einheiten benötigt (Bridge, Router oder Brouter).

- Die Node-Adressen der einzelnen Stationen in den zu koppelnenden Segmenten müssen unterschiedlich sein, da durch einen Repeater keine logische Trennung des Netzes durchgeführt wird. Für die Stationen handelt es sich um ein physikalisches Netzwerk. Jedes Signal wird ohne Rücksicht auf Verluste auf das andere Segment übertragen.

Sie sollten sich auf alle Fälle fragen, ob durch den Einsatz von Repeatern das erwartete Ziel erreicht wird. Man ist zwar in der Lage, die Längenausdehnung eines LAN damit zu erhöhen, hat aber keine Möglichkeit, eine Lasttrennung im LAN durchzuführen. Am Ende dieses Kapitels werden Sie sehen und erkennen, wann welche Koppelemente für welchen Zweck benötigt werden.

Abbildung 10.1
Der mögliche Ein-
satz von Repeatern



10.2 Bridge

Wie schon erwähnt, führen Repeater keine logische Trennung von Netzen durch. Signale, die im Segment 1 erzeugt werden, transportiert der Repeater fast uneingeschränkt auf alle anderen durch ihn gekoppelten Netzwerksegmente weiter.

In vielen Situationen wird jedoch die Forderung gestellt, durch die Kopplung von LANs auch gleichzeitig eine logische Trennung der Netze durchzuführen. Die Gründe hierfür können unter anderem sein:

10 Internetworking

1. Die Kopplung durch Repeater genügt nicht den Anforderungen.
2. Durch die Integration eines Koppelements soll nicht nur die Längenausdehnung vergrößert werden, sondern es soll auch die Anzahl der Stationen in den neuen Segmenten berechnet werden können.
3. Es soll eine logische Trennung des LANs durchgeführt werden, so daß eine Lastaufteilung erfolgt. Nicht jedes Datenpaket wird unbedingt in das andere Segment übertragen.

Es ließe sich noch eine Vielzahl von Gründen finden. Sie werden jedoch anhand der Funktionsbeschreibung einer Bridge selbst feststellen, worin die Vorteile dieses Koppelementes liegen.

Durch eine Bridge werden in der Regel gleichartige Netze miteinander verbunden, also Token-Ring mit Token-Ring und Ethernet mit Ethernet. Es gibt jedoch inzwischen eine kleine Anzahl von Anbietern von Bridges, die es ermöglichen, auch Token-Ring und Ethernet miteinander zu koppeln. Die Bridge trennt dabei die Netze in zwei »unabhängige« LANs, wobei jedes LAN einen eigenen Token bzw. das eigene CSMA/CD-Zugriffsverfahren realisiert. Man unterscheidet dabei mehrere Arten von Bridges:

■ *Lokale Bridges*

Es werden physikalisch zwei LANs miteinander verbunden. In der lokalen Bridge sind zwei oder mehrere Adapterkarten angeschlossen, an denen die LANs direkt angebunden sind.

■ *Remote Bridges*

Diese Bridges bestehen immer aus zwei Paaren und werden eingesetzt, wenn sich die zwei LAN-Segmente nicht am gleichen Ort befinden und sich somit nicht über die normale Standardverkabelung verbinden lassen. Jede Bridge ist physikalisch an ein LAN angebunden. Zwischen den beiden Bridges befindet sich eine Remote-Verbindung. Es handelt sich dabei in der Regel um Leitungen der Telekom (Standleitung, ISDN, X.25, T1 etc.). Beim Einsatz von Remote-Bridges erfolgt der Übergang vom LAN zum WAN.

■ *Multiport Bridges*

Lange Zeit waren ausschließlich 2-Port-Bridges im Einsatz. Damit konnten genau zwei Netzwerke miteinander verbunden werden. Da Netze jedoch immer größer werden, besteht die Forderung, über eine Bridge mehr als zwei LANs koppeln zu können. Man kann davon ausgehen, daß dies eine allgemeine Forderung für Bridges ist.

Dabei ist jedoch zu berücksichtigen, daß die Multiport Bridge sehr leistungsfähig sein muß, um allen angeschlossenen LANs die notwendige Performance bieten zu können.

10.2 Bridge

LANs verbinden eine Vielzahl von Endgeräten über ein und denselben Kabelstrang. Aus diesem Grund müssen die Endgeräte im LAN (Nodes) eindeutig identifizierbar sein, und sie benötigen eine eindeutige Adresse. Diese Adresse wird als MAC-Adresse (Media Access Control Address) bezeichnet. Bei Ethernet, Token-Ring, FDDI und ATM ist die MAC-Adresse auf der Karte fest eingestanzt und braucht in der Regel nicht angepaßt zu werden. Bei ARCNET-Karten mußten die Adressen früher manuell eingestellt werden.

Eine Änderung der eingestanzten Adressen bedeutet für den LAN-Verwalter zusätzlichen Aufwand, da er eindeutige Adressen vergeben muß. Wie Sie noch sehen werden, ist dies beim Einsatz von Bridges äußerst wichtig, da in den gekoppelten Segmenten, im Gegensatz zur Kopplung mit Routern, die Adressen auch in den gekoppelten Netzen eindeutig sein müssen.

Die MAC-Adressen werden im ISO/OSI-Schichtenmodell auf Ebene 2 benötigt. Dies bedeutet, daß auf dieser Ebene das Protokoll mit den physikalischen Adressen arbeitet. Protokollebenen hingegen sind in der Lage, mit logischen Adressen zu arbeiten. Dies erfolgt ab Ebene 3 des Schichtenmodells. Die logischen Adressen sind stark protokollabhängig. Dies hat spezielle Auswirkungen auf den Einsatz von Routern.

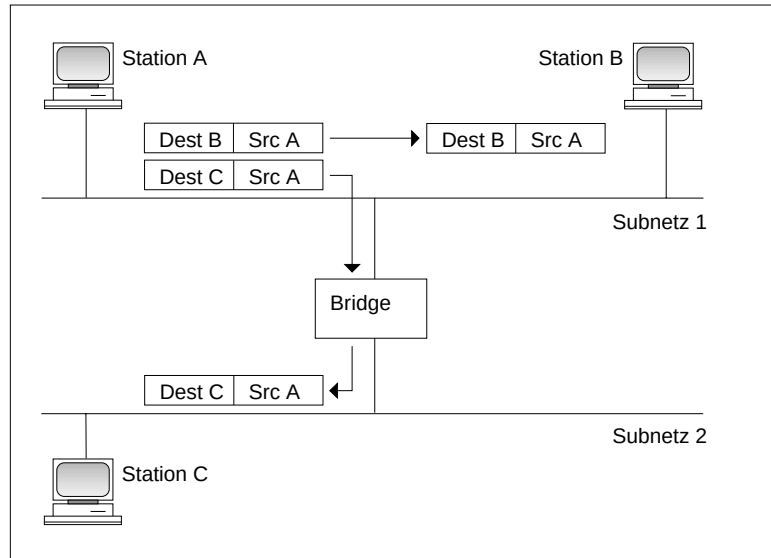
- Eine Bridge arbeitet auf der MAC-Ebene (untere Hälfte der Schicht 2, darüber liegt die LLC-Ebene). Deshalb sind für die Bridge die oberen Protokollebenen vollkommen gleichgültig, also alles, was über der MAC-Ebene liegt. Man spricht deshalb auch davon, daß die Bridge protokolltransparent ist.
- Die Bridge entscheidet über die Weiterleitung von Paketen aufgrund der physikalischen MAC-Adresse. Dies ist auch der Grund dafür, warum die MAC-Adresse in allen über Bridges gekoppelten LANs eindeutig sein muß.

Bridges sind anders als der Router für die Endstationen vollkommen transparent. Die Endstation interessiert sich für die MAC-Adresse und somit für die Anwesenheit einer Bridge in keiner Weise. Nachfolgend will ich Ihnen die Funktionsweise einer Bridge etwas näher erläutern. Ich werde mich dabei auf das Wesentliche beschränken, da eine Darstellung im Detail den Rahmen dieses Buchs sprengen würde.

Eine Bridge kann als äußerst neugieriges Element im LAN bezeichnet werden, da sie sich jedes Paket im LAN ansieht. Man bezeichnet diese Arbeitsweise der Bridge auch als Promiscuous Mode.

10 Internetworking

Abbildung 10.2
Vereinfachter Da-
tentransport über
eine Bridge



Eine Bridge trifft ständig eine Entscheidung: Alle Pakete, die bei einer Bridge vorbeikommen, egal auf welchem Segment, müssen daraufhin überprüft werden, ob die einzelnen Pakete über die Bridge auf das andere Segment übertragen werden müssen oder nicht.

Die generellen Funktionselemente einer Bridge zur Durchführung seiner Aufgaben sind gemäß Standard IEEE 802.1d:

- Filtern und Weiterleiten von Paketen (Frames)
- Pflege von Adreß- und Filtertabellen und Durchführung entsprechender Filter- und Transportentscheidungen
- Managementfunktionen für die oben aufgeführten Funktionen

Die Kopplung von LAN-Segmenten über Bridges erfolgt auf MAC-Ebene. Daraus ergibt sich:

- Es erfolgt keine direkte Adressierung der Bridge durch die Endstation. Pakete zwischen Endstationen beinhalten als Zieladresse die MAC-Adresse der Empfängerstation, für die das Datenpaket bestimmt ist, und nicht die MAC-Adresse der Bridge.
- Verbindungsorientierter Dienst zwischen Brücken und Endstationen oder zwischen verschiedenen Brücken wird generell nicht unterstützt. Es erfolgt somit keine Empfangsbestätigung und Paketwiederholung. Diese Vorgänge müssen auf höherer Protokollebene geregelt werden.
- Alle MAC-Adressen in einem Netzwerk, das durch Bridges verbunden ist, sind eindeutig.

10.2 Bridge

- Die Topologie und die Konfiguration eines LAN mit Bridges dürfen keine Restriktionen für die MAC-Adressen der Endstationen mit sich bringen.
- Bei Ausfall einer Bridge-Verbindung muß die Unterstützung redundanter Wegpfade im LAN möglich sein, um das Netz funktionsfähig zu halten.

Auf einen Nenner gebracht heißt dies:

Ein Netz mit MAC-Bridges soll sich genauso verhalten, als ob es sich um ein großes gesamtes Netzwerk ohne Bridges handeln würde. Bridges müssen die entsprechenden Dienste unsichtbar erfüllen.

Damit eine Bridge die ihr gestellten Aufgaben erfüllen kann (vor allem das Weiterleiten von Paketen), muß sie wissen, was wo liegt. Hierzu ist in der Bridge ein Lernalgorithmus implementiert.

Fast jede der angebotenen Bridges unterstützt einen sogenannten Lernalgorithmus, mit dessen Hilfe die Bridge selbständig lernt, wo im LAN, d.h. in welchem Segment, sich die einzelnen Stationen befinden, wenn die MAC-Adresse des Empfängerfelds im Datenpaket interpretiert wird. Eine manuelle Konfiguration einer Bridge ist in diesem Falle nicht mehr notwendig und wäre auch viel zu aufwendig.

Die Bridge baut nach dem Einschalten automatisch eine Adreßtabelle auf. Wenn die Bridge auch noch Filterfunktionen unterstützen kann und muß, wird auch hierfür eine kleine Tabelle bzw. Datenbank aufgebaut und gepflegt. Diese Funktionen können über das Weiterleiten oder Vernichten von eingehenden Paketen entscheiden.

Die Bridge prüft jedes Datenpaket, das auf einem Port empfangen wird. Wie bereits erwähnt, muß die Bridge dies uneingeschränkt für alle eingehenden Pakete tun. Im Datenpaket wird die Source-Adresse geprüft. Befindet sich diese nicht in der Adreßtabelle, wird sie in die Adreßdatenbank eingetragen. Damit weiß die Bridge, auf welchem Port sich die eingetragene Quellstation befindet. In diesem Falle hätte die Bridge nur eine Tabelle, da die Quelladresse mit dem Port in Verbindung gebracht wird. Es gibt jedoch auch Bridges, die pro Port eine eigene Tabelle pflegen, da dadurch das Durchsuchen einfacher wird.

Eine Bridge kann immer nur individuelle Quelladressen erlernen und ist nicht in der Lage, Broadcasts und Gruppenadressen zu erlernen. Solche Adressen werden von der Bridge immer auf alle anderen Ports verteilt, außer wenn in die Bridge zum Beispiel ein besonderer Broadcast-Filter eingesetzt worden ist.

10 Internetworking

Nachdem wir nun wissen, wie eine Bridge die Stationen im LAN sukzessive erlernt, ist noch von Bedeutung, wie eine Bridge die Transportentscheidung für Pakete durchführt. Nach dem Lernprozeß einer Bridge wird für das Datenpaket die Transportentscheidung getroffen. Hierfür wird zusätzlich zur Quelladresse (Source) die Zieladresse (Destination) interpretiert. Befindet sich die Zieladresse in der Adreßtabelle, d.h., ein Datenpaket mit dieser Adresse ist bereits einmal eingetroffen und wurde von der Bridge gelernt, so ergeben sich mehrere Möglichkeiten:

1. Das Datenpaket ist auf dem gleichen Port eingegangen, der mit der Zieladresse assoziiert worden ist. In diesem Fall wird das Datenpaket als lokaler Datenverkehr erkannt und auf keinen anderen Port transportiert. Das Datenpaket wird einfach zerstört.
2. Das Datenpaket ist nicht auf dem Port, der mit der Zieladresse in Verbindung gebracht worden ist, angekommen. Somit wird das Datenpaket als segmentübergreifend erkannt und auf den Port weitergegeben, der mit der Zieladresse in Verbindung steht.
3. Wenn sich die Zieladresse hingegen nicht in der Adreßtabelle befindet, muß die Bridge das Datenpaket auf alle aktiven Ports weitertransportieren. Es ist einleuchtend, daß das Datenpaket nicht auf dem Port ausgegeben werden muß, auf dem das Datenpaket eingetroffen ist. Dadurch entsteht ein gewisser Overhead im gesamten Netzwerk.

Mit der Zeit kennt die Bridge alle Stationen im Netz, und die zusätzliche Belastung durch Weiterleiten nicht bekannter Zieladressen nimmt ab. Kritisch wird die Situation allerdings, wenn die Anzahl der Stationen im LAN größer ist, als die Tabelle an Einträgen aufnehmen kann. Darauf wird mit dem sogenannten Aging-Mechanismus reagiert. Nach einer gewissen Zeit werden ältere Einträge in der Tabelle gelöscht, wenn ein neuer Eintrag erfolgen muß und die Tabelle bereits voll ist.

Wichtig ist, daß mehrere parallel geschaltete Bridges oder LAN-LAN-Verbindungen mit Hilfe von Bridges mit mehreren Wegen von der Quelle zur Zielstation zu Loops führen. In diesem Fall würden Datenpakete unendlich im LAN kreisen und das Netz vollständig lahmlegen. Dieses Problem wird mit Hilfe eines Spanning-Tree-Algorithmus gelöst. Dieser dient dazu, genauso viele Bridges in Stand-by-Modus zu schalten, daß zwischen allen Stationen im LAN genau ein Weg existiert. Für den Fall, daß eine Bridge ausfällt, schaltet sich eine Bridge, die bislang im Stand-by-Modus lag, wieder zu.

10.2 Bridge

Bislang sind wir immer davon ausgegangen, daß die Entscheidung für den Weitertransport eines Pakets in der Bridge erfolgt. Für den Token-Ring gibt es jedoch ein anderes Verfahren, das vor allem von IBM eingesetzt wird. Es handelt sich um das Source-Routing-Verfahren.

Obwohl das Source-Routing-Verfahren theoretisch auch für Token-Bus und CSMA/CD-Netze eingesetzt werden könnte, ist es bislang nur für Token-Ring implementiert. Source Routing Bridges sind im Vergleich zu den anderen Bridges ziemlich dumm und lassen andere die Arbeit machen. Die Bezeichnung »Source Routing« ist eigentlich nicht ganz korrekt, da es sich nicht um Routing im eigentlichen Sinne handelt, vielmehr müßte man von »Source Bridging« sprechen. Um Source Routing implementieren und diesen Mechanismus auch erfolgreich durchführen zu können, müssen im Datenpaket zusätzliche Informationen eingetragen werden können. Es handelt sich dabei um folgende zusätzliche Felder: Routing Information Indicator und Routing-Information-Feld.

Beim Source Routing weiß die Quellstation, über welchen Weg, d.h. über welche Source Routing Bridges, das Datenpaket transportiert werden muß, um die Zielstation zu erreichen. Dieser Weg wird, solange sich an der Netzkonfiguration im laufenden Betrieb nichts ändert, von der Zielstation immer genutzt. Die Frage, die sich stellt, lautet: Woher kennt die Quellstation den Weg zur Zielstation? Ganz einfach – sie muß ihn erlernen. Ich will Ihnen nachfolgend diesen Lernalgorithmus für das Source Routing kurz beschreiben.

Angenommen, Station A will ein Datenpaket an Station B schicken. Station A sendet eine »Find«-Nachricht an alle Stationen im eigenen Ring, um feststellen zu können, ob die Zielstation im eigenen Ring existiert. Wird die Zielstation nicht im eigenen Ring gefunden, wird eine »Find-Broadcast«-Nachricht (Path-Explorer-Paket) über alle Bridges in alle Netze verschickt. Damit ist gewährleistet, daß das Datenpaket mit Sicherheit zur Zielstation kommt.

Jede Source Routing Bridge fügt dem Datenpaket im Routing-Information-Feld die notwendigen Angaben hinzu, um später den exakten Weg von der Quelle zum Ziel bestimmen zu können. Wenn das Datenpaket bei der Station B eintrifft, schickt diese das Paket unverändert in umgekehrter Richtung zurück. Da beim Einsatz mehrerer Bridges im LAN mehrere Datenpakete bei der Station B eintreffen, werden somit auch mehrere Datenpakete zur Station A zurückgeschickt. Die Station A nimmt das erste Datenpaket, das bei ihr von der Station B wieder eintrifft, auf und nimmt von nun an den im Datenpaket vorgefundenen Weg.

10 Internetworking

Source Routing vermeidet somit, daß Frames von den Bridges kopiert werden, obwohl diese eigentlich gar nicht weitertransportiert werden müßten. Das Source-Routing-Verfahren stellt einen wesentlichen Unterschied zu den anderen Bridges-Verfahren dar, in denen die Bridge erst das Datenpaket empfängt und danach entscheidet, ob es weitertransportiert werden muß oder nicht. Beim Source Routing sind die Wegwahltabellen von den Bridges in die Endstation verlagert.

Im Gegensatz zu klassischen Bridges entsteht beim Source Routing je nach Komplexität des Gesamtnetzes durch die Broadcast-Pakete beim Suchen eines Wegs von A nach B eine deutliche Erhöhung der Netzwerklast. Der Overhead beim Source Routing steigt genau dann, wenn viele Stationen senden. Das bedeutet andererseits steigenden Overhead bei steigender Nutzlast. Genau dann, wenn man im Netz den Overhead am wenigsten brauchen kann, steigt dieser rapide an. Eine andere Art der Kopplung von Netzen ist der Einsatz von Routern. Diese sollen im nächsten Abschnitt näher erläutert werden.

10.3 Router

Router gibt es schon länger als Bridges, da WANs in seinen Anfängen durch Vermittlungsknoten gekoppelt wurden, die Funktionalitäten eines Routers besaßen. Nach und nach wurden auch in LANs Router verwendet. Router der ersten Generation konnten allerdings immer nur ein Protokoll routen (TCP/IP, DECnet, IPX etc.). Wurden nun in einem LAN die verschiedensten Rechnerwelten mit den unterschiedlichsten Protokollen eingesetzt, bedeutete dies, für jedes routingfähige Protokoll einen eigenen Router zu installieren. Früher mußten dafür hohe Investitionen getätigt werden.

Mit der zunehmenden Notwendigkeit, LANs mit unterschiedlichen Protokollen zu betreiben, und der Entwicklung von MAC Layer Bridges verloren die Router immer mehr an Bedeutung, da sie nicht nur teurer (vor allem wenn mehr als ein Protokoll eingesetzt wurde), sondern auch weniger flexibel (ein Protokoll pro Router) waren als die MAC Layer Bridges. Denken Sie daran, daß sich Bridges durch ihre Protokolltransparenz auszeichnen. Durch die Weiterentwicklung und Verbesserung der Router in den vergangenen Jahren gewinnen diese Systeme jedoch wieder an Bedeutung, wenn es um die Kopplung von LANs geht, da Router im Vergleich zu Bridges einige große Vorteile bieten. Diese sind unter anderem:

10.3 Router

1. Aufgrund der verbesserten Architektur ist der Durchsatz eines Routers der neuen Generation mit dem einer Bridge vergleichbar.
2. Mit der zunehmenden Erweiterung von Netzen, also der Vernetzung von Netzen, und den unterschiedlichsten Endgeräten, die in ein Gesamtkonzept integriert werden müssen, steigt die Komplexität der Netzwerke derart, daß Bridges überfordert sein können. Mit Routern läßt sich eine wesentlich bessere Strukturierung mit geringerem Overhead durchführen.
3. Durch die Entwicklung von sogenannten Multi-Protokoll-Routern lassen sich ähnliche Ergebnisse erzielen, wie sie durch protokolltransparente Bridges erzielt werden können. Problematisch wird es allerdings, wenn Protokolle zum Einsatz kommen, die sich nicht routen lassen (z.B. NetBIOS oder LAT). Solche Protokolle können nur über Bridges transportiert werden. Auch hierfür gibt es inzwischen eine gute Lösung. Es handelt sich dabei um die sogenannten Brouter, die anschließend kurz betrachtet werden sollen.

Wie für Bridges gibt es auch für Router bestimmte Merkmale: Gemäß Definition stellen Router eine Verbindung zwischen zwei oder mehreren Subnetzwerken auf Ebene 3 des ISO/OSI-Schichtenmodells (Network Layer) her und realisieren somit die Funktionen bis zur Ebene 3 (Physical, MAC, LLC, Network). Eine zentrale Funktion der Ebene 3 ist die Wegwahl von der Sende- zur Empfängerstation. Router gehen somit etwas weiter als Bridges und müssen das Protokoll oberhalb der LLC-Ebene kennen und verstehen. Deswegen spricht man davon, daß Router protokollabhängig sind. Bekannte routingfähige Protokolle sind unter anderem:

- TCP/IP
- IPX
- XNS
- DNA
- X.25

Bezüglich der Wesensmerkmale bei den Restriktionserweiterungen für Subnetzwerke leisten Router dasselbe wie Bridges und erweitern diese Funktionalitäten auch noch in einigen Punkten.

1. Der Router erweitert die Grenzen eines Netzes hinsichtlich Stationenanzahl und Längenausdehnung, wie dies auch von Bridges gemacht wird. Wird ein Netzwerk durch einen Router in Subnetze aufgeteilt, kann jedes Subnetz wieder die volle Anzahl Stationen beinhalten und eine Längenausdehnung entsprechend dem vorgegebenen LAN-Standard aufweisen.

10 Internetworking

2. Router weisen eine Fehlerbegrenzung auf den Ebenen 2 und 3 auf. Fehlerhafte Pakete auf Data-Link-Ebene oder Datenpakete mit korrekter Data-Link-Ebene, aber fehlerhafter Netzwerkebene werden nicht in das andere Subnetzwerk transportiert. Somit bleiben die fehlerhaften Pakete im Subnetz ihres Entstehens beschränkt und wirken sich nicht negativ auf die anderen Subnetze aus. Zum Teil generieren Router sogar Fehlermeldungen mit dem Hinweis des Nichttransportierens. Eine Bridge führt so etwas nicht durch. Eine Bridge vernichtet ein als fehlerhaft erkanntes Paket, ohne etwas darüber zu »sagen«.
3. Der Router kümmert sich um die Prüfung eines Datenpakets zum Weitertransport erst dann, wenn man ihn explizit dazu auffordert. Das bedeutet auch, daß ein Router im Gegensatz zur Bridge nicht jedes Paket prüfen muß.
4. Ein wichtiges Unterscheidungsmerkmal zwischen Router und Bridge liegt darin, daß Router Wegwahl-Funktionen (Routing-Funktion) unterstützen, um zwischen Sender und Empfänger den günstigsten Weg zu nehmen, wenn dieser über Router erreichbar ist.
5. Bei einer Bridge wird das LAN in zwei Subnetze geteilt, wobei es aus der Perspektive der Bridge immer noch das gleiche große Netz bleibt. Bei einem Router hingegen wird das LAN in »echte« Subnetze mit unterschiedlichen Netzwerkadressen unterteilt. Es erfolgt also eine logische Unterteilung des Netzes in Subnetze. Dies ist auch der Grund, warum Router bei der Installation konfiguriert werden müssen, im Gegensatz zur Bridge, bei der man die beiden Segmente an die Bridge anschließt und in der Regel sonst nichts zu tun hat, außer die Bridge in Betrieb zu nehmen. Somit arbeitet man bei Routern, im Gegensatz zur Bridge, nicht mehr mit flachen MAC-Adressen, sondern mit Subnetzwerk-Hierarchien.

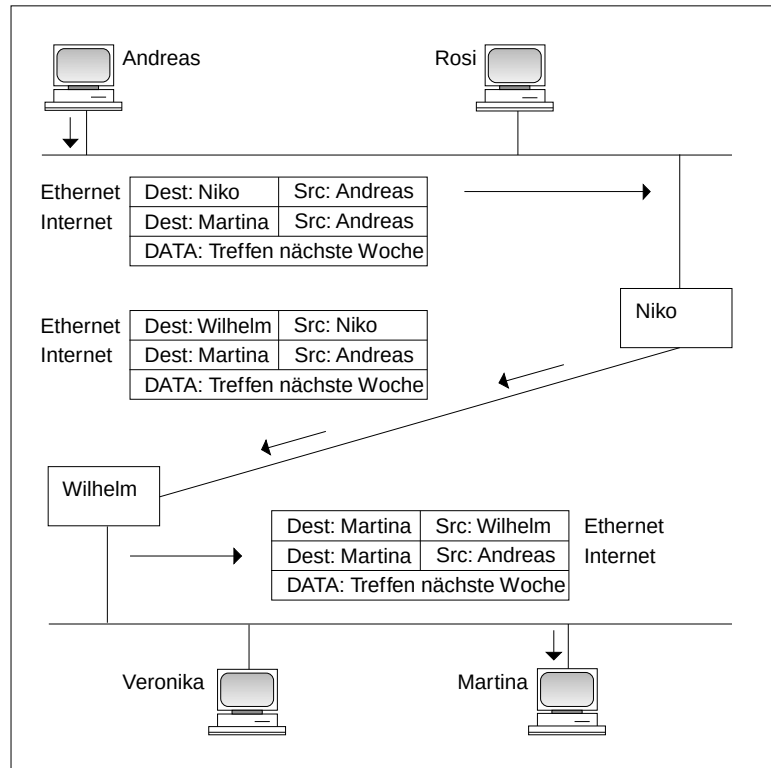
Aus all diesen Wesensmerkmalen läßt sich für den Router folgende Definition aufstellen:

Unter einem Router versteht man ein Koppellement, das unterschiedliche Subnetze auf Ebene 3 des ISO/OSI-Schichtenmodells verbindet. Wichtigstes Wesensmerkmal von Routern ist die Interpretation von Netzwerkprotokollen der Ebene 3. Deshalb ist der Router nicht protokolltransparent. Der Router führt eine optimierte Wegwahl zwischen Sender- und Empfangsstation durch. Außerdem unterteilt der Router das Netzwerk in logische Subnetzwerke. Alle Protokolle, die in den verbundenen Subnetzwerken eingesetzt werden, müssen vom Router verstanden werden, damit er in der Lage ist, bei Bedarf die Pakete in das jeweilige Zielnetzwerk zu transportieren. Durch die Nutzung der Netzwerkprotokolle ist der Router, bezogen auf die darunterliegenden Ebenen, »transparent«. Dies bedeutet auf

10.3 Router

der anderen Seite, daß die Schichten bis zur Ebene 2 ziemlich leicht ausgetauscht werden können. Ein Router verhält sich damit in diesem Fall ähnlich wie eine Bridge.

Abbildung 10.3
Adressierung beim
Router auf Ebene 2
und 3



Inzwischen gibt es eine Vielzahl unterschiedlicher Router mit den jeweiligen dem Bedarf entsprechenden Leistungsanforderungen und Möglichkeiten. Die wichtigsten Systeme sollen kurz aufgeführt werden, wobei zur Vertiefung auf die weiterführende Literatur verwiesen sei.

■ Einprotokoll-Router

Dies ist der einfachste aller Router. Er verliert immer mehr an Bedeutung, da in den heutigen LANs, die mit Routern gekoppelt werden, meist mehr als ein Protokoll eingesetzt wird. Dieser Router ist nur in der Lage, jeweils ein Protokoll zu verstehen.

■ Multiprotokoll-Router

Dieser Typ Router gewinnt aufgrund der LAN-Entwicklung immer mehr an Bedeutung, da man mit diesem System in der Lage ist, ein Koppellement einzubinden, das mehr als ein Protokoll ver-

10 Internetworking

stehen kann. Hierzu wird der Router mit Protokoll-Stacks ausgerüstet, d.h., es werden mehrere Ebene-3-Protokolle implementiert. Somit kann vermieden werden, pro eingesetztem Protokoll einen eigenen Router installieren zu müssen; vielmehr werden alle notwendigen Protokolle über ein Gerät bedient, sofern für den Router der entsprechende Protokoll-Stack zur Verfügung steht. Man sollte bei der Auswahl eines Routers darauf achten, ob sich dieser auch im nachhinein mit zusätzlichen Protokollen ausstatten läßt, wenn die Installation dies erfordert.

■ *Bridging Router (Brouter)*

Das ist ein System, welches sinnvoll in einer Umgebung eingesetzt werden kann, in dem sowohl routingfähige als auch nicht routingfähige Protokolle im Einsatz sind. Damit wird vermieden, Bridges und Router parallel einsetzen zu müssen. Alle Pakete, die nicht geroutet werden können (NetBIOS oder LAT), werden gemäß einer Bridge-Funktion behandelt und transportiert. Somit arbeitet der Brouter wieder im Promiscuous Mode, in dem alle Pakete zur weiteren Verarbeitung überprüft werden. Erst nachdem die entsprechenden Kontrollinformationen analysiert worden sind, kann entschieden werden, ob das Paket wie von einer Bridge oder einem Router kommend behandelt wird.

Anschließend soll noch kurz auf die Funktionsweise von Routern eingegangen werden, um die Beschreibung dieses Koppellements zu vervollständigen. Aufgrund der vorherigen Erläuterung dürfte klar sein, daß ein Router im Vergleich zur Bridge nicht alle Pakete, die bei ihm vorbeikommen, auf Routing-Notwendigkeit überprüfen muß, sondern daß er sich nur um die Pakete kümmert, die direkt an den Router adressiert sind. Der Router ist somit für das Netzwerk im Vergleich zur Bridge nicht mehr transparent.

Die prinzipielle Aufgabe eines Routers ist, zwischen zwei kommunikationswilligen Endsystemen auf Netzwerkebene eine Ende-zu-Ende-Verbindung herzustellen. Um die notwendige Verbindung von Endgeräten in verschiedenen Subnetzwerken auf Netzwerkebene zu leisten, muß ein Router eine Vielzahl von Basisbestandteilen implementiert haben:

- Einen Mechanismus für Stationen (Endgeräte), um sich dem Router gegenüber zu identifizieren und umgekehrt.
- Einen Algorithmus für nichtlokale Datenpakete, damit der nächste Router ausgewählt werden kann, der das Datenpaket empfangen soll. Dieser Algorithmus wird als Routing bezeichnet. Daher auch die Bezeichnung Router für das Koppellement.
- Verwaltung einer Routing-Tabelle, um Informationen über Routing-Wege und Filterfunktionen speichern zu können.

10.4 Gateway

- Sammlung von Informationen, um die Routing-Tabellen aktualisieren zu können.
- Weitergabe von Informationen an andere Router, damit diese in der Lage sind, die Routing-Tabellen zu pflegen. Dieser und der vorherige Punkt sind dafür verantwortlich, daß Router einen gewissen Overhead erzeugen. Das hängt stark vom verwendeten Routing und von Router-Protokollen ab.
- Ein Router muß die jeweiligen Verbindungswege berechnen und deren Existenz aufrechterhalten. Hierzu gehört vor allem auch die Entscheidung, ob ein Datenpaket überhaupt weitertransportiert werden muß. Wenn dies der Fall ist, muß der Router wissen, wohin das Paket soll.

Wir haben bereits erfahren, daß Bridges im Lauf der Zeit die einzelnen Stationen (MAC-Adressen) im LAN kennen. Ein Router kennt nicht die einzelnen Stationen im Netzwerk, sondern weiß nur von der Existenz der einzelnen Netzwerke. Deshalb ist es bei der Kopplung von Subnetzen mit Routern erlaubt, daß in den gekoppelten Subnetzen die gleichen MAC-Adressen vorhanden sind.

10.4 Gateway

Die Installation von Netzwerken bereitet inzwischen keine allzu großen Probleme mehr, sofern es sich um eine homogene Welt handelt. Wer nur PCs miteinander vernetzen will, kann dies bei vernünftiger Planung in relativ kurzer Zeit durchführen. Anders sieht die Angelegenheit jedoch aus, wenn neben PCs auch noch Apple-Macintosh-Rechner, Unix-Systeme oder gar andere Netzwerke integriert werden sollen. Es kann sich dabei entweder um Großrechnernetzwerke, wie zum Beispiel IBM SNA, Siemens Transdata, oder die Verbindung zu anderen Netzwerken unter Einbeziehung der Telekom-Dienste, z.B. Datex-P, Datex-L, HfD, T1 oder auch ISDN, handeln.

Sobald Sie ein heterogenes Netzwerk bilden wollen, fängt die Suche schon an, wie Sie eine sinnvolle und funktionsfähige Kopplung bzw. Integration dieser heterogenen Struktur realisieren können. Wie Sie bereits gesehen haben, kann eine Kopplung von Netzwerken entweder über Bridges, Router, Brouter oder – was uns in diesem Abschnitt interessiert – Gateways durchgeführt werden.

Bei der Weiterentwicklung der Netzwerktechnologie war es schon immer ein besonderes Problem, aber auch immer eine interessante Aufgabe, die Kopplung von Netzwerken durchzuführen, vor allem dann, wenn es sich um Netzwerke unterschiedlicher Hersteller handelte. Die einzelnen Hersteller neigen leider dazu, eigene Protokolle und Zeichensatzdarstellungen in ihren Netzwerken zu verwenden.

10 Internetworking

Die Aufgabe von Gateways ist es letztendlich, diese unterschiedlichen Welten einander näherzubringen, so daß der Anwender ohne großen Aufwand von einem Netzwerk in das andere Netzwerk kommen kann, und das alles unter dem Aspekt, die Transparenz für den Endanwender zu erhalten.

Die Kopplung von mehreren unterschiedlichen Netzwerken verlangt mehr Intelligenz, als man das von festverdrahteten Einrichtungen gewohnt ist. Um diese Intelligenz auch aufbringen zu können, erfordert das Gateway immer den Einsatz eines Rechners, der die gestellten Anforderungen und Leistungen auch erbringen kann. Deshalb werden Rechner, die mit mehreren Kommunikationssystemen zusammenarbeiten und somit Komponenten mehrerer Netzwerke sind, als Gateway bezeichnet.

Aus den bisherigen Ausführungen ist bereits ersichtlich, daß ein Gateway nicht nur die reine Verbindung zwischen Netzwerken übernimmt, so wie dies für einen klassischen Repeater der Fall ist. Eine Forderung, die beim Einsatz von Gateways aufgestellt wird, ist die bleibende Unabhängigkeit der Netzwerke, die über das Gateway miteinander verbunden werden. Es ist in der Praxis fast unmöglich, zur Erleichterung des Netzwerkverbunds die Protokolle und Nachrichtenübermittlungskomponenten aller im Verbund teilnehmenden Komponenten zu ändern und auf den gleichen Stand zu bringen. Versuchen Sie das mal bei einer Kopplung zwischen IBM-SNA-Netzwerken und DEC-Netzwerken. Um diese beiden Systeme zueinanderzubringen, benötigen Sie teure und leistungsfähige Gateways.

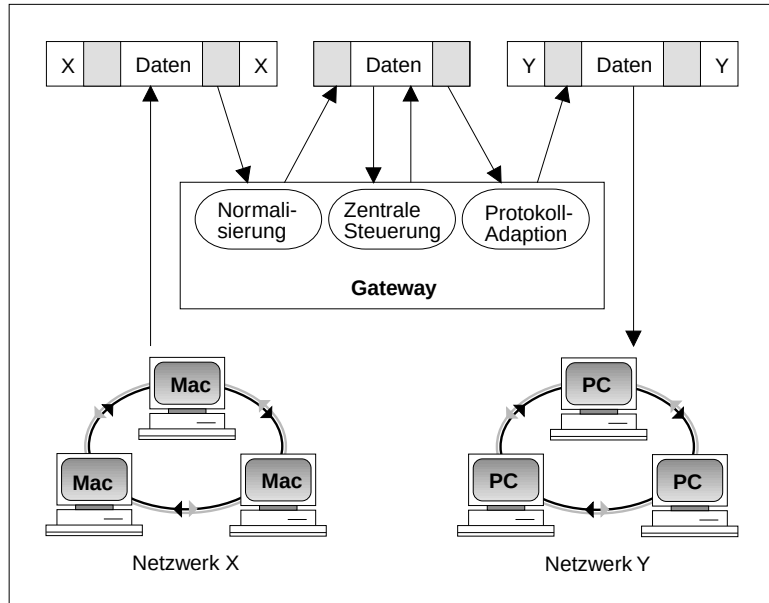
Durch die Forderung der Unabhängigkeit der Netze im Verbund ist es notwendig, daß das Gateway den für den Internet-Verkehr notwendigen Kommunikationsmechanismus über eine Knotenrechnerfunktion übernimmt. Das Gateway kann somit auch als Knotenrechner bezeichnet werden. Die Aufgaben, die damit verbunden sind, werden wie folgt festgelegt:

- Adreßinterpretation und Routenwahl (Wegfindung)
- Flußsteuerung und Fehlerbehandlung
- Fragmentierung und Reassemblierung bei ungleichen Framegrößen für die Nachrichten- oder Paketlängen in den einzelnen Netzen

Um die Unabhängigkeit der zu koppelnden Netzwerke bewahren zu können, ergibt sich eine weitere Aufgabe, die vom Gateway erfüllt werden muß. Das Gateway muß die in den einzelnen Kommunikationssystemen vereinbarten und eingesetzten Übertragungsprotokolle vollständig gegeneinander isolieren. In der nachfolgenden Abbildung ist dargestellt, wie dies in etwa aussehen kann.

10.4 Gateway

Abbildung 10.4
Funktionsweise
eines Gateway



Handelt es sich um Nachrichten für das Übernetz, dann wird der Rahmen für das Zwischennetzprotokoll in die Protokollrahmen der jeweils durchlaufenden Einzelnetze eingebettet. Somit wird es vom Kommunikationssystem als Teil der zu übermittelnden Nutzdaten betrachtet und auch nicht interpretiert.

Die Aufgaben, die das Gateway zu erfüllen hat, sind:

- Den alten Protokollrahmen des übergebenden Kommunikationssubsystems zu entfernen,
- die Adressierung und weitere Informationen des Zwischennetz-Protokollrahmens zu interpretieren und
- aus diesen Informationen für die Weiterleitung einen neuen Protokollrahmen aufzubauen, der entsprechend den Anforderungen des nächsten Kommunikationssubsystems aufgebaut sein muß.

Ein weiteres Problem besteht in der Adressierung, um Daten in ein anderes Netzwerk transportieren zu können. Man unterscheidet hierbei in der Regel zwei Möglichkeiten, die eingesetzt werden können:

- laufwegorientierte
- hierarchische Adressierungsmethode

Bei der laufwegorientierten Adressierung werden die Adressen der zu durchlaufenden Gateways jeweils nach den Konventionen des gerade für den Weitertransport zuständigen Einzelnetzwerks in der

10 Internetworking

Reihenfolge des Gesamtlaufwegs miteinander verkettet. Auf diese Weise wird die vollständige Adresse gebildet. Die zentrale Steuerung eines jeden Gateways entnimmt dann aus dieser Adreßkette die jeweils nächste benötigte Teiladresse. Im neu generierten Teilnetz-Protokollrahmen benutzt sie diese zur Adressierung, um das Paket zum nächsten Gateway oder zum Ziel-Host zu transportieren.

Bei der hierarchischen Adressierung werden hingegen nur zwei Adreßangaben genutzt:

- die Adresse des Teilnetzes, an dem der Ziel-Host angeschlossen ist, und
- die Hostadresse des Ziel-Hosts in diesem Teilnetz.

Jedes Gateway des Übernetzes verfügt über eigene Wegtabellen. Mit Hilfe dieser Tabellen wird die hierarchische Adresse ausgewertet:

- Ist das Ziel-Teilnetz nicht an dieses Gateway angeschlossen, sendet das Gateway das Datenpaket entsprechend seinem Laufwegalgorithmus an den nächsten zuständigen Gateway-Rechner.
- Im zweiten Fall wird das Datenpaket an den Ziel-Host weitergereicht.

Die Erfahrung zeigt, daß es sich bei der zweiten Methode um die günstigere handelt, da man von einer definierten Länge der Gesamtadresse ausgehen kann, denn diese besteht immer aus zwei Feldern. Die zweite Methode ist auch bezüglich der Wegfestlegung (Routing) wesentlich besser.

Die laufwegorientierte Adressierung impliziert notwendigerweise bereits bei der Generierung der Gateway-Software eine zentrale Festlegung der Laufwege. Dadurch wird eine spätere Änderung bei neuen Anforderungen, zeitweisen Ausfällen oder Überlastsituationen von Teilnetzen erschwert. Bei der hierarchischen Adressierung hingegen ist eine dynamische Wegwahl und Wegadaption möglich. Ich will nachfolgend auf weitere Aspekte eingehen, die für den Einsatz von Gateways relevant sind.

Protokollanpassung

Ich habe bereits mehrfach darauf hingewiesen, daß Gateways dafür eingesetzt werden, unterschiedliche Netzwerke miteinander zu verbinden, in denen auch verschiedene Protokolle eingesetzt werden. Es kann zum Beispiel die Aufgabe eines Gateways sein, zwei höhere Protokollebenen miteinander zu koppeln oder einen File-Transfer zwischen den Netzwerken zu ermöglichen. Solche Gateways werden Sie benötigen, um Internetworking mit unterschiedlichen Technologien zu ermöglichen. Dies ist auch dann der Fall, wenn Sie LANs

10.4 Gateway

und WANs nutzen wollen, damit ein Datenaustausch zwischen diesen ermöglicht wird bzw. Netzwerke über WANs miteinander gekoppelt werden.

Bei einem File-Transfer ist es aber unter Umständen auch notwendig, eine Code-Konvertierung durchzuführen. Das gleiche muß übrigens auch erfolgen, wenn Sie Terminalemulation einsetzen und diese auf unterschiedlichen Systemen erfolgt. Eine Darstellung der 3270 Emulation auf einem PC oder einem DEC-Terminal erfordert einige Anpassungen. Gelangen Daten von einem Netzwerk in ein anderes Netzwerk, in dem auch noch andere Zeichendarstellungen gewählt werden, müssen diese adaptiert werden. Beim File-Transfer zwischen PC und IBM-Großrechner zum Beispiel muß die zu übertragende Datei von EBCDIC-Code in den ASCII-Code konvertiert werden und umgekehrt, je nachdem in welche Richtung der Datentransfer (Download, Upload) erfolgt.

Anpassung der Paketgröße

Bei der Kopplung von Netzwerken mit unterschiedlichen maximalen Paketgrößen besteht die Aufgabe des Gateways auch noch darin, das eingehende Datenpaket entsprechend zu fragmentieren, um es dann im anderen Netzwerk übertragen zu können. Das Gateway muß also unter Umständen aus einem eingehenden Datenpaket mehrere kleinere Datenpakete bilden und gewährleisten, daß diese beim Empfänger auch wieder in der richtigen Reihenfolge eintreffen.

Für die Kopplung von Netzwerken werden Ihnen die unterschiedlichsten Gateways angeboten, in Abhängigkeit von den Netzwerken, die Sie miteinander koppeln wollen, und vor allem in Abhängigkeit von den Kommunikationsdiensten, über die die Kopplung erfolgen soll. Ich will in diesem Abschnitt bewußt nicht auf einzelne Produkte eingehen, da es von der jeweiligen Situation und dem eingesetzten Netzwerkbetriebssystem abhängt, welche Alternativen zur Verfügung stehen.

Bei der Entscheidung für den Einsatz von Gateways muß vorher immer genau geklärt werden, wie die Systemumgebung aussieht und was mit dem einzusetzenden Gateway gelöst werden soll. Hierbei muß noch in Betracht kommen, ob Sie die Kopplung über Telekom-Dienste realisieren wollen oder ob die Kopplung lokal innerhalb Ihres Unternehmens zu erfolgen hat.

Abschließend sei noch angeführt, daß das Gateway bezogen auf das ISO/OSI-Schichtenmodell auf der obersten Ebene (Ebene 7) aufsetzt, somit alle Ebenen durchlaufen werden müssen und das Gateway somit das komplexeste aller Koppelemente darstellt.

10.5 Layer-2-Switch

Die neuen Techniken in LANs, schnellere Rechner, schnellere Server und immer anspruchsvollere Anwendungen, führten dazu, daß die Performance in bestimmten Fällen schlechter wurde. Das liegt allerdings auch darin begründet, daß im LAN ständig weitere Benutzer integriert und aufgrund der Zunahme der Datenlast die Bandbreiten im Netzwerk immer kleiner werden. Daher überlegt man, ob man im LAN nicht bereits mit 100 Mbit/s oder mehr bis zum Arbeitsplatz arbeiten soll. Damit verbunden ist natürlich auch die Tatsache, daß aufgrund des erhöhten Datenaufkommens und der großen Anzahl von Benutzern die Übertragungszeiten im LAN geringer werden. Da mit einer vorgegebenen Bandbreite im LAN natürliche Grenzen vorgegeben sind, ist ein weiterer Ausbau und der Einsatz datenintensiver Anwendungen nicht möglich. Die oben aufgeführten Probleme treten aber auch dann auf, wenn das LAN im klassischen Sinn als Shared Medium aufgebaut ist. Dies trifft für alle klassischen LAN-Installationen zu, egal ob es sich um Ethernet-, Token-Ring- oder FDDI-Netzwerke handelt. Alle Netzwerknutzer müssen sich die gemeinsame Bandbreite im Netzwerk teilen. Wenn dann noch der oder die Server im gleichen LAN-Segment installiert sind, auf die alle Anwender zugreifen wollen, nimmt die Performance mit Sicherheit stetig ab. Ebenso kritisch ist die Situation, wenn Netzwerke miteinander gekoppelt werden.

Man hat deshalb nach Wegen gesucht, um die Bandbreitennutzung zu verbessern und dadurch den Durchsatz im gesamten LAN zu steigern. Bereits vor Jahren wurden im Ethernet-Bereich von der Firma Kalpana entsprechende Entwicklungen durchgeführt. Durch die rasche Weiterentwicklung im ATM-Bereich verstärkte dieser Trend sich noch. Die Rede ist in diesem Zusammenhang von der Switching-Technologie. Durch die LAN-Switching-Technik wurden Wege gefunden, um Datenpakete zwischen Sender und Empfänger mit der vollen Bandbreite zu transportieren, d.h., die Datenpakete können zwischen einer Vielzahl von Ports gleichzeitig vermittelt werden. Jedem Port wird auf diesem Weg die volle Bandbreite verfügbar gemacht. Betrachtet man die Arbeitsweise von Bridges und Routern, dann stellt man fest, daß die Koppelemente durch Software realisiert werden. Bei den Switches hingegen wird der größte Teil der Transportfunktion auf Hardwarebasis implementiert. Durch die Hardware-Implementierung kann eine wesentlich höhere Performance erreicht werden. Zudem kann man davon ausgehen, daß die Kosten pro Port dadurch stark reduziert werden können.

10.5 Layer-2-Switch

Bei näherer Betrachtung der am Markt befindlichen Switches können zwei Techniken unterschieden werden: Cut-Through-Switches und Store-and-forward-Switches.

Cut-Through-Switches

Bei einem Cut-Through-Switch wird das Datenpaket zum Zielport transportiert, sobald die Zieladresse im Header des Datenpakets erkannt wird. Bei diesem Verfahren hat man den Vorteil, daß die Verzögerungszeit zum Weitertransport des Datenpakets sehr gering ist, unabhängig davon, wie lang das Datenpaket ist. Ein Nachteil ist darin zu sehen, daß Fehler im Datenpaket nicht erkannt werden können, da bereits beim Erkennen der Zieladresse mit dem Weitertransport begonnen wird, und somit keine CRC-Prüfung, wie dies in der Regel auf Ebene 2 des Schichtenmodells definiert ist, durchgeführt werden kann. Somit wird ein eventuell fehlerhaftes Paket an den Empfänger transportiert, sofern es tatsächlich der richtige Empfänger ist und der Fehler nicht im Feld der Zieladresse aufgetreten ist. Stellt nun der Empfänger aufgrund der Prüfung des CRC-Feldes fest, daß ein fehlerhaftes Datenpaket übertragen worden ist, wird dieses verworfen. Auf den höheren Protokollebenen wird erkannt, daß auf ein gesendetes Datenpaket keine Reaktion erfolgt, und das Datenpaket wird erneut gesendet. Es muß sich dann jedoch um gesicherte Protokolle handeln (z.B. IPX, TCP oder DECnet). Bei unsicheren Protokollen, wozu UDP, LAT oder auch netBOIS zählen, kann der Verlust eines Datenpakets zu einem Abbruch der Kommunikation führen.

Cut-Through-Switches sind auch nicht in der Lage, unterschiedliche Netzwerke miteinander zu verbinden, d.h. den Übergang von zum Beispiel Ethernet auf Token-Ring oder FDDI durchzuführen. Der Übergang auf eine andere Netzwerktopologie erfordert, daß das Datenpaket vollständig eingetroffen sein muß, um dann für die andere Topologie konvertiert werden zu können. Ebenso sind Cut-Through-Switches nicht in der Lage, Filtermechanismen zu realisieren, da auch diese Mechanismen den vollständigen Empfang des Datenpakets erfordern, um dann die gesetzten Filter zu prüfen, die entscheiden, ob das Datenpaket transportiert wird oder nicht.

Store-and-forward-Switches

Diese doch sehr einschränkenden Funktionen haben dazu geführt, Switches auf Basis der Store-and-forward-Technik zu entwickeln. Bei einem Store-and-forward-Switch wird ein eingehendes Paket vollständig zwischengespeichert. Da nun ein Datenpaket vollständig im Puffer vorliegt, können nicht nur notwendige Filterfunktionen für

10 Internetworking

diese Switches implementiert werden, sondern die Switches dienen auch dazu, unterschiedliche Topologien miteinander zu koppeln. Dieses Verfahren hat jedoch den Nachteil (im Vergleich zum Cut-Through-Switch), daß die Verarbeitungszeiten etwas höher sind und daß alles in Abhängigkeit der Paketlänge zu sehen ist. Erinnern Sie sich daran, warum ATM-Switches mit enorm hohen Durchsatzraten aufwarten können: Es werden immer gleich lange Zellen für den Datentransport genutzt.

In der Praxis haben Meßergebnisse gezeigt, daß Store-and-forward-Switches ihre Stärke im Backbone-Bereich voll ausnutzen können. Da in der Regel Backbone-Systeme auch noch einen Topologieübergang ermöglichen müssen, kommt hierfür nur ein Store-and-forward-Switch in Frage.

Die Cut-Through-Switches sind gut geeignet für Netzwerkumgebungen mit einem sporadischen Datenverkehr und einer gleichen Topologieumgebung – d.h., wenn keine unterschiedlichen Netzwerkstrukturen verwendet werden, sondern z.B. nur Ethernet oder Token-Ring.

Alle renommierten Hersteller sind inzwischen in der Lage, für alle Topologien passende Switches zur Verfügung zu stellen, egal ob es sich dabei um Ethernet-, Token-Ring-, FDDI- oder ATM-Switches handelt. Entsprechende Netzwerkübergänge zwischen diesen LAN-Strukturen werden ebenfalls unterstützt.

Im Zuge der Switching-Technologie hat sich ein weiterer Bereich herauskristallisiert, der immer mehr an Bedeutung gewinnt. Die Rede ist vom Aufbau sogenannter Virtueller Netze bzw. Virtueller LANs, die sich durch den Aufbau und den Einsatz von Switches realisieren lassen.

Virtuelle Netze

Beim Aufbau klassischer LANs werden Endgeräte immer in einem bestimmten LAN-Segment installiert. Dieses Segment ist über eine Bridge oder über einen Router mit dem Gesamtnetzwerk verbunden. Wird dieses Endgerät an einem anderen Standort installiert, weil beispielsweise der Benutzer ein neues Büro bekommen hat, bedeutet dies auch, daß der Anwender mit seinem PC in einem anderen Segment eingebunden ist. Damit können sich bezüglich Performance, Belastung oder Anschlußtechnik neue Bedingungen ergeben. Dies kann auch bedeuten, daß der Zugriff auf ursprünglich direkt vor Ort befindliche Ressourcen über mehrere Koppelelemente erfolgen muß. Mit Virtuellen LANs (VLANs) können dynamisch konfigurierbare LANs gebildet werden. Es ist somit möglich, die Zugehörigkeit von

10.6 Layer-3-Switch

Endgeräten zu einer Workgroup frei zu definieren. Dann ist es vollkommen egal, wo das Endgerät des Benutzers installiert wird, da die Anpassung des Virtuellen LAN die Möglichkeit zur Verfügung stellt, das Endgerät, egal wo dieses installiert ist, der bisherigen Workgroup zuzuordnen. In einem Virtuellen LAN kann ein Endgerät somit seinen physischen Ort wechseln und dennoch Mitglied der ursprünglichen Workgroup bleiben. Die einzelnen Nutzer einer Workgroup sind also ortsunabhängig. Andererseits kann der Nutzer einer neuen Workgroup zugewiesen werden, wenn es das Aufgabengebiet erfordert, ohne daß physikalische Änderungen im Netzwerk durchgeführt werden müssen. Die Anpassung und Modifikation der VLANs wird in der Regel über die vom Hersteller zur Verfügung gestellte Netzwerkmanagement-Software durchgeführt. Eine gut konzipierte Netzwerkmanagement-Software erlaubt die Rekonfiguration der VLANs durch einfache Drag&Drop-Funktionen.

Ein weit verbreitetes Einsatzgebiet von Switches ist das der Collapsed Backbones. Da in vielen modernen Switches die internen Switching-Strukturen auf Basis von ATM aufgebaut werden, wird dadurch auch die Migration zu ATM wesentlich erleichtert.

Bei der Planung und dem Aufbau von LANs ist nur darauf zu achten, Switching-Komponenten zu verwenden, die erweiterbar, zukunftssicher und entsprechend leistungsfähig sind. In diesem Zusammenhang ist es nicht nur von Bedeutung, wie viele Einschübe ein Switch besitzt und welche unterschiedlichen Einschübe hierfür zur Verfügung gestellt werden können, ein wesentlicher Anhaltspunkt ist auch die gesamte Leistungsfähigkeit des Backplane, um auch tatsächlich die Summe der angeschlossenen Endgeräte bzw. LANs bedienen zu können, ohne Leistungseinbußen zu erleiden. Man sollte also darauf achten, daß der Backplane mit Übertragungsraten in einer Größenordnung von über 2 Gbit/s arbeiten kann. In Abhängigkeit der zu koppelnden LANs und Endgeräte können auch noch leistungsfähigere Backplanes benötigt werden.

10.6 Layer-3-Switch

Zu Beginn der LAN-Kopplung wurden Bridges eingesetzt. Der Einsatz dieser Bridges war damals sehr geeignet, da diese Koppellemente relativ einfach zu handhaben sind. Nachteilig war, daß Bridges kaum skalierbar sind. Als nächste Generation der Koppellemente kamen die Router auf den Markt, um damit die Skalierbarkeit durchführen zu können – jedoch waren Router langsam und komplex. Dies war in Ordnung, solange man sich an die 80/20-Regel halten konnte. Die 80/20-Regel besagt, daß 80% des Datenverkehrs im eigenen lokalen

10 Internetworking

Netzsegment bleiben und nur 20 % des Datenverkehrs segmentübergreifend durchgeführt werden. Als jedoch die Netzwerke immer größer wurden, stiegen auch die Anforderungen an die verfügbaren Bandbreiten. Dadurch gewinnen Switches immer mehr an Bedeutung und ersetzen dadurch Shared-Media-LANs. Dies geschah auch unter dem Aspekt, daß Ressourcen wie Server, Gateways etc. nicht mehr im lokalen Segment installiert sind, sondern zentral im Backbone integriert werden und somit die 0/100-Prozent-Regel zum Tragen kommt. Damit wird zum Ausdruck gebracht, daß 100 % des Datenverkehrs zwischen den Clients und den Servern über das Koppellement zum Backbone übertragen werden müssen. Dadurch wird ersichtlich, daß die Verzögerungszeiten, die in Routern, die das Etagen-LAN mit dem Backbone verbinden, auftreten, eine immer größere Bedeutung bekommen und gelöst werden müssen. Zu Beginn der Entwicklungen ging man davon aus, daß der Ersatz von Shared-Media-Hubs durch Switching-Hubs und die Kopplung der Etagen-LANs mit dem Backbone mit Hilfe von herkömmlichen Routern durchaus ausreichend wäre. Man ist mit dieser Art von Netzkopplung im Etagenbereich zwar schnell, jedoch leidet man dann immer noch an Performance-Engpässen im Router-Übergang.

Man kam somit auf die Idee, die Performance nicht nur auf Ebene 2 durch die Switching-Technik zu erhöhen, sondern die gleichen Performance-Vorteile auf Ebene 3 zu erzielen, d. h., es begann die Entwicklung von Layer-3-Switches. Zu beachten ist dabei nur, daß von Herstellern Layer-3-Switches angeboten werden, die in Wirklichkeit nicht in diese Kategorie gehören – dadurch werden Endanwender ziemlich verunsichert.

Obwohl es mindestens ein Dutzend »Pre-Standard«, »Quasi-Standard« und herstellerspezifische Typen von Layer-3-Switch-Technologien gibt, lassen sich jedoch zumindest drei Klassen definieren: ASIC-basierendes Routing, Cut-Through-Routing und Label Swapping. Bevor jedoch näher auf einzelne Techniken eingegangen werden soll, möchte ich noch kurz auf einen Begriff eingehen, der oft mit Layer-3-Switching verwechselt bzw. in einem falschen Zusammenhang erläutert wird. Es geht in diesem Zusammenhang um Layer-3-VLANs.

Vor einiger Zeit haben die Hersteller bereits erkannt, daß LAN-Switches unter dem gleichen Problem leiden, wie es bereits von Bridges bekannt ist, da Switches ebenso auf Ebene 2 des ISO-Modells arbeiten. (Switches sind, wie bereits erwähnt, sehr schnelle, hardwarebasierende Bridges.) Um dieses Problem besser in den Griff zu bekommen, hat man die VLAN-Technologie eingeführt, um dadurch eine Segmentierung und die Einrichtung von Broadcast-Domänen zu ermöglichen. Der Aufbau von VLANs ist im Prinzip bei allen Herstel-

10.6 Layer-3-Switch

lern gleich – es handelt sich um eine Layer-2-Broadcast-Domäne. Der Datenverkehr wird weitergeleitet durch die angegebene MAC-Adresse. Broadcast-, Multicast- und Unknown-Unicast-Datenverkehr bewirkt ein »Fluten« des VLAN. Zum Aufbau von VLAN-Topologien wird innerhalb des VLAN das Spanning-Tree-Verfahren eingesetzt. Die Implementierung von VLANs der einzelnen Hersteller unterscheidet sich in der Art und Weise, wie sich diese bei den einzelnen Produkten implementieren lassen. Da VLANs innerhalb von LAN-Switches implementiert werden und einige VLANs zum Einrichten Layer-3-Kriterien verwenden, schließt man daraus, daß es sich somit auch um einen Layer-3-Switch handeln muß. Diese Schlußfolgerung ist falsch; das Switching im VLAN erfolgt immer auf Layer 2. Der Übergang von einem VLAN zu einem anderen muß durch den Einsatz eines Routers (spezieller VLAN-Router) erfolgen. Wenn VLANs Layer-2-Broadcast-Domänen sind, dann ist ein Layer-3-Frame-Forward-Mechanismus notwendig, um VLANs untereinander zu verbinden – Routing übernimmt diese Aufgaben.

Die Idee bei Layer-3-Switching besteht darin, wesentlich höhere Performance-Eigenschaften zu erreichen, als mit herkömmlichen Router-basierenden Netzwerken erreicht werden können. Die erste Form für das Layer-3-Switching bestand im ASIC-basierenden Routing, um einfach diese Beschränkungen zu umgehen, ohne auch noch neue Protokolle oder Standards einführen zu müssen. Im ASIC-basierenden Routing ist die Frame-Forwarding-Komponente des konventionellen Routing-Modells in einem ASIC (Application-Specific Integrated Circuits) implementiert, statt auf Basis einer Software-realisation (so wie dies bereits auch für Layer-2-Switching der Fall ist). Die Route-Discovery und Service/Name-Advertisement-Funktionen, die im Prinzip nicht zeitkritisch sind, werden nach wie vor durch Software realisiert.

Die Vorteile von ASIC-basierendem Routing ergibt sich vor allem aufgrund der Tatsache, daß es sich immer noch um herkömmliches Routing handelt, nur schneller und billiger. Hierzu zählen:

1. Die Möglichkeit, konventionelle Routing-Protocol-Stacks ohne Modifikation einzusetzen, z.B. RIP, RIP II, OSPF, IP, IPX, IP Multicast, IGMP, BGP 4 etc.
2. Die Kompatibilität zu existierenden Routern und Endgeräten bleibt erhalten.
3. Sehr hohe Geschwindigkeit und sehr niedriger Preis bei der Implementierung.

Es sei an dieser Stelle darauf hingewiesen, daß Flow-based Cut-Through-Routing und Address-based Cut-Through-Routing Techniken zur Verfügung stehen, die meist im Zusammenhang mit ATM-

10 Internetworking

Netzwerken eingesetzt werden. Berücksichtigt werden muß bei diesen Techniken auch, ob es sich nicht um proprietäre Lösungen des Herstellers handelt und damit die Kompatibilität zu anderen Herstellern verlorengelht, was beim klassischen ASIC-basierenden Routing nicht der Fall ist

Da in diesem Kapitel die Wissensgrundlagen für die Kopplung von Netzwerken geschaffen worden sind, sollen im nächsten Abschnitt die Möglichkeiten aufgezeigt werden, LANs über öffentliche Datendienste miteinander zu verbinden.

11

Rechnernetze – Basis der Kommunikation

Ein Rechnernetz ist ein Verbund von räumlich getrennten Rechnern oder Gruppen von Rechnern zum Zweck des Datenaustauschs und der Zusammenarbeit dieser Rechner. Das Rechnernetz dient also im wesentlichen der Verbindung zu einem Gesamtsystem. Im folgenden sollen die diesbezüglich wichtigsten Aspekte näher betrachtet werden.

- Datenverbund** Unabhängig vom Ort der Speicherung steht die Menge der Daten der Gesamtheit der Rechner zur Verfügung. Die Bearbeitung der Daten erfolgt unabhängig von den unterschiedlichen Applikationen. Dadurch wird eine Datenredundanz vermieden, es muß aber eine sorgfältige Pflege der Daten gewährleistet sein.
- Funktionsverbund** Hierunter versteht man die Bereitstellung von erweiterten Funktionen für die angeschlossenen Arbeitsplätze in Form von Spezialrechnern, Peripheriegeräten, Speicherplatz usw., auf die mit Hilfe des Rechnernetzes zugegriffen werden kann.
- Verfügbarkeitsverbund** Durch diesen Mechanismus wird die Verfügbarkeit des Gesamtsystems gesteigert bzw. bei verminderter Leistungsfähigkeit des Gesamtsystems durch den Ausfall mehrerer Komponenten der volle Leistungsumfang im Rechnernetzwerk aufrechterhalten.
- Leistungsverbund** Mit Hilfe des Netzwerks können komplexe oder aufwendige Probleme auf mehrere Rechner verteilt werden. Voraussetzung hierfür ist natürlich, daß sich das Problem in entsprechende Teilprobleme zerlegen läßt, die wiederum auf mehrere Rechner verteilt werden können (verteilte Anwendungen).
- Lastverbund** In diesem Fall besteht das Ziel darin, die Verteilung von Lasten innerhalb des Netzwerks durchführen zu können. Es können beispielsweise überlastete Stationen einzelne Aufgaben an weniger belastete Stationen abgeben. Dies ist auch heute noch bei den teuren Großrechnern ein wichtiger Aspekt.

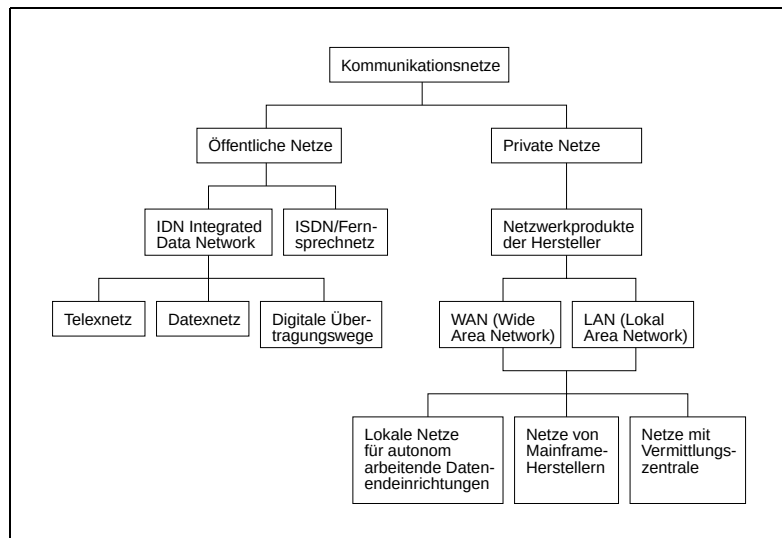
Da Datenaustausch und Kommunikation immer mehr an Bedeutung gewinnen, steigen auch die Anforderungen, die an die hierfür zur Verfügung gestellten Mechanismen und Methoden gestellt werden. Ein immer dringlicher werdendes Problem ist dabei die Steigerung der Übertragungsgeschwindigkeit, die nicht nur gewünscht wird, sondern auch notwendig ist, da die Anwendungen und Datenmen-

11 Rechnernetze – Basis der Kommunikation

gen, die transportiert werden müssen, immer größer werden. Neben der reinen Netzwerkkopplung werden aber auch die installierten Komponenten zur Einbindung von Remote-Workstations immer größer. Der Bedarf, auch von unterwegs die Verbindung zum Unternehmensnetzwerk aufzubauen, wird ebenfalls immer größer. In diesem Zusammenhang sind auch die Forderungen zu sehen, die Möglichkeiten der Telearbeit zu verstärken. All das sind Gründe dafür, daß die gestellten Leistungsanforderungen an die DFÜ-Strecken immer größer werden.

11.1 Die Einteilung von Rechnernetzen

Abbildung 11.1
Kommunikations-
netze im Überblick



Bevor die einzelnen Kommunikationsnetze näher betrachtet werden, will ich Ihnen drei wichtige Begriffe zu Abbildung 11.1 erläutern:

■ *Local Area Network (LAN)*

Ein Lokales Netzwerk ist laut ISO »ein innerhalb von Grundstücksgrenzen unter rechtlicher Kontrolle des Benutzers befindliches Netzwerk für die bitserielle Übertragung von Informationen zwischen dessen unabhängigen, miteinander gekoppelten Elementen«. Der Betreiber eines LAN ist also nicht von den Postverwaltungen oder Telekommunikationsunternehmen abhängig.

■ *Wide Area Network (WAN)*

Im Gegensatz dazu ist ein WAN oder auch Weitverkehrsnetz ein Netzwerk ohne Beschränkung auf Grundstücksgrenzen. Es dient

11.2 Öffentliche Datenkommunikationseinrichtungen

der Verbindung weit verteilter Computersysteme unter Zuhilfenahme der Kommunikationsnetze und -dienste der Telekom, wenn man von den Gegebenheiten in der BRD bis 1997 ausgeht. Seit dem 1. Januar 1998 existiert dieses Monopol nicht mehr. Alle großen und renommierten Elektrizitätswerke zum Beispiel haben sich zum Teil zu größeren Verbunden zusammengeschlossen, um entsprechende DFÜ-Dienste in Deutschland anbieten zu können. Aus heutiger Sicht haben sich daraus keine allzu großen Nachteile ergeben, im Gegenteil – Konkurrenz belebt das Geschäft.

■ *Metropolitan Area Network (MAN)*

Der Aufbau von WANs über herkömmliche Telekom-Dienste führt oftmals aufgrund zu geringer Übertragungsraten beim Übergang vom LAN zum WAN nicht zu den gewünschten Ergebnissen. Die Forderung nach schnelleren Verbindungen wird immer stärker. Ein neuer Standard 802.6 (MAN) wird dazu beitragen, diesen noch vorhandenen Mißstand zu lösen. Nach der Erläuterung von ISDN werde ich Ihnen den Aufbau und die Arbeitsweise von MAN näher beschreiben. Beim Aufbau von MANs geht es aber auch darum, welche schnellen Übertragungsmechanismen eingesetzt werden können. Viel diskutiert wird dabei vor allem auch der Einsatz von ATM – dies wird auch im Zuge von Breitband-ISDN immer wieder damit in Verbindung gebracht.

11.2 Öffentliche Datenkommunikations-einrichtungen

Aufgrund der gesetzlichen Bestimmungen in der BRD unterlag die Datenübertragung außerhalb des eigenen Grundstücks bis 31.12.1997 noch der Hoheit der Telekom. Seit 1.1.1998 ist dieses Monopol gefallen, und seitdem gibt es eine Vielzahl von Drittanbietern, die entsprechende Dienste offerieren können. Bis zum Zeitpunkt der Erstellung dieses Buches war es jedoch nicht immer ganz einfach, die ausreichenden und notwendigen Informationen der einzelnen Anbieter zu erhalten. Dies lag zum einen an der relativ schlechten Dokumentation der angebotenen Dienste und zum anderen an der noch nicht vollständig verfügbaren Infrastruktur, um alle in Frage kommenden Dienste auch tatsächlich anbieten zu können. Es werden deshalb noch einige Monate vergehen müssen, bis sich alle Anbieter auf die neue Situation eingespield haben. Ebenso war es bislang zum Teil schwierig, exakte Preise für die in Frage kommenden Dienste zu erhalten. Auch hier zeigten sich bei einigen Anbietern enorme Schwächen. Der Versuch, sich aktuell Informationen aus dem Internet zu holen, wich auch sehr schnell großer Ernüchterung.

11 Rechnernetze – Basis der Kommunikation

Entweder fand man sich bei dem einen oder anderen Anbietern nur sehr schwer zurecht, oder man fand nicht unbedingt die Informationen, die man haben wollte. Auch Preisinformationen direkt über das Internet wurden nur von wenigen Anbietern zufriedenstellend zur Verfügung gestellt. Ich nenne an dieser Stelle bewußt keine Namen, aber auch die Gespräche mit Kunden haben gezeigt, daß die Bereitstellung ausführlicher Informationen immer noch zu wünschen übrigläßt. Einen vollständigen Vergleich aller in Frage kommenden Drittanbieter würde den Rahmen dieses Buches bei weitem sprengen, deshalb beschränke ich mich auf zwei wesentliche Anbieter, um aufzuzeigen, mit welchen Diensten die Netzintegration bzw. Kopplung von Netzwerken durchgeführt werden kann. Es handelt sich um die Deutsche Telekom AG und Arcor mannesmann telecommunications.

Dabei bietet die Deutsche Telekom im Bereich der Datenkommunikation Netzwerkdienste an, bei denen die Spezifikationen maximal bis zur Schicht 3 des OSI-Modells vorgegeben sind. Auf diesen Spezifikationen kann der Teilnehmer mit Datenkommunikationseinrichtungen aufsetzen, ohne dabei auf die Vorschriften der Telekom Rücksicht nehmen zu müssen. Bei der Telekom werden diese Netz- bzw. Transportdienste als Übermittlungsdienste bezeichnet. Neben diesen Diensten werden inzwischen aber auch Leistungen angeboten, die man als Teledienste bzw. Telematikdienste bezeichnet. Bei diesen Diensten reichen die Vorgaben der Telekom bis zur Schicht 7 im OSI-Schichtenmodell. Das heißt, es müssen auch die angeschlossenen Endgeräte den Vorschriften der Telekom entsprechen oder nur Anwendungen darauf aufgesetzt werden, die von der Telekom stammen. Alle Endgeräte, die an Übertragungsdiensten der Telekom teilnehmen, müssen entsprechende Zulassungen besitzen. Es ist also darauf zu achten, daß die Endgeräte bzw. notwendigen Adapterkarten im PC oder in einem Router eine ZZF-Zulassung besitzen. Das ZZF ist das Zentralamt für Zulassungen im Fernmeldewesen, das Zulassungen auf der Grundlage von Richtlinien des FTZ, dem Fernmeldetechnischen Zentralamt, erteilt. Nachfolgend soll kurz aufgezeigt werden, welche Möglichkeiten hierfür zur Verfügung stehen.

11.2.1 Netze der Telekom

Die Leitungen bzw. Netze, die Ihnen von der Telekom zum Zweck der Datenübertragung zur Verfügung gestellt werden, lassen sich in zwei Gruppen einteilen:

11.2 Öffentliche Datenkommunikationseinrichtungen

Wählnetze

- *Fernsprechnetz*
Leitungsvermittelte Wählverbindungen
Analoges Übertragungsverfahren
Übertragung von Sprache und von Daten
- *Telexnetz*
Leitungsvermittelte Wählverbindungen
Digitales Übertragungsverfahren: Übertragung von schriftlichen Informationen
- *SwitchedLink*
Besonders geeignet für den Datenaustausch mit wechselnden Kommunikationspartnern, somit auch für den Zugang zum Internet gedacht

Mietleitungsnetze – LeasedLink (feste Verbindungen)

Die Vorteile von Wählleitungen gegenüber Mietleitungen sind:

- Es sind Verbindungen zu verschiedenen Teilnehmern durch Wahlen herstellbar.
- Sie sind kostengünstiger bei kurzen Übertragungszeiten, da meist nur die Kosten für die Verbindungsdauer anfallen.

Die Vorteile von Mietleitungen gegenüber Wählleitungen sind:

- Da die Verbindung ständig vorhanden ist, entfallen Verbindungsaufbauzeiten.
- Wähleinrichtungen sind nicht notwendig.
- Sie sind kostengünstiger bei langen Übertragungszeiten. Es fallen pauschale Kosten an, egal ob Daten übertragen werden oder nicht.
- Wirtschaftlich für den ständigen Datenaustausch mit einem vorher definierten Kommunikationspartner.

Die folgende Übersicht zeigt, welche Möglichkeiten mit den einzelnen Diensten zur Verfügung gestellt werden. Nähere Beschreibungen darüber finden Sie dann im weiteren Text dieses Kapitels.

	Produkte	Verbindungsart	Übertragungsgeschwindigkeit
LeasedLink (Festverbindungen)	City-Netz	(D/S)	(64 Kbit/s); 2 Mbit/s bis 155 Mbit/s
	LeasedLink International	(D/S)	von 16 Kbit/s bis 155 Mbit/s

11 Rechnernetze – Basis der Kommunikation

	Produkte	Verbindungsart	Übertragungsgeschwindigkeit
	LeasedLink Analog/Digital	(D/S)	kleiner 64 Kbit/s
	LeasedLink Digital	(D/S)	von 64 Kbit/s bis 1920 Kbit/s
SwitchedLink	T-InterConnect	(D)	64 Kbit/s bis 34 Mbit/s
	T-Net-ATM	(D/S*)	2 bis 155 Mbit/s
	Datex-M	(D)	64 Kbit/s bis max. 34 Mbit/s
	FrameLink Plus	(D)	64 Kbit/s bis max. 1,92 Mbit/s
	Datex-P (X.25)	(D*)	2400 Bit/s bis max. 1,92 Mbit/s
Data Solutions	Access Solution	(D/S)	n*64 Kbit/s bis 1,92 Mbit/s (ab n=1)
	LAN to LAN	in Vorbereitung	in Vorbereitung

D=Daten, S=Sprache, *=vermittelndes Netz, feste (virtuelle) Verbindungen möglich

Dienstintegration

Die Anzahl der angebotenen Dienste wird immer größer. Das macht es immer aufwendiger, sich durch das gesamte Angebot durchzuarbeiten, um das jeweils richtige System zu finden bzw. den richtigen Dienst einzusetzen. Zudem können nicht ständig weitere Netze für jeden neuen Dienst geschaffen werden. So wird bereits von Anfang an der Telefax-Dienst über das herkömmliche Telefonnetz abgewickelt. Die Integration von Diensten in einem Netzwerk mit einem einheitlichen Transportsystem führt schließlich zu einem dienstintegrierenden Nachrichtennetz (Stichwort ISDN).

ISDN ist ein Fernmeldenetzwerk, das darauf ausgerichtet ist, unterschiedliche Fernmeldedienste abwickeln zu können. Durch ISDN können sowohl Dienste mit völlig neuen Merkmalen als auch Dienste durch das Anbieten von Zusatzmerkmalen zu bestehenden Diensten, wie dem Fernsprechen, angeboten werden.

Zu den neuen Merkmalen im ISDN zählen unter anderem:

- Bildschirmtext
- Fernwirken

11.2 Öffentliche Datenkommunikationseinrichtungen

- Telefax
- Datenübertragung
- Teletex
- Textfax
- Fernzeichnen
- Festbildübertragung
- Bewegtbildübertragung
- Voice Mail
- Text Mail
- Fax Mail
- virtuelles privates Netz
- Kreditkartendienste
- Verteildienste

Zu den Zusatzmerkmalen beim Telefonieren können unter anderem gezählt werden:

- Anzeige der Rufnummer des Anrufers
- einheitliche Rufnummer
- persönliche Rufnummer
- Anrufumleitung, Anrufweitschaltung
- Sammelruf
- Rundruf
- Konferenzschaltung
- Rückruf
- Kurzwahl
- Rufnummernsperre für abgehende Verbindungen
- Anklopfen
- Ruhe vor dem Telefon

11.2.2 Die Dienste der Telekom

In diesem Kapitel sollen die Datendienste der Telekom im Überblick dargestellt werden, um einen Eindruck davon zu gewinnen, welche Möglichkeiten zur Datenübertragung bzw. zur Kopplung von Netzwerken zur Verfügung stehen.

Datenkommunikation über Modems

Diese Übertragungsform ist am weitesten verbreitet, da der Einsatz von Modems zur Datenkommunikation über das analoge Fernsprechnetz vor allem in den privaten Haushalten vermehrt zum Einsatz kommt. Im Zuge der Maßnahmen der Telekom, ISDN attraktiver und auch billiger zu machen, könnte es jedoch in den nächsten Jahren eine Verschiebung geben, so daß Zug um Zug das digitale Fernsprechnetz immer mehr an Bedeutung gewinnt und auch die

11 Rechnernetze – Basis der Kommunikation

analoge Modemkommunikation an Bedeutung verliert. Das Fernsprechnetz ist nicht nur für die Sprachkommunikation verfügbar, sondern läßt sich auch als Träger für nichtsprachliche Dienste einsetzen. Hierzu zählen das Telefax, T-Online und alle anderen Dienste, die zur Datenübertragung Modems nutzen. Vor allem die Angebote von Online-Diensten haben hierzu sehr viel beigetragen, vor allem auch unter dem Aspekt, daß immer mehr private Haushalte einen PC oder ein Notebook im Einsatz haben. Die Zuwachsraten bei den bekannten Online-Dienst-Anbietern CompuServe, AOL oder auch T-Online spiegeln diese Tatsache wider. Inzwischen stellen alle Online-Anbieter einen Zugang zum Internet zur Verfügung, was sicher mit zu ihrer raschen Verbreitung beiträgt. Um die Datenkommunikation zu beschleunigen, sind fast alle der entsprechenden Einwählknoten mit mindestens 28.800 Bit/s erreichbar, es werden jedoch immer mehr analoge Anschlüsse mit bis zu 56 Kbit/s zur Verfügung gestellt. Dabei sind fast alle Modems in der Lage, einen Abgleich der möglichen Übertragungsgeschwindigkeit durchzuführen, in Abhängigkeit von der unterstützten Übertragungskapazität, die vom jeweiligen Modem zur Verfügung gestellt wird. Der Zugang über ISDN-Einwählknoten ist inzwischen bei allen Online-Anbietern gegeben. Nachteilig ist aber, daß die Einwählknoten nur in größeren Städten verfügbar sind und Nutzer von außerhalb die höheren Telefonkosten in Kauf nehmen müssen. Durch die Änderung der Gebührenstrukturen hat sich dies jedoch zum Teil wieder relativiert. Da auf den Datenbanken der Online-Anbieter bzw. im Internet schon mal Daten abgelegt sein können, die einen Umfang von 1 bis 8 Mbyte haben können, ist es erforderlich, schnelle Datenübertragungswege verfügbar zu haben. Diese sind bei den analogen Fernsprechleitungen, auch wenn man mit 28.800 Bit/s und höher arbeitet, nicht immer gegeben. Deutlich wird das am Modem, wenn immer wieder neue Abstimmungen zwischen Sender und Empfänger durchgeführt werden. Beim Einsatz von ISDN stehen nicht nur höhere Datenübertragungsraten zur Verfügung, sondern auch echte digitale Verbindungen, die weniger fehleranfällig sind im Vergleich zu analogen Leitungen bzw. Verbindungen. Zu beachten ist dabei nur, daß man zur Unterstützung von ISDN-Zugängen nicht nur als Anwender einen ISDN-Anschluß benötigt, sondern auch die Gegenstelle ISDN-Zugänge haben müssen und der PC des Anwenders mit einer ISDN-Karte ausgestattet werden muß. Besonders wichtig ist dabei auch, daß die Kommunikationssoftware, mit der die Verbindung zum Online-Dienst hergestellt werden soll, ebenfalls ISDN-Karten unterstützt. Dies erkennt man bei den Software-Produkten immer an der Unterstützung einer sogenannten CAPI-Schnittstelle bzw. den verfügbaren RAS-Treibern für ISDN. Man sollte sich auf alle Fälle vor dem Einsatz einer ISDN-Karte davon überzeugen, daß der Online-Dienst entsprechende Zu-

11.2 Öffentliche Datenkommunikationseinrichtungen

gänge unterstützt und die Kommunikationssoftware ebenfalls eine Unterstützung für ISDN bereitstellt. Da der größte Teil der Online-Dienste inzwischen durch das Internet abgelöst wird, muß nur geprüft werden, ob der Internet-Service-Provider (ISP) ISDN-Zugänge unterstützt (analoge Modem-Zugänge sind standardgemäß vorhanden). Elegant ist es auch, wenn es für den Zugangsknoten nur eine Telefonnummer gibt, so wie dies bei T-Online der Fall ist, und der Zugangsknoten entscheidet, ob es sich beim Kunden um einen Modem- oder ISDN-Anschluß handelt.

Telex

Dabei handelt es sich um die Textkommunikation mit Fernschreiber, d.h., die Telexteilnehmer können mit allen anderen Telexteilnehmern schriftliche Nachrichten austauschen. Als Transportmedium wird das Telexnetz zur Verfügung gestellt. Die Übertragungsdauer für eine DIN-A4-Seite (ca. 2000 Zeichen) beträgt ungefähr fünf Minuten. Im Telexnetz wird nur mit einer Übertragungsgeschwindigkeit von 50 Bit/s gearbeitet. Das Telexnetz stellt Zugangsmöglichkeiten zum Teletexnetz zur Verfügung. Dieser Dienst wird weniger zur Kopplung von LANs eingesetzt werden. Da jedoch immer häufiger der Einsatz von zentralen Fax-Servern im Netzwerk gefordert wird, soll darüber auch die Verbindung zum Telex-Netzwerk der Telekom hergestellt werden können.

LeasedLink – Festverbindungen und City-Netz

Die Telekom bietet unter der Bezeichnung SFV analoge und digitale Mietleitungen. Es handelt sich bei allen angebotenen Mietleitungen dieser Kategorie um festgeschaltete physikalische Verbindungen mit einer permanenten Bereitschaft, Daten zwischen den miteinander verbundenen Partnern zu übertragen. Der Anwender verfügt in diesem Fall über eine duplexfähige, transparente und dienstneutrale Übertragungsstrecke. Die Verbindung steht rund um die Uhr zur Verfügung und bedarf keiner zusätzlichen Vermittlungstechnik. Standardfestverbindungen werden aus Kostengründen bei Störungen nicht automatisch ersatzgeschaltet.

Soll die Verfügbarkeit erhöht werden, indem Ersatzwege zusätzlich nutzbar sind, muß auf die Datendirektverbindungen ausgewichen werden.

Standardfestverbindungen erlauben preiswerte Übertragungen mit stark reduziertem Leistungsumfang. Diese Leistungen beschränken sich auf das funktional unerläßliche Minimum einer physikalischen Übertragung. Auch als kostenpflichtige Option werden für diese Verbindungen keine Mehrwertdienste angeboten.

11 Rechnernetze – Basis der Kommunikation

Festverbindungen gewährleisten somit eine permanente Verbindung zwischen zwei oder mehreren festen Kommunikationspartnern, um damit Sprache, Daten und Bilder übertragen zu können. In Abhängigkeit der Unternehmensgröße bietet die Telekom eine sehr große Bandbreitenauswahl an. Das Angebot reicht von einer analogen Sprachverbindung mit nur 3,1 kHz bis zu einer digitalen Dateninfo-bahn mit einer Übertragungsgeschwindigkeit von 155 Mbit/s.

Das LeasedLink-Angebot eignet sich deshalb besonders gut für:

- häufige Kommunikation mit festen Partnern
- höchste Qualität und Verfügbarkeit der Leitungsverbindung
- Verbindung von TK-Anlagen untereinander
- häufigen Austausch von Daten, Texten und Bildern mit bestimmten Partnern (z.B. Filialen mit der Zentrale, Lager mit Hauptlager etc.).

Der Einsatz von LeasedLink bietet die folgenden Vorteile:

- Die Leitung steht jederzeit und exklusiv zur Verfügung, d.h., es gibt keine Wartezeiten beim Verbindungsaufbau, und es können auch keine Besetztzeiten auftreten, wenn man eine Verbindung herstellen will.
- Die Leitungen sind sehr wirtschaftlich, sofern es sich bei der Kommunikation zwischen den Partnern um ein permanentes Kommunikationsaufkommen handelt.
- Man hat eine sehr große Planungssicherheit, da pro Monat feste Kosten entstehen, die deshalb sehr gut kalkulierbar sind.

Das LeasedLink-Angebot der Telekom kann mit folgenden Zusatzleistungen eingesetzt werden:

- Für besonders hohe Sicherheitsansprüche wird für LeasedLink typenabhängig Netzmanagement (d.h. eine automatische Fehlersignalisierung) und Ersatzwegeschaltung angeboten. Dabei wird der Ersatzweg in der Fernebene oder als Ende-zu-Ende-Ersatzweg (ISDN-Backup) zur Verfügung gestellt. Auf diese Art und Weise wird im Jahresmittel eine erhöhte Verfügbarkeit von bis zu 99,8% garantiert. Auf ein Jahr (mit 365 Tagen gerechnet) bezogen bedeutet diese Verfügbarkeit immerhin eine erlaubte Ausfallzeit von 17,52 Stunden.
- Ebenso wird typenabhängig für LeasedLink eine Schnittstellenvervielfachung und Kanalteilung angeboten.

Daneben kann man noch auswählen zwischen einem Standardservice, der eine Entstörung werktags innerhalb von 24 Stunden beinhaltet, und einem Express-Service, bei dem eine tägliche Entstörung innerhalb von acht Stunden garantiert wird.

11.2 Öffentliche Datenkommunikationseinrichtungen

Bei der Preisgestaltung ist zu beachten, daß die Leitung exklusive 24 Stunden pro Tag zu einem festen Monatsbetrag zur Verfügung steht, egal wieviel und wie oft diese Leitung genutzt wird. Die Preisgestaltung hängt nur davon ab, mit welcher Übertragungsgeschwindigkeit die LeasedLink-Verbindung aufgebaut werden soll und wie weit die beiden Standorte, die miteinander verbunden werden sollen, voneinander entfernt liegen. Ich werde Ihnen am Ende dieses Abschnitts ein paar Beispiele zeigen, mit welchen Kosten bei unterschiedlichen Anforderungen gerechnet werden muß. Man kann sich beim Aufbau einer LeasedLink-Verbindung mühsam mit Tabellen auseinandersetzen, sich die Preise von der Telekom ausrechnen lassen oder aber auch ein Programm einsetzen, mit dem man in der Lage ist, für die unterschiedlichsten Konstellationen sehr schnell die passenden Preise ausrechnen zu lassen. Man benötigt hierzu nur die folgenden Angaben:

- Anschlußgeschwindigkeit (Bandbreite/Geschwindigkeit)
- Verbindungslänge der Leitung

Unterteilt man LeasedLink für grobe Einsatzzwecke, so kann man bereits jetzt die folgende Forderung aufstellen:

- Wird hauptsächlich telefoniert und gefaxt, dann entscheidet man sich für eine analoge LeasedLink-Verbindung, da in diesem Fall eine solche die wirtschaftlichste Alternative ist.
- Sollen häufig Daten, Bilder und Texte zwischen den Standorten transportiert werden, dann ist die digitale LeasedLink-Verbindung die bessere Alternative.

Nachfolgend will ich die für LeasedLink in Frage kommenden Festverbindungen kurz beschreiben, um Ihnen einen Überblick darüber zu geben, mit welchen Möglichkeiten Sie planen können.

City-Netz

Gemäß der Beschreibung der Telekom versteht diese unter einem City-Netz eine Hochgeschwindigkeitsplattform für ausgewählte Wirtschaftszentren in Deutschland. Auf diesen Plattformen werden von der DTAG standardisierte Kundenlösungen für High-Speed-Anwendungen höchster Qualität realisiert. Zielgruppe für die City-Netz-Angebote sind Unternehmen, Behörden und Institutionen in deutschen Wirtschaftszentren, die hohe Sicherheit und Qualität auch im direkten City-Bereich benötigen. Zum Produktspektrum zählen deshalb im Bereich für Data-Solution:

- Festverbindungen im City-Netz für transparente Übertragungsleistungen mit Geschwindigkeiten von 2, 34 und 155 Mbit/s, die auch das Grundangebot der City-Dienste darstellen. Im Zugangsbereich lassen sich niedrige Geschwindigkeiten schalten, wobei

11 Rechnernetze – Basis der Kommunikation

auch alle gängigen elektrischen und optischen Schnittstellen unterstützt werden. Aufgrund der besonders aufgebauten Ringstruktur für City-Netze werden nach Aussagen der DTAG Verfügbarkeiten von 99,9% garantiert. Diese Strukturen können auch in Verbindung mit anderen Produktangeboten (z.B. T-Net-ATM) genutzt werden.

- Es werden zum Zeitpunkt der Erstellung dieses Buches Verbindungen zwischen den 29 City-Netzen der DTAG in Deutschland und der im Aufbau befindlichen City-Netze in Europa zur Verfügung gestellt.
- LAN-Verbindungen im City-Netz dienen der Vernetzung von mehreren im Stadtgebiet verteilten LANs auf High-Speed-Netzwerkbasis. Hierbei kommen Router zum Einsatz, die alle dazu notwendigen LAN-Schnittstellen und Netzwerkprotokolle unterstützen. Auf diese Art und Weise wird aus der Stadt mit Hilfe des City-Netzes ein klassisches Campus-Netzwerk.
- Sprachverbindungen im City-Netz ermöglichen einfach und bequem die Bereitstellung von Punkt-zu-Punkt-Sprach- und Faxverbindungen. Dabei sind sowohl analoge als auch digitale Verbindungen realisierbar. Aufgrund der Möglichkeit, Sprachkompression einzusetzen, lassen sich sehr günstige Verbindungen realisieren.
- Der T-Net-ATM-Dienst im City-Netz bietet weitere Möglichkeiten für die Sprach-, Video- bzw. Multimedia-Kommunikation. Hierzu jedoch an anderer Stelle mehr.

Die DTAG stellt für das City-Netz einen Standard- und Premiumservice zur Verfügung. Im Standardservice wird bei Festverbindungen im City-Netz eine Verfügbarkeit von 99,5% garantiert, im Premiumservice hingegen garantiert die DTAG für die Festverbindung im City-Netz eine Verfügbarkeit von immerhin 99,9%. Die DTAG garantiert diese hohe Verfügbarkeit von 99,9% unter anderem dadurch, daß man sich auf zwei Netzknoten abstützt, falls man den Premium-Service abschließt; zudem wird im aufgebauten Ring zusätzliche Redundanz eingesetzt und ein zentrales Netzmanagement verwendet. Besondere betriebliche Regeln helfen zusätzlich, die Ausfallzeiten zu minimieren. Zu diesen besonderen Regeln zählen unter anderem ein 24-Stunden-Service, schnelle Entstörzeiten oder auch eine entsprechende Hotline.

Die DTAG beschreibt die Leistungen des City-Netzes kurz wie folgt:

»Wir bieten unseren Kunden ein Kommunikationsmedium, das Büros, Außenstellen, Produktionsstätten und externe Partner innerhalb einer Stadtregion und zwischen Wirtschaftszentren flexibel und doch fest miteinander verbindet. Die City-Netze der Deutschen Tele-

11.2 Öffentliche Datenkommunikationseinrichtungen

kom ermöglichen hohe Performance für verteilte Anwendungskopplungen zwischen Geschäftspartnern und Filialen innerhalb einer Wirtschaftsregion. Sie lassen Metropolen zu einem Campus-Netzwerk mit hoher Leistungsfähigkeit zusammenwachsen.“

LeasedLink International

Hierbei handelt es sich um exklusive und transparente Übertragungskanäle für weltweite Verbindungen für international tätige Unternehmen. Hierfür unterscheidet man als Einsatzgebiete typabhängige Anwendungsbereiche, zu denen unter anderem gehören:

- Übertragung von Sprache, Daten und Video
- Verbindung von LANs und Rechenzentren
- Bildung von weltweiten Internet/Intranet-Netzplattformen
- Dialoganwendungen

Wenn man LeasedLink-International-Verbindungen aufbauen will, kann man zwischen den folgenden Produkten wählen:

- Analog: aIML Voice Link 16 Kbit/s
- Digital: dIML n*64 Kbit/s bis 155 Mbit/s
- Digital: Global Managed Bandwidth n*64 Kbit/s bis 2 Mbit/s auf vordefinierten Städtekombinationen

LeasedLink-Analog/Digital

Analoge LeasedLink-Verbindungen eignen sich vor allem für die Sprachübertragung und Datenübertragung mit begrenzter Kapazität. Zu den typabhängigen Anwendungsbeispielen zählen für diese Kopplungsart unter anderem:

- Verbindung von Telefonanlagen mit einer außenliegenden analogen oder digitalen Nebenstelle
- Verbindung von zwei analogen oder digitalen TK-Anlagen
- besonders günstige Sprachverbindungen in ausgewählten Wirtschaftszentren
- langsame Datenübertragung zwischen zwei Standorten

Zu den verfügbaren Verbindungsarten für LeasedLink-Analog/-Digital zählen:

- SFV Analog TG (300-3400 Hz); dies ist der typische analoge Anschluß
- DDV VoiceLink 16 Kbit/s; Einsatz für komprimierte Sprachübertragung
- DDV 9600 bit/s mit Ersatzweg in der Fernebene; Einsatz für Datenanwendungen mit geringer Übertragungsrate

LeasedLink-Digital (64 Kbit/s bis 1920 Kbit/s)

Diese Verbindungsarten sollen zum Aufbau von Festverbindungen für komplexere Anwendungen eingesetzt werden. Dies bedeutet auch, daß ein höherer Kapazitätsbedarf für die Übertragung von Sprache, Daten und Bildern notwendig ist. Zu den typabhängigen Anwendungen dieser Verbindungsart zählen unter anderem:

- Verbindung von Telefonanlagen mit außenliegender Nebenstelle oder von zwei digitalen Telefonanlagen
- Übertragung von Daten, Video und Sprache
- Verbindung des Campus-Backbone mit regionalen Niederlassungen
- Verbindung von LANs und Rechenzentren
- Bildung von Kundennetzen

Der Aufbau von LeasedLink-Digital kann über die folgenden Verbindungsarten aufgebaut werden:

- SFV Digital 64S
- SFV Digital 64S2
- SFV Digital TS01
- SFV Digital TS02
- DDV $n \cdot 64$ Kbit/s ohne Ersatzweg ($n=1-8$)
- DDV 64 Kbit/s, 128 Kbit/s mit Ersatzweg in der Fernebene
- DDV 64 Kbit/s, 128 Kbit/s mit ISDN-Backup

Als Zusatzleistungen bietet die DTAG an:

- Netzmanagement inklusive Fehlersignalisierung
- Ersatzweg in der Fernebene oder ISDN-Backup (Ende-zu-Ende-Ersatzweg)

LeasedLink-Digital (ab 2 Mbit/s)

Wird ein noch höherer Bandbreitenbedarf benötigt, dann empfiehlt sich unter Umständen diese Verbindungsstrecke für noch komplexere Anwendungen und einen noch größeren Kapazitätsbedarf zur Übertragung von Sprache, Daten und Bildern. Zu den typischen Anwendungen zählen in diesem Falle:

- Verbindung von LANs und Rechenzentren
- Verbindung von zwei digitalen TK-Anlagen für große Sprach- und Datenaufkommen
- Übertragung von Video-Signalen
- Verbindung des Campus-Backbone mit regionalen Niederlassungen
- Bildung von Kundennetzen
- Dialoganwendungen

11.2 Öffentliche Datenkommunikationseinrichtungen

Für LeasedLink-Digital (ab 2 Mbit/s) stehen die folgenden Verbindungsarten zur Verfügung:

- SFV T2MS – 2 Mbit/s
- SFV 34M – 34 Mbit/s
- SFV 155M – 155 Mbit/s
- DDV – 1,92 Mbit/s mit Ersatzweg

Als typabhängige Zusatzleistungen werden angeboten:

- Netzmanagement inklusive Fehlersignalisierung
- Ersatz in der Fernebene und als ISDN-Backup (Ende-zu-Ende-Ersatzweg)

Man liest bei den oben aufgeführten Diensten immer wieder SFV und DDV. Die Bezeichnung SFV steht hierbei für Standardfestverbindung und DDV für Datendirektverbindung. Welche Merkmale SFV und DDV vorweisen, soll anhand der nachfolgenden Erläuterungen näher beschrieben werden.

Standardfestverbindungen (SFV)

Die Telekom bietet unter der Bezeichnung SFV analoge und digitale Mietleitungen. Es handelt sich dabei bei allen angebotenen Mietleitungen dieser Kategorie um festgeschaltete physikalische Verbindungen mit einer permanenten Bereitschaft, Daten zwischen den miteinander verbundenen Partnern übertragen zu können. Der Anwender verfügt in diesem Fall über eine duplexfähige, transparente und dienstneutrale Übertragungsstrecke. Die Verbindung steht rund um die Uhr zur Verfügung und bedarf keiner zusätzlichen Vermittlungstechnik. Standardfestverbindungen werden aus Kostengründen bei Störungen nicht automatisch ersatzgeschaltet.

Soll die Verfügbarkeit erhöht werden, indem Ersatzwege zusätzlich nutzbar sind, muß auf die Datendirektverbindungen ausgewichen werden.

Standardfestverbindungen erlauben preiswerte Übertragungen mit stark reduziertem Leistungsumfang. Diese Leistungen beschränken sich auf das funktional unerläßliche Minimum einer physikalischen Übertragung. Auch als kostenpflichtige Option werden für diese Verbindungen keine Mehrwertdienste angeboten.

Nicht selten findet man digitale Festverbindungen zunehmend für die Verbindung räumlich verteilter Unternehmen. Die Standardfestverbindungen bilden die Basis für die sogenannten Corporate Networks, darunter versteht man private Netze für anwendungsübergreifende Sprach-, Daten- und Bildkommunikation in einem Unternehmen. In der Regel werden Standardfestverbindungen über

11 Rechnernetze – Basis der Kommunikation

den zuständigen Netzanschlußknoten zur Endstelle des Anwenders geführt. Auf Wunsch stellt die Telekom auch davon abweichende Anschlußpunkte und Kabeltrassen zur Verfügung (kostenpflichtige Option). Auf den Verbindungsabschnitten des Netzinnersen sind, im Gegensatz zu den Datendirektverbindungen, keine automatisch aktivierten Ersatzschaltungen vorgesehen. Gestörte Verbindungen bleiben somit bei den Standardfestverbindungen so lange unterbrochen, bis die verursachenden Fehler erkannt, lokalisiert und behoben sind. Dies hat auch enormen Einfluß auf die Verfügbarkeit, die geringer ist als bei den Datendirektverbindungen.

Wenn es sich um sehr kritische und sensible Anwendungen handelt, sollte deshalb entweder auf Datendirektverbindungen ausgewichen oder die Sicherheit über vermittelte Backup-Anschlüsse erhöht werden. Die Zusatzoption Sonderentstörung ist durch die verkürzte mittlere Entstörungszeit geeignet, die Verfügbarkeit einer Standardfestverbindung zu erhöhen. Diese Dienstleistung garantiert die Entstörung außerhalb der Regelarbeitszeit und eine vorrangige Entstörung während der Regelarbeitszeit. Zu beachten ist noch, daß bei den analogen SFV sowohl die 2-/4- als auch die 6-Draht Technik mit unterschiedlichen garantierten Dämpfungswerten unterstützt und angeboten werden. Die nachfolgende Aufstellung soll zeigen, welche SFV-Angebote insgesamt zur Verfügung stehen:

SFV Analog

300-3400 Hz	Analog G / 2-Draht
300-3400 Hz	Analog G / 4-Draht
300-3400 Hz	Analog 1025 / 2-Draht
300-3400 Hz	Analog 1025 / 4-Draht
300-3400 Hz	Analog 1020 / 2-Draht
300-3400 Hz	Analog 1020 / 4-Draht
300-3400 Hz	Analog TG0 / 2-Draht $\frac{3}{4}$ 2 dB bei 1000 Hz
300-3400 Hz	Analog TG0 / 4-Draht = 0 dB bei 1000 Hz
300-3400 Hz	Analog TG0 / 6-Draht = 0 dB bei 1000 Hz
300-3400 Hz	Analog TG5 / 2-Draht $\frac{3}{4}$ 5 dB bei 1000 Hz
300-3400 Hz	Analog TG5 / 4-Draht $\frac{3}{4}$ 5 dB bei 1000 Hz
300-3400 Hz	Analog TG5 / 6-Draht $\frac{3}{4}$ 5 dB bei 1000 Hz
300-3400 Hz	Analog TG / 2-Draht $\frac{3}{4}$ 24 dB bei 1000 Hz
300-3400 Hz	Analog TG / 4-Draht $\frac{3}{4}$ 24 dB bei 1000 Hz
300-3400 Hz	Analog TG / 6-Draht $\frac{3}{4}$ 24 dB bei 1000 Hz

11.2 Öffentliche Datenkommunikationseinrichtungen

SFV Digital

64 Kbit/s	Digital 64 S	/I.430
64 Kbit/s	Digital 64U	/G.703
64 Kbit/s	Digital 64S	in Doppelanschluß an ein Ende
64 Kbit/s	Digital 64S	in Doppelanschluß an zwei Enden
2*62 Kbit/s	Digital S02	2 B-Kanäle / 1 D-Kanal
2*64 Kbit/s	Digital 64S2	2 B-Kanäle / 0 D-Kanal
1,984 Mbit/s	Digital 2MS	G.703/704
2,048 Mbit/s	Digital 2MU	G.703
34 Mbit/s	Digital 34M	G.703/751
140 Mbit/s	Digital 140M	G.703/751
155 Mbit/s	Digital 155M	G.703

Datendirektverbindungen (DDV)

Unter Datendirektverbindungen sind feste, digitale Verbindungen zu verstehen, die der Anwender ohne Einschränkung nutzen kann. Da es sich um feste Verbindungen handelt, entfallen deren Aufbauzeiten oder Besetztzeiten, wie dies bei Wählverbindungen der Fall sein könnte. Die Übertragungswege werden im IDN geführt. Die Anwenderdaten werden transparent und ohne Einschränkung der Protokolle oder des Codes übertragen (außer bei asynchroner Übertragung, bei der der Coderahmen festgelegt ist).

Datendirektverbindungen werden im Fernbereich über ausgesuchte Übertragungssysteme mit einer automatischen Ersatzschaltung geführt. Durch den Anschluß der DDV an das Datennetzsteuersystem der Telekom ist eine schnelle Entstörung möglich. Wenn noch höhere Verfügbarkeiten benötigt werden, dann muß eine zweite DDV als Backup-Variante eingerichtet werden. Als Zusatzoptionen stehen zudem die Umwegführung und die Sonderanschaltung zur Verfügung.

Für alle Datendirektverbindungen gilt, daß der Anwender Sprache für sich selbst übertragen kann, und dies bei entsprechender Technik ohne Einschränkung. Die Vermittlung von Sprache für andere ist jedoch nicht erlaubt.

Wie die vorherigen Ausführungen gezeigt haben, eignen sich die vorherigen Festverbindungen für ständig existierenden Kommunikationsbedarf zwischen zwei Partnern. Steht man jedoch vor dem Problem, einen ständig wechselnden Kommunikationsbedarf zwischen unterschiedlichen Partnern zu haben, der auch noch nur von Zeit zu Zeit stattfindet, dann ist eine Festverbindung nicht mehr die geeignetste Lösung. Das gleiche trifft zu, wenn man einen Anschluß mehrfach nutzen will.

11 Rechnernetze – Basis der Kommunikation

In diesem Fall wird man sich für die sogenannte SwitchedLink-Lösung entscheiden. Die nachfolgende Übersicht zeigt, welche DDV insgesamt zur Verfügung stehen:

1200 bit/s	mit Ersatzweg
2400 bit/s	mit Ersatzweg
4800 bit/s	mit Ersatzweg
9600 bit/s	mit Ersatzweg oder als CityLink
19,2 Kbit/s	mit Ersatzweg oder als CityLink
64 Kbit/s	mit und ohne Ersatzweg
128 Kbit/s	ohne Ersatzweg
1,92 Mbit/s	mit Ersatzweg
n*64 Kbit/s	CityLink

SwitchedLink

Bei SwitchedLink kann jeder mit jedem, und in diesem Falle jedes »Datenendgerät« mit jedem anderem »Datenendgerät«, kommunizieren. Gleichzeitig können bis zu 255 virtuelle Verbindungen pro Anschlußleitung aktiv sein, woraus zu ersehen ist, daß die Möglichkeiten, international zu kommunizieren, sehr groß sind. Dies hängt unter anderem auch damit zusammen, daß bei SwitchedLink nicht nur dafür gesorgt wird, daß jeder mit jedem verbunden ist, sondern auch, daß jeder auch jeden versteht. Das liegt unter anderem auch daran, daß international standardisierte Protokolle eingesetzt werden und somit auch die Kompatibilität untereinander gewährleistet werden kann. Die nachfolgenden Ausführungen zeigen, welche Dienste SwitchedLink zur Verfügung stellt.

T-InterConnect

Will man den Zugang zum Internet für ein Unternehmen realisieren, dann erwartet man hierfür eine performante und qualitativ hochwertige Netzdienstleistung. Mit T-InterConnect stellt die DTAG sehr gute Zugänge zum weltweiten Internet mit allen dazugehörigen Diensten zur Verfügung. Durch die flächendeckende Präsenz und ein extrem engmaschiges Netz aus Einwählknoten, moderne Technologie, die ständig weiterentwickelt wird, und ein Rund-um-die-Uhr-Netzmanagement wird der T-InterConnect-Dienst für den Internet-Zugang durchaus interessant. Als Zielgruppe für T-InterConnect sieht die DTAG:

11.2 Öffentliche Datenkommunikationseinrichtungen

»Geschäftskunden mit hohen Anforderungen, Internet-Service-, Content- und E-Commerce-Provider, Online-Dienste und Unternehmen mit Filialstrukturen profitieren besonders von T-InterConnect. Grundsätzlich steht für uns und unsere Kunden das Merkmal Qualität an vorderster Stelle.

T-InterConnect definiert sich als eine netznahe Dienste-Plattform, auf deren Basis sich professionell Internet-Mehrwertleistungen realisieren lassen. Somit liefert T-InterConnect die Voraussetzung zu allen Überlegungen, hochwertige und kommerzielle Dienstleistungen auf Basis der Internet-Technologie anzubieten.«

Die DTAG bietet zudem zwei unterschiedliche Dienst-Bereiche an:

■ *Classic*

Hierbei handelt es sich um die klassische Festanbindung direkt an einen der leistungsfähigen Internet-Backbones mit weltweiten Anbindungen in mehreren Zugangsklassen von bis zu 34 Mbit/s. Damit verbunden ist auch die Bereitstellung der notwendigen zugangsspezifischen Dienste wie IP-Adreßvergabe.

■ *Traffic*

Hierbei handelt es sich um Intranet- und Extranet-Lösungen. Traffic umfaßt kundenindividuelle Netzlösungen, basierend auf der Internet-Technologie für geschlossene Nutzergruppen. Die Intranet-Lösung stellt somit unternehmensinterne Geschäftsprozesse auf Basis der Internet-Technologie zur Verfügung, auch über mehrere Standorte verteilt. Die Lösungen für Extranet fallen auch unter die Bezeichnung VPN (Virtual Private Network). Unter VPN versteht man die Kopplung von LANs, verteilt über mehrere Standorte, mit Hilfe des Internet. Das heißt, jeder Firmenstandort hat einen Internet-Zugang, und statt eigene zusätzliche Leitungen zur Kopplung dieser LANs anzumieten, nutzt man den bereits vorhandenen Internet-Zugang. Hierzu installiert man für jeden Standort einen VPN-Zugang, der über das Internet eine gesicherte Verbindung zwischen den eigenen Firmen-LANs zur Verfügung stellt. Auf diese Art und Weise ist gewährleistet, daß keine unberechtigten »Personen« eines fremden LAN in das firmeneigene Netzwerk eindringen.

An dieser Stelle sei darauf hingewiesen, daß der Aufbau von Extranets (VPN-Verbindungen) auch mit FireWall-Systemen unterschiedlicher Hersteller möglich ist; für die VPN-Verbindungen müssen dann nur die FireWall-Systeme entsprechend konfiguriert werden.

11 Rechnernetze – Basis der Kommunikation

Für den Internet-Zugang stellt die DTAG ebenfalls unterschiedliche Varianten zur Verfügung. Zu diesen Varianten zählen:

■ *Basic*

Hierbei kann man zwischen einer Anschluß-Bandbreite von 64 Kbit/s bis 34 Mbit/s auswählen. Auf Basis der Anschluß-Bandbreite errechnen sich der einmalige Anschlußpreis sowie das monatliche und verbrauchsabhängige Nutzungsentgelt. Man zahlt dabei nur die durchschnittlich genutzte Bandbreite nach einem entsprechenden Stufensystem. Somit hat man eine sehr gute Planbarkeit und Transparenz.

■ *SmartStart*

Dieser Anschlußdienst ist für Einsteiger gedacht, die noch nicht genau wissen, was sie wollen. Das heißt, der 64 Kbit/s-Anschluß ist im Preis ermäßigt und zugleich verbunden mit einem Wechsel auf das Angebot Basic mit einer Bandbreite von 2 Mbit/s, wenn der Wechsel innerhalb eines Jahres durchgeführt wird.

■ *WorldWideTransit*

Hierbei wird ein Servicepaket angeboten, das vor allem für nationale und internationale Internet-Service-Provider (ISP) und Großkunden mit eigenen Netzplattformen gedacht ist. Über WorldWideTransit wird eine sehr performante internationale Anbindung auf Basis des sogenannten Border-Gateway-Protokolls (BGP) angeboten. Somit entfällt die Anmietung von Transatlantikkapazitäten und weiteren internationalen Mietleitungen. Dies ist deshalb möglich, da die DTAG direkte Peering-Vereinbarungen mit allen bedeutenden nationalen und internationalen Internet-Service-Providern besitzt.

■ *PartnerPlus*

In diesem Fall können Kunden relativ preiswert Anschlüsse bündeln. Dies hat vor allem für Kunden mit Filialstruktur preisliche Vorteile.

Neben diesen »öffentlichen« Netzzugängen bietet die DTAG aber auch Möglichkeiten, um »private« Netzwerke aufzubauen. Auch hierfür stellt die DTAG drei unterschiedliche Varianten zur Verfügung: OnlineConnect, IntraConnect und ServiceConnect.

■ *OnlineConnect*

Bei diesem Dienste-Angebot ist es möglich, einer beliebigen Anzahl von Benutzern Zugang zu entsprechenden »Dienste-Angeboten« zu gewähren, egal ob es sich dabei um Online-Dienste oder Extranet-Dienste handelt. Die Einwahl der »externen« Kommunikationspartner kann dabei analog oder digital über ISDN zum City-Tarif erfolgen.

11.2 Öffentliche Datenkommunikationseinrichtungen

■ *IntraConnect*

Hiermit hat man die Möglichkeit, auf Basis der T-InterConnect-Plattform ein virtuelles Unternehmensnetzwerk aufzubauen. Durch zusätzliche spezielle Sicherheitsverfahren, wie z.B. das »Tunneln« des Datenverkehrs, wird ein hohes Maß an Sicherheit erreicht.

■ *ServiceConnect*

Dieser Dienst richtet sich an Anbieter und Nutzer von Online-basierenden Service- und Wartungsdiensten, die alle hierfür notwendigen Verbindungen über T-InterConnect abwickeln wollen. Spezielle Sicherheitsmechanismen sorgen zudem dafür, daß nur Kunden des Service-Anbieters Zugriff auf die entsprechenden Dienstleistungen haben bzw. erhalten.

Laut Angaben der DTAG besitzt T-InterConnect derzeit eine Backbonekapazität von $n \cdot 34$ Mbit/s im Kernbereich und $n \cdot 2$ Mbit/s in den im Randbereich angeschlossenen Knoten. Der Ausbau auf 155 Mbit/s ist bereits in Vorbereitung. Jeder Punkt des Netzes ist bei einer Netzdurchlaufzeit von deutlich unter 150 ms über maximal vier Hops zu erreichen. Alle Knoten verfügen zudem über redundante Anbindungen, um dadurch Ausfälle zu vermeiden, da zu jeder Zeit auf Alternativwege ausgewichen werden kann. Ein Team des zentralen Network Operation Center (NOC) ist dafür verantwortlich, rund um die Uhr Störungen zu erkennen und zu bereinigen. Sollten Engpässe erkannt werden, d.h., wenn Schwellenwerte erreicht werden, dann kann eine Vergrößerung der Netzkapazitäten eingeleitet werden. Dies kann durch die eng vermaschte Struktur erreicht werden, da jede Verbindungsstörung dadurch durch mindestens eine alternative Strecke kompensiert werden kann. Zum Zeitpunkt der Erstellung dieses Buches besteht der T-InterConnect Backbone aus 74 Knoten innerhalb von Deutschland, und es stehen 220 Einwahlpunkte für den Zugang über das analoge Telefon oder ISDN zur Verfügung. Zudem existiert eine Vielzahl von Peering-Punkten, um damit eine Anbindung an das globale Internet mit einer Kapazität von derzeit mehr als 150 Mbit/s zu realisieren. Der Internet-Backbone ist somit vollständig in alle nationalen und internationalen Netzstrukturen integriert und verfügt über breitbandige Verbindungen zu allen wichtigen Internet-Kontenpunkten. Dies sind unter anderem Washington DC, New York, Moskau, Palo Alto, Madrid, London, Paris, Rom und viele andere mehr. So beträgt die USA-Anbindung derzeit 135 Mbit/s, wobei ein Ausbau auf 214 Mbit/s geplant ist. Hinzu kommen Verbindungsmöglichkeiten über die Netze der Partner France Télécom und Sprint im Rahmen des sogenannten »Global One«.

11 Rechnernetze – Basis der Kommunikation

Durch das Weglassen jeglicher Filterung von IP-Paketen ist für ein transparentes Routing der Daten im Internet gesorgt, wobei dies auch noch durch die Unterstützung der gesamten TCP/IP-Protokollfamilie ergänzt wird. Hierzu zählen unter anderem:

- WorldWideWeb (WWW): TCP/IP, UDP, ICMP, IGMP, SNMP, NTP, HTTP
- E-Mail: SMTP, POP3, IMAP4
- Filetransfer: FTP und Gopher
- Newsgroups: NNTP
- Remote Login-in: Telnet

Für den Zugang zum Internet reichen jedoch nicht nur die reinen Anschlußmöglichkeiten, es sind auch noch weitere Dienste zu erbringen. Auch diese werden von der DTAG angeboten und gliedern sich auf in:

- Vergabe offizieller IP-Adressen, die für den Zugang zum Internet unabdingbar sind
- Bereitstellung der Internet-Domain-Namen (DNS Namen) unter den Top-Level-Domains .de, .com, .org und .net
- IP-Adreß- und Domain-Pflege
- Accounting- und Statistik-Dienste zur besseren Auswertung und Überwachung der Internet-Zugänge

T-Net-ATM

Die DTAG bietet unter der Bezeichnung T-Net-ATM den ATM-Dienst an, der für die Telekommunikation Zugangsgeschwindigkeiten von 2, 34 und 155 Mbit/s ermöglicht. Auf diese Art und Weise spielt die räumliche Entfernung zwischen den Kommunikationspartnern keine Rolle mehr, vorausgesetzt, man kann sich die ATM-Verbindungen auch preislich leisten. Somit kann man mit T-Net-ATM breitbandige Corporate-Network-Lösungen zur Vernetzung von TK-Anlagen, LANs, Mainframes und bei Bedarf auch Telearbeitsplätzen ermöglichen.

In Abhängigkeit von den Anforderungen bietet T-Net-ATM einen einfachen ATM-Access und eine gesamte Komplettlösung (ATM-Solution) an. ATM-Access ist eine einfache Zugangsmöglichkeit zum T-Net-ATM ohne zusätzliche Dienste-Funktionen, wohingegen ATM-Solution eine Lösungsvariante inklusive Endgerät anbietet. Darin enthalten sind auch der Aufbau, der Betrieb und das Management der Einrichtungen. Mit T-Net-ATM erhält man eine sehr flexible Integration für Sprache, Daten, Video und Multimedia – und das alles über nur einen Anschluß.

11.2 Öffentliche Datenkommunikationseinrichtungen

Bestehende Kommunikationsanwendungen können ohne Schwierigkeiten in ein T-Net-ATM-System eingebunden werden und erlauben somit eine sehr sanfte Migration zu ATM. Das Unternehmen ist dadurch mit einer sehr großen Investitionssicherheit ausgestattet und garantiert dem Anwender, daß die Lösung auch bei wachsendem Kommunikationsbedarf mitwachsen kann. Egal für welche Anschlußvariante man sich entscheidet, es können die Vorteile der integrierten Sprach-, Daten- und Videoübertragung mit flexibler Bitrate genutzt werden. Es können auch die Kennzeichen von ATM genutzt werden, d.h., daß über einen einzigen Anschluß gleichzeitig mehrere Verbindungen aufgebaut werden können, und das zu unterschiedlichen Kommunikationspartnern mit verschiedenen Anwendungen. Für jede dieser Verbindungen kann zudem eine garantierte Dienstqualität (QoS = Quality of Service) vereinbart werden. Dies gilt sowohl für Selbstwahlverbindungen, bei denen die QoS-Verkehrspartner durch die Endstationen in den Signalisierungsnachrichten festgelegt werden, als auch für die festgeschalteten und zyklisch wiederkehrenden virtuellen Verbindungen. Dieser Service wird nicht nur flächendeckend in ganz Deutschland angeboten, bei Bedarf kann die Vernetzung auch weltweit durchgeführt werden.

Der Preis von T-Net-ATM setzt sich aus folgenden Bestandteilen zusammen:

- Installationspreis, abhängig von der Zugangs-klasse
- Monatlicher Grundpreis, abhängig von der Zugangs-klasse und der gewünschten Anschlußverfügbarkeit
- Verbindungsentgelt, abhängig von der Verkehrskategorie, der angeforderten Zellrate, der Entfernung und Dauer der Verbindung

Beim Einsatz von T-Net-ATM unterscheidet man noch zusätzlich sogenannte Verkehrskategorien. T-Net-ATM bietet als Verkehrskategorie die konstante Bitrate (CBR) und die variable Bitrate (VBR). Abhängig von der Anwendung werden deshalb sehr unterschiedliche Erwartungen an das Netz gestellt:

- Bei der Anschaltung einer TK-Anlage darf nur eine geringe Verzögerungszeit durch das Netz erzeugt werden, was mit der Verkehrskategorie CBR erreicht werden kann.
- Im Gegensatz dazu werden bei der Anschaltung von Legacy Services hohe Anforderungen bezüglich der Datenfehler- und der Verlustrate gestellt, und Verzögerungsraten spielen in diesen Fällen hingegen eine untergeordnete Rolle. In diesem Fall wird als einzig sinnvolle Verkehrskategorie VBR gewählt. Die Verbindungen können je nach Bedarf entweder als festgeschaltet, zyklisch wiederkehrend oder durch Selbstwahl hergestellt werden.

FrameLink Plus

Hierbei handelt es sich eigentlich um eine Interimslösung, um bis zur allgemeinen Verfügbarkeit von Breitband-ISDN schnelle Datenleitungen zur Verfügung zu stellen, die effizient für die unterschiedlichsten Anwendungen eingesetzt werden können. Von der Technik her gesehen ist FrameLink Plus ein verbindungsorientierter Datenübermittlungsdienst, der auf der Fast-Packet-Switching-Technologie Frame Relay basiert. Wenn schnelle Datenleitungen benötigt werden, setzt man derzeit hauptsächlich auf T1- (1,544 Mbit/s) bzw. E1-Verbindungen (2,048 Mbit/s). Einsatzgebiete sind dabei fast ausschließlich die Verbindung von LANs über WAN-Strecken. Die Implementierung von Frame Relay erfolgt hauptsächlich in privaten Netzen auf Standleitungen hoher Geschwindigkeit. Bekannte Hersteller wie Northern Telecom bieten bereits Frame-Relay-Vermittlungseinrichtungen an, Rechnerhersteller wie IBM und DEC unterstützen Frame Relay in ihren Kommunikationsprodukten. Wie andere bitsynchrone Protokolle verwendet Frame Relay eine Frame- bzw. Paket-Struktur. Die Technik von Frame Relay basiert auf dem LAPD-Protokoll des ISDN-D-Kanals, wodurch die Funktionen der OSI-Data-Link-Layer definiert werden. Hierbei handelt es sich um ein abgewandeltes HDLC-Protokoll. Daher kann Frame Relay auch mit einem relativ geringen Entwicklungsaufwand umgesetzt werden.

Wie bereits von ATM bekannt, leistet Frame Relay ein asynchrones Multiplexing unterschiedlicher Datenströme auf Basis von variablen Rahmenlängen im Gegensatz zu ATM, das Zellen fester Länge verwendet. Dies ist auch der Grund, weshalb Frame Relay nicht unbedingt für die Übertragung isochroner Datenströme geeignet ist. Die ATM-Zellen besitzen nur einen vorangestellten Header mit entsprechenden Kontrollinformationen. Die Prüfsequenz bezieht sich nur auf die Header-Information. Frame Relays hingegen besitzen neben einem vorangestellten Header von 3 Byte einen nachgestellten Trailer von 3 Byte, in dem sich die Prüfsequenz (2 Byte) für Kontroll- und Nutzinformation und eine Rahmenkennung (1 Byte) befinden.

Im LAPD-Protokoll ist bereits eine Ende-zu-Ende-Kennung der an der Kommunikation beteiligten Endgeräte implementiert, wobei die Ebene-2-Adresse als DLCI (Data Link Connection Identifier) bezeichnet wird. Beim Einsatz von Frame Relay wird der DLCI-Eintrag von 10 Bit Länge für die Adressierung und die Weiterleitung der Pakete auf Ebene 2 eingesetzt. Dabei haben alle Frame-Relay-Pakete, die zur gleichen Verbindung gehören, auch die gleichen DLCI-Einträge im Frame-Relay-Header.

11.2 Öffentliche Datenkommunikationseinrichtungen

FrameLink Plus ist deshalb um so wirtschaftlicher,

- je mehr Standorte vernetzt werden sollen,
- je weiter die Standorte voneinander entfernt sind,
- je höher der Vermaschungsgrad des Netzes ist.

Datex-P

Datex-P gehört in den Bereich der paketvermittelnden Netzwerke, so wie dies auch bei ISDN, Modacom und dem City-Datennetz der Fall ist. Paketvermittlung bedeutet, daß die Daten in einzelnen Datenpaketen übertragen werden. Jedes Datenpaket wird dabei mit einer Zielangabe versehen, um sicherzustellen, daß die Datenpakete auch den gewünschten Partner erreichen. Bei der Übertragung werden die Datenpakete in den Vermittlungsstellen kurzzeitig zwischengespeichert, so daß eine Geschwindigkeitsanpassung vorgenommen werden kann. Dieses Verfahren wird als store-and-forward bezeichnet. Aufgrund der Zwischenspeicherung können über Datex-P langsamere und schnelle Endgeräte Daten miteinander austauschen. Die Geschwindigkeit am Anschluß kann damit allein nach den Möglichkeiten der verwendeten Endeinrichtung und den Anforderungen der Anwendung unabhängig vom Kommunikationspartner gewählt werden.

Darüber hinaus bietet Datex-P durch die paketweise Datenübertragung die Möglichkeit, gleichzeitig mehrere Verbindungen über sogenannte logische Kanäle eines einzigen physikalischen Anschlusses aufzubauen. Datex-P ist dennoch ein verbindungsorientierter Dienst, wobei es sich bei den logischen Übertragungswegen um virtuelle Verbindungen handelt.

Alle Übertragungswege und Vermittlungseinrichtungen für Datex-P arbeiten digital. Die Datex-P-Knotenstellen sind voll vermascht, so daß sie flächendeckend bereitgestellt werden können. Ein zentrales Netzkontrollzentrum sorgt dafür, daß das paketvermittelnde Netzwerk überwacht und gesteuert wird, bis hin zum übertragungstechnischen Teil der angeschlossenen Datenendeinrichtungen. Das Netzkontrollzentrum und die Datex-P-Vermittlungsstellen sind 24 Stunden besetzt, um auf eventuelle Störungen sofort reagieren zu können.

Datex-P-Anschlüsse enden beim Kunden an einer sogenannten Datennetzanschlußdose (DNAE), womit die Signalanpassung an die Übertragungsparameter der Leitung übernommen wird. Sie ist Bestandteil des Anschlusses und bietet eine genormte Schnittstelle zur Anbindung der synchronen und asynchronen Datenendeinrichtungen.

11 Rechnernetze – Basis der Kommunikation

Datex-P entspricht den Konventionen des X.25 CCITT. Somit stehen auch unterschiedliche Zugangsmöglichkeiten bzw. -dienste für Datex-P zur Verfügung. Hierzu zählen:

- *Datex-P Remote Access*
Zugang zu Datex-P über das Telefonnetz und ohne Sicherungsprotokoll auf der Anschlußleitung bei Asynchronbetrieb
- *Datex-P Business User*
9600-Bit/s-Anschluß mit X.25-Protokoll
- *Datex-P Business Office*
19,2-Kbit/s-Anschluß mit X.25-Protokoll
- *Datex-P Business Host*
64-Kbit/s-Anschluß mit X.25-Protokoll. Die Datenendeinrichtungen müssen das X.25-Protokoll unterstützen.
- *Datex-P ISDN Access*
Zugang zu Datex-P über den D-Kanal des ISDN. Die Datenendeinrichtungen müssen das X.31-Protokoll unterstützen.

Jede Zugangsmöglichkeit bietet zudem unterschiedliche Abstufungen, die bei der Antragstellung für die unterschiedlichen Datex-P-Zugänge berücksichtigt werden müssen bzw. deren Funktionen sich auch auf den monatlichen Datex-P-Preis auswirken.

Datex-P Remote Access (Telefonzugang mittels NUI)

Analog 2.400 Bit/s	asynchron über Modem zum PAD
Analog 4.800 Bit/s	asynchron über Modem zum PAD
Analog 9.600 Bit/s	asynchron über Modem zum PAD
Analog 19,2 Kbit/s	synchron über Modem zum PAD
Analog 28,8 Kbit/s	asynchron über Modem zum PAD
Analog 14,4 Kbit/s	synchron über Modem zum X.25
ISDN 19,2 Kbit/s	asynchron über Multifunktionszugang

Datex-P Business

Für den Transfer größerer Datenmengen wird man sich bei der Entscheidung für Datex-P unter Umständen für eine dieser Anschlußmöglichkeiten entscheiden. Es stehen dabei die nachfolgend aufgeführten Möglichkeiten zur Verfügung:

- *Datex-P Business User*
Übertragungsgeschwindigkeit 9.600 Bit/s
- *Datex-P Business Office*
Übertragungsgeschwindigkeit 19,2 Kbit/s
- *Datex-P Business Host*
Übertragungsgeschwindigkeit 64 Kbit/s

11.2 Öffentliche Datenkommunikationseinrichtungen

Bei diesen Anschlußmöglichkeiten kann gewählt werden zwischen:

- segmentweiser Volumenberechnung (ein Datenpaket besteht dabei immer aus zwei Segmenten, und ein Segment enthält maximal 64 Zeichen); in diesem Fall werden die tatsächlich angefallenen Segmente berechnet;
- oder dem Kauf von Volumen-Paketen. Der Preis für die gekauften Datenmengen ist günstiger im Vergleich zur vorherigen Berechnungsmethode, jedoch sind nicht verbrauchte Volumina verloren und werden nicht erstattet und können auch nicht auf andere Anschlüsse übertragen werden. Volumenpakete decken nur die Datenmengen ab, die innerhalb von Datex-P transferiert werden. Werden in einem Abrechnungszeitraum (Monat) die vereinbarten Mengen überschritten, dann muß das überzählige Volumen pro Kbyte bezahlt werden. Ein Wechsel von einem Volumenpaket zu einem anderen erfordert eine Änderung des Auftrages, und diese Änderung muß zusätzlich bezahlt werden. Die Datenvolumina können dabei in Größen von 10, 100 oder 350 Mbyte gekauft werden.

Datex-P ISDN Access

Die ISDN-Basispakete von Datex-P sind speziell auf den Versand von kleineren bis mittleren Datenmengen konzipiert. In Abhängigkeit von den zu übertragenden Datenmengen wählt man einfach eines der drei Festpreispakete mit vorgegebenem Datenvolumen. Bei diesen Festpreispaketen handelt es sich um folgende Varianten:

- ISDN Access 100 300 Kbyte und maximal 2 Kanäle
- ISDN Access 200 3 Mbyte und maximal 10 Kanäle
- ISDN Access 300 5 Mbyte und maximal 10 Kanäle

Man kann somit auch hier sehr preisgünstige Leistungspakete erhalten, muß sich jedoch bewußt sein, daß nicht genutzte Volumina verloren sind, d.h., auch hier erfolgen keine Erstattung und keine Übertragung auf andere Anschlüsse. Werden in einem Abrechnungszeitraum (Monat) die vereinbarten Mengen überschritten, muß für die überschrittene Menge pro Kbyte nachgezahlt werden.

Es sei nochmals darauf hingewiesen, daß vor einem Datex-P-Antrag untersucht werden muß, ob nicht andere Verbindungstypen der Telekom kostengünstiger sind als Datex-P-Anschlüsse. Zudem sollten vor der Beantragung von Anschlüssen die aktuellen Preis- und Tarifinformationen der Telekom eingeholt werden. Da die Telekom im Zuge der Wettbewerbssituation immer wieder Anpassungen an den Gebührenstrukturen und Dienstleistungsmerkmale einführen wird bzw. immer wieder einführt, sollte man auf alle Fälle die aktuelle

11 Rechnernetze – Basis der Kommunikation

Entwicklung ständig verfolgen. Es kann deshalb an dieser Stelle nur auf die jetzt vorhandenen Informationen zurückgegriffen werden, die vielleicht zum Zeitpunkt der Drucklegung dieses Buchs schon nicht mehr ganz korrekt sind.

Fernsprechen

Für die gelegentliche bis regelmäßige Übertragung geringer Datenmengen ist das Fernsprechnet bestens geeignet. Mit dem Fernsprechnet kann eine große Anzahl von Teilnehmern erreicht werden, da es flächendeckend ausgebaut ist, und das weltweit. Mit Hilfe von Modems oder Akustikkopplern für den mobilen Einsatz können mit einer Datenübertragungsgeschwindigkeit von maximal 4800 Bit/s Daten übertragen werden. Die Datenübertragung im Fernsprechnet ist code- und protokolltransparent. Die Bit-Fehlerwahrscheinlichkeit liegt bei nur 0,0001. Die Gebühren sind sowohl von der Tageszeit als auch von der Entfernung abhängig – sehen Sie einfach nur Ihre Telefonrechnung etwas genauer an.

Telefax

Hierunter versteht man die Möglichkeit des Fernkopierens, d.h. die originalgetreue Abbildung und Übertragung von Schrift und Grafik mit einer Auflösung von bis zu 1728 Bildpunkten/Zeile und 7,7 Zeilen/mm (schwarzweiß). Dieser Dienst benutzt das weitverbreitete Fernsprechnet. Als Datenendeinrichtung werden sogenannte Telekopiergeräte (Telefaxgeräte) verwendet.

Neben diesen Möglichkeiten bietet die DTAG auch noch einen speziellen Dienst, der als Access Solution bezeichnet wird. Hierbei handelt es sich um eine Netzlösung, die nicht nur Anschlußleitungen verschiedener Produkte bündelt (mindestens 256 Kbit/s), sondern auch unter Umständen hilft, Kosten zu senken, die Verfügbarkeit zu erhöhen und eine größere Flexibilität bei der Bereitstellung neuer Produkte erlaubt. Hierzu wird von der DTAG der AccessLink angeboten.

AccessLink

Alle klassischen Produkte (LeasedLink Standard-Festverbindungen und Datendirektverbindungen, Datex-P, FrameLink) der DTAG benötigen eine eigene Anschlußleitung, d.h. eine Verbindung zwischen dem Kunden und der DTAG. Mit AccessLink besteht die Möglichkeit, diese Leitungen zu bündeln, d.h., es ist nicht mehr eine Vielzahl von Leitungen für jedes Produkt erforderlich, sondern nur noch eine einzige Leitung: der AccessLink. In diese Lösung lassen sich Produkte

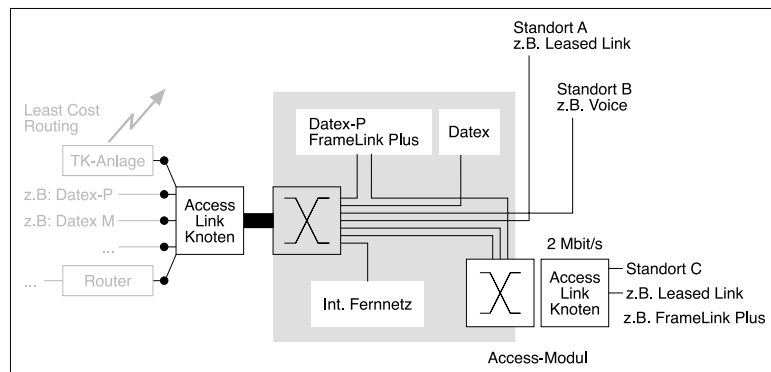
11.2 Öffentliche Datenkommunikationseinrichtungen

aus der LeasedLink-Familie, Datex M, Datex-P und FrameLink Plus integrieren.

Der AccessLink ist dann preislich interessant, wenn mindestens drei Produkte gebündelt werden und die Summenbitrate aller Produkte zusammen zwischen 256 Kbit/s und 1,92 Mbit/s beträgt. Die maximale Bitrate je Produkt (Kanal) beträgt derzeit 512 Kbit/s. Interessant ist AccessLink vor allem auch dann, wenn die Kommunikationspartner weit voneinander entfernt sind. Das größte Risiko bei der Konstellation von einer Leitung und vielen Produkten ist der Ausfall der Leitung – auch hierfür ist gesorgt. So bietet z. B. der Premium-Service mehr Sicherheit aufgrund einer Verfügbarkeit von 99,9 %, die man mit Hilfe von Ersatzleitungen erreicht.

In vielen Fällen werden durch den Einsatz von AccessLink Kosten gespart. Als weiterer Vorteil von AccessLink wird von der DTAG gesehen, daß eine hohe und garantierte Verfügbarkeit mit geringen Entstörzeiten angeboten wird. Die Bereitstellungszeiten zusätzlicher Produkte kann innerhalb von 2–3 Tagen erfolgen, sofern die »Zubringerleitung« noch über freie Kapazitäten verfügt. Zu den wesentlichen Preiskomponenten zählen die erforderlichen Bandbreiten und die Anzahl der Access-Module. Der Preis muß individuell für jeden AccessLink ermittelt werden. In Abbildung 11.2 ist dargestellt, wie der prinzipielle Funktionsmechanismus von AccessLink aussieht.

Abbildung 11.2
AccessLink-
Mechanismus

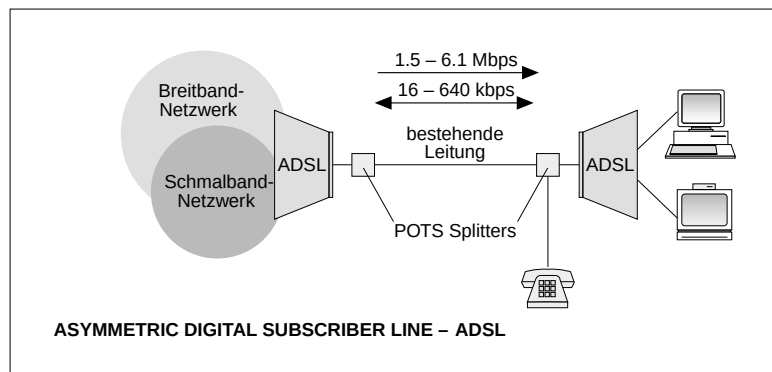


Um das Angebot an breitbandigen Internet-Anwendungen noch attraktiver zu machen, startet die DTAG die ersten Pilotversuche mit ADSL. Der folgende Abschnitt soll kurz aufzeigen, was sich hinter ADSL verbirgt und welche Vorteile damit verbunden sind.

11 Rechnernetze – Basis der Kommunikation**ADSL – Was sich dahinter verbirgt**

ADSL ist die Abkürzung für Asymmetric Digital Subscriber Line und bezieht sich im Prinzip nicht auf eine echte Verbindung, sondern den Einsatz spezieller Modems, um aus einer herkömmlichen Twisted-Pair-Kupferleitung für das Telefon eine sehr schnelle, digitale Verbindung herstellen zu können. Das Modem wird deshalb als asymmetrisch bezeichnet, weil der Empfang von Daten mit einer höheren Geschwindigkeit erfolgt als die Datenübertragung zur Gegenstelle. ADSL benötigt zwei ADSL-Modems auf beiden Seiten der Telefonleitung. Die Modems unterteilen die Telefonleitung in drei getrennte Kanäle, wobei ein Kanal den Datenverkehr mit hoher Geschwindigkeit abwickelt, ein Kanal mit geringerer Geschwindigkeit steht als Duplex-Kanal zur Verfügung, und der andere Kanal realisiert die herkömmliche Telefonie, deshalb bezeichnet man diesen Kanal auch als Plain Old Telephone Service (POTS). Der POTS-Kanal ist mit Hilfe von Filtern vom digitalen Modem getrennt, so daß ein ununterbrochener POTS-Kanal zur Verfügung steht, auch wenn ADSL nicht funktionieren sollte. Der Hochgeschwindigkeitskanal weist Datenübertragungsraten von bis zu 8 Mbit/s auf, hingegen kann der Duplex-Kanal Datenraten von 16 bis 640 Kbit/s realisieren. Wenn man bedenkt, daß es sich bei diesem Kanal immer nur um den Datenverkehrstransport handelt, der vom Endgerät zum Beispiel zum Web-Server im Internet übertragen wird, dann reicht diese Performance durchaus. In Abbildung 11.3 ist der generelle Aufbau von ADSL aufgezeigt. Jeder Kanal kann bei Bedarf durch Multiplex-Mechanismen in mehrere Kanäle mit geringeren Übertragungsraten unterteilt werden. ADSL ist normalerweise kompatibel zur amerikanischen und europäischen digitalen Hierarchie.

Abbildung 11.3
Der Aufbau von
ADSL



11.2 Öffentliche Datenkommunikationseinrichtungen

Zum Zeitpunkt der Erstellung dieses Buches wurden bereits die ersten Pilotprojekte der DTAG in Nordrhein-Westfalen durchgeführt. Dabei geht es vor allem darum, die breitbandigen Angebote auf Basis der ADSL-Technologie in allen Punkten zu prüfen. Dazu gehört auch die Prüfung der Online-Dienste und der schnelle Internet-Zugang. Zusätzlich zu den bestehenden Internet-Zugängen sollen für die Pilotkunden auch Inhalte von Content-Providern bereitgestellt werden, die hohe Übertragungsraten der ADSL-Anschlüsse bedienen können. Über den herkömmlichen Kupferdraht ist die DTAG bereits in der Lage, bis zu 8 Mbit/s zu übertragen (z.B. aus dem Internet zum Kunden), und in die Gegenrichtung (z.B. vom Kunden zum Internet) können dies immerhin auch noch 786 Kbit/s sein. Daß daneben auch noch der herkömmliche Telefondienst abgewickelt werden kann, muß zwecks Einhaltung der Standardvorgaben angeboten werden. Es gibt neben ADSL auch noch andere DSL-Technologien. Tests mit diesen anderen DSL-Technologien haben ergeben, daß sie Übertragungsraten von bis zu 25 Mbit/s zulassen. Es sei nochmals darauf hingewiesen, daß man bei der ADSL-Technologie die Tatsache ausnutzt, daß bei vielen Diensten die Datenraten vom und zum Kunden sehr unterschiedlich, also asymmetrisch, sind. So transportiert ein interaktiver Videodienst oder das Arbeiten im Internet die Daten mit 2 bis 8 Mbit/s zum Kunden, hingegen werden für Rückmeldungen zum Anbieter niedrige Datenraten von 18 bis 640 Kbit/s benötigt. Die Reichweite für die Übertragungsraten von 2 Mbit/s beträgt derzeit ca. drei Kilometer, hingegen können bei einer Übertragungsrate von 6 Mbit/s nur noch zwei Kilometer überbrückt werden.

Die Zukunft wird zeigen, inwiefern sich die ADSL-Technologie unter Umständen gegen ISDN durchsetzen wird, da man inzwischen mit 64 Kbit/s bzw. 128 Kbit/s (gebündelter S0-Anschluß) starke Performance-Engpässe bekommt, aber immer mehr Leistung gefordert wird.

11.2.3 Der Weg zum ISDN-Netz

Nach den bisherigen Ausführungen über die Möglichkeiten einer LAN-Kopplung mit anderen Rechnernetzen und dem Aufbau von Wide Area Networks kann festgestellt werden, daß die Kommunikation derzeit über zwei Netze der Telekom durchgeführt werden kann, das sind

- das Telefonnetz und
- das integrierte Text- und Datennetz (IDN).

11 Rechnernetze – Basis der Kommunikation

Das IDN ist der erste wichtige Schritt im Bereich der Kommunikation in Richtung Vereinheitlichung der Netzwerkstruktur und Netzwerktechnologie. Gleichzeitig tragen die Dienste, die ein solches Netz zur Verfügung stellen, dazu bei, Qualität und Funktionalität zu steigern.

Beim ISDN wird ein weiterer Schritt vorwärts getan, um alle schmalbandigen Dienste wie Sprache, Daten, Text und Faximile zu integrieren. ISDN ist das Akronym für Integrated Services Digital Network. Aus der Bezeichnung lassen sich zwei wichtige Funktionen dieses Netzes ableiten:

1. *DN – Digital Network*

Hier handelt es sich um ein digitales Netz.

2. *IS – Integrated Services*

Das Netz ist dadurch gekennzeichnet, daß die Kommunikationsdienste integriert sind, d. h., es wird mehr als ein Dienst über das gleiche Netz unterstützt.

Die CCITT definiert ISDN wie folgt:

„An ISDN is a network, in general evolving from telephony IDN, that provides end-to-end digital connectivity to support a wide range of services, including voice and non-voice services, to which users have access by a limited set of standard multi-purpose user-network interfaces.“

Es gibt einige vernünftige Argumente, die für die Einführung eines universellen öffentlichen Datennetzes sprechen:

Qualität

Bei der analogen Übertragung ist das Signal relativ ungeschützt gegenüber einer Störung, also Verfälschung, durch andere Signale. Bei der Überlagerung eines analogen Signals mit anderen Signalen entsteht ein neues analoges Signal. Das originale Signal läßt sich nur sehr schwer wieder rekonstruieren. Die Elemente der analogen Übertragung, wie zum Beispiel Verstärker, unterscheiden nicht zwischen Original-, Stör- oder Summensignal. Somit wird eine Störung, wenn diese vorhanden ist, genauso verstärkt. Ein digitales Signal hingegen kann auf mehrere Arten vor Störungen geschützt werden. Ein digitales Signal kann sich nur innerhalb bestimmter Schwellenwerte bewegen, die binäre Darstellung einer 0 oder einer 1. Durch geeignete Hardware, einem Schmitt-Trigger zum Beispiel, können verstümmelte Signale wieder zurückgewonnen werden. Zudem kann durch eine redundante Kodierung der darzustellenden Zeichen zusätzliche Sicherheit bei der Datenübertragung eingebaut werden. Als weitere Sicherungsmaßnahme kann eine blockweise Absicherung der Daten durch Anfügen von Prüfsummen erreicht werden.

11.2 Öffentliche Datenkommunikationseinrichtungen

Somit stellt man fest, daß beispielsweise durch folgende Maßnahmen die Qualität der Datenübertragung deutlich verbessert werden kann:

- Bitweise Regenerierung
- Wortweise Kodierung
- Blockweise Prüfung

Die Umsetzung der analogen Signale in digitale Signale und umgekehrt stellt heute kein Problem mehr dar.

Rationalisierung

Es wurde bereits mehrfach darauf hingewiesen, daß die Informationsflut in der heutigen Zeit rasch steigt und damit auch der Bedarf an Kommunikation. Durch den Einsatz von offenen multifunktionalen Endgeräten wird die Vereinheitlichung der Systeme am Arbeitsplatz wesentlich einfacher. Bei genauer Betrachtung der Anforderung für die Kommunikation von Netzwerken untereinander ist ein ISDN langfristig die einzig mögliche und sinnvolle Einrichtung. Die Mannigfaltigkeit der Individuallösungen wird dadurch zwar auch geschmälert, allerdings mit dem positiven Nebeneffekt, daß die Systeme aufgrund der Standardisierung billiger werden.

Schrittweise Einführung von ISDN

Die flächendeckende Einführung von ISDN kann nicht derart durchgeführt werden, daß sofort alle bekannten Fernmeldedienste in das ISDN eingebunden werden. Ausgangspunkt für ISDN ist die Digitalisierung des Telefonnetzes. In diesem Bereich ist die meiste Arbeit zu erbringen, da es sich beim Telefonnetz der Telekom um ein rein analoges Netz handelt. Ist erst einmal das Telefonnetz digitalisiert, so können neben dem Fernsprechen alle anderen auf diesem Netz basierenden Dienste digital angeboten werden.

Das Fernsprechnetzt besteht aus den Bereichen Anschlußtechnik, Vermittlungstechnik, Übertragungstechnik und der Zentralkanalzeichengabe. Arbeiten die letzten drei Bereiche digital, kann von einem digitalen Telefonnetz gesprochen werden. Einfacher formuliert: Beim digitalen Fernsprechnetzt reicht die digitale Verbindung von Ortsvermittlungsstelle zu Ortsvermittlungsstelle; die Teilnehmeranschlußleitung wird unverändert analog betrieben, so daß sich auch bezüglich der angeschlossenen bzw. anschließbaren Endgeräte keine Änderungen ergeben. Um nun dieses digitale Telefonnetz zu einem ISDN-Telefonnetz zu machen, müssen die analogen Anschlüsse durch digitale Anschlußleitungen ersetzt werden. Zudem müssen die Vermittlungsstellen mit den genormten ISDN-Leistungsmerkmalen ausgestattet sein.

11 Rechnernetze – Basis der Kommunikation

Die Weiterführung der Digitaltechnik bis zum Teilnehmer ist die logische Weiterentwicklung des digitalen Fernsprechnetzes. Eine durchgehende digitale Verbindung von Teilnehmer zu Teilnehmer erlaubt die Realisierung einer Reihe neuer Leistungsmerkmale. Der durchgehende 64-kbps-Kanal hat – abgesehen von der Festlegung der für Sprachübertragung geeigneten Bitrate – keine dienstspezifischen Eigenschaften. Er kann deshalb für alle Kommunikationsdienste benutzt werden, für die eine Datenrate von 64 kbps ausreichend ist; auf dieser Basis kann also ein dienstintegrierendes Netz – das ISDN – aufgebaut werden.

Die Digitalisierung des Telefonnetzes heißt, daß die anfallenden analogen Sprachsignale binärkodiert auf elektronischem Weg übertragen werden. Im Vergleich zur herkömmlichen Technik bedeutet dies eine einfachere Verarbeitung. Neben der höheren Qualität der Sprachübertragung (kein Rauschen in der Leitung, kein Übersprechen der Leitung) zeichnet sich das digitale Telefonieren auch durch schnellere Verbindungsaufbauzeiten aus.

Struktur, Schnittstellen und Anschlußarten des ISDN

ISDN wird auf den herkömmlichen Zweidrahtkabeln aus Kupfer realisiert. Dies liegt vor allem daran, daß bereits ein sehr großes flächendeckendes Kupferdoppeladernetz – das Telefonnetz – existiert und damit einer Realisierung von ISDN das Feld schon bereitet ist.

Die Kupferdoppelader gestattet technisch bedingt eine maximale Nettodatenrate von 144 Kbit/s. Diese Übertragungsrate ist der Ausgangspunkt für die Kanalstruktur von ISDN. ISDN besteht aus zwei Kanälen (B1 und B2) mit je 64 Kbit/s Kapazität und einem D0-Kanal mit 16 Kbit/s Leistung. Dies ergibt $64+64+16=144$ Kbit/s. Diese Struktur wird als ISDN-Basisanschluß bezeichnet. Die verfügbare Bruttoübertragungsrate liegt jedoch über 144 Kbit/s, da zusätzliche Kapazität benötigt wird, um diverse Steuerungsaktivitäten nutzen zu können, zum Beispiel zu Prüfzwecken oder fehlerkorrigierenden Maßnahmen.

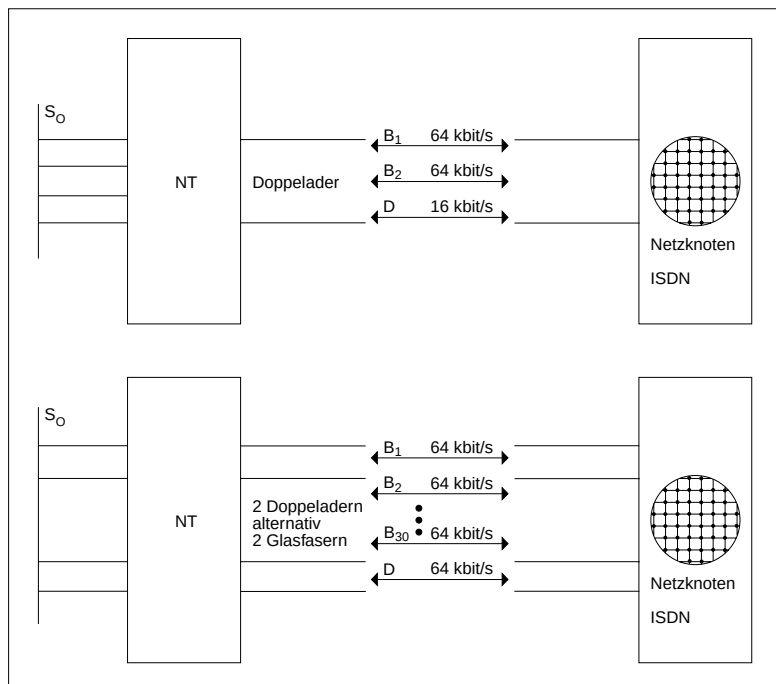
Über die beiden Kanäle können alle Dienste durchgeführt werden, für die eine Übertragungsrate von 64 Kbit/s ausreichend ist. Der D-Kanal wird zur Übertragung von Steuerungsinformationen für die eingesetzten Dienste benötigt, die über die beiden B-Kanäle ausgeführt werden. Alle Kanäle werden dabei wechselseitig betrieben. Der D-Kanal (Steuerkanal) dient hauptsächlich zur Übertragung der Zeicheneingabeinformationen zwischen den Endeinrichtungen beim Kunden und der Ortsvermittlungsstelle. Der Steuerkanal kann im Euro-ISDN zusätzlich auch für die paketorientierte Datenübertragung, z.B. für die Kommunikation mit Endgeräten an Datex-P-

11.2 Öffentliche Datenkommunikationseinrichtungen

Anschlüssen, benutzt werden. Zu beachten ist dabei, daß der Steuerkanal nicht als durchgängiger Kanal zwischen den Endeinrichtungen installiert ist.

Daneben wird auch noch der Primärmultiplexanschluß angeboten, der für Kunden mit hohem Kommunikationsbedarf gedacht ist. Dieser Anschluß umfaßt nicht weniger als 30 Kanäle mit einer Datenrate von 64 Kbit/s und einen Steuerkanal mit einer Datenrate von 64 Kbit/s. Daran werden mittlere und große TK-Anlagen oder auch Anlagen zur Datenübertragung (z. B. Großrechner) angeschlossen. Der Netzanschluß (NT) für den Basisanschluß wird mit einer Kupferdoppelader bereitgestellt, der Netzanschluß für den Primärmultiplexanschluß wird durch einen speziellen Netzanschluß zur Verfügung gestellt: entweder über zwei herkömmliche Kupferdoppeladern oder über zwei Glasfasern. Die B-Kanäle beider Anschlußarten können gleichzeitig und vollkommen unabhängig voneinander genutzt werden, also so wie jeweils eigene Leitungen zu unterschiedlichen Partnern. Über den einen B-Kanal kann zum Beispiel telefoniert werden, wohingegen über den anderen B-Kanal ein Telefax empfangen oder versendet werden kann. In Abbildung 11.4 sind diese beiden Varianten dargestellt.

Abbildung 11.4
Basis- und Primär-
multiplexanschluß



11 Rechnernetze – Basis der Kommunikation

Die getrennt nutzbaren B-Kanäle lassen sich andererseits aber auch von einem Endgerät, z. B. einem Router mit ISDN-Karte, zu einer einzigen Verbindung zusammenfassen, um dadurch einen höheren Datendurchsatz erzielen zu können. So sind am Basisanschluß Verbindungen mit 128 Kbit/s ($2 \cdot 64$ Kbit/s) und am Primärmultiplexanschluß Verbindungen mit 1,92 Mbit/s ($30 \cdot 64$ Kbit/s) möglich.

Die Schnittstelle, mit der zum Beispiel Telefone, Fernkopierer, Btx-Geräte, Personalcomputer – kurz, alle ISDN-Endgeräte – an den Basisanschluß angeschaltet werden, ist die international standardisierte Schnittstelle S0. Das ISDN-Konzept sieht auf der Teilnehmerseite Mehrgerätekonfigurationen vor, d. h., es können mehrere Endgeräte installiert sein, wovon aber – da beim Basisanschluß zwei B-Kanäle zur Verfügung stehen – nur zwei gleichzeitig aktiv sein können. Man hat sich bei der Festlegung der S0-Schnittstelle darauf geeinigt, diese am Netzabschluß als passiven Bus für den Anschluß von maximal acht Endgeräten zu konzipieren. Beim Primärmultiplexanschluß existiert an der Ortsvermittlungsstelle eine eigenständige Leitungsendeinrichtung. Die Benutzerschnittstelle wird in diesem Fall als S2M bezeichnet und stellt das Bindeglied zwischen dem Netzabschluß (Posteigentum) und der Teilnehmereinrichtung (z. B. ISDN-fähige digitale Nebenstellenanlage) dar.

Die einzelnen Komponenten im ISDN sind die Endgeräte, die Kommunikationssteckdose, das Netzabschlußgerät (NT) mit der definierten Schnittstelle, die Übertragungswege und die Vermittlungseinrichtungen. Der technische Verantwortungsbereich der Telekom endet an der Schnittstelle zwischen den Endeinrichtungen und dem Anschluß. Diese Schnittstelle befindet sich physikalisch gesehen im Netzabschlußgerät und stellt den definierten Übergabepunkt für Informationssignale dar. Alle anderen Komponenten, wie Endgeräte und Kommunikationssteckdosen, fallen zwar in den Zuständigkeitsbereich des ISDN-Kunden, doch bietet die Telekom eine Vielzahl von Lösungen an.

Der Netzabschluß (NT) am Basisanschluß hat folgende Aufgaben:

- Der Netzabschluß (NT) kann als Übergang zwischen dem öffentlichen Netz und der Teilnehmerinstallation auf der Kundenseite betrachtet werden. Dem NT kommen die Aufgaben zur Bereitstellung der standardisierten S0-Schnittstelle, Fehlerdiagnose und Störungseingrenzung, die Anpassung an die Übertragungseigenschaften des Netzes, die Spannungsversorgung der Telefone und der Schutz des Netzes bei Fehlern im Endstellenbereich zu.
- Wie im analogen Netz genügt auch für einen ISDN-Basisanschluß eine herkömmliche Kupferdoppelader als Anschlußleitung. Deshalb müssen zur Realisierung eines ISDN-Basisanschlusses keine

11.2 Öffentliche Datenkommunikationseinrichtungen

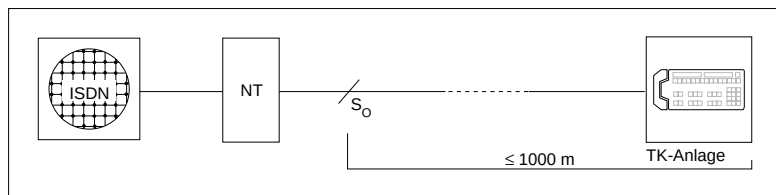
neuen Leitungen zum Gebäude des Kunden verlegt werden. Eine einfache Doppelader wird am NT des Teilnehmers angeschlossen. Die Leitung verläuft dann, vom NT abgehend, mit zwei Doppeladern weiter zu den Endgeräten. In der Regel können wiederum die im Gebäude bereits vorhandenen Leitungen verwendet werden. Der Übergang von der Anschlußleitung auf den NT wird als UK0-Schnittstelle und der Übergang vom NT auf die Busleitung zu den Endgeräten als S0-Schnittstelle bezeichnet.

Zum Anschluß aller Endgeräte mit der international standardisierten S0 gibt es im ISDN eine einheitliche Telekommunikationssteckdose IAE (ISDN-Anschluß-Einheit), die ebenfalls international standardisiert ist. Diese universelle Anschlußtechnik gewährleistet, daß Sie Ihre ISDN-Endgeräte, egal ob Telefon oder PC, flexibel und Ihren Bedürfnissen entsprechend einsetzen können. Der ISDN-Basisanschluß kann in zwei Konfigurationen realisiert werden.

1. Punkt-zu-Punkt-Konfiguration

Es wird an einem ISDN-Basisanschluß nur ein einzelnes Endgerät angeschlossen. Dabei kann die Entfernung zwischen einem NT und der angeschlossenen Endeinrichtung bis zu 1000 Meter betragen. Abbildung 11.5 stellt dies dar.

Abbildung 11.5
Punkt-zu-Punkt-
Konfiguration



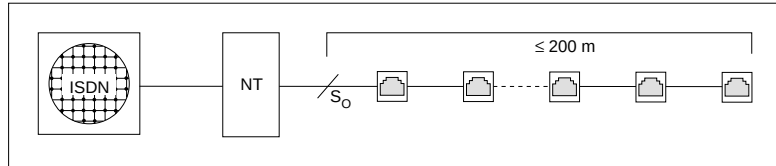
2. Punkt-zu-Mehrpunkt-Konfiguration

Diese Art der Konfiguration wird auch als passiver Bus bezeichnet. Hier können an einem ISDN-Basisanschluß bis zu zwölf einheitliche ISDN-Steckdosen angeschlossen werden. Die Entfernung vom NT bis zur letzten Dose kann bis zu 200 Meter betragen. Bei anderen Varianten des passiven Busses können aber auch größere Entfernungen erreicht werden. So lassen sich zum Beispiel beim erweiterten passiven Bus, das sind mehrere Endeinrichtungen am Ende einer langen Installationsleitung, Reichweiten bis zu 500 Meter realisieren. An die zwölf ISDN-Steckdosen können nicht mehr als acht Endgeräte angeschlossen werden, wobei das Anschlußkabel zwischen Endgerät und Steckdose maximal zehn Meter lang sein darf. In Abbildung 11.6 ist auch diese Möglichkeit dargestellt.

11 Rechnernetze – Basis der Kommunikation

Neben Basis- und Primärmultiplexanschluß gibt es auch noch Standardfestverbindungen im ISDN.

Abbildung 11.6
Punkt-zu-Mehr-
punkt-Konfigura-
tion



Standardfestverbindungen mit ISDN-verwandten Strukturen sind als Alternative zu Wählverbindungen von Vorteil, wenn die Leitungsauslastung hoch ist und schnelle Zugriffszeiten und dauernde Verfügbarkeit gefordert sind. Als Standardfestverbindungen werden eingesetzt:

- **Digital S01**
Hierbei stehen ein Basiskanal und ein Steuerkanal zur Verfügung (1B + D16).
- **Digital S02**
Diese Anschlußform stellt zwei Basiskanäle und einen Steuerkanal bereit (2B + D16).
- **Digital 2MS**
Dieser Anschluß bietet bis zu 30 Basiskanäle und einen Steuerkanal (30B + D64).

Euro-ISDN

Das Euro-ISDN arbeitet mit dem E-DSS1. Die Telekom hat inzwischen alle bestehenden ISDN-Vermittlungsstellen aufgerüstet, um jedem ISDN-Kunden Euro-ISDN-Anschlüsse zur Verfügung stellen zu können, so daß keine 1TR6-Anschlüsse mehr beantragt werden können. Euro-ISDN nutzt Basis- und Primärmultiplexanschlüsse mit der gleichen Struktur wie das deutsche ISDN. Die Anzahl, Art und Übertragungskapazität der B- und D-Kanäle sind mit dem bisher besprochenen identisch. Das deutsche ISDN und Euro-ISDN unterscheiden sich lediglich durch das verwendete Signalisierungsverfahren im D-Kanal (D-Protokoll). Die Änderungen bei der Einführung von Euro-ISDN reduzieren sich auf die der Software. Hardware-Änderungen in den Vermittlungsstellen oder am Netzabschluß beim Kunden sind ebenfalls nicht notwendig. Der bereits seit 1991 von der Telekom eingesetzte ISDN-Stecker nach Norm ISO 8877, der Western-Stecker, entspricht bereits der Norm im Euro-ISDN.

11.2 Öffentliche Datenkommunikationseinrichtungen

Im Euro-ISDN kann mit Partnern im normalen ISDN kommuniziert werden. Die Telekom sorgt dafür, daß bei solchen Verbindungen die Umsetzung in das jeweils andere Protokoll durchgeführt wird. Die Endeinrichtungen des nationalen ISDN können nicht ohne weiteres am Euro-ISDN-Anschluß eingesetzt werden. Dennoch können vorhandene Terminals weiter genutzt werden, weil die Telekom noch die nächsten Jahre das nationale D-Kanal-Protokoll 1TR6 neben dem europäischen European Digital Subscriber Signalling System No. 1 (E-DSS1) in den Vermittlungsstellen unterstützen wird. Somit können Endgeräte, die dem nationalen, und Endgeräte, die dem neuen europäischen Standard entsprechen, parallel und gleichzeitig im Netzwerk eingesetzt werden.

In der Regel sollten die ISDN-Karten, so wie diese in PCs, Routern etc. in einem Netzwerk eingesetzt werden und mit einem nationalen ISDN-Protokoll arbeiten, durch einfachen Softwarewechsel auf das europäische Protokoll umgestellt werden können. Die Telekom bietet zusätzlich einen bilingualen Basisanschluß an. Daran lassen sich Endgeräte anschließen, die sowohl dem nationalen Standard als auch dem Euro-ISDN-Standard entsprechen. Hierzu installiert die Telekom einen speziellen Netzabschluß. Dieser verwendet in Richtung Netz das europäische E-DSS1 und unterstützt auf der Endgeräteseite zusätzlich das deutsche 1TR6-Protokoll.

Für Tk-Anlagen mit mehreren ISDN-Anschlüssen kann man in der Regel bei Bedarf Anschlüsse zur Unterstützung beider Standards installieren. In Abhängigkeit von Anschluß und Konfiguration können so Endgeräte des jeweiligen Standards eingesetzt werden.

Im Memorandum of Understanding on the Implementation of European ISDN Services haben sich bislang 26 Netzbetreiber aus 20 europäischen Ländern verpflichtet, ISDN nach dem europäischen Standard einzuführen. Jeder Betreiber verpflichtet sich zudem, sowohl Basis- als auch Primärmultiplexanschlüsse anzubieten. Dazu muß ein Minimum an Telekommunikationsdiensten und Leistungsmerkmalen angeboten werden. Zu diesem Mindestangebot gehören:

- 64 Kbit/s transparente Übermittlung ohne Einschränkung
- 3.1 kHz a/b Übermittlungsdienst
- Übermittlung der Rufnummer des Anrufers zum gerufenen Teilnehmer
- Unterdrückung der Übermittlung der Rufnummer
- Durchwahl zu den Nebenstellen an Tk-Anlagen
- Mehrfachrufnummer am Mehrgeräteanschluß
- Umstecken von Endgeräten am Mehrgeräteanschluß

11 Rechnernetze – Basis der Kommunikation

Das Leistungsmerkmal der Mehrfachrufnummer ersetzt die im nationalen ISDN angebotene Endgeräteauswahlziffer. Bei der Endgeräteauswahlziffer stehen durch Anhängen einer weiteren Ziffer an die ISDN-Rufnummer genau zehn Rufnummern in aufsteigender Reihenfolge zur Verfügung. Das Euro-ISDN hingegen ist dabei viel leistungsfähiger. Bis zu zehn beliebige Rufnummern aus dem Rufnummernvolumen der Vermittlungsstelle können als Mehrfachrufnummern vergeben werden. Aber was hat man eigentlich davon? – Der Anwender kann seine Rufnummern von analogen Anschlüssen auf den ISDN-Anschluß übernehmen, sofern die analogen Anschlüsse an einer digitalen Vermittlungsstelle angeschaltet waren. Auf diese Weise erspart man sich einen Rufnummernwechsel.

Für das Euro-ISDN gilt grundsätzlich, daß sich die Leistungsmerkmale auf die Rufnummer beziehen und nicht auf den Anschluß.

Die im ISDN verfügbaren Dienste und Möglichkeiten sollen nachfolgend näher erläutert werden. Hierbei wird man auch feststellen, daß es durchaus Dienste gibt, die für Netzwerke notwendig und interessant sind.

Im einzelnen sind folgende Dienste im *Schmalband-ISDN* möglich:

ISDN-Fernsprechen

Die wichtigste Neuerung auf diesem Gebiet ist die verbesserte Qualität beim Telefonieren. Sie kann bis zur Rundfunktonqualität verbessert werden. Die Verbindungsaufbauzeiten werden drastisch verkürzt. Störgeräusche beim Telefonieren (Nebensprechen, Knacken und dergleichen) treten nicht mehr auf. Folgende Dienste können zusätzlich genutzt werden:

■ *Dienstwechsel*

Unter Dienstwechsel versteht man die Möglichkeit, mit einem Partner zu telefonieren und während des Telefonats ein Fax zu senden. Wenn sich eine solche Situation ergibt, wird das Telefonat kurzfristig unterbrochen und nach dem Versenden des Faxes das Gespräch wieder aufgenommen, ohne daß das Gespräch neu initiiert werden müßte.

■ *Umsteckmöglichkeit*

Das ist vor allem dann interessant, wenn man während des Telefonats den Raum wechseln will bzw. muß. In diesem Fall zieht man einfach den Stecker aus der ISDN-Dose und steckt ihn im anderen Raum wieder in die ISDN-Dose. Man nennt diese Funktion auch Parken, wobei die Zeit vom Ziehen des Steckers bis zum erneuten Einstecken maximal zwei Minuten betragen darf. Man

11.2 Öffentliche Datenkommunikationseinrichtungen

sollte also in einen Raum wechseln, den man innerhalb dieser Zeitspanne erreichen kann, damit das Gespräch nicht verlorengeht.

■ *Gerätewechsel*

Sind mehrere ISDN-Telefone am gleichen ISDN-Anschluß vorhanden, kann man ein Telefonat an einen anderen Apparat weiterleiten.

■ *Endgeräteauswahl*

In diesem Fall kann jedes am ISDN-Bus angeschlossene Endgerät direkt von außen adressiert werden. Jedes angeschlossene Gerät verfügt über eine EAZ (Endgeräteauswahlziffer), um exakt adressiert werden zu können. Sind zum Beispiel vier Telefone am ISDN-Bus angeschlossen, kann jedes Telefon direkt von außen einen Anruf entgegennehmen, und die restlichen drei Telefonate klingeln beim eingehenden Anruf nicht.

■ *Anzeigen der Rufnummer und Anklopfen*

Im ISDN können Sie bereits vor dem Zustandekommen der eigentlichen Verbindung dem gewünschten Kommunikationspartner Ihre Rufnummer mitteilen. So wird ein Verbindungswunsch auch dann signalisiert, wenn der andere Anschluß bereits besetzt ist. Der Anruf wird einfach auf dem Display des ISDN-Telefons angezeigt, und der Angerufene kann entsprechend reagieren. Man bezeichnet diesen Vorgang als Anklopfen.

■ *Anzeigen der Rufnummer und Anklopfen*

Hier wird die Rufnummer des Anrufers nicht nur angezeigt, sondern auch durch Anforderung des Anrufenden die tatsächlich erreichte ISDN-Rufnummer übermittelt. Der Abgleich von gewünschter und erreichter Rufnummer erhöht die Sicherheit vor allem dann, wenn vertrauliche Informationen im ISDN übertragen werden.

■ *Feststellen ankommender Wählverbindungen*

Auf ähnliche Weise lassen sich die Rufnummern von sogenannten Klingelstörern, bedrohenden oder belästigenden Anrufern durch einen Auftrag an die Telekom identifizieren. Auf Wunsch lassen sich in der Vermittlungsstelle ankommende Wählverbindungen feststellen. Ganz gleich, ob eine Verbindung zustandekam oder nicht, die Informationen können ermittelt werden. Als Ergebnis erhalten Sie einen Ausdruck mit der Rufnummer des Anrufers, Datum und Uhrzeit des Anrufs oder Anrufversuchs. Dieser Dienst ist allerdings nicht kostenlos.

■ *Durchwahl mit Basisanschluß*

Bereits ab einem Basisanschluß mit nur zwei B-Kanälen sind entsprechend konzipierte ISDN-Tk-Anlagen durchwahlfähig zu allen angeschlossenen Nebenstellen. Bei einer analogen Tk-Anlage ist

11 Rechnernetze – Basis der Kommunikation

dies erst ab acht Leitungen möglich. Für die Tk-Anlage erhält man eine einheitliche Rufnummernbasis, vergleichbar mit der Sammelrufnummer am analogen Anschluß.

■ *Geschlossene Benutzergruppe*

Vor allem beim Datenaustausch schützt eine geschlossene Benutzergruppe gegen den unbefugten Zugriff von Dritten. Nur Mitglieder der geschlossenen Benutzergruppe haben Zugang zu den Rufnummern der Gruppe. Geschlossene Benutzergruppen können je Mehrfachrufnummer und je Dienst eingerichtet werden. Berechtigte Benutzer können Teilnehmer aus den verschiedenen öffentlichen Netzen sein. Bis zu 100 verschiedene geschlossene Benutzergruppen sind pro Anschluß möglich und maximal 20 pro Dienst.

■ *Anrufweiterschaltung*

Im ISDN kann jeder eingehende Anruf dienstspezifisch zu einem anderen Anschluß weitergeschaltet werden. Dabei spielt es keine Rolle, wo sich das Ziel der Weiterschaltung befindet. Ohne Einschränkung lassen sich Anrufe zu jedem Anschluß auf der Welt weiterschalten, auch zu Funktelefonen. Werden bei der Anrufweiterschaltung I ankommende Anrufe sofort zum angegebenen Ziel weitergeschaltet, erfolgt die Weiterschaltung bei der Anrufweiterschaltung II erst nach 15 Sekunden.

Es kann hierbei zwischen den folgenden Modi unterschieden werden:

- ständig
- bei »Besetzt«
- bei »Nichtmelden« (erst nach 15 Sekunden, so daß der gerufene Teilnehmer die Gelegenheit hat, den Anruf entgegenzunehmen)

■ *Dauerüberwachung*

Dieser Dienst wird von der Telekom als Sonderservice angeboten. In diesem Fall wird die Funktionalität des Anschlusses permanent überwacht, um bei auftretenden Störungen sofort reagieren zu können. Das ist vor allem bei Datenübertragungen wichtig, da damit die Fehlerhäufigkeit gesteuert werden kann.

■ *Semipermanente Verbindungen*

Hier handelt es sich um vorbestellte Dauerwählverbindungen. Es wird eine Verbindung mit einem vordefinierten Teilnehmer aufgebaut, wobei dieser Verbindungsaufbau über den D-Kanal geschieht. Der B-Kanal als echter Nutzkanal wird erst dann aktiviert, wenn er auch tatsächlich belegt werden muß. Der Verbindungsaufbau wird dadurch beschleunigt, daß es nicht dazu kommen kann, daß besetzt ist. Vor allem bei der Datenübertragung ist dies ein interessanter Aspekt.

11.2 Öffentliche Datenkommunikationseinrichtungen

Wenn man einen ISDN-Anschluß beantragt, ist zwischen einem Mehrgeräte- und einem Tk-Anlagenanschluß zu unterscheiden. Die für den Mehrgeräteanschluß und den Tk-Anlageanschluß angebotenen Leistungsmerkmale weichen teilweise voneinander ab. Dies liegt vor allem auch daran, daß ein Teil der durch die Telekom bereitgestellten Leistungsmerkmale beim Vorhandensein einer privaten Tk-Anlage nicht selten bereits von dieser erbracht werden. Zudem muß bei der ISDN-Anschlußbeantragung unterschieden werden zwischen einem Standardanschluß und einem Komfortanschluß. Damit Sie sich ein Bild über die einzelnen Leistungsmerkmale in Abhängigkeit vom beantragten ISDN-Anschluß machen können, soll die nachfolgende Tabelle die wichtigsten Merkmale aufzeigen. Bevor ein ISDN-Antrag gestellt wird, sollte man sich vorher darüber informieren, wie bei der Telekom die aktuellen Dienste strukturiert sind, da es durchaus passieren kann, daß Dienste als neuer Standard kostenfrei übernommen worden sind, die vielleicht vor kurzem nur gegen Aufpreis zur Verfügung standen.

Tabelle 11.1
ISDN-Fernsprech-
dienste

● Leistung im Grundpreis enthalten ▲ Leistung im Grundpreis nicht enth. — Leistung hier nicht verfügbar	Standardanschluß		Komfortanschluß	
	Mehrgeräte- anschluß	Anlagen- anschluß	Mehrgeräte- anschluß	Anlagen- anschluß
Übermittlung der Rufnr. des Anrufers	●	●	●	●
Halten einer Verbindung (Rückfrage)	●	—	●	—
Umstecken am Bus	●	—	●	—
Mehrfachrufnummer (3 Rufnummern)	●	—	●	—
Durchwahl inkl. Regelrufnummernblock	—	●	—	●
Dauerüberwachung	▲	●	▲	●
Anrufweiterschaltungen S, B und N	▲	▲	●	●
Anklopfen	▲	—	●	—
Übermittlung der Verbindungsentgelte am Ende der Verbindung	▲	▲	●	●

1991 erweiterte die Telekom den ISDN-Telefondienst um das Bildtelefonieren im ISDN. Die Bitrate von 64 Kbit/s ermöglicht die Übertragung fester und bewegter Bilder. Für die Bildtelefonverbindung benötigen Sie zwei Nutzkanäle. Ein Kanal wird für das Bild, der andere für die Sprachübertragung genutzt.

ISDN-Teletex

Teletex ist ein Fernmeldedienst der Telekom, bei dem zeichenorientiert Dokumente (Texte) von Speicher zu Speicher übertragen werden. Vergleicht man den Telex-Betrieb mit Teletex, so wie er heute zur Verfügung steht, dann zeichnet sich Teletex bereits jetzt durch ei-

11 Rechnernetze – Basis der Kommunikation

nen höheren Zeichenvorrat aus. Zudem nutzt Teletex momentan mit einer Übertragungsgeschwindigkeit von 2,4 Kbit/s im integrierten Text- und Datennetz (IDN) eine fünfzigmal höhere Geschwindigkeit als der Telexdienst. Das Übermitteln einer DIN-A4-Seite benötigt im IDN zwischen 8 und 12 Sekunden. Mit 64 Kbit/s im ISDN liegt die Übertragungszeit unter einer Sekunde.

ISDN-Telefax

Durch ISDN wurde die Einführung einer ganz neuen Generation von Fernkopierern möglich, den Fernkopierer der Gruppe 4. Diese nutzen die hohe Übertragungsgeschwindigkeit von 64 Kbit/s und bieten darüber hinaus noch weitere interessante Vorteile.

Beim Fernkopierdienst werden Bilder oder Texte dadurch übermittelt, daß die Vorlage punktartig abgetastet wird und die Informationen verschlüsselt und über die Leitung zur Gegenstelle übertragen werden. Die Auflösung bei Fernkopierern der Gruppe 4 beträgt bis zu 400 Bildpunkte pro Inch. Bei Fernkopierern der Gruppe 3 (analogen Geräten) beträgt die Auflösung maximal 300 Bildpunkte pro Inch. Die Übertragungsgeschwindigkeit von Fernkopierern der Gruppe 4 ist fast sechsmal schneller als bei Geräten der Gruppe 3. Das Fernkopieren einer Seite dauert heute noch zwischen einer und drei Minuten. Beim Einsatz unter ISDN sieht die Sache dagegen wesentlich besser aus. Neben der verbesserten Qualität, die zur Verfügung steht, wird zudem die Übertragung einer DIN-A4-Seite in weniger als zehn Sekunden erfolgen. Über Endgeräteadapter a/b lassen sich auch die bisher an einem analogen Anschluß betriebenen Fernkopierer am ISDN-Anschluß weiter verwenden. Bei dieser Kommunikation muß jedoch bedacht werden, daß die Vorteile des ISDN auf der Strecke bleiben.

ISDN-Datenübermittlung

Die Telekom bietet zur Zeit eine Fülle von unterschiedlichen Datenübermittlungsdiensten an. Sie stehen in mehreren Netzen mit unterschiedlichen Übertragungskapazitäten und Schnittstellen zur Verfügung. Es sei auf die vorherigen Ausführungen für SFV und DDV hingewiesen.

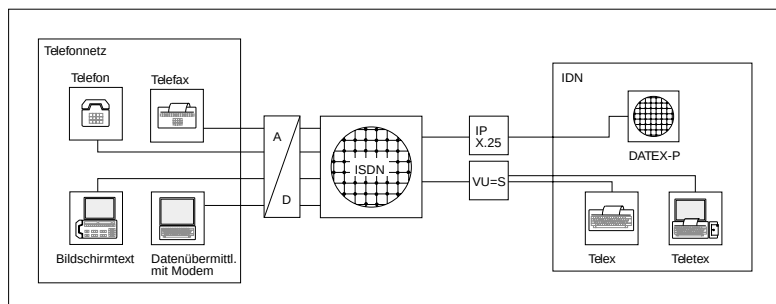
Die zur Verfügung stehenden Kanäle von 64 Kbit/s für das Übertragen von Daten im ISDN eröffnen eine Vielzahl neuer Anwendungsmöglichkeiten sowohl im geschäftlichen als auch im privaten Bereich. Es kann davon ausgegangen werden, daß eine ISDN-Standarddatenübertragung mit 64 Kbit/s dazu beitragen wird, die zur Zeit vorhandene Vielfalt unterschiedlicher Übertragungsgeschwindigkeiten mittelfristig entscheidend zu verringern.

11.2 Öffentliche Datenkommunikationseinrichtungen

Im Geschäftsbereich wird die 64 Kbit/s-Datenübertragung die Bürokommunikation sehr stark beeinflussen und mitgestalten. Diese wird aber den immer komplexer werdenden Anforderungen und dem steigenden Datenvolumen im Netzwerk immer noch nicht gerecht. Hier wird es neue Lösungen geben. Das Schlagwort lautet MAN oder auch DQDB. Darauf soll im nächsten Abschnitt näher eingegangen werden.

Die Basis- und die Primärmultiplexanschlüsse mit den Schnittstellen S0 und S2m erlauben eine transparente Datenübermittlung. Das heißt, die Protokolle der Schicht 1 im Nutzkanal (B-Kanal) und die Protokolle der Schichten 1, 2, 3 im Steuerkanal (D-Kanal) sind gemäß OSI-Schichtenmodell standardisiert. Für die Übermittlung der Daten im B-Kanal stimmen die Kommunikationspartner die verwendeten File-Transfer-Protokolle miteinander ab, oder sie bedienen sich standardisierter Protokolle, z.B. Teletex-Transparent-Mode. Eine Alternative für die transparente Datenübermittlung stellen die Basisfest- und die Primärmultiplexfestanschlüsse mit den Schnittstellen S0FV und S2MFV dar. Diese Anschlüsse unterscheiden sich von den Wählanschlüssen dadurch, daß die bereitgestellten Festverbindungen nicht über eine ISDN-Vermittlungsstelle geführt werden. Deshalb muß einer der Kommunikationspartner die Signalisierungsaufgaben der Vermittlungsstelle übernehmen. Ansonsten müssen die verwendeten Übertragungsverfahren miteinander abgestimmt werden. Wie in Abbildung 11.8 dargestellt ist, können zur Datenübertragung in erster Linie Dateneneinrichtungen mit integrierter S0-Schnittstelle verwendet werden. In Frage kommen zum Beispiel PCs, eine Datenverarbeitungsanlage oder ein Schnittstellen-Controller in einem LAN. Durch den modularen Aufbau können diese Endgeräte problemlos mit einer S0-Schnittstelle ISDN-fähig gemacht werden. Für die Anpassung eines PC an die S0-Schnittstelle verwendet man eine ISDN-Adapterkarte mit der passenden Kommunikationssoftware. Zur LAN-LAN-Kopplung sind entsprechende Karten in den Gateway-Rechnern einzusetzen.

Abbildung 11.7
ISDN-Anschluß
über Terminal-
adapter



11 Rechnernetze – Basis der Kommunikation

Hinzu kommt dabei die LAN-Software, um über die ISDN-Karte beide LANs miteinander koppeln zu können. Es gibt inzwischen eine Vielzahl von Herstellern auf dem Markt, die sowohl Einplatz- als auch Netzwerklösungen anbieten.

Es ist aber auch möglich, herkömmliche Datenendgeräte mit V- oder X-Schnittstelle im ISDN zu betreiben. Um das zu realisieren, bedient man sich entsprechender Terminaladapter. In Abbildung 11.7 wird auch diese Anschlußmöglichkeit gezeigt.

Der Terminaladapter a/b dient zur Anpassung von Endgeräten mit analoger Leitungsschnittstelle an die S0-Schnittstelle. Auf diese Weise können analoge Modems für die Datenübermittlung adaptiert werden, auch wenn sie bisher im herkömmlichen Telefonnetz betrieben worden sind.

Voraussetzung für die Datenübertragung ist, daß bei der Gegenstelle im ISDN entweder die gleiche Konfiguration vorliegt oder die V.24-Endeinrichtung – wie bisher – über ein Modem an einem analogen Telefonanschluß angeschaltet ist.

Es können auch Endgeräte über direkten V.24/V.28-Schnittstellenanschluß an das ISDN angeschlossen werden. Sie benötigen hierzu einen Terminaladapter V.24. Mit diesem Terminaladapter wird die erforderliche Umsetzung auf die standardisierte S0-Schnittstelle im ISDN durchgeführt. Der Einsatz ist der Funktion eines Modems ähnlich. PCs können somit über die vorhandene V.24-Schnittstelle ohne großen Aufwand und vor allem ohne besondere Systemeingriffe über einen TA V.24 im ISDN kommunizieren.

Herkömmliche Datenendeinrichtungen mit einer X.21/X.21bis-Schnittstelle von 2,4 bis 64 Kbit/s können mit Hilfe von Terminaladaptern X.21/X.21bis am ISDN-Netz teilnehmen. Die Gegenstelle muß sich ebenfalls im ISDN-Netz mit entsprechendem Adapter und gleicher Geschwindigkeit befinden. Verbindungen von und zu Datex-L-Anschlüssen über TA X.21/X.21bis sind nicht möglich.

Zudem stellt die Telekom Mechanismen zur Verfügung, um die Übergänge zwischen ISDN und drei weiteren wichtigen Diensten im IDN zu ermöglichen. Es handelt sich dabei um die Übergänge für Teletex, Telex und Datex-P.

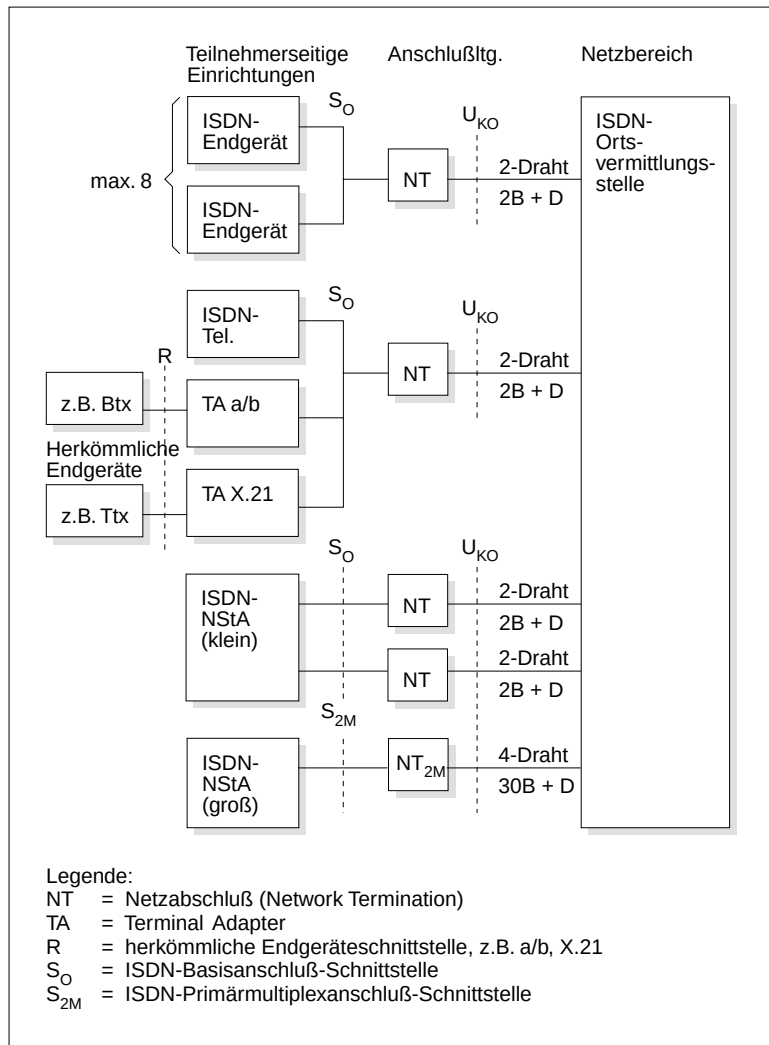
ISDN-IDN für Datex-P

Der Übergang vom ISDN zum Datex-P-Dienst im IDN wird durch einen Interworking-Port X.25 (IP X.25) ermöglicht. Vom ISDN-Anschluß wird der Zugang zum Datex-P im IDN ermöglicht, ohne daß vom ISDN spezielle Paketvermittlungsfunktionen ausgeführt wer-

11.2 Öffentliche Datenkommunikationseinrichtungen

den. Das ISDN bietet lediglich über eine 64-Kbit/s-Wählverbindung den Zugang. Das bedeutet, daß der ISDN-Anschluß von anderen Datex-P-Anschlüssen nicht über die ISDN-Rufnummer des Teilnehmers, sondern über eine Datex-P-Rufnummer erreicht werden kann. Diese Anschlußform ist deshalb auch von Vorteil, weil ein vorhandener ISDN-Anschluß auch für Datex-P-Endgeräte, die über einen Terminaladapater angepaßt werden, mitbenutzt werden kann und somit keine weiteren Installationskosten anfallen.

Abbildung 11.8
ISDN-Schnittstellen im Netz
der Telekom



11 Rechnernetze – Basis der Kommunikation

Die einheitliche ISDN-Anschlußtechnik sorgt darüber hinaus für ein hohes Maß an Beweglichkeit im Endgerätebereich. Ein Standortwechsel des Endgeräts ist ohne zusätzlichen Installationsaufwand möglich.

Für den Zugang zu Datex-P werden Endgeräte mit X.25-Schnittstelle verwendet. Diese werden über einen Endgeräteadapter TA X.25 an das ISDN angepaßt. Dem TA X.25 ist ein IP X.25 fest zugeordnet, der den Übergang zwischen dem ISDN und Datex-P im IDN realisiert. Die bei diesem Zugangsverfahren am TA X.25 angebotenen Übertragungsgeschwindigkeiten sind 2400, 4800 und 9600 Bit/s. In Abbildung 11.7 sind diese Möglichkeiten dargestellt. Damit Sie sich einen Gesamtüberblick über ISDN verschaffen können (Schnittstellen, Anschlüsse etc.), ist dies in Abbildung 11.8 nochmals zusammengefaßt dargestellt.

ISDN-Bilddienste

Mit der Bildkommunikation kann ein neuer Dienst im ISDN angeboten werden. Hierbei sind unterschiedliche Anwendungen denkbar:

- *Fernskizzen*
 - Übermitteln von Skizzen während des Entstehens
 - Gleichzeitiges Darstellen auf Bildschirmen
 - Kombination mit Fernsprechern
- *Fernzeichnen*
 - Hohe Auflösung
 - Geeignet für Grafikabstimmung
- *Festbildübertragung*
 - Betrachten eines Katalogs
 - Austausch technischer Darstellungen
- *Langsames Bewegtbild*
 - Betrachten von Personenbildern
 - Betrachten von Funktionsabläufen
- *Bewegtbild mit einfacher Bewegungsdarstellung*
 - Übertragen von Personenbildern
 - Bildbegleitung beim Telefonieren
 - Einsatz bei Telekonferenzen

ISDN-Fernwirken

Darunter sind Anwendungen zu verstehen wie:

- *Fernüberwachen*
 - Fernanzeigen: Übermitteln einfacher Meldesignale wie Alarmer an eine Zentrale
 - Fernmessen: Übertragen von Meßdaten an eine Leitstelle

11.2 Öffentliche Datenkommunikationseinrichtungen

■ Fernsteuern

- Fernschalten: An- und Abschalten einer Maschine durch einfache Befehlssignale
- Ferneinstellen: Einstellen mittels Befehlssignalen, zum Beispiel den Druck eines Druckkessels

ISDN-Textfax

Dieser Dienst vereinigt die Eigenschaften von Teletex und Telefax und gewährt die originalgetreue Übermittlung von Schwarzweißdokumenten.

Da unter ISDN alle Dienste über ein gemeinsames Netz laufen, sind inzwischen Bestrebungen im Gange, nicht nur ISDN-fähige Geräte zu entwickeln, sondern multifunktionale Endgeräte herzustellen.

Die Vorteile liegen auf der Hand:

- Mehrfachnutzung der Endgerätekomponenten für verschiedene Dienste
- Integration verschiedener Nachrichtenformen in einem Gerät
- Raumersparnis im Büro

Auch die Kommunikation von LANs über ISDN ist sehr vorteilhaft. Um jedoch die Möglichkeiten sinnvoll im Bürobereich nutzen zu können, ist es notwendig, die herkömmlichen Nebenstellenanlagen durch ISDN-fähige Nebenstellenanlagen zu ersetzen.

Diese neuen Nebenstellenanlagen bieten nicht nur die Vorteile der Kommunikation außerhalb des Firmengeländes, sondern auch innerhalb einer Firma. In Abbildung 11.9 sind die Nutzungsmöglichkeiten zukünftiger ISDN-Kommunikationsanlagen dargestellt.

Aus Abbildung 11.9 ist ersichtlich, daß durch ISDN Lokale Netze nicht abgelöst, sondern die Möglichkeiten der Verbindung von LANs, sowohl innerhalb eines Gebäudes als auch durch WANs, verbessert und vereinfacht werden sollen. Den Funktionen der Server, die Sie in Abbildung 11.9 sehen, kommt folgende Bedeutung zu:

■ Telekommunikations-Server

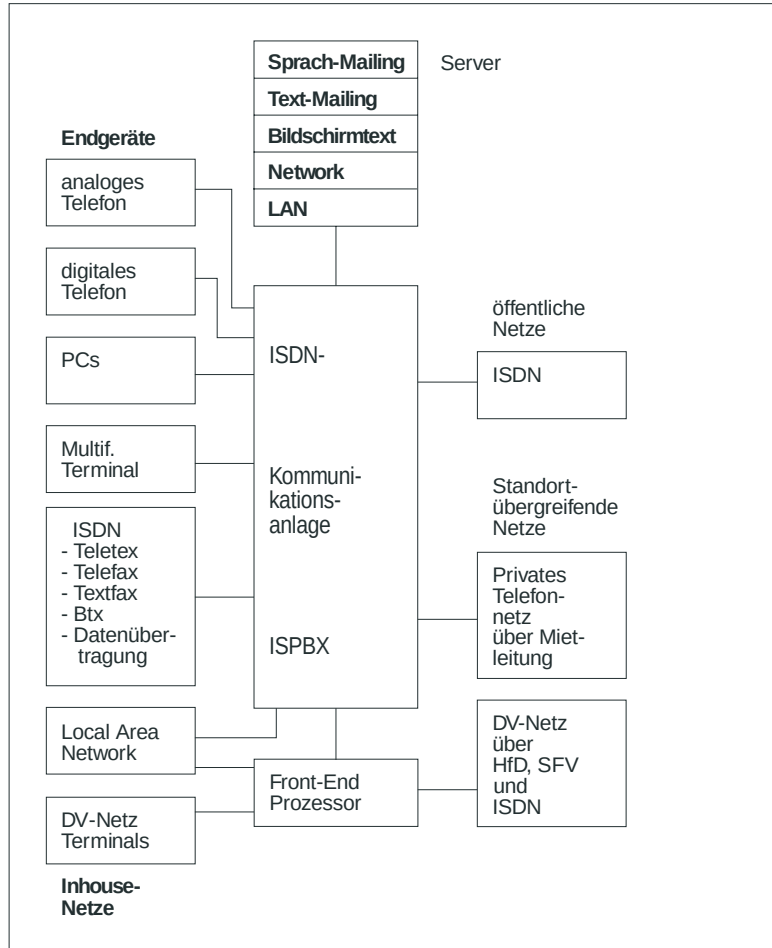
- Übernimmt die Aufgaben für Mailbox-Dienste
- Zuständig für die Abwicklung von Teletex- und Telexverkehr
- Übernimmt die Protokollumwandlung, wenn Datenterminals oder Workstations den Zugang zu Teletex oder Telex durchführen

■ Fax-Server

- Abwicklung des Teletex- oder Telefaxverkehrs
- Zuständig für interne oder externe Kommunikation
- Zuständig für die Umwandlung von Teletex in Telefax

11 Rechnernetze – Basis der Kommunikation

Abbildung 11.9
Nutzungsmöglichkeiten der ISDN-fähigen Nebenstellenanlagen

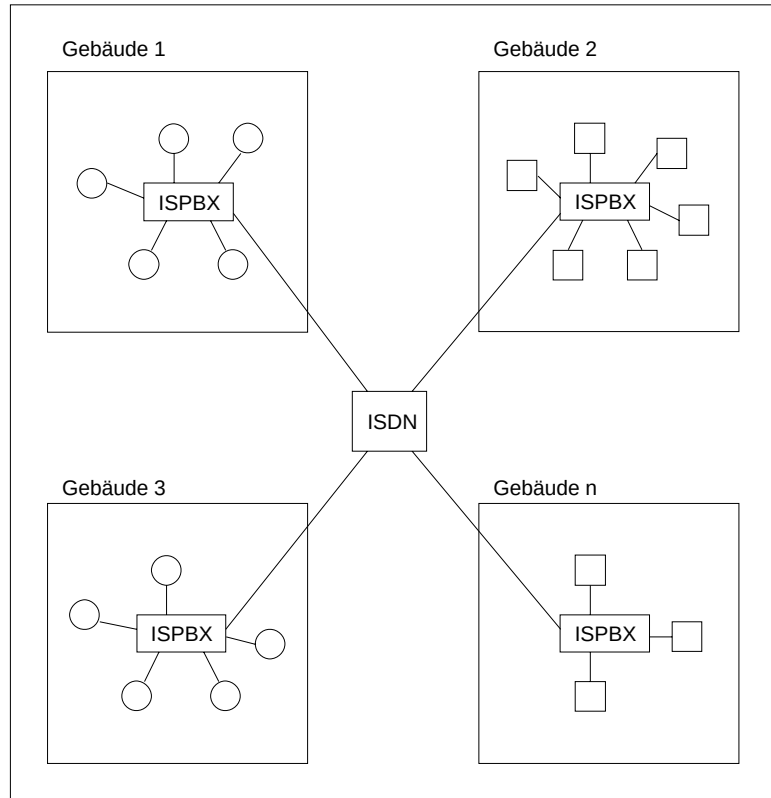


- **Sprach-Server**
 - Speicherung von Sprachmitteilungen
 - Abruf von Sprachmitteilungen
 - Verschicken von Broadcast-Messages
- **Network-Server**
 - Gateway-Rechnerfunktion für Netzwerkübergänge
 - Gateway zu öffentlichen Netzen
- **LAN-Server**
 - Gateway oder Bridge zu einem anderen LAN
 - Zugang für asynchrone Terminals in einem LAN
- **Btx-Server**
 - Zuständig für Btx-Verbindungen

11.2 Öffentliche Datenkommunikationseinrichtungen

In Abbildung 11.10 ist dargestellt, wie ein WAN-Konzept mit Hilfe von ISDN bzw. ISDN-fähigen Anlagen aussehen könnte.

Abbildung 11.10
Kommunikation
unter ISDN



LANs und ISDN werden also nebeneinander bestehen und sich gegenseitig ergänzen. Die Möglichkeiten der Kopplung von LANs über große Strecken hinweg werden in Zukunft wesentlich einfacher und besser werden.

In diesem Zusammenhang wird auch sehr oft von Corporate Networks gesprochen. Was steckt hinter diesem Begriff?

Corporate Networks

Hierunter sind im wesentlichen Telekommunikationsnetze zu verstehen, mit denen Kommunikationsleistungen erbracht werden können, die genau auf die Bedürfnisse eines Unternehmens abgestimmt sind.

11 Rechnernetze – Basis der Kommunikation

Das Strategic Review Committee 5 befaßt sich mit der Standardisierung des Begriffs »Corporate Network« und gibt hierfür folgende Erklärung:

»Ein Corporate Telecommunication Network (CTN) besteht aus einer Anzahl von Einrichtungen, die dem Kunden gehören oder von ihm gemietet sind (Customer Premises Equipment – CPE und/oder Customer Premises Networks – CPNs), die sich an geografisch verschiedenen Orten befinden und miteinander verbunden sind, um einer bestimmten Gruppe von Anwendern einheitliche Netzwerkdienste anzubieten.«

Die charakteristischen Merkmale von Corporate Networks werden wie folgt beschrieben:

- Ein Corporate Telecommunications Network kann als Weitverkehrsnetz von verbundenen CPEs oder CPNs betrachtet werden. Es kann national, kontinental oder weltweit betrieben werden. Es hat die gleiche geografische Ausdehnung wie das Unternehmen, das es benutzt.
- Ein Corporate Telecommunications Network ist für die Nutzung durch eine begrenzte Benutzeranzahl bestimmt. Im Gegensatz zu einem öffentlichen Netz besteht für das Corporate Telecommunications Network keine Verpflichtung, seine Dienste der Öffentlichkeit zugänglich zu machen.
- Die Anforderungen, die an ein Corporate Telecommunications Network gestellt werden, spiegeln die Bedürfnisse der internen Benutzer, Lieferanten und Kunden sowie die gemeinsamen Bedürfnisse und Ziele wider.
- Die Leistungen, die Abrechnung, die Bereitstellung und das Management eines Corporate Telecommunications Network sind spezifisch auf die Anforderungen des CTN zugeschnitten und unterscheiden sich im allgemeinen von den Anforderungen der Öffentlichkeit.

Bei den oben aufgeführten Aspekten werden keine Unterscheidungen dahingehend getroffen, ob es sich um die Übertragung von Daten oder Sprache handelt (Multimedia für die Zukunft nicht zu vergessen). Ein Corporate Network kann einem Unternehmen gehören (dann ist er Eigentümer) oder gemietet sein. Im oben aufgeführten ETSI-Entwurf werden vier Formen der Eigentumsverhältnisse festgelegt:

1. Das gesamte Corporate Network einschließlich der Übertragungswege befindet sich im Eigentum des Unternehmens. Diese Form ist in Deutschland nur vereinzelt anzutreffen, da es auf der Basis des Fernmeldegesetzes nur wenigen Unternehmen gestattet ist, eigene Übertragungswege zu errichten und zu betreiben.

11.2 Öffentliche Datenkommunikationseinrichtungen

2. Es werden Mietleitungen von einem oder mehreren Anbietern genutzt.
3. Es werden virtuelle private Netze (VPN) genutzt, die durch Netzdienstleistungsunternehmen bereitgestellt werden, die in Deutschland dazu von der Telekom und anderen Diensteanbietern Übertragungswege gemietet haben.
4. Es werden öffentliche Netze genutzt. In Deutschland stehen hierfür eine Reihe öffentlicher Netze der Telekom (Telefonnetz, ISDN, Datex-P etc.) oder auch Mobilfunknetze (D1/D2, Modacom, Inmarsat etc.) zur Verfügung.

Unternehmen, die keine eigenen Übertragungswege betreiben dürfen, müssen diese also bei der Telekom oder bei anderen Unternehmen mieten, die selbst Übertragungswege bei der Telekom gemietet haben oder eigene Übertragungswege besitzen und diese weiterveräußern.

Corporate Networks können Kommunikationsleistungen für die Datenkommunikation, die Sprachkommunikation oder für andere Kommunikationsformen erbringen. Die Übertragung und Übermittlung von Daten auf der Basis von Fest- und Wählverbindungen, die von der Telekom oder anderen bereitgestellt werden, ist ohne Einschränkungen möglich. Das schließt Dienstleistungen für Dritte ein. Auf dieser Basis sind die Corporate Networks für Daten durch beliebige Unternehmen und Unternehmensgruppen realisierbar.

Somit können Netzwerke inzwischen individuell aufgebaut werden. Voraussetzung hierfür sind nicht nur Änderungen im FAG, sondern auch die Bereitstellung von leistungsfähigen Übertragungswegen. ISDN selbst reicht hierfür langfristig gesehen mit Sicherheit nicht mehr aus.

Was ist als Weiterentwicklung für ISDN geplant? Nachdem das derzeitige ISDN auch als Schmalband-ISDN bezeichnet wird, ist daraus zu folgern, daß es irgendwann auch ein Breitband-ISDN geben wird.

Glasfasernetze – Basis für Breitband-ISDN

Für die Kommunikation mit Hilfe von metallischen Leitern gibt es physikalisch bedingte Grenzen der Übertragungsgeschwindigkeiten. Da eine schnelle Kopplung auch über große Entfernungen für die Zukunft gefordert wird, ist das Übertragungsmedium der Zukunft die Glasfaser bzw. der Lichtwellenleiter. Im Bereich der PC-LANs werden inzwischen von allen führenden Herstellern Kopplungseinrichtungen angeboten, um die Netzwerke durch den Einsatz von Lichtwellenleitern (LWL) über die bisher möglichen Entfernungen weiter

11 Rechnernetze – Basis der Kommunikation

ausdehnen zu können. Zudem sind Übertragungen über LWL, wie zu Beginn der Einführung bereits erwähnt wurde, störunempfindlich gegen äußere Einflüsse.

Die zu übertragende Information wird durch Lichtsignale von Ort A nach Ort B transportiert. Zur Zeit sind mit dieser Technik Übertragungsgeschwindigkeiten von 600 Mbit/s möglich, wenn die Leitungslänge nur einige Kilometer beträgt. Auf längeren Strecken müssen entweder Verstärker eingesetzt oder die Übertragungsgeschwindigkeiten gesenkt werden. Die Vorteile der Glasfasertechnik sollen nochmals zusammengefaßt aufgeführt werden:

- Unempfindlich gegenüber elektrischen und magnetischen Strahlungen
- Vollständige elektrische Trennung von Sender und Empfänger
- Kein Auftreten von Potentialproblemen (Erdschleifen)
- Risikofrei in explosionsgefährdeter Umgebung
- Kein Auftreten von Nebensprechen
- Gegen Abhören sicher
- Sehr hohe Übertragungskapazitäten
- Sehr geringe Dämpfung, damit Verlustarmut
- Geringes Kabelgewicht und kleiner Querschnitt des Kabels
- Unbegrenzte Materialverfügbarkeit

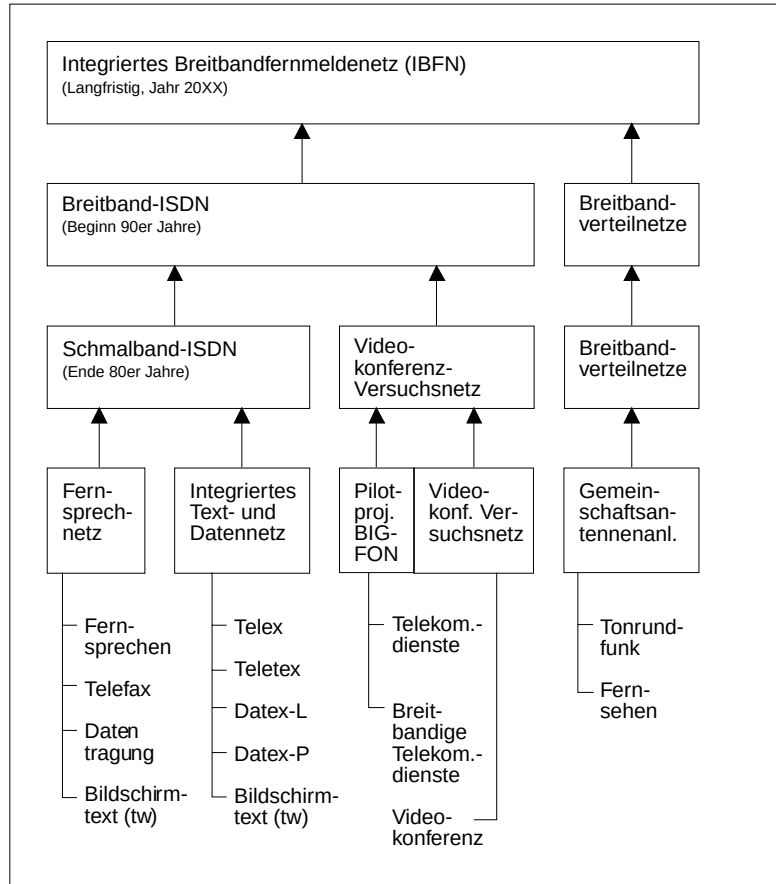
Die Schwachstelle bei den Systemen, die mit LWL als Übertragungstechnik arbeiten, liegt in der Ansteuerungselektronik. Mit elektrooptischen Bauelementen sind durchaus Übertragungsbandbreiten von einigen hundert Giga-Hertz denkbar (einige 100 Gbit/s). Aber erst mit der Verfügbarkeit der notwendigen technischen Ausrüstung werden Kopplungen mit diesen Geschwindigkeiten denkbar sein.

Im Fernnetzbereich sind Lichtwellenleiter dort interessant, wo Telefonleitungen die notwendige Übertragungsgeschwindigkeit nicht mehr erbringen können. Die geplanten neuen Dienste, wie Bildfernsprechen, Videokonferenzen und ähnliches, erfordern allein beim Teilnehmeranschluß Datenraten von bis zu 140 Mbit/s.

Die ersten Versuche werden von der Telekom bereits durchgeführt und sind unter dem Kürzel BIGFON bekannt (breitbandiges integriertes Glasfaser-Fernmeldeortsnetz). In Abbildung 11.11 ist dargestellt, wie die einzelnen Netze zu einem Universalnetz vereint werden sollen. Bis dieses jedoch im vollen Umfang zur Verfügung stehen wird, werden noch einige Jahre, wenn nicht sogar Jahrzehnte, verstreichen. Deshalb ist es nicht unbedingt sinnvoll, sich über diese zukünftigen Entwicklungen jetzt schon zu viele Gedanken zu machen. Wichtiger ist es, die in naher Zukunft verfügbaren Dienste sinnvoll auszunutzen und einzusetzen.

11.3 Metropolitan Area Network

Abbildung 11.11
Stufen der
Integration



Am Ende dieses Kapitels werden Sie mehr über das zukünftige Breitband-ISDN erfahren.

11.3 Metropolitan Area Network

Es wurde bereits mehrfach darauf hingewiesen, daß das immer größer werdende Datenvolumen im lokalen und im standortübergreifenden Kommunikationsbereich den Einsatz leistungsfähiger Netzwerktechnologien erforderlich macht. Als Gründe für das Wachstum können angesehen werden:

- Die Anzahl der installierten Rechner am Arbeitsplatz wird immer größer (PCs, CAD-Stationen, DTP-Stationen etc.).
- Die Qualität der Dokumente steigt (komplexe Farbgrafik, hochauflösende Drucke, Scanner Images etc.).

11 Rechnernetze – Basis der Kommunikation

- Kommunikationsorientierte Anwendungen werden verstärkt eingesetzt.
- Der Datenaustausch zwischen unterschiedlichen Standorten wird intensiver.

Diese Entwicklung wird auch stark durch den Einsatz von LANs, basierend auf internationalen Standards, gefördert und vorangetrieben. Nicht zu vergessen ist dabei, daß die gesamte Entwicklung und die Forderungen der Anwender immer größer werden. Die Standardisierung auf diesem Gebiet hat auch dazu beigetragen, daß die Kommunikation zwischen heterogenen Netzwerken ermöglicht wird. Hätte man vor einigen Jahren daran gedacht, Netzwerkbetriebssysteme wie NetWare, NT Server, Vines, Unix, AppleShare etc. in ein Gesamtkonzept zu integrieren, um von einem Arbeitsplatz aus auf alle diese Systeme zugreifen zu können, könnten die Systeme unter- und miteinander Daten und Informationen austauschen.

Die Entwicklung leistungsfähiger Koppelemente wie Bridges, Router, Brouter, Switches und Gateways haben dazu beigetragen, einzelne LANs und Hostsysteme zu einem unternehmensweiten Netzwerk zusammenführen zu können. Damit werden auch neue Informationstechniken ermöglicht. Denken Sie an die Entwicklung der Client-Server-Datenbanken und an den Aufbau verteilter Datenbanken. Ganz groß im Trend liegen derzeit die Möglichkeiten, die durch Multimedia bereitgestellt werden, um Text, Grafik, Daten, Sprache und Video zu integrieren. Damit verbunden sind allerdings auch riesige Datenmengen, die nicht nur bewältigt (immer leistungsfähigere Rechner), sondern auch bewegt werden müssen, vor allem wenn diese im LAN bzw. Internet zu transportieren sind.

Damit die Datenvolumen im LAN bewältigt werden können, wird in vielen Unternehmen inzwischen Gigabit Ethernet, zumindest im Backbone-Bereich, eingesetzt. Es gibt auch Installationen, bei denen Gigabit Ethernet bzw. ATM bis zum Arbeitsplatz installiert wird, nur um die benötigten Datenmengen in einer annehmbaren Zeit von A nach B verschicken zu können.

Die Möglichkeit, ein solches unternehmensweites Netzwerk standortübergreifend zu realisieren, ist beim heutigen Stand der Technik der angebotenen Telekommunikationsdienste kaum durchzuführen. Die Übertragungsraten in öffentlichen Netzen von momentan 9.600 Bit/s, 64 Kbit/s oder auch 2 Mbit/s (T1-Verbindung) liegen um ein Vielfaches unter der Leistungsfähigkeit von LANs. Noch krasser wird der Gegensatz, wenn Sie durchgängig Gigabit Ethernet mit 1000 Mbit/s einsetzen.

11.3 Metropolitan Area Network

Die Möglichkeit zur effektiven Gestaltung der Kommunikation sind schnelle Paketvermittlungsdienste, basierend auf der Frame-Relay-Technik. Deren Funktionsweise ist vergleichbar mit der von LANs, und sie können zur Übertragung von Daten und Bildern genutzt werden. Noch wird diese Technik nur in privaten Netzen und unter dem Einsatz nicht standardisierter Formate realisiert. Derzeit werden allerdings CCITT-Dienste, die auch auf der Frame-Relay-Technik aufbauen, für das Schmalband-ISDN standardisiert.

Die Telekom erkannte den wachsenden Bedarf an breitbandiger, schneller und sicherer Kommunikation und ging im Herbst 1991 in die Pilotphase für den Einsatz der MAN-Technologie. An dieser Pilotphase sind die drei Standorte Stuttgart, München und Frankfurt beteiligt. Das Metropolitan Area Network setzt auf dem 802.6-Standard auf und verwendet als Technik DQDB (Distributed Queue Dual Bus). Die DQDB-Technik wurde Mitte der achtziger Jahre an einer Universität in Australien entwickelt. Mit der Unterstützung des australischen Postwesens wird die Technologie von der Firma QCL vermarktet. Die Zugriffsmethode wird als QPSX (Queued Packet Switch Exchange) bezeichnet. Ein kurzer Überblick soll Ihnen einen Eindruck über die Möglichkeiten der MAN-Technologie vermitteln.

Sinn und Zweck eines MAN ist es, integrierte Dienste wie Daten, Sprache und Video über große Distanzen hinweg übertragen zu können. Das MAN besteht aus untereinander verbundenen DQDB-Teilnetzwerken. Die Verbindung dieser Teilnetze erfolgt entweder über Bridges, Router oder Gateways. Ein auf der Basis von DQDB konzipiertes MAN stellt sowohl asynchrone Übertragungsdienste (Paketvermittlung), wenn es um die Kopplung von Netzen geht, als auch isochrone Übertragungsdienste (Durchschaltvermittlung), wenn es um die Übertragung von Sprache und Video geht, zur Verfügung. Man muß dabei bedenken, daß die Übertragung von Daten in herkömmlichen LANs tatsächlich asynchron ist. Erwünscht ist eine größere Menge von Daten in kurzer Zeit. Wenn es im Gegensatz dazu um die Übertragung von Bildern geht, braucht man über einen längeren Zeitraum eine »feste« Verbindung zwischen den Partnern.

Da sich das MAN an 802.6 orientiert, wird gefordert, daß ein MAN eine Distanz von mindestens 50 Kilometern überbrücken kann (Metropolitan Area = Region) und die Übertragungsstrecken mit sehr großen Geschwindigkeiten bereitgestellt werden. Das MAN wird dabei mit Übertragungsraten von 34 Mbit/s oder 140 Mbit/s arbeiten. Aufgrund dieser hohen Übertragungsgeschwindigkeit kommt bei der Telekom nur der Einsatz von Glasfaser in Betracht.

11 Rechnernetze – Basis der Kommunikation

Damit nicht jeder MAN-Teilnehmer plötzlich mit Teilnehmern kommuniziert, mit denen er dies nicht dürfte, sind entsprechende Sicherheitsmechanismen vorgesehen oder schon implementiert. Es erfolgt eine Address Validation, d.h. eine syntaktische Prüfung der Adresse, um festzustellen, ob die vorgegebene Adresse dem Aufbau und der Form für das MAN entspricht. Zudem wird auch eine Address Authorization durchgeführt, mit der eine Source-Adresse auf Zugangserlaubnis überprüft wird.

Das Address Screening stellt sicher, daß die Zieladresse, die unter der betrachteten Source-Adresse angegeben ist, auch als Kommunikationspartner anerkannt wird. Bei der Konzeption wurde großer Wert auf Fehlertoleranz gelegt, so daß bei einem Kabelbruch zum Beispiel eine automatische Rekonfiguration des MAN erfolgt. Hierzu jedoch später mehr.

Durch die Vereinbarungen zwischen IEEE 802.6 und der CCITT-Studienkommission XVIII, die Empfehlungen für das Breitband-ISDN auf ATM-Basis erarbeitet, wird sichergestellt, daß die Definitionen des CCITT bezüglich der ATM-Zellenlänge und ATM-Struktur für DQDB übernommen wird. Somit ist die Integration von MAN in ein Breitband-ISDN und der länderübergreifende Aufbau von MAN abgesichert.

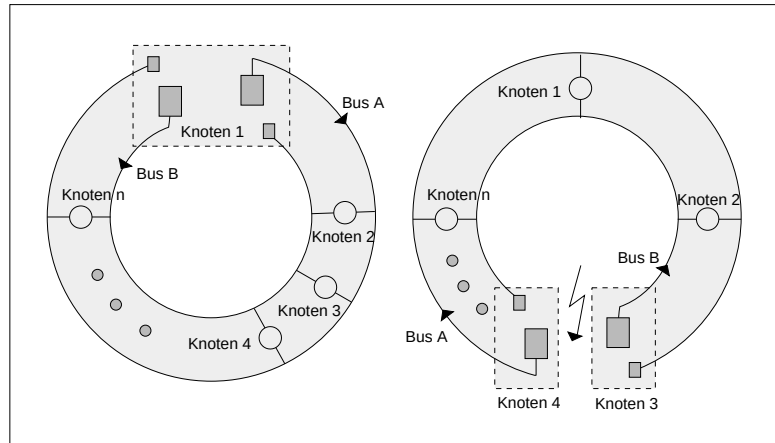
11.3.1 Der DQDB-Standard

Die Begriffsbildung DQDB setzt sich aus der Bezeichnung für das Medienzugriffsverfahren (Distributed Queue) und der Bezeichnung für die Topologie (Dual Bus) zusammen. DQDB wurde Ende 1990 standardisiert (IEEE 802.6). Die wesentlichen Elemente des Standards sind der DQDB-Bus, die Rahmenstruktur und der Medienzugriff für den isochronen und den asynchronen Datenverkehr. In Abbildung 11.12 ist der prinzipielle Aufbau eines DQDB-Bussystems dargestellt.

Ein MAN-Teilnetz, basierend auf dem DQDB-Standard, besteht generell aus zwei unidirektionalen Bussystemen, als Bus A und Bus B bezeichnet, und mehreren angeschlossenen Knoten. Die Übertragungsrichtung von Bus A und Bus B ist gegenläufig und erlaubt Vollduplexverkehr. Die beiden Bussysteme arbeiten unabhängig voneinander, womit auf beiden Bussystemen die gesamte Übertragungskapazität zur Verfügung steht. Jeder einzelne Knoten ist an jedem der beiden Busse sowohl mit einer Lese- als auch mit einer Schreibeinheit verbunden, wie es in Abbildung 11.13 dargestellt ist.

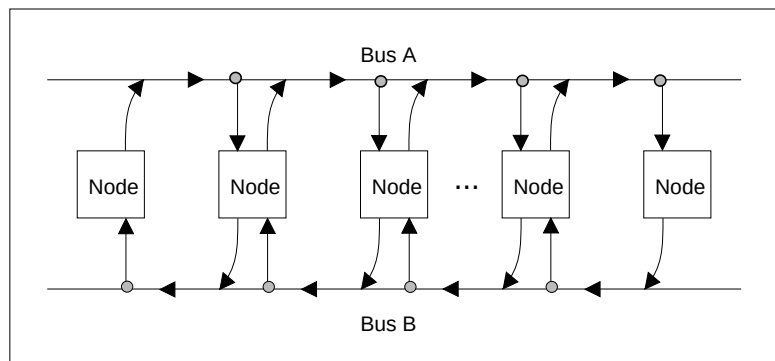
11.3 Metropolitan Area Network

Abbildung 11.12
Aufbau eines
DQDB-Bussystems



Der Zugriff auf das Medium wird von einer – in jedem Knoten installierten – Zugriffseinheit realisiert. Der vorbeikommende Bitstrom wird zuerst gelesen, bevor in einen freien Slot über ein logisches ODER geschrieben werden kann. Die Generierung der Frames geschieht am Kopf der Busse: Kopfstation, Head of Bus (HOB). Der Datenfluß endet am Busende: End of Bus (EOB). Die Knoten enthalten Tabellen, in denen eingetragen ist, über welchen Bus die anderen Knoten erreichbar sind.

Abbildung 11.13
Anschluß eines
Knotens im MAN



Zwischen Head of Bus (HOB) und End of Bus (EOB) fließt ein kontinuierlicher Bitstrom von 34 bzw. 140 Mbit/s. Der im HOB befindliche Rahmen-(Frame-)Generator formatiert diesen in einem 125-Mikrosekunden-Rahmen. Jeder Rahmen wird in Frame Header, n Slots und ein Stuffing Field unterteilt. In Abhängigkeit von der Übertragungsgeschwindigkeit (34 Mbit/s=4.296 Bit/Frame, 140 Mbit/s=17.408 Bit/Frame) enthält ein Rahmen 6 bzw. 27 Slots.

11 Rechnernetze – Basis der Kommunikation

Der Rahmen wird wiederum in Zeitschlitze, auch als Slots oder Zellen bezeichnet, aufgeteilt und setzt sich zusammen aus:

- *Access Control Field (ACF) (1 Byte)*
Dieses Feld beinhaltet das Kontrollbit für request/non-request, das Busy- bzw. Empty-Bit und den Slot-Typ (isochron oder asynchron).
- *Segment Header (4 Byte)*
Der Datenteil enthält die segmentierten Daten des LAN-Pakets einschließlich MAC-Adressen und Protokoll-Header der höheren Schichten.
- *Datenteil (payload) 48 Byte*
Bevor die Daten über ein DQDB-MAN übertragen werden können, müssen sie zuvor in 44-Byte-Segmente (Segmentation Unit) aufgeteilt sowie mit Header und Trailer (je 2 Byte) versehen werden. Man unterscheidet dabei vier Segmenttypen:
 - BOM – Beginning of Message
 - COM – Continuation of Message
 - End of Message
 - SSM – Single Segment Message (wenn Daten nur aus einer Segmentation Unit bestehen)

Die BOM Segmentation Unit enthält die MAN-Adresse, die Teilnehmeradresse und die ersten Daten.

Es wurde bereits erwähnt, daß die MAN-Technologie sowohl für isochronen Datenverkehr als auch für asynchronen Datenverkehr genutzt werden kann. Es sollen anschließend die Medienzugriffe für die beiden Möglichkeiten erläutert werden.

- *Zugriff für isochronen Datenverkehr*
Aufgrund der Anforderungen einer Station im Netzwerk wird über die Kopfstation die Vorbelegung von Zellen bzw. Bytes für die Übertragung isochroner Dienste vorgenommen. Die durch isochrone Kanäle verbundenen Stationen erkennen ihren Kanal an der Position der Bytes, die durch die Kopfstation reserviert wurden. Wird eine Verbindung nicht mehr benötigt, so erfolgt der Verbindungsabbau ebenfalls über die Kopfstation.
- *Zugriff für den asynchronen Datenverkehr*
Das Zugriffsprotokoll setzt voraus, daß in jedem Knoten für jeden Bus sowohl ein Request Counter (RC) als auch ein Countdown Counter (CD) vorhanden ist. Eine Station, die ein Segment auf Bus A übertragen möchte, sendet einen Request auf Bus B zu allen »stromaufwärts« liegenden Stationen. Jede Station, die einen Request auf Bus B empfängt, inkrementiert den RC für Bus A.

11.3 Metropolitan Area Network

Für jede freie Zelle (Busy Bit = 0), die den Bus A passiert, wird der RC für Bus A dekrementiert. Hat eine Station einen Sendewunsch, wird der Inhalt des RC in den CD geladen und der RC zurückgesetzt. Für jede freie Zelle, die den Bus A passiert, wird nun der CD für Bus A dekrementiert. Ist der CD = 0, wird die nächste freie Zelle zur Übertragung genutzt. Mit diesen beiden Zählern (pro Bus) in jedem Knoten wird eine verteilte Warteschlange (pro Bus) für den Zugriff auf freie Zellen gebildet (-> Distributed Queue).

Durch die modulare Bauweise des MAN-Vermittlungssystems wird eine flexible Anpassung an die lokalen Gegebenheiten, die bereits existierende Verkabelungsinfrastruktur und die Anforderungen bezüglich der Verfügbarkeit erreicht.

Bezüglich der möglichen Topologien unterscheidet man:

- *Punkt-zu-Punkt-Topologie*

Es handelt sich hier um die einfachste Form des Open Bus. Immer wenn zwei Teilnetze miteinander verbunden werden, geschieht dies mit einer einfachen Punkt-zu-Punkt-Verbindung.

- *Offener Bus*

Der Offene Bus (Open Bus) ist eine Erweiterung der Punkt-zu-Punkt-Verbindung durch ein Ein- oder Anfügen weiterer Knoten.

- *Looped Bus*

Diese Art des Aufbaus (Looped Bus, Ringbus) stellt eine Sonderform des Offenen Busses dar. Er zeichnet sich vor allem dadurch aus, daß die Kopfstationen der Busse A und B in einem Knoten vereinigt werden. Dadurch wird eine einfache und schnelle Rekonfiguration des Busses im Fehlerfall ermöglicht.

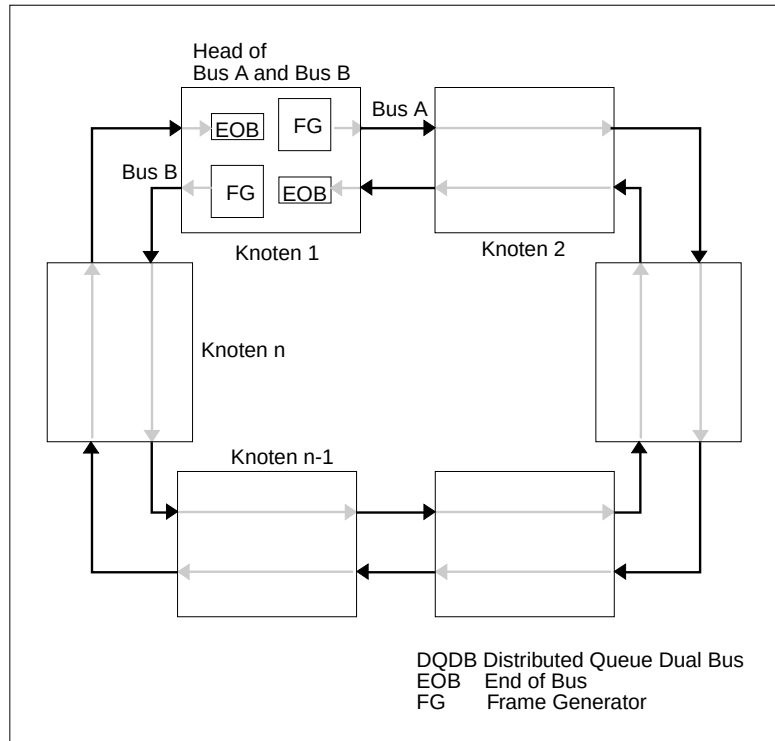
Aus Sicherheitsgründen kommen beim Einsatz öffentlich betriebener MANs vor allem die Looped-Bus-Konfigurationen vor. Dies liegt darin begründet, daß der Looped Bus einen hervorragenden Rekonfigurationsmechanismus verwendet.

Unterbrechungen der Übertragungsstrecke können nur durch eine Rekonfiguration des Netzes behoben werden. Handelt es sich dabei um einen Looped Bus, wird dies dadurch erreicht, daß in der Kopfstation sowohl Bus A als auch Bus B vereinigt sind, wie das in Abbildung 11.15 dargestellt ist.

Tritt nun eine Leitungsunterbrechung auf, wird die Funktion der Kopfstation in den von der Unterbrechung unmittelbar betroffenen Knoten verlagert, und die bisherige Kopfstation schaltet die Busse einfach durch.

11 Rechnernetze – Basis der Kommunikation

Abbildung 11.14
Aufbau eines
Looped Bus



Die Funktions- und Leistungsfähigkeit des Netzes wird dadurch in keiner Weise vermindert. Die Abbildung 11.15 zeigt, wie ein rekonfigurierter Looped Bus aussieht.

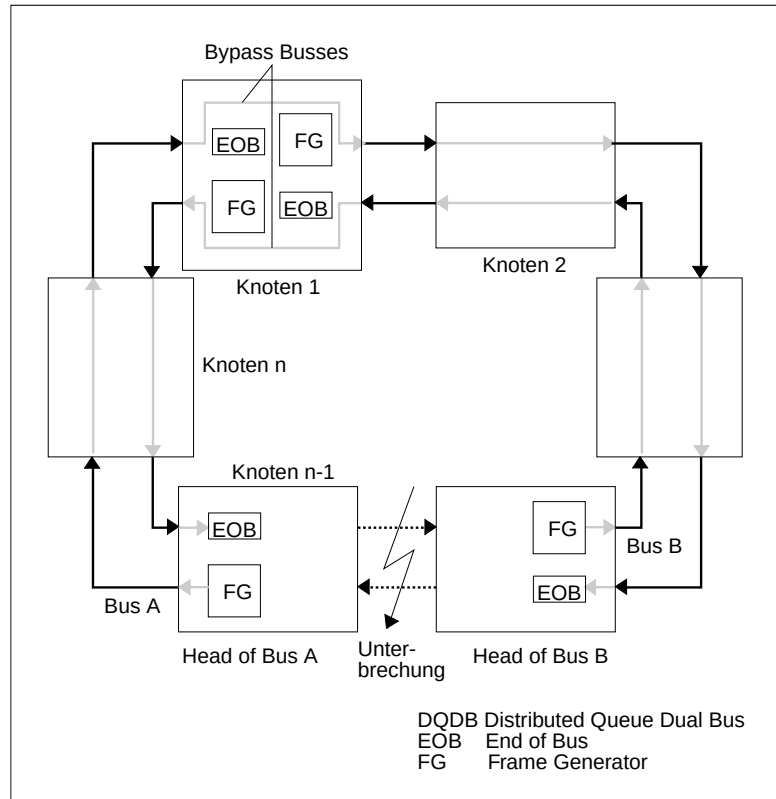
Eine Leitungsunterbrechung bei einem Offenen Bus führt zu einer Teilung des Netzes. Das ist aus Sicherheitsgründen nicht unbedingt zu empfehlen.

Beim Einsatz von MANs in öffentlichen Bereichen ist eine Strukturierung in mehrere Netzebenen notwendig. Man unterscheidet dabei zwischen dem Teilnehmeranschlußnetz (Customer Access System, CAN) und dem eigentlichen Transportnetz (MAN Switching System, MSS).

Im Teilnehmeranschlußnetz werden nur die Daten eines Teilnehmers übertragen. Das Teilnehmeranschlußnetz kann eine Punkt-zu-Punkt-Verbindung, ein Offener Bus oder ein Looped Bus sein. Die eigentlichen Teilnehmernetze, wie Ethernet, Token-Ring oder andere, werden über sogenannte Customer Gateways (CGW) an das Teilnehmeranschlußnetz angekoppelt.

11.3 Metropolitan Area Network

Abbildung 11.15
Rekonfigurierter
Looped Bus



Für das Transportnetz gilt, daß abhängig von der Ausdehnung des Versorgungsbereichs oder des zu übertragenden Datenvolumens mehrere MAN-Subnetze gebildet werden können. Die MAN-Subnetze werden mit Hilfe von Subnetwork-Routern zu einem MAN-Switching-System (MSS) aneinander gekoppelt. Durch die Kopplung immer größerer Netzwerkeinheiten können Hierarchien aufgebaut werden.

Das MAN-Switching-System besteht aus mehreren Bussen und einer Anzahl Knoten. Als MAN-Netzwerkelemente können eingesetzt werden:

- *Customer Gateway (CGW)*

Das Customer Gateway wird in der Regel beim Teilnehmer selbst installiert und beinhaltet die notwendigen Koppellemente, z.B. eine Bridge für das 802.x-LAN, um das Teilnehmernetz an das Teilnehmeranschlußnetz anbinden zu können – der Übergang vom LAN zum MAN.

11 Rechnernetze – Basis der Kommunikation

■ Edge Gateway (EGW)

Das Edge Gateway stellt eine Vermittlungseinheit innerhalb eines MAN-Switching-Systems für den Teilnehmeranschluß dar. Das EGW wird in den Gebäuden der Telekom installiert sein – der Übergang vom Teilnehmeranschlußnetz zum MAN-Switching-System.

■ Customer Network Interface Unit (CNIU)

In der Customer Network Interface Unit sind die Funktionen eines EGW und eines CGW zusammengefaßt installiert. Mit dieser Einheit wird es möglich sein, Teilnehmernetze direkt an ein MAN-Subnetz zu koppeln. Die CNIU ist für die Installation privater MANs konzipiert worden.

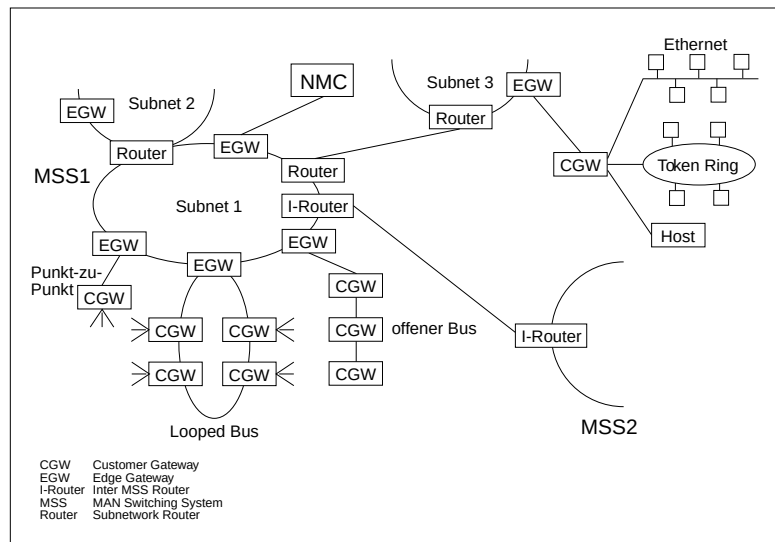
■ Subnetwork Router

Der Subnetwork Router ist eine Vermittlungseinheit innerhalb eines MAN-Switching-Systems und verbindet MAN-Subnetze miteinander. Der Subnetwork Router führt Relay- und Routing-Funktionen durch.

■ Inter-MSS Router (I-Router)

Es wird damit ermöglicht, eigenständige MAN-Switching-Systeme zusammenzuschalten. Die nachfolgende Abbildung zeigt den Zusammenhang der einzelnen Netzwerkelemente.

Abbildung 11.16
Metropolitan-Area-
Network-Netzwerk-
elemente



11.4 Die Zukunft der Breitbandkommunikation

Die Telekom unterstützt die von der EU-Kommission beschlossenen Maßnahmen zum Aufbau europäischer Breitbandnetze. Zusammen mit der France Télécom, der britischen BT, der spanischen Telefonica und der italienischen STET wurde bereits 1992 der Beschluß gefaßt, ein europäisches digitales Hochgeschwindigkeitsnetz (Global European Network – GEN) aufzubauen.

Ziel von GEN soll es sein, zwischen den Knoten der Netzbetreiber ein vermaschtes, europäisches und dienstunabhängiges Transportnetz auf Basis von Glasfaserverbindungen zur Verfügung zu stellen. Dabei sollen Übertragungsgeschwindigkeiten von bis zu 140 Mbit/s möglich sein. In einer nächsten Entwicklungsstufe soll GEN dann durch ein Managed European Transmission Network (METRAN) abgelöst werden. Dies soll Übertragungsgeschwindigkeiten von bis zu 155 Mbit/s ermöglichen. METRAN wird dabei ein Transportnetz sein, das die Leistungsfähigkeit der Synchronen Digitalen Hierarchie (SDH) nutzt und den Asynchronen Transfer Modus (ATM) des künftigen europäischen Breitband-ISDN unterstützt. Derzeit arbeiten am Projekt METRAN 26 europäische Netzbetreiber.

11.4.1 IDN Plus – die Netzinfrastruktur von morgen

Die Telekom wird das bestehende IDN weiterentwickeln zum IDN Plus. Man hat erkannt, daß sich die Kundenanforderungen gewandelt haben und auch für die Vernetzung von LANs bereits seit langem transparente Kommunikationswege mit weit größeren und flexibleren Bandbreiten, als dies momentan der Fall ist, gefordert werden.

Das IDN Plus ist logisch in zwei Teile unterteilt. Das Transportnetz wird flächendeckend aufgebaut. Es dient dazu, als Kernnetz reine Transportfunktionen zur Verfügung zu stellen. Zugleich werden jedoch auch verbesserte und neue Produkte verfügbar sein. Das Mehrwertnetz hingegen stellt Leistungsmerkmale für am Markt geforderte Anwendungen (LAN-LAN-Kopplung, Frame Relay, Sprach- und Datenintegration) zur Verfügung. Die Mehrwerttechnik wird im Gegensatz zur Transporttechnik bedarfsorientiert aufgebaut und steht somit nicht flächendeckend zur Verfügung.

IDN Plus setzt sich aus dem flächendeckenden Transportnetz und dem bedarfsorientierten Mehrwertnetz, das in das Transportnetz integriert ist, zusammen. Betrachten wir zunächst den geplanten Aufbau des Transportnetzes.

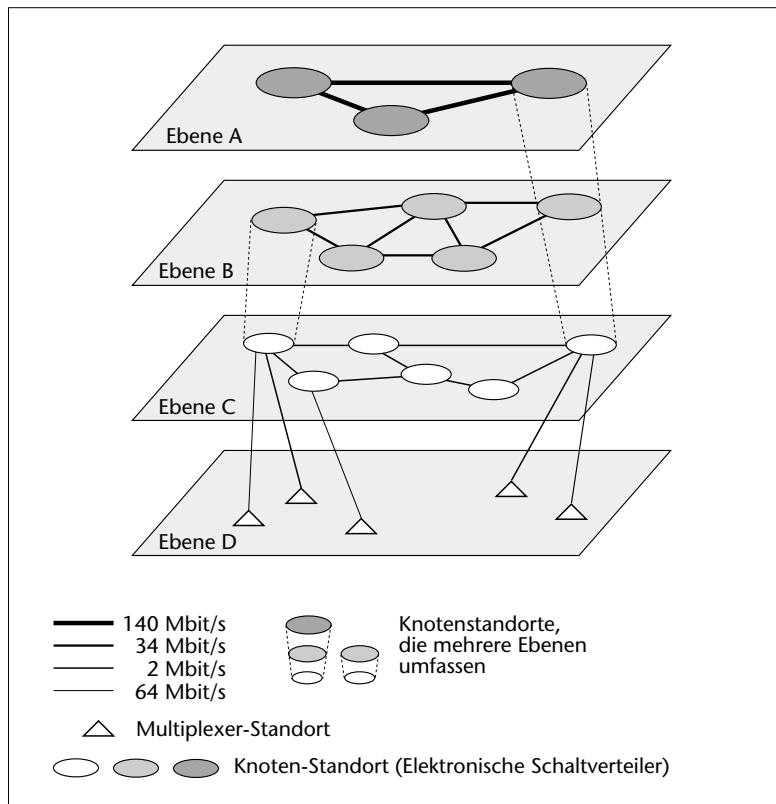
11 Rechnernetze – Basis der Kommunikation

Transportnetz

Im Transportnetz des IDN Plus werden elektronische Schaltverteiler, sogenannte Crossconnector, eingesetzt, um mit Hilfe eines Zeitmultiplexverfahrens die bittransparente Übertragung von Daten und Sprache unterstützen zu können. Somit wird es möglich, unter anderem 64-Kbit/s-Kanäle ohne manuellen Schaltaufwand zwischen ankommenden und ausgehenden Leitungen beliebig zu schalten. Auf diese Weise können die vorhandenen Netzressourcen optimal genutzt werden.

Für das IDN Plus wird das Transportnetz in vier Ebenen unterteilt. Dieser Aufbau ist in Abbildung 11.17 zu sehen. Dabei werden die Ebenen als A, B, C und D bezeichnet. Jede einzelne Ebene stellt unterschiedliche Transportkapazitäten zur Verfügung.

Abbildung 11.17
Aufbau des Transportnetzes im IDN Plus



11.4 Die Zukunft der Breitbandkommunikation

Die Ebene A stellt das schnelle Kernnetz dar. Über elektronische Schaltverteiler – sie sind mit einer Übertragungsgeschwindigkeit von 140 Mbit/s vernetzt – lässt sich der Datenverkehr schnell über große Entfernungen verteilen. Somit wird eine hohe Übertragungskapazität für Systeme bereitgestellt, wenn sie hierfür benötigt werden.

Die Knoten auf der Ebene B sind über Leitungen mit Übertragungskapazitäten von 34 Mbit/s verbunden. Der Datenverkehr wird richtungsbezogen gebündelt und an die Knoten der Ebene A zugeführt.

Die Ebene C führt das gleiche Verfahren durch. Die Knoten sind mit Übertragungswegen von 2 Mbit/s verbunden, und der Datenverkehr wird an die Knoten der Ebene B zugeführt. Auf Ebene D befinden sich die ZD-A-Systeme (Zeitmultiplex-Datenübertragungssystem) zur Bildung sogenannter Subbitraten mit Bitraten kleiner als 64 Kbit/s. Die Subbitraten werden dabei mittels Multiplexerhierarchien in 64-Kbit/s- oder 2-Mbit/s-Übertragungswegen gebündelt und der Netzebene C zugeführt.

Mehrwertnetz

Auf das Transportnetz kann die Mehrwerttechnik modular und somit individuell und bedarfsgerecht für den einzelnen Kunden aufgesetzt werden. Zu den wichtigsten Netzfunktionen der Mehrwerttechnik zählen:

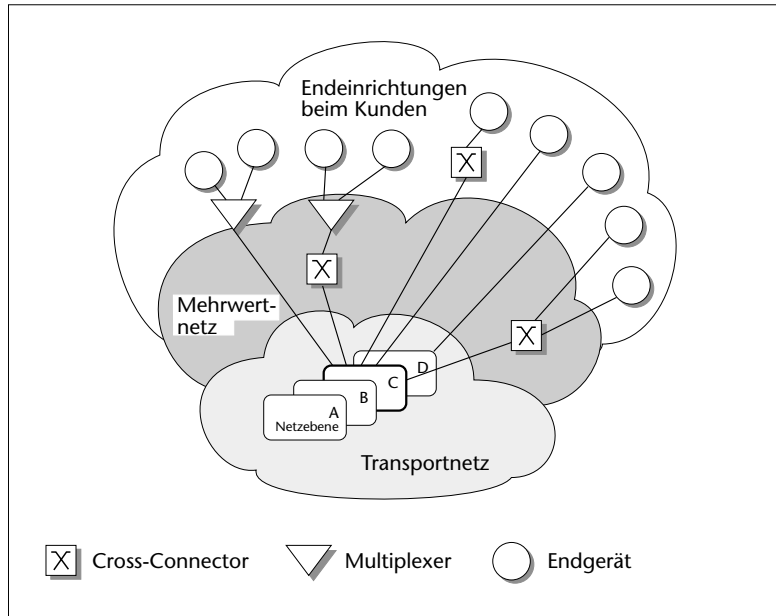
- Digitale Sprachübertragung, unkomprimiert (64 Kbit/s) oder komprimiert (32, 16 oder 8 Kbit/s)
- Frame Relay (FR-)Switching zur Bildung von FR-Netzen für die Vernetzung von LANs
- Integration von Bridges und Routern, auch für Multiprotokoll, um die Verkehrsführung zu steuern und Netzübergänge zu bilden
- Punkt-zu-Mehrpunkt-Verbindungen, wie sie bei der Nachrichtenverteilung erforderlich sind
- Videoübertragung
- T1/E1-Konvertierung, mit der die Primärrate der US-Digitalhierarchie (Summenbitrate 1,544 Mbit/s, 24 Nutzkanäle) auf die europäische Hierarchie (2 Mbit/s, 32 Nutzkanäle) umgesetzt wird

In Abbildung 11.18 ist die Integration von Transport- und Mehrwertnetz dargestellt.

Das IDN Plus wird auch das Switched-Multimegabit-Data-Service-Backbone-Netz (SMDS) unterstützen, das mit einem zellorientierten IEEE-802.6-Protokoll arbeitet.

11 Rechnernetze – Basis der Kommunikation

Abbildung 11.18
Integration von
Transport- und
Mehrwertnetz



Wie bereits beschrieben, handelt es sich hierbei um ein Hochgeschwindigkeitsnetzwerk, in dem die Bitraten dynamisch, in Abhängigkeit vom Verkehrsaufkommen, zugeordnet werden. Dieses Protokoll ist auch die Grundlage für Datex-M der Telekom.

Mit dem SMDS-Backbone wird auch bereits die Migration zum Breitband-ISDN berücksichtigt. IEEE 802.6 ist protokollverträglich mit ATM, wobei ATM wiederum die Grundlage für das Breitband-ISDN ist. Somit wird allen am SMDS-Backbone angeschlossenen Teilnehmern zu einem sehr frühen Zeitpunkt ATM-Funktionalität angeboten und zugleich ein gleitender Übergang zu ATM und Breitband-ISDN garantiert.

11.4.2 Datex-M

Mit Datex-M bietet die Telekom erstmals ein Hochgeschwindigkeitsnetz an. Das M steht für Multimegabit, Multimedia oder Metropolitan. Datex-M ist das SMDS-Produkt der Telekom auf Basis des 802.6-Protokolls. Datex-M ist ein standortübergreifender Service von Metropole zu Metropole, um mit hohen Geschwindigkeiten arbeiten zu können. Es ist unter anderem hervorragend geeignet für die Kopplung von LANs, weil Datex-M hohe Datenraten (auch im Burst) übertragen kann und mit den in LANs üblichen Protokollen kompatibel

11.4 Die Zukunft der Breitbandkommunikation

ist. Durch die Flexibilität von Datex-M kann es aber auch für den Einsatz von Videokonferenzen oder die Kopplung von Tk-Anlagen an verschiedenen Standorten genutzt werden.

In einem LAN werden die Endgeräte gleichberechtigt an ein Bussystem oder einen Ring angeschlossen. Die Datenstationen nutzen das Übertragungsmedium gleichberechtigt und gemeinsam. Damit kurze Zugriffs- und Antwortzeiten erreicht werden, wie dies unter anderem bei Datenbankanwendungen oder CAD-Programmen notwendig ist, müssen große Datenmengen in sehr kurzer Zeit übertragen werden. In einem LAN kommt es deshalb immer zu einem schubweisen Datenverkehr, dem sogenannten Traffic Burst, bei ungleichmäßiger Auslastung der Datenleitungen (mal ist viel los, mal weniger). Damit dennoch keine Engpässe auftreten (zumindest so wenig wie möglich), richtet man Netzwerke mit einer großen Bandbreite ein. Bei den meisten Protokollen werden die Daten paketvermittelt übertragen, d. h. mit einer Sende- und Empfangsadresse versehen und seriell zum Empfänger übertragen. Die Übertragung erfolgt ohne zeitintensiven Verbindungsaufbau (connectionless). Es gibt aber auch Protokolle, die verbindungsorientiert arbeiten. Eine hohe Bandbreite und paketorientierte Übertragung ohne Verbindungsaufbau gestatten den schnellen Durchsatz auch großer Datenmengen. Zwischen den einzelnen Übertragungen, den Bursts, bleibt aber in den meisten LANs auch Bandbreite ungenutzt. Diese Arbeitsweise von LANs wirkt sich deshalb besonders negativ auf die Kopplung von LANs aus, weil hierbei große Datenraten, also große Bandbreiten, benötigt werden.

Die Kopplung von LANs ist bislang aufgrund zu geringer Bandbreiten als problematisch einzustufen, vor allem unter dem Aspekt, daß die Forderungen nach schnellen Verbindungen immer dringlicher werden. Die Folge davon ist, daß bei einer Kopplung von LANs Kompromisse zwischen Preis und Leistung einzugehen sind. Je schneller die Datenübertragungsstrecken der Telekom sind, um so mehr muß dafür bezahlt werden. Mit Datex-M soll dies jedoch anders werden, zumindest was die Datenraten anbelangt.

Mit Datex-M hat man Zugang zu einem öffentlichen, vermittelnden Hochgeschwindigkeitsdatendienst, über den alle anderen Partner erreicht werden können, die ebenfalls an Datex-M angebunden sind. Obwohl Datex-M ein vermittelnder, öffentlicher Dienst ist, bleiben die Daten vor dem Zugriff Dritter geschützt. Durch die Bildung geschlossener Benutzergruppen wird zusätzliche Datensicherheit gewährleistet, d. h., keine Daten landen aus Versehen bei unbefugten Empfängern. Obwohl bei Datex-M alle angeschlossenen Kunden den gleichen Übertragungsweg nutzen, verhält sich Datex-M wie ein eigenes, privates Netz für den Kunden.

11 Rechnernetze – Basis der Kommunikation

Datex-M stellt eine transparente Schnittstelle zur Verfügung, womit gewährleistet ist, daß alle gängigen Protokolle eingesetzt werden können. Jeder Kunde kann unabhängig von der Geschwindigkeit des eigenen Datex-M-Anschlusses mit jedem anderen Datex-M-Kunden kommunizieren, da die Anpassung der Geschwindigkeit von Datex-M durchgeführt wird. Die technische Plattform von Datex-M arbeitet mit zwei Bussystemen, die gegenläufig Daten übertragen und somit dem Protokoll Distributed Queue Dual Bus (DQDB) nach dem IEEE 802.6 entsprechen. Durch den Vollduplexbetrieb kann die Datenübertragung gleichzeitig in beide Richtungen durchgeführt werden. Datex-M arbeitet zellorientiert und greift somit die paketerorientierte Übermittlung der LANs auf. Am Anfang jedes der beiden Busse werden kontinuierlich Leerrahmen erzeugt, die dann, wie ein Container, Informationen der Endgeräte aufnehmen und weitertransportieren können. Durch die Empfängeradresse in jedem Container wird garantiert, daß die Daten auch beim richtigen Empfänger ankommen. Es werden auch sogenannte Gruppenadressen unterstützt, so daß alle Mitglieder einer Gruppe die Daten im Container erhalten.

Datex-M ist wie ein herkömmliches LAN auch auf Traffic Burst eingerichtet. Die hohe Bandbreite der Übertragungsstrecken garantiert jedem Kunden, der an Datex-M angeschlossen ist, große Geschwindigkeiten. Dadurch, daß viele Kunden die Datex-M-Strecken gemeinsam nutzen, wird die Auslastung der Übertragungsstrecken wirtschaftlicher, als wenn jeder Kunde selbst seinen eigenen exklusiven Datenweg nutzen würde. Somit können günstigere Preise für die Kunden angeboten werden.

Mit Datex-M können regionale, nationale und internationale Netze aufgebaut werden. International ist die Kommunikation durch eine weltweit eindeutige Adressierung gesichert. Internationale Normungsgremien haben die Migration vom DQDB-Protokoll zum Asynchronen Transfer Modus (ATM) sichergestellt. Die Zellgrößen und der Zellaufbau beider Technologien sind eng miteinander verwandt. Auf diese Weise wird der Übergang zum Breitband-ISDN möglich. Bereits im Pilotprojekt für das Breitband-ISDN werden Übergänge zum Datex-M angeboten. Die Telekom plant, Datex-M als einen der ersten Dienste auch im Breitband-ISDN anzubieten.

Für den Datex-M Zugang werden die folgenden Geschwindigkeiten angeboten:

64 Kbit/s	Zugang über Service Switch mit DNAE
128 Kbit/s	Zugang über Service Switch mit DNAE
192 Kbit/s	Zugang über Service Switch mit DNAE
256 Kbit/s	Zugang über Service Switch mit DNAE

11.4 Die Zukunft der Breitbandkommunikation

384 Kbit/s	Zugang über Service Switch mit DNAE
512 Kbit/s	Zugang über Service Switch mit DNAE
1,92 Mbit/s	Zugang über Service Switch mit DNAE
34 Mbit/s	Zugang über Data-Service-Unit

Als Anschlußleitungen werden SFV eingesetzt, die sich wie folgt ergeben:

bei 64 Kbit/s	→ SFV	Digital 64S
bei 128 Kbit/s	→ ISDN-FV	Digital S02
bei 2 Mbit/s	→ SFV	Digital 2MS
bei 34 Mbit/s	→ SFV	Digital 34M

Die technische Ausführung von Datex-M richtet sich somit nach der Zugangsgeschwindigkeit und der Art des Anschlusses. Die DXI-Schnittstelle ist die »Protokoll-Schnittstelle«, standardmäßig die Regelschnittstelle bei Datex-M. Im Datex-M-Servicepreis sind die Data-Service-Unit und das Datennetz-Anschalte-Endgerät enthalten. Als weitere Option bietet die DTAG auch die Ausrüstung des kompletten Zugangs an, in diesem Falle inklusive dem dazugehörigen Endgerät (Router). Zudem kann vereinbart werden, daß zusätzliche Leistungen erbracht werden sollen. Hierzu zählen unter anderem:

- Ersatzschaltung über die gesamte Leitungsführung
- Installation eines Datex-M-Anschlusses in Sonderbauweise

Die Telekom bietet für Datex-M zwei Anschlußarten an, die je nach Anforderungsprofil des Kunden gewählt werden müssen oder können.

- *Individual Customer Access Network (ICAN)*

Bei diesem Anschluß werden Nutzzugänge in Abhängigkeit von den Kundenanforderungen zur Verfügung gestellt. Es stehen Übertragungsgeschwindigkeiten von 2, 34 und 140 Mbit/s mit den Schnittstellen IEEE 802.3 (Ethernet), IEEE 802.5 (Token-Ring) oder Router-Direktzugang über Data Exchange Interface (DXI) oder Subscriber Network Interface (z.B. für FDDI) zur Verfügung. Der Aufbau von Videokonferenzen oder die Vernetzung von Tk-Anlagen wird über den synchronen Zugang mit den Schnittstellen CCITT G.703/G.704 realisiert.

- *Data Service Unit (DSU)*

An die DSU können die eigenen Router des Kunden angeschlossen werden, um somit transparenten Zugang zum Datex-M-Netzwerk mit Geschwindigkeiten von 2 Mbit/s bis zu 34 Mbit/s zu ermöglichen.

Preise

Der Preis für Datex-M setzt sich zusammen aus den Kosten für die Anschlußleitung zum nächsten Datex-M-Netzknoten und einer Pauschale für die Nutzung von Datex-M. Die Höhe der Pauschale wiederum hängt von der Übertragungsgeschwindigkeit, dem Volumen, den Verkehrsbeziehungen (regional, national, international) und sonstigen zusätzlichen Leistungen ab (z.B. synchrone Übertragung oder Backup-Anwendung). Pro Anschluß gibt es ein monatliches Freivolumen von einem Gbyte. Für die Tarife der Übertragungen gibt es gestaffelte Volumenpreise, die je angefangenem Mbyte berechnet werden.

11.4.3 ATM und Breitband-ISDN

Auf die Eigenschaften und Funktionen von ATM bin ich bereits bei der Behandlung von Netzwerktopologien eingegangen. In diesem Abschnitt sollen deshalb nur noch die wichtigsten Aspekte erläutert werden.

ATM (Asynchronous Transfer Mode) ist das von CCITT empfohlene Transportverfahren für das Breitband-ISDN. Die Wahl für ATM wurde deshalb getroffen, weil es wie kein anderes Transportverfahren die Flexibilität besitzt, die Netzkapazität je nach Anforderung bereitzustellen. Dabei ist es egal, ob die Kapazitäten für die Übertragung von Videokonferenzen, die Vernetzung von Tk-Anlagen, die Kopplung von LANs oder andere Kommunikationsvorgänge benötigt werden. Mit der Entscheidung für ATM sind auch die Möglichkeiten vorhanden, das 64-Kbit/s-ISDN und das Breitband-ISDN nicht mehr als getrennte Netzwerke zu betreiben, sondern als umfassendes ISDN, das sowohl Schmalbanddienste als auch Breitbanddienste unterstützt. ATM verbindet die Vorteile der verbindungsorientierten Vermittlung mit denen eines paketorientierten Netzes.

In einem ATM-Netz werden in jedem Übertragungsabschnitt permanent ATM-Zellen fester Länge übertragen; das entspricht Containern gleicher Länge in einer unendlichen Reihe. Die Container bewegen sich fort, egal ob sie mit Daten gefüllt sind oder nicht. Eine ATM-Zelle besteht aus einem Informationsfeld (zur Aufnahme der Daten) und einem Zellkopf (zur Aufnahme der Adresse). Die Struktur der ATM-Zellen und die Bitrate sind international genormt und effizient gewählt. Eine ATM-Zelle besteht aus 5 Byte für den Zellkopf und 48 Byte für Daten. Die Flexibilität von ATM ist darin zu sehen, daß die Daten nicht an festen Positionen in einem Rahmen transportiert werden müssen. Die Verbindungen sind nicht durch ihre Zeitlage im

11.4 Die Zukunft der Breitbandkommunikation

Multiplexrahmen gekennzeichnet; vielmehr sorgt die Adressierung der ATM-Zellen dafür, daß die Zuordnung der Verbindung in den Netzknoten und am Ende der Verbindung aufgebaut werden kann.

ATM-Zellen einer Verbindung folgen in dem Abstand aufeinander, wie es die Bitrate des Nutzsignals erfordert und wie freie ATM-Zellen verfügbar sind. Eine ATM-Zelle wird immer vollständig gefüllt, und bei hohen Bitraten werden die ATM-Zellen dicht hintereinander für die Verbindung belegt. Bei niedrigen Bitraten hingegen erfolgt dies in entsprechend größeren Abständen. Somit bleiben die dazwischenliegenden ATM-Zellen leer und sind für den Transport von Daten anderer Verbindungen verfügbar. Das asynchrone Zeitmultiplexverfahren kann sich somit optimal auf den während einer Verbindung schwankenden Kapazitätsbedarf einstellen. Anwender in einem ATM-Netz können damit die Geschwindigkeit für den Informationsaustausch weitgehend frei wählen.

ATM-Netze arbeiten verbindungsorientiert: Beim Verbindungsaufbau wird geprüft, ob die Kapazität im Netz für diese Verbindung vorhanden ist oder ob ein anderer Weg mit ausreichender Kapazität gewählt werden muß. Anschließend ordnet die Steuerung des Vermittlungsknotens der Verbindung abschnittsweise virtuelle Kanäle zu. Die Summe der virtuellen Abschnitte bildet die virtuelle Verbindung; eine virtuelle Verbindung beschreibt den Weg durch das Netz. Die abschnittsweise festgelegte Adresse im Zellkopf ordnet die ATM-Zellen dieser Verbindung eindeutig zu, und alle ATM-Zellen einer Verbindung nehmen in der Reihenfolge ihrer Belegung denselben Verbindungsweg, d.h., sie werden in der gleichen Ordnung empfangen, wie sie auch beim Senden bestand.

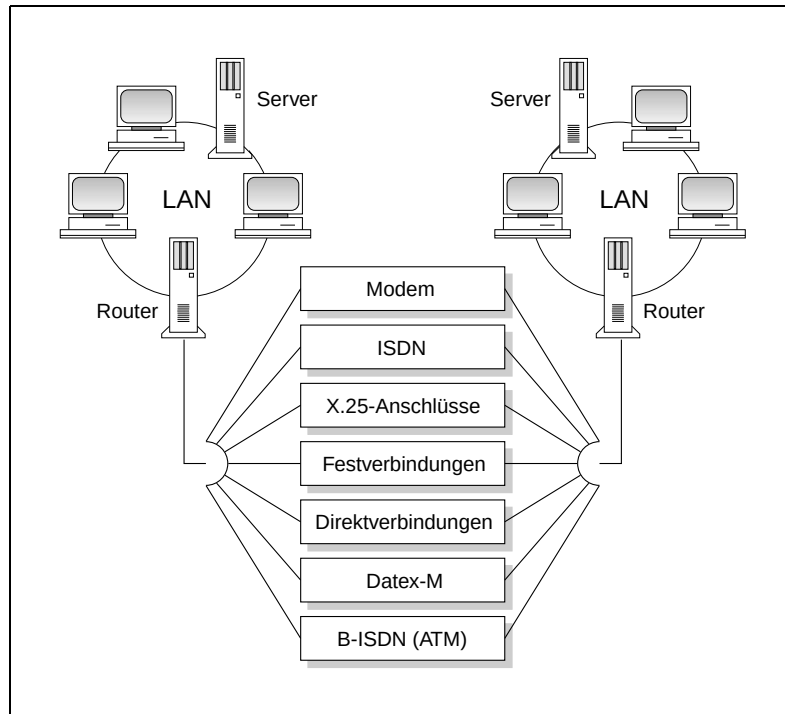
In einer ATM-Zelle sind alle Funktionen zur Realisierung bestimmter Dienste dem Informationsfeld zugeordnet; sie sind also Teil der Nutzlast. Die Informationen im Zellkopf sind vollkommen dienstunabhängig. Der Dienst und die Netzsteuerung lassen sich daher sehr gut trennen.

Für den Übergang vom LAN zum WAN steht eine Vielzahl von Möglichkeiten zur Verfügung. Dieses Kapitel sollte eine Übersicht darüber geben, was heute und in Zukunft möglich sein wird bzw. möglich sein muß. Im Zuge der immer höher werdenden Anforderungen bezüglich der Datenübertragungsraten muß es bald möglich sein, High-Speed-Verbindungen auch im WAN-Bereich zu erhalten. Betrachtet man sich die derzeitige Situation im Internet, dann kann man sehr schnell feststellen, daß die herkömmlichen DFÜ-Strecken nicht mehr ausreichend sind. Nicht umsonst wird das Angebot im Internet, das sogenannte World Wide Web (WWW), auch als World Wide Wait

11 Rechnernetze – Basis der Kommunikation

bezeichnet. Abschließend soll die Abbildung 11.19 zeigen, welche Gesamtlösungen für eine LAN-WAN-LAN-Kopplung zur Verfügung stehen.

Abbildung 11.19
LAN-WAN-LAN-
Kopplung



Berücksichtigt werden muß nur, daß für die einzelnen Koppelmöglichkeiten auch entsprechende Adapterkarten bzw. Endgeräte notwendig sind, die in Verbindung mit der Kommunikationssoftware die gewünschten Ergebnisse bringt. Da es eine Vielzahl von Router-Herstellern gibt und ebenso viele Hersteller Router-Lösungen für PCs bereitstellen, wäre es zu aufwendig, im Detail auf die Lösungen der einzelnen Hersteller eingehen zu wollen. Die Anforderungen an die Leistungsfähigkeit, der Preis und das Management sind ausschlaggebend, ob man sich für externe Lösungen von Cisco oder 3Com entscheidet und nicht für Einsatzmöglichkeiten »interner« Lösungen von AVM oder auch ITK. Bei den internen Lösungen handelt es sich um solche für PC-Server, deren Basis entweder NetWare oder NT Server bildet, also eine RISC-Architektur und nicht eine CISC-Architektur.

Da ich Ihnen jetzt sehr viel über das Dienstleistungsspektrum der DTAG erzählt habe, möchte ich exemplarisch einen Drittanbieter aufzeigen, der ebenfalls ähnliche Dienste zur Verfügung stellt, seit

11.5 Arcor – Was wird angeboten?

die Öffnung des Kommunikationsmarkts in Deutschland erfolgt ist. Es handelt sich hierbei um Mannesmann Arcor AG & Co., im nachfolgenden Arcor genannt. Es sei auch nochmals darauf hingewiesen, daß sich die Deinstleistungsangebote der einzelnen Anbieter zum Teil sehr schnell ändern können und werden, so daß diese Übersicht nur einen Querschnitt aufzeigen kann, der zum Zeitpunkt der Erstellung dieses Buches Gültigkeit hatte. Es ist also immer empfehlenswert, vor der Entscheidungsfindung für den einen oder anderen Dienst aktuelle Informationen einzuholen.

11.5 Arcor – Was wird angeboten?

Nach der Öffnung des Telekommunikationsmarkts gibt es eine Vielzahl von Firmen, die entsprechende Dienste anbieten können und dürfen. Diese Firmen bieten neben herkömmlichen Telefondiensten auch Dienste zur Kopplung von Netzwerken oder den Zugang zum Internet an. Da bereits bekannt ist, daß mit herkömmlichen analogen und digitalen Telefonverbindungen LANs miteinander gekoppelt werden können und hierfür die dafür anfallenden Kosten kalkuliert werden müssen, will ich mich nachfolgend nur auf die speziellen LAN-LAN Verbindungsangebote konzentrieren, ohne jedoch im einzelnen Preise hierfür anzugeben – es geht nur um die verfügbaren Dienste.

Die sogenannten Daten Services bieten für individuelle Unternehmensanforderungen die richtigen Verbindungen. Diese Dienste basieren auf einem Kommunikationsnetz, das für sehr hohe Ansprüche an Dienstqualität, Zukunftssicherheit und Wirtschaftlichkeit konzipiert und eingerichtet worden ist. Die Services, die Direktanbindung und das Einwählen über ein Drittnetz per Modem oder ISDN in das Netzwerk von Arcor und die Zugangsgeschwindigkeiten sind dabei individuell konfigurierbar. Das Angebot der Daten Services sieht dabei wie folgt aus:

- LAN-Connect-Service
- Frame-Relay-Service
- X.25-Service
- Internet Access Service
- Bandwith/ATM-Service

In den nachfolgenden Ausführungen sollen die Inhalte und Möglichkeiten der einzelnen Dienste etwas näher beschrieben werden.

11.5.1 Frame-Relay-Service

Hierbei handelt es sich um einen standardisierten, verbindungsorientierten Datenübertragungsdienst, der sich besonders für die LAN-LAN-Kopplung eignet. Zu den wichtigsten Merkmalen zählt ein einfaches Übertragungsprotokoll mit geringem Overhead, wodurch auch hohe Durchsatzraten und geringe Netzverzögerungen gewährleistet werden können. Hinzu kommt ein variables Bandbreitenmanagement, indem man die Bandbreite nach Bedarf einsetzt, und Multiprotokollfähigkeit. Die Länge der Datenpakete (Frames) ist variabel, so daß diese in der gleichen Länge wie in den angeschlossenen Netzen transferiert werden. Dadurch ist man in der Lage, Nutzdaten von bis zu mehreren Kbyte innerhalb eines Frame zu übertragen.

Die Vernetzung von mehreren Standorten erfolgt dabei über virtuelle Festverbindungen (Permanent Virtual Circuit – PVC). Pro angeschlossenem Standort ist nur ein Port notwendig, so daß alle Unternehmensstandorte über eine einzige Zugangsleitung zum Frame Relay Netz erreicht werden können. Abhängig vom durchschnittlichen Datendurchsatz wird eine sogenannte Committed Information Rate (CIR) vereinbart. Darunter versteht man die für eine Verbindung dauerhaft verfügbare Übertragungsrate. Die CIR ist auf die speziellen Bedürfnisse des Kunden zugeschnitten und läßt sich in kleinen Schritten individuell an jeden angebundenen Standort anpassen. Da bei LAN-LAN-Kopplungen immer wieder Lastspitzen auftreten, die abgefangen werden müssen, kann und darf die CIR für eine gewisse Zeit überschritten werden.

Die Datenübertragung wird über Permanent Virtual Circuits (PVCs) realisiert, wobei der Datentransport mit Frames variabler Länge erfolgt. Der Frame-Relay-Service ist dabei in Übereinstimmung mit den durch ITU-T, ANSI und FRF gesetzten Standards realisiert. Der Netzzugang erfolgt in direkter Anschaltung über einen sogenannten Frame-Relay-Access-Knoten, wobei Zugangsgeschwindigkeiten zwischen 64 Kbit/s und 2 Mbit/s unterstützt werden. Die CIR wird in Größenordnungen von 4 Kbit/s und 1024 Kbit/s zur Verfügung gestellt.

11.5.2 X.25-Service

Mit diesem Dienst kann eine große Anzahl Anwendungen abgedeckt werden, die den Einsatz von X.25 sinnvoll erscheinen lassen. Aufgrund der Kosten- und Mengenstruktur eignet sich X.25 in der Regel besonders gut für Dialoganwendungen wie

- Point of Sales (POS)
- Point of Information (POI)

11.5 Arcor – Was wird angeboten?

- Vernetzung von Warenwirtschaftssystemen
- E-Mail und elektronischer Datenaustausch

In Abhängigkeit des Einsatzgebietes hat der Einsatz von POS in vielen Branchen durchaus einen Sinn. Deshalb bietet Arcor, abgestimmt auf das Nutzungsverhalten, drei Anbindungsoptionen an:

- POS Direkt, POS über eine exklusive Teilnehmeranschlußkennung
- POS Light, POS über analoge Wählleitungen
- POS ISDN, POS über den ISDN-D-Kanal

Bei diesen POS-Angeboten handelt es sich bei den Preisen um einen monatlichen Festpreis, der den Anschluß, ein bestimmtes Datenvolumen und das Modem bzw. den Terminaladapter beim Kunden beinhaltet. Der Vorteil besteht darin, daß eine gesicherte Datenübertragung zur Verfügung steht, weltweite Verbindungen damit aufgebaut werden können und der monatliche Endpreis vom Datenvolumen abhängt.

Zu den technischen Merkmalen ist zu sagen, daß man auf das X.25-Protokoll setzt und somit eine Paketvermittlung auf den OSI-Schichten 1–3 erfolgt. Nach Angaben von Arcor beträgt die mittlere Netzdurchlaufzeit in 98% der Anschaltzeit weniger als 300 ms. Für die Netzanbindung stehen die V.24- und die X.21-Schnittstelle zur Verfügung, womit sich je nach Anschlußvariante Zugangsgeschwindigkeiten von 4,8 Kbit/s bis n*64 Kbit/s ergeben.

Als Zugänge werden unterstützt:

- Direktzugang über X.25-Access-Node
- Indirekter Zugang über den ISDN-D-Kanal nach der ITU-T-Empfehlung X.31, Case B
- Indirekter Zugang über den ISDN-B-Kanal über dezentral verfügbare Einwählpools
- Indirekter Zugang über PSTN-Anschluß (analog) über dezentral verfügbare Einwählpools

11.5.3 LAN-Connect-Service

LAN-Connect erweitert den Frame-Relay-Anschluß um einen LAN-Router, der von Arcor nicht nur installiert, sondern überwacht und betreut wird. Durch die rund um die Uhr vorhandene Überwachung der LAN-Verbindung erhöht sich damit auch die Sicherheit des Gesamtsystems. Die Vorteile einer solchen Verbindung liegen auf der Hand:

11 Rechnernetze – Basis der Kommunikation

- Die eigenen Personalressourcen werden optimiert, da Routinetätigkeiten entfallen.
- Im Vergleich zu Mietleitungen ist dieser sehr kostengünstig und effektiv.
- Es ist die Vernetzung von unterschiedlichen LAN-Strukturen möglich.
- Die Anbindung läßt sich flexibel rekonfigurieren.
- LAN-Connect bildet die Basis für Mehrwertdienste, um damit Zugänge zum Internet, zu Datenbanken und Online-Diensten realisieren zu können.
- Durch feste monatliche Preise sind die Kosten sehr gut kalkulierbar.

LAN-Connect unterstützt die Protokolle TCP/IP und IPX/SPX (somit OSI-Schicht-3 und -4-Protokolle) über das WAN-Protokoll Frame Relay (OSI-Schicht 1 und 2). Die Datenübertragung wird über permanente virtuelle Verbindungen (PVC) mit Geschwindigkeiten von bis zu 2 Mbit/s realisiert. Durch den Einsatz einer End-to-End-Backup-Option, die über ISDN realisiert wird, erreicht man ein Höchstmaß an Verfügbarkeit der Datenübertragungsfunktionen. Als LAN-Schnittstelle werden derzeit Ethernet und Token-Ring unterstützt.

Von Arcor werden die folgenden Service-Leistungen in Verbindung mit LAN-Connect angeboten:

- Installation der benötigten Komponenten (Router)
- Dokumentation und Pflege des Netzwerks
- Management und Rekonfiguration des Netzwerks, Reaktion je nach Servicelevel und Störungsbeseitigung innerhalb der gewünschten Servicezeiten

11.5.4 Internet-Access-Service

Arcor bietet für den Internet Zugang einen sehr modernen Hochgeschwindigkeits-Backbone. An über 100 Standorten hat man Zugriff auf diesen von Arcor zur Verfügung gestellten Backbone, der mit 2*155 Mbit/s vermascht ist, um somit einen ziemlich reibungslosen Datenaustausch gewährleisten zu können. In Zusammenarbeit mit AT&T/Unisource wird eine weltweite Anbindung an das Internet zur Verfügung gestellt. Für den Internet-Zugang werden die unterschiedlichsten Dienste angeboten, die nachfolgend näher beschrieben werden.

11.5 Arcor – Was wird angeboten?

Netzzugang

Internet-Connect (für große Unternehmen und Internet-Service-Provider (ISP)):

- Festanschluß mit 64 Kbit/s, 128 Kbit/s, 256 Kbit/s, 512 Kbit/s, 2 Mbit/s, 4 Mbit/s, 6 Mbit/s, 34 Mbit/s
- 2-Mbyte-Webpage
- IP-Adressen-Registrierung
- Eigener Domain-Name
- Secondary DNS

Dies sind die Standard-Features, optional stehen zur Verfügung:

- Basis Firewall
- Managed Router Service
- Basis- oder Plus-Mailbox
- Mail Relay
- News Feed
- Primary DNS

Internet-Dial Business (für große/mittelständische Unternehmen und SOHOs):

- Einwahl über ISDN oder Modem
- Channel Bundling von bis zu sechs ISDN-B-Kanälen
- Basis Mailbox (4x) sowie Plus-Mailbox (1x)
- 2-Mbyte-Webpage
- Eigener Domain-Name

Dies sind die Standard-Features, optional können beantragt werden:

- Basis Firewall
- Router (vorkonfiguriert)
- Plus Mailbox

Internet-Dial Premium (für kleine Internet-Service-Provider und/oder große bis mittelständische Unternehmen):

- Dial-in und Dial-out
- Channel Bundling von bis zu 6 ISDN-B-Kanälen
- Basis Mailbox (4x) sowie Plus Mailbox (1x)
- 2-Mbyte-Webpage
- Eigener Domain-Name

Neben diesen Standard-Features stehen optional zur Verfügung:

- Basis Firewall
- Router (vorkonfiguriert)
- Plus Mailbox
- Mail Relay
- News Feed

11 Rechnernetze – Basis der Kommunikation

Internet-Dial Privat (kleine Büros und Home Office)

- Einwahl über ISDN oder Modem
- Channel Bundling bis zu 2 ISDN-B-Kanälen
- Basis Mailbox (1x)
- 2-Mbyte-Webpage

Als optionales Feature kann neben diesen Standard-Features beantragt werden:

- Eigener Domain-Name

Man sieht am Ende dieser Ausführungen, daß sich in der Regel die Angebote ziemlich ähnlich sind. Trotzdem ist es empfehlenswert, eine exakte Untersuchung durchzuführen, bevor man sich für den ein oder anderen Anbieter entscheidet. Im Vergleich zur DTAG waren bislang die Preis- und Produktübersichten aller anderen Telekommunikationsanbieter nicht so überzeugend, so daß man sehr viel Zeit investieren mußte, um an alle in Frage kommenden Informationen zu kommen. Die nächsten Monate werden zeigen, inwieweit sich Verbesserungen bei den anderen Anbietern ergeben und wie groß die Kundenabgänge bei der DTAG sein werden. Bislang war die Resonanz nicht so groß wie erwartet. Dies mag auch daran liegen, daß sich die Angebote der DTAG nicht sehr von denen anderer Anbieter unterscheiden.

12

Lokale Netzwerke im PC-Bereich

Im Vordergrund der Aufgaben von PC-LANs steht im Prinzip das Ressourcen-Sharing, d.h. die Nutzung zentraler Betriebsmittel (Festplatten, Drucker, CD-ROMs, MO-Laufwerke etc.) durch die angeschlossenen Stationen. Natürlich spielen auch die Kommunikation der Teilnehmer untereinander und der Austausch von Daten eine sehr große Rolle. Das Hauptziel ist jedoch der Zugriff auf zentrale Datenbestände mit Hilfe multi-user-fähiger Programme. Da beim Zugriff auf zentrale Datenbestände auch Datenschutz und Datensicherheit gewährleistet werden müssen, ist darauf zu achten, daß diese beiden Aspekte nicht vernachlässigt werden, wie dies beim Einsatz von Standalone-PCs meistens der Fall ist.

Es zeigt sich auch die Tendenz, den Einsatz von Gateways und Kommunikationseinrichtungen zur Verbindung mit anderen Netzen immer weiter auszubauen, damit nicht nur LANs, sondern auch WANs aufgebaut werden können. Dies betrifft sowohl die Ausnutzung der öffentlichen Datennetze als auch die Verbindung zu Host-Rechnern und Rechnern der mittleren Datentechnik. Auf diese Weise soll jeder Anwender im Netzwerk die Möglichkeit erhalten, von seinem Arbeitsplatz aus über das Datex-P-Netz, T-Online oder ISDN-Netz die Verbindung zu anderen Systemen aufzubauen oder mit Hilfe von Gateway-Rechnern und den Einsatz von Terminalemulationen den PC im Netz zeitweise als Host-Terminal einzusetzen.

Besondere Bedeutung bekommt in diesem Zusammenhang der Zugang zum Internet. Dabei ist zu unterscheiden, ob er nur für einen Einzelplatzrechner oder für das gesamte Netzwerk realisiert werden soll. Es geht dabei nicht nur um die Möglichkeit, alle erdenklichen Informationen und Kontakte im Internet zu nutzen, sondern auch um die damit verbundene Funktion, als Anbieter im Internet einen sogenannten Web-Server zur Verfügung zu stellen. Betrachtet man die Entwicklungen bei Novell und bei Microsoft, so kann man sehr gut sehen, daß dieser Kommunikationsschiene immer mehr Bedeutung zugesprochen wird. Dies beginnt bei der Entwicklung der TCP/IP-basierenden Tools und Programme, um den Zugang zum Internet zu ermöglichen (Netscape, Web-Browser etc.), und hört bei der Internet-Software für einen Web-Server bzw. bei Anwendungen zur einfachen Gestaltung und zum einfachen Aufbau von Web-Seiten auf.

12 Lokale Netzwerke im PC-Bereich

Somit ist es nicht mehr notwendig, daß auf dem Schreibtisch der Mitarbeiter mehrere Bildschirmarbeitsplätze eingerichtet werden, sondern es besteht die Möglichkeit, mit dem PC alle notwendigen Arbeiten an den unterschiedlichsten Rechnern in den verschiedensten Netzwerken durchzuführen. Wie solche Netzwerke aufgebaut werden können und welche technischen Möglichkeiten hierfür derzeit angeboten werden, ist Thema der nächsten Kapitel. Zunächst will ich Ihnen zeigen, welche Kriterien für die Auswahl von LANs entscheidend sind. Da ich durch meine Tätigkeit im Beratungsbereich immer wieder mit der Frage konfrontiert werde, ob ein LAN der MDT (Mittleren Datentechnik) zu bevorzugen ist, werde ich mich auch mit diesem Problem auseinandersetzen.

12.1 Auswahlkriterien für LANs

Wenn Sie sich einmal entschieden haben, Lokale Netze einzusetzen, fangen die Schwierigkeiten meistens erst an. Mit dieser Entscheidung ergeben sich eine ganze Reihe von Fragen: Welches LAN soll man für welche Einsatzgebiete verwenden? Welche Form der Verkabelung ist die günstigste? Welches Netzwerkbetriebssystem ist am besten geeignet? Welche Client-Software ist in Verbindung mit den notwendigen Anwendungen im Netzwerk optimal? Welche Entwicklungen bringt die Zukunft? Gerade die letzte Frage wird wohl nur ein Orakel beantworten können.

Der Grundsatz »Planung vor Technik« sollte auf jeden Fall strikt eingehalten werden. In diesem Kapitel will ich Ihnen einige Entscheidungskriterien auflisten, mit deren Hilfe es leichterfällt, Planungen und letztendlich Kaufentscheidungen gezielt zu treffen.

12.1.1 Die Erstellung eines Kriterienkataloges

Bevor Sie eine anwendergerechte Entscheidung treffen können, müssen Sie eine Reihe von Fragen beantworten, um die richtigen Produkte zur richtigen Zeit auswählen zu können. Diese Fragen können meist mit Hilfe von Datenblättern der verschiedensten Hersteller abgeklärt werden. Ich werde Ihnen die einzelnen Kriterien zuerst einmal in geeigneten Blöcken zusammengefaßt auflisten und sie anschließend etwas genauer behandeln.

- *Technische Eigenschaften*
 - Topologie
 - Übertragungsmedium
 - Übertragungsgeschwindigkeit
 - Zugriffsverfahren

12.1 Auswahlkriterien für LANs

- Übertragungsverfahren
- Minimale und maximale Entfernung zwischen zwei Stationen
- Maximale Gesamtlänge des LAN
- *Art der anzuschließenden Stationen*
 - Voraussetzung für den Anschluß von Workstations
- *Anzahl der anschließbaren Rechner*
 - Wie viele Stationen können in einem LAN maximal angeschlossen werden?
 - Wie viele Stationen sind realistisch?
- *Konzept des Netzwerkbetriebssystems*
 - Anforderungen an den Server
 - Maximale Anzahl von Servern in einem LAN
 - Welche zentralen Betriebsmittel verwaltet der Server?
 - Wie viele zentrale Betriebsmittel kann der Server verwalten?
 - Welches Lizenzierungsverfahren verwendet der Hersteller für die Clients?
 - Welche Server-Plattformen stehen zur Verfügung?
 - Wie groß ist der Marktanteil?
- *Leistungsfähigkeit des Netzwerkbetriebssystems*
 - Effektive Übertragungsrate
 - Unterstützung von Multiprozessorsystemen
 - Ausfallsicherheitsmechanismen
 - Welche unterschiedliche Clients werden unterstützt?
 - Welche unterschiedlichen Protokolle werden unterstützt?
 - Datensicherungskonzept (zentral/dezentral)
 - Realisierung von Datei-Sharing
 - Netzwerkfähige Software vorhanden?
- *Einbindung von Fremdsystemen*
 - Kommunikationsalternativen
 - Unterstützung vom Netzwerkbetriebssystem
 - Einbußen bei der Übertragungsgeschwindigkeit
 - Unterstützt der Fremdrechner die Software?
 - Welche Übergänge zu anderen Systemen werden angeboten?
 - Handelt es sich bei der Software um herstellereigene oder die von Drittherstellern?
- *E-Mail- und Workflow-Mechanismen im Netz*
 - Welche Anforderungen werden an die E-Mail gestellt?
 - Welche Anforderungen werden an das Workflow gestellt?
 - Soll es sich um ein integriertes Paket handeln, oder dürfen die Komponenten von unterschiedlichen Herstellern stammen?
 - Welche Gateways zu anderen Systemen müssen integrierbar sein?

12 Lokale Netzwerke im PC-Bereich

Dieser Kriterienkatalog kann als Grundlage für die Erstellung eines Pflichtenhefts herangezogen werden, wenn man ein LAN (Hardware und Software) aus den vielen Angeboten den eigenen Bedürfnissen entsprechend auswählen möchte.

Technische Eigenschaften

Topologie

Für den Betrieb des Netzes ist es zwar nicht relevant, unter welcher Topologie das Netzwerk betrieben wird, hinsichtlich Durchsatz und Leistungsfähigkeit spielt das jedoch eine nicht zu unterschätzende Rolle. Daneben ist es auch für die Verkabelung innerhalb eines Gebäudes nicht unerheblich, ob Sie als Topologie ein Stern-, Ring- oder Bus-LAN einsetzen wollen.

Es ist auch wichtig, wie die Verteilung der einzelnen Stationen innerhalb eines Gebäudes aussehen wird. Die strukturelle Begebenheit des Gebäudes oder der Gebäude, in denen ein LAN aufgebaut werden soll, muß bei diesem Punkt unbedingt mit ins Kalkül gezogen werden. Sie sollten dabei auf alle Fälle überprüfen, ob Kabelschächte vorhanden sind und in diesen noch Platz für zusätzliche Kabel ist. Haben Sie keine Kabelschächte oder keinen Platz mehr in bestehenden Schächten, ist zu prüfen, ob und wie neue verlegt werden können, um diese eventuell an die topologischen Gegebenheiten anpassen zu können.

Übertragungs- medium

Bei der Auswahl des Kabels sind verschiedene Punkte zu beachten:

1. Können normale Kupferkabel verwendet werden? Soll ein LAN zum Beispiel in einem Bereich mit starken magnetischen Feldern installiert werden, scheiden Kupferkabel aufgrund der Störanfälligkeit meistens aus. In diesem Fall sind nur noch Lichtleiterkabel einsetzbar.
2. Die Kosten der Kabel sind in den meisten Fällen wesentlich höher als man allgemein annimmt; das betrifft besonders Lichtleiterkabel. Auch die Netzwerkkarten für den LWL-Anschluß sind teurer als Karten für Kupferkabelanschluß.
3. Bei einer notwendigen maximalen Übertragungsgeschwindigkeit können nur ganz bestimmte Kabeltypen verwendet werden; darauf ist vor allem im Bereich der High-Speed-Netzwerke zu achten. Existieren bereits Kabel, die unter Umständen weiterverwendet werden sollen, ist deren Tauglichkeit unbedingt zu prüfen.
4. Bei der Verlegung der Kabel müssen die nicht zu überschreitenden Längen und Biegeradien berücksichtigt werden. Die verschiedenen Kabeltypen besitzen unterschiedliche Eigenschaften. Es muß auch berücksichtigt werden, ob die Kabel in den bestehenden Kabelschächten untergebracht werden können.

12.1 Auswahlkriterien für LANs

5. Im Zuge einer vollständigen Neuverkabelung wird man nur noch CAT-5- bzw. CAT-6-Twisted-Pair-Kabel (evtl. auch CAT-7-Twisted-Pair-Kabel) verlegen, wenn es die Umgebungsbedingungen zulassen. Ansonsten wird man dazu übergehen, in kritischen Bereichen LWL-Kabel zu verwenden.

Die Eigenschaften der verschiedenen Kabelarten haben wir bereits in den vorherigen Abschnitten behandelt, dort kann bei Bedarf nachgelesen werden.

Übertragungs- geschwindigkeit

Darunter versteht man die Brutto-Datenrate. Es handelt sich dabei um die Bitrate, mit der Daten, Informationen oder Nachrichten über das Netz transportiert werden. Wie Sie bereits wissen, ist dem Aufbau und der Funktionsweise des Kommunikationsprotokolls das ISO-OSI-Modell zugrunde gelegt. An diesem Modell ist zu ersehen, daß jede Nachricht, die über das Netzwerk transportiert wird, mit Zusatzinformationen versehen wird. Aufgrund dieser und anderer Aspekte, die wir in einem späteren Kapitel behandeln werden, gibt der Bruttowert für die Übertragungsgeschwindigkeit keinen klaren Anhaltspunkt. Wichtiger und wesentlich interessanter ist die Angabe eines Netto-Durchsatzwerts. Dieser Wert zeigt, wie groß der Durchsatz von wirklichen Nachrichten ist.

Das Spektrum der angebotenen Übertragungsraten reicht meist von 4 Mbit/s bis 1 Gbit/s. Diese Netze sind in der Praxis von Interesse. Es kommen in der Regel Ethernet-, Token-Ring-, FDDI-, FastEthernet-, Gigabit-Ethernet- oder ATM-Netzwerke zum Einsatz. Zu prüfen ist im High-Speed-LAN-Bereich nur, ob jeder Arbeitsplatz mit hohen Übertragungsraten ausgestattet werden muß, da aus Kostengründen meist eine Mischung aus konventionellen Arbeitsplätzen und High-Speed-Arbeitsplätzen günstiger ist.

Zugriffs- verfahren

Das Zugriffsverfahren ist neben anderen Faktoren entscheidend für den Durchsatz in Lokalen Netzen, wenn es sich um ein Shared-Media-Netzwerk handelt. Beim Einsatz von Switches wird dieses wieder relativiert. Hierbei spielt es eine wesentliche Rolle, wie hoch die Auslastung des Gesamtsystems sein wird. Da das Token-Passing-Protokoll eine maximale Übertragungszeit garantiert (proportional zur Anzahl der Stationen), sind diese Mechanismen (Token-Ring- oder Token-Bus-Topologie) bei stark belasteten Systemen eher zu empfehlen als solche Netze, die auf CSMA/CD basieren. Bezüglich der Notwendigkeit, hohe Übertragungsraten bis zum Arbeitsplatz zur Verfügung zu stellen, sind alle Anwendungen und Gesamtanforderungen genauestens zu untersuchen.

12 Lokale Netzwerke im PC-Bereich

Eine Faustregel für Ethernet besagt, daß bei ca. 20 bis 25 Stationen ein Netz unter CSMA/CD noch sehr gute Antwortzeiten aufweist, wenn davon ausgegangen wird, daß alle Stationen aktiv sind und gleichmäßig hohe Datenlasten verursachen.

Durch den Einsatz von Switches sieht die Situation inzwischen etwas anders aus. In diesem Fall ist nicht mehr die Anzahl der Stationen pro Segment ausschlaggebend, da jeder Switchport im Prinzip ein eigenes Segment darstellt, sondern die Leistungsfähigkeit der Switching-Engine. Ist diese leistungsfähig genug, dann können auch viele Anschlüsse über einen Switch bedient werden.

Ab einer größeren Anzahl von Stationen sind Token-Passing-Protokolle dem CSMA/CD vorzuziehen. Dabei spielt es aber eine wesentliche Rolle, ob alle Stationen gleichzeitig aktiv sind oder nicht und welche Applikationen mit welchen I/O-Transferraten auf die File-Server-Platte zugreifen. Ein schwach ausgelastetes Netz kann mit 100 Stationen unter CSMA/CD hervorragende Antwortzeiten bieten. Der Einsatz von High-Speed-Netzen ist nicht immer von Anfang an notwendig. Das Netzwerk sollte nur so konzipiert werden, daß eine Umstellung auf High-Speed-Arbeitsplätze ohne Änderung der physikalischen Infrastruktur möglich ist.

Bevor Sie diese Entscheidung treffen, sollten Sie prüfen, wie I/O-intensiv die einzusetzenden Programme sein werden bzw. wie die Entwicklung für die nächsten Jahre aussehen wird!

Übertragungsverfahren

Für das LAN ist dies von nachrangiger Bedeutung. Diese Wahl hat nur Auswirkung auf die einzusetzenden Kabel. Eine Frage ist, ob für einen späteren Zeitpunkt geplant ist, dieses Kabel als Breitbandsystem zum Beispiel für die gleichzeitige Übertragung von Text, Daten, Bild und Sprache zu verwenden. Eines sollte Ihnen dabei jedoch klar sein: Breitbandnetze sind teurer als Basisbandsysteme.

Entfernung zwischen zwei Stationen

Diese Restriktion hat Auswirkungen auf das aufzustellende Verkabelungskonzept. Entscheidend ist, in welchem geringsten Abstand zwei Rechner aufgestellt werden können. Der Abstand zwischen zwei Stationen muß zum Beispiel bei der Thick-Ethernet-Verkabelung mindestens 2,5 Meter betragen.

Ein Beispiel für die maximale Entfernung ist der IBM-Token-Ring. Die Entfernung zwischen zwei Stationen darf nicht größer als 300 Meter sein. Die Angaben werden benötigt, um festlegen zu können, an welchen Stellen eventuell Zwischenverstärker eingebaut werden müssen. Bei den minimalen Abständen hat dies nur Auswirkungen auf die Kabelführung. Sollte ein Kabel den Anforderungen nicht entsprechen, brauchen Sie es nur etwas länger zu verlegen.

12.1 Auswahlkriterien für LANs

Maximale Gesamt- ausdehnung

Da die Tendenz bei Neuverkabelungen jedoch dahin geht, eine sternförmige Verkabelung auf Basis von Twisted-Pair-Kabeln aufzubauen, muß keine große Rechnerei mehr durchgeführt werden. Folgt man der Standardisierung, so beträgt die maximale Twisted-Pair-Kabellänge insgesamt 100 Meter, wobei sich diese Kabellänge zusammensetzt aus: 90 Meter für die Strecke von Datendose bis Patch-Feld im Verteilerschrank und insgesamt 10 Meter Kabellänge für das Patchkabel für den Anschluß des PC an die Datendose und das Patchkabel für die Verbindung vom Patchanschluß im Verteilerschrank und dem Hubsystem im Verteilerschrank.

Entscheidend hierbei ist, ob die Gesamtlänge eines Lokalen Netzes ausreicht, um die geplanten Stationen innerhalb eines Gesamtnetzes miteinander zu verbinden. Sollte die Lokation der Workstations die angegebene Gesamtausdehnung überschreiten, müssen Überlegungen angestellt werden, wie dieses Problem gelöst werden kann.

Angebracht sind in solchen Fällen zum Beispiel der Einsatz von Lichtleiterkabeln, die größere Entfernungen überbrücken können, oder man kann mit Hilfe von Repeatern Kabelsegmente miteinander verbinden. Eine andere Alternative könnte sein, durch den Einsatz von Bridge-Rechern physikalisch getrennte Netze rein logisch zu einem Gesamtnetz zu vereinen. Die Möglichkeiten, die dafür zur Verfügung stehen, werden in einem späteren Kapitel im einzelnen besprochen.

Art der anzuschließenden Stationen

Der Einzug der PCs in die Unternehmen ist nicht mehr aufzuhalten. So ist es auch nicht verwunderlich, daß die meisten Endgeräte in einem LAN PCs sind. Entscheidend ist an dieser Stelle nur, welche Betriebssysteme auf den PCs eingesetzt werden können (in Abhängigkeit vom Netzwerkbetriebssystem). Die Unterstützung von DOS/Windows, Windows 95/98, Windows NT und Unix muß dabei auf alle Fälle gegeben sein.

Bei den PCs muß noch berücksichtigt werden, ob es sich um ISA-, EISA- oder PCI-Bus-Systeme handelt. Wichtig dabei ist nur, daß für die einzelnen Systeme die entsprechenden Netzwerkadapter erhältlich sind und vom einzusetzenden Netzwerkbetriebssystem unterstützt werden. Vor allem für neue Techniken wie ATM oder 100VG-AnyLAN kann es hierbei zu Verzögerungen bei den einzelnen Herstellern kommen.

Inzwischen werden jedoch auch Möglichkeiten angeboten, Unix-Systeme (keine PC-Systeme), DEC-Systeme und Apple-Macintosh-Geräte in ein und demselben Netzwerk einzusetzen. Alle Systeme kön-

12 Lokale Netzwerke im PC-Bereich

nen dann ohne Schwierigkeiten miteinander betrieben werden. Vom jeweiligen Netzwerkbetriebssystem hängt es ab, ob die heterogenen Systeme nicht nur nebeneinander, sondern auch miteinander kommunizieren können. Vor einer Entscheidung müssen die Anforderungen definiert werden, die an das Netzwerkbetriebssystem gestellt werden. Hierbei sind die genannten Aspekte zu berücksichtigen und zu quantifizieren.

Anzahl der anschließbaren Rechner

Wie viele Stationen können in einem LAN maximal angeschlossen werden? Die Antwort auf diese Frage hängt wiederum vom einzusetzenden Netzwerk ab.

Ethernet

Bei der Erläuterung der Bus-Topologie wurde bereits darauf hingewiesen, daß in einem Ethernet-Segment nicht mehr als 100 Transceiver vorhanden sein dürfen. Wenn Sie an jeden Transceiver einen Rechner anschließen, können Sie pro Segment 100 Workstations installieren. Wie Sie inzwischen jedoch auch wissen, ist es möglich, einzelne Kabelsegmente mit Repeatern untereinander zu verbinden. Das Datensignal muß jedoch nach dem zweiten Repeater, den es passiert, die Empfängerstation erreicht haben.

Token-Ring

Beim Token-Ring-Netz können aus bereits angeführten Gründen (Jitter-Effekt) nicht mehr als 260 Stationen in einem Netzwerk installiert werden. Generell haben Sie jedoch immer die Möglichkeit, physikalisch getrennte Netze durch geeignete Zusatzeinrichtungen (Bridge, Router) zu einem gesamten logischen Netzwerk zusammenzuschließen.

FDDI

In einem FDDI-Netzwerk dürfen nicht mehr als 500 Stationen installiert werden. Diese Zahl ist allerdings so groß, daß sie in der Praxis nur sehr selten erreicht wird. Hierbei ist vor allem zu berücksichtigen, daß FDDI vor allem im Backbone-Bereich eingesetzt wird. FDDI als Netzwerklösung bis zum Arbeitsplatz kommt ebenfalls selten vor.

ATM

In einem ATM-Netzwerk könnten rein theoretisch beliebig viele Stationen integriert werden. Die sternförmige Verkabelung und die begrenzte Kapazität der einzelnen Hub-Systeme zwingen einen dazu, in einem großen Netzwerk mehrere Hubs zu einem Gesamtnetzwerk zusammenzuschalten. Da ATM jedoch derzeit noch hauptsächlich als Backbone-Lösung zum Einsatz kommt, gelten ähnliche Aussagen, die bereits vorher für FDDI gemacht worden sind. ATM bis zum Arbeitsplatz wird derzeit noch sehr selten realisiert, so daß in der Regel ATM im Backbone eingesetzt wird und im Etagenbereich Ethernet, Token-Ring oder auch FastEthernet eingesetzt wird.

12.1 Auswahlkriterien für LANs

Wie viele Stationen sind realistisch?

Die Anzahl der wirklich einsetzbaren Stationen hängt von mehreren Faktoren ab, die genau untersucht werden müssen. Einerseits spielt hier die Übertragungsgeschwindigkeit eine maßgebende Rolle, andererseits müssen die I/O-Belastung des Systems bei der täglichen Arbeit, die Anzahl der gleichzeitig arbeitenden Stationen (im Normalbetrieb und bei Spitzenbelastung), das Netzverhalten der eingesetzten Applikationen und natürlich das ausgewählte Zugriffsverfahren berücksichtigt werden. Nicht zu vergessen sind die physikalischen Kapazitäten, die von den einzelnen Netzwerkkomponenten zur Verfügung gestellt werden, vor allem unter dem Aspekt, daß man sich für den Einsatz von Hubs entscheidet. Die Entscheidung, wie viele Stationen in einem LAN-Segment integriert werden sollen, hängt aber auch davon ab, ob man sich für eine klassische Bridge- bzw. Router-Kopplung oder den Einsatz einer Switching-Technologie entscheidet.

Konzept des Netzbetriebssystems

Anforderung an den Server

Es ist die Frage zu beantworten, ob das Netzbetriebssystem einen bestimmten Rechnertyp als Server voraussetzt. Unterschieden wird dabei zwischen PCs oder Fremdgeräten als Server. Beim Einsatz von PC-LANs ist es bisher üblich gewesen, aufgrund der Homogenität auch einen PC als Server einzusetzen. Es kann sich aber auch die Forderung ergeben, aufgrund der notwendigen Leistungsreserven RISC-Architekturen einzusetzen. Notwendig ist dabei nur, daß die Netzbetriebssysteme in der Lage sind, auf unterschiedlichen Hardware-Plattformen eingesetzt werden zu können.

Bei der Funktion des Servers ist noch zu klären, ob dieser dedicated (reiner Server) oder non-dedicated eingesetzt werden kann oder soll (non-dedicated bedeutet, daß der Server gleichzeitig als Workstation benutzt werden kann). In kleineren Netzen mag der Einsatz von Non-dedicated-Servern durchaus sinnvoll erscheinen. Aus Sicherheitsgründen sollte diese Variante jedoch nach Möglichkeit vermieden werden, sofern diese Funktion vom Netzbetriebssystem überhaupt unterstützt wird. So kann NetWare 4 im Native Mode nur im Dedicated-Modus betrieben werden, hingegen kann ein Windows NT Server im Non-dedicated-Modus betrieben werden.

Das jeweilige Netzbetriebssystem (z. B. NetWare oder NT Server) gibt auch vor, welche minimalen Voraussetzungen an die Server-Hardware gestellt werden. Dies beginnt bei der Hauptspeicherausstattung und endet bei der Plattenkapazität. Abhängig von den einzusetzenden Anwendungen, der Anzahl der aktiven Benutzer und den zu unterstützenden Peripherie-Einheiten müssen diese Hardware Anforderungen entsprechend nach oben korrigiert werden.

12 Lokale Netzwerke im PC-Bereich

Maximale Anzahl von Servern in einem Netz

Wenn die Kapazität des Servers im LAN nicht ausreicht oder gewisse Aufgabenbereiche auf verschiedene Server aufgeteilt werden sollen, stellt sich die Frage, wie viele Server in einem Netzwerk installiert werden können. Damit verbunden ist eine weitere Frage, auf wie vielen Servern nämlich ein Anwender gleichzeitig arbeiten kann, bzw. wie übersichtlich es für den einzelnen Anwender bleibt, wenn er zwischen einer Vielzahl von Servern auswählen kann. Ein großes Netzwerk wird auch die Installation von vielen Servern notwendig machen, entscheidend ist dabei nur die Aufteilung der Server auf die einzelnen Anwender.

Welche zentralen Betriebsmittel verwaltet der Server?

In diesem Fall ist zu prüfen, wieviel periphere Speicherkapazität ein Server verwalten kann (im Mbyte- oder Gbyte-Bereich) und wie viele Drucker an einem Server angeschlossen werden können, die dann jedem Benutzer im Netzwerk zur Verfügung stehen. Zu unterscheiden ist dabei die Anzahl der parallelen und seriellen Schnittstellen. Interessant ist auch die Frage, wie und ob ein Streamer zur Datensicherung am Server angeschlossen werden kann. Da der Komplex Datensicherung sehr wichtig für den Betrieb von Lokalen Netzen ist, wird diesem Thema ein eigenes Kapitel gewidmet. Wie viele zentrale Betriebsmittel der Server verwalten kann, wurde bereits im vorherigen Abschnitt behandelt. Hinzu kommen die Mechanismen zur Kommunikation nach außen und von außen. Typische Aufgaben hierfür werden mit dem Begriff »Mobile Computing« beschrieben. Dabei geht es unter anderem darum, über Remote-Verbindungen die Kommunikation mit dem »Firmennetz« aufzubauen, um ständig auf die aktuellen Daten zurückgreifen zu können. Im Bereich von E-Mail kommen ähnliche Mechanismen zum Einsatz. In diesem Fall spricht man meist von einem Remote-E-Mail-Client. Neben diesen Funktionen sind auf Server-Maschinen nicht selten auch noch Faxdienste, Mail-Dienste, Kommunikationsdienste oder auch Backup-Dienste integriert. Es ist dabei nur zu prüfen, ob die Leistungsfähigkeit der Server-Maschine ausreicht oder eine Verteilung von diesen und anderen Diensten auf mehrere Server sinnvoller ist. Vergessen werden darf in diesem Zusammenhang nicht, daß bei einer hohen Integrationsdichte von Server-Diensten auf ein und derselben Maschine bei einem Serverausfall alle diese Dienste auf einmal ausfallen und nicht mehr zur Verfügung stehen.

Es ist vom jeweiligen Netzwerkbetriebssystem abhängig, welche Server-Dienste zur Verfügung stehen und wie diese auf den Server-Maschinen integriert werden können.

12.1 Auswahlkriterien für LANs

Leistungsfähigkeit des Netzbetriebssystems

In den Beschreibungen der einzelnen Netzbetriebssysteme werden überall die unterschiedlichsten Methoden zur Erhöhung der Leistungsfähigkeit angepriesen. Jeder Hersteller versucht dabei, mit den verschiedensten Mechanismen Leistungsfähigkeit, Sicherheit, Zugangsschutz und vieles mehr zu realisieren. Bei der Beschreibung von Novell NetWare bzw. NT Server werden diese Komponenten auf ihre Tauglichkeit und Komplexität hin untersucht und beschrieben.

In diesem Zusammenhang muß auch das Umfeld der netzwerkfähigen Software untersucht werden. Sie müssen zwischen im Netz lauffähiger Software und netzwerkfähiger Software unterscheiden.

Unter im Netz lauffähiger Software sind Programme zu verstehen, die ursprünglich Single-User-Systeme waren und auf dem Server installiert werden, um von den einzelnen Workstations benutzt werden zu können. Es gibt allerdings bei diesen Programmen zum Beispiel keinerlei Mechanismen zum Schutz gegen parallelen Zugriff auf ein und denselben Datensatz in einem Datenbanksystem. Das kann katastrophale Folgen haben. Solange das Programm und die Datendatei nur von einem Anwender benutzt werden, stellt dies noch kein Problem dar. Anders verhält es sich, wenn mehrere Benutzer gleichzeitig die Programme und Datendateien verwenden.

Nicht zu vergessen ist dabei die rechtliche Folge von Einplatzversionen, die im Netz installiert werden. Es sei hier auf die Rechtsprechung in puncto Urheberrechtsschutz für Programme hingewiesen.

Netzwerkfähige Software ist vom Konzept her auf Multi-User-Fähigkeit ausgelegt. Die vorher angeführten Probleme treten bei diesen Programmen nicht auf.

Einbindung von Fremdsystemen

Dem Problem der Einbindung von PC-Netzen in bestehende DV-Konzepte ist ein eigenes Kapitel gewidmet, da es zentrale Bedeutung hat. Deshalb soll an dieser Stelle darauf nicht näher eingegangen werden.

Zur Abrundung des bisher Besprochenen sollen die wichtigsten LAN-Funktionen noch einmal zusammengefaßt werden: Ein Lokales Netzwerk ist ein System zur Verbindung von Computern mit Peripherie zum elektronischen Austausch von Programmen und Informationen. Eine derartige Kopplung von Einheiten ist auf eine Grundstücksfläche beschränkt. Die normale Ausdehnung von Lokalen Netzen reicht von einigen 100 Metern bis zu ca. 10 Kilometern.

12 Lokale Netzwerke im PC-Bereich

Ein LAN wird häufig zuerst als Insellösung innerhalb einer Abteilung realisiert und im Lauf der Zeit zu einem Gesamtnetzwerk zusammengefaßt. Die Verbindungen innerhalb eines Lokalen Netzes können mit verschiedenen Kabeltypen erfolgen:

- Koaxialkabel
- und/oder Glasfaser
- vieradrige Twisted-Pair-Kabel (100 Ohm)
- achtadrige Twisted-Pair-Kabel (100 Ohm)
- IBM-Kabel Typ1 (150 Ohm, nur noch selten)
- Infrarotübertragung für kabellose LANs (selten)
- Satellitenübertragung

Die Übertragungsgeschwindigkeiten liegen im Bereich von 4 Mbit/s bis 1 Gbit/s und werden in einiger Zeit sogar 10 Gbit/s betragen können.

Ein LAN sollte Systeme und Peripherie von unterschiedlichen Herstellern unterstützen. Ein LAN muß die Möglichkeit zur gemeinsamen Nutzung von Programmen, Daten und Peripherie bieten. Dabei sollte der Anwender nach Möglichkeit keine Einschränkung in Bezug auf die Zugriffszeit bemerken.

Die Anwendung von PC-Lösungen für den Benutzer im Netzwerk darf – trotz der erweiterten organisatorischen Möglichkeiten – nicht komplizierter werden im Vergleich zu Standalone-Systemen, die er vielleicht bereits gewohnt ist. Die einfachste Durchführung dieser Forderung ist der Einsatz von komfortablen Menüsystemen, mit denen der Anwender innerhalb seiner Netzwerkumgebung geführt wird und somit von der Existenz eines LAN gar nichts bemerken muß.

Bei der Auswahl und dem Einsatz von Lokalen Netzen ist ein wichtiger Faktor die Geschwindigkeit, mit der Daten von einer Workstation zum File-Server oder umgekehrt transportiert werden können. Ich will Ihnen im nächsten Abschnitt eine Methode vorstellen, mit der Sie einen Einblick in das Thema der Übertragungsgeschwindigkeit des Netzes erhalten.

12.1.2

Entwicklung eines Leistungsmeßverfahrens

Beim Einsatz von Lokalen Netzen ist die zentrale Frage, wie schnell das Netz wirklich ist.

Gemeint ist die effektive Übertragungsrate, d.h. die Übertragungsgeschwindigkeit, die der Anwender an seinem Arbeitsplatz beim Zugriff auf Ressourcen des oder der Server zu spüren bekommt, also das Antwortzeitverhalten.

12.1 Auswahlkriterien für LANs

Die effektive Übertragungsgeschwindigkeit liegt weit unter der technischen Übertragungsgeschwindigkeit. Ein LAN mit 10 Mbit/s Bruttoübertragungsrate arbeitet im Netzwerkbetrieb nie mit dieser Transferrate. Technisch bedingt ist die Nettorate $\ll$ Bruttorate. Es gibt Möglichkeiten, um diese Nettodatenrate zu erhöhen. Dies kann durch den Einsatz eines sehr leistungsstarken Netzwerkbetriebssystems geschehen (File-Caching, Directory-Caching, Hauptspeicher etc.) und durch die Verwendung von schnellen File-Servern in Kombination mit schnellen Plattenlaufwerken, schnellen Netzwerkadapterkarten (Onboard-Processor, Puffer-Speicher etc.).

Für die Unterscheidung verschiedener Netzwerke reichen einfache Verfahren aus, um ein Gespür dafür zu bekommen, welches LAN schneller arbeitet. Das Netzwerk muß im Bereich der Zugriffe zum File-Server gute Antwortzeiten aufweisen, d.h., der Zugriff zu den Plattenlaufwerken des File-Servers muß schnell erfolgen. Da die hauptsächlichen Arbeiten des File-Servers im Bereich der Dateiverwaltung liegen, ist dies sehr wichtig.

Um diese Geschwindigkeit abschätzen zu können (Netzübertragung, Suchzeit, Übertragungszeit der Platte etc.), genügt ein einfaches Meßverfahren – man kann einfach einen Vergleich anstellen: Wird das Laden von Programmen im Netz schneller vom File-Server durchgeführt oder ist das Laden von der lokalen Platte schneller?

Für den Vergleich sollten es die gleichen Systeme sein. Zur Durchführung des Tests erzeugen Sie auf dem Server (oder auf der lokalen Platte) eine 256 Kbyte große Datei. Diese Datei kopieren Sie vom File-Server auf Ihre Workstation. Das gleiche tun Sie mit dem zu vergleichenden System. Um die Zeiten auch messen zu können, erstellen Sie folgende BATCH-Datei:

```
LADEN.BAT  
TIME 00:00  
COPY x:TEST.DAT NUL:  
TIME
```

Für *x* müssen Sie in Ihrer BATCH-Datei das entsprechende Laufwerk (lokales oder Netzwerklaufwerk) einsetzen.

Nach Ausführung der BATCH-Datei wird Ihnen am Bildschirm die Ladezeit angezeigt, die für die Übertragung der Datei erforderlich war. Zwei Dinge sind dabei zu beachten:

1. Der COPY-Befehl von DOS kann verwendet werden, weil DOS beim Kopieren die Datei in den Hauptspeicher der Workstation lädt.

12 Lokale Netzwerke im PC-Bereich

2. Die Ausgabe auf das Dummy-Gerät NUL bewirkt, daß die Daten nicht, wie sonst beim COPY-Befehl, zurück auf Platte geschrieben, sondern vernichtet werden. Die damit erzielten Ergebnisse geben Ihnen nur einen Anhaltspunkt für den Geschwindigkeitsvergleich. Nicht berücksichtigt werden dabei Faktoren, die durch Hard- und Software bedingt einfließen. Sie sollten dieses Verfahren deshalb nur zum Vergleich von Geschwindigkeiten mit und ohne Netzwerk und zum Vergleich zweier Netzwerke verwenden.

Interessanter ist es, die Datentransferrate in einem Netzwerk zu bestimmen. Dies soll im nächsten Abschnitt erfolgen.

12.1.3 Bestimmung der Datentransferrate für LANs

Es soll die Geschwindigkeit gemessen werden können, mit der Daten von der File-Server-Platte in den Hauptspeicher der Workstation geladen werden können.

Dieses Meßverfahren berücksichtigt sowohl die Geschwindigkeit des Netzes als auch die Zugriffszeit der verwendeten Festplatte. Sie könnten damit zum Beispiel auch einen Vergleich aufstellen, wie sich das LAN beim Einsatz von verschiedenen Plattenlaufwerken verhält bzw. ob dieser Faktor durch das Netzwerkbetriebssystem aufgefangen werden kann (z.B. durch File-Caching).

Zur Durchführung dieses Tests verwenden Sie folgendes BATCH-Programm:

```
TIME 00:00
COPY D256K.DAT NUL:
TIME
TIME 00:00
COPY D1B.DAT NUL:
TIME
```

Dieses Verfahren verwendet wieder den COPY-Befehl von DOS. Es werden neben der eigentlichen Zeit für das Lesen der Datei und der Übertragung über das Netzwerk auch noch die Zeiten für das Öffnen der Datei und die Initialisierung zur Netzwerkübertragung einbezogen. Diese Anteile sind jedoch störend für das Meßverfahren und sollten ausgeschaltet werden können. Deshalb wird bei diesem Meßverfahren noch eine zweite Datei gelesen, die jedoch nur 1 Byte groß ist. Bei dieser Datei fallen im Endeffekt nur die Zeiten für das Öffnen der Datei und der Initialisierung zur Netzwerkübertragung an. Wenn beide Meßwerte vorliegen, kann mit folgender Formel die Transferrate bestimmt werden:

12.2 Konzeption und Realisierung eines LAN

$$\text{Transferrate} = \frac{256 \text{ Kbyte}}{(t_2 - t_1) \text{ s}} = X \text{ Kbyte/s}$$

- t_2 ist die Zeit, die zum Lesen der 256 Kbyte großen Datei benötigt wird.
- t_1 ist die Zeit, die zum Lesen der 1 Byte großen Datei benötigt wird.

Mit dem letztgenannten Meßverfahren könnte auch ein Gesamttest für ein Netzwerk durchgeführt werden. Man läßt an mehreren Rechnern gleichzeitig die Batch-Prozedur starten und erhält damit einen Anhaltspunkt, wie sich das Zeitverhalten der einzelnen Arbeitsplätze ändert.

Dieses Verfahren soll nur ein Vorschlag sein, wie die Leistungsfähigkeit eines LAN ermittelt werden kann. Inzwischen wird eine Vielzahl von Programmen angeboten, die es Ihnen gestatten, die Leistungsfähigkeit Ihres Netzwerks zu ermitteln. Bei Bedarf kann auch auf diese Systeme zurückgegriffen werden, um gezielte Meßergebnisse zu erhalten.

12.2 Konzeption und Realisierung eines LAN

Die Diskussion über die Frage, ob ein LAN eingesetzt werden soll, ist noch lange nicht abgeschlossen. Dies liegt zum einen daran, daß die Leistungsfähigkeit dieser Systeme erst nach und nach erkannt wird, die Entscheidung, ob LAN oder MDT, immer noch zur Debatte steht und Erfahrungen im Bereich der PC-LANs erst allmählich zutage treten.

Zum anderen ist es von jeher so, daß eine neue Technik immer mit Skepsis betrachtet wird und viele erst einmal abwartend dem Neuen gegenüberstehen. Ich werde im folgenden Abschnitt versuchen, Ihnen die wichtigsten Phasen bei der Entscheidungsbildung und bei der Realisierung von LANs aufzuzeigen.

Bevor irgend jemand mit Kabeltrommel, Schraubendreher und Zange bewaffnet durch die Bürogänge huscht, um Kabel für ein zu installierendes LAN zu verlegen, sollte man sich erst einmal überlegen:

1. Warum soll ein LAN installiert werden? Welchen organisatorischen und betriebswirtschaftlichen Nutzen bringt diese Investition?
2. In welchen Bereichen soll vernetzt werden? Betrifft dies nur eine einzelne Abteilung, oder ist es sinnvoller, gleich mehrere Büros unterschiedlicher Fachabteilungen mit einzubeziehen?

12 Lokale Netzwerke im PC-Bereich

3. Wird Kommunikation nach außen verlangt, oder geht es um eine reine insuläre Lösung?

Ausgangssituationen, die anzutreffen sind

Es lassen sich im Prinzip vier verschiedene Ausgangssituationen beim Anwender feststellen, bevor dieser eine Vernetzung ins Auge faßt:

1. *Vernetzung vorhandener Einplatz-PCs*

Dieses Territorium bietet nicht mehr sehr viel Spielraum für die Planung. Aufgrund der vorhandenen PCs und der damit verbundenen Investitionen sind gewisse Systemkomponenten bereits vorhanden. An diesen läßt sich auch meist nichts mehr ändern. Die Entscheidungen, die hier noch getroffen werden können, sind die Auswahl des File-Servers (wenn überhaupt) und der Einsatz des richtigen Netzwerkbetriebssystems. Hauptaugenmerk wird auf die problemlose Einbindung der vorhandenen PCs und der Peripherie gelegt. Ein Netzwerk dient in solchen Fällen meist als Medium zum Austausch von Daten, die früher über Diskette weitergegeben werden mußten, und zum Zugriff auf ein eventuell neues und teures Peripheriegerät (Laserdrucker, Telefax u.ä.). Die bereits vorhandene Anwendersoftware (in den meisten Fällen ohne Ausnutzung des Netzwerks in der Eigenschaft als Multi-User-System) wird weiterhin benutzt. Das heißt, die Einplatzversionen werden von den lokalen Platten (wenn man Glück hat) auf den File-Server kopiert und von dort geladen. Sehr oft wird jedoch die Software lokal gestartet und nur der neue Datenbestand auf der Platte des Servers abgespeichert. Erst wenn neue Software installiert werden soll, wird netzwerkfähige Software eingesetzt.

2. *Neuinstallation von PCs und PC-LAN*

Der Aufbau einer Erstinstallation bietet, da keinerlei Zwänge in bezug auf vorhandene Hardware und Software bestehen, die meisten Möglichkeiten für eine anwendungsgerechte Planung und Realisierung eines Gesamtnetzwerks. Man kann so richtig schön aus dem vollen schöpfen und für alle Beteiligten die optimalen Bedingungen und Lösungen auswählen.

An den Planer selbst werden die höchsten Anforderungen gestellt, da ein solches Lösungskonzept nicht selten als Gegenprojekt zur Mittleren Datentechnik angesehen wird. Da es in Konkurrenz zur Mittleren Datentechnik läuft, ist der Einsatz von netzwerkfähiger Software unumgänglich. Nicht selten werden jedoch auch MS-DOS-Einplatz-Versionen eingesetzt. Das Angebot an netzwerkfähiger Software ist inzwischen wesentlich besser als früher.

12.2 Konzeption und Realisierung eines LAN

3. *Verbindung PC-LANs mit Großrechner- und MDT-Systemen*

Der Datenaustausch zwischen Systemen der Mittleren Datentechnik und des Großrechnerbereichs ist nach wie vor ein ernstzunehmendes Problem. Schwierigkeiten treten bei diesen Kopplungen auf, da unterschiedliche Kodierungen, Datenformate und Protokolle verwendet werden. Ein PC-LAN kann beim Anschluß an den Großrechner oder einer MDT-Anlage organisatorische und technische Erleichterungen bringen. Möglichkeiten zur Einbindung bestehen für die gängigsten Rechnersysteme (IBM, Siemens, DEC, verschiedene Unix-Systeme).

Die möglichen Lösungen zur Integration der Host- und MDT-Rechner hängt von den einzelnen Herstellern ab. Für Novell NetWare stehen dabei andere Systeme und Produkte zur Verfügung, als dies für den NT Server von Microsoft der Fall ist. Die zur Anbindung notwendige Software wird häufig auch als Host-Gateway-Software bezeichnet. Bevor man sich für die Installation des einen oder anderen Systems entscheidet, bedarf es einer gründlichen Analyse und Untersuchung, welche Anforderungen an die Integration gestellt werden und welche Hersteller diese Anforderungen am besten erfüllen. Nicht vergessen werden darf, daß für die Integration der Host- und MDT-Rechner auch noch eine passende Client-Software benötigt wird. Hier ist ebenfalls zu prüfen, welche Host-Gateway-Lösung mit welcher Client-Front-End-Software zusammen eingesetzt werden kann und welche Merkmale und Leistungsfähigkeit die Client Front-End- Software bietet.

4. *Restrukturierung eines bestehenden Netzwerks*

Es gibt eine Vielzahl von Unternehmen, die bereits vor einigen Jahren die ersten LANs installiert haben. Da sich die Netzwerktechnik und auch die Anforderungen an das Netzwerk in dieser Zeit dramatisch geändert haben, besteht sehr häufig der Bedarf, ein Redesign des Netzwerks durchzuführen. Handelt es sich dabei um ein Netzwerk, das auf Basis von Koaxialkabeln installiert worden ist, wird meist auch die gesamte Verkabelung erneuert, da man dann die zukunftsweisende Twisted-Pair-Verkabelung einsetzen wird. Ist bereits eine physikalische Infrastruktur auf Basis dieser Twisted-Pair-Verkabelung vorhanden, geht es nur darum, die Netzwerkkomponenten zu erneuern. Dies beginnt beim Neuaufbau des Backbone und endet in der Redesigning-Phase der Etagennetze. Nicht selten wird dabei zwar der Wunsch geäußert, so weit wie möglich vorhandene Komponenten weiter zu verwenden, wenn es sich jedoch um Komponenten handelt, die nicht modular aufgebaut sind oder gar technisch nicht mehr in das Bild eines modernen, leistungsfähigen und flexiblen Netzwerks passen, müssen auch solche Komponenten vollständig erneuert werden. Enorme Redesign-Probleme treten zum Beispiel auf,

12 Lokale Netzwerke im PC-Bereich

wenn die LWL-Verkabelung im Backbone für FDDI klassisch von Hub zu Hub verlegt worden ist und auf Basis dieser Verkabelung eine sternförmige ATM-Technik eingesetzt werden soll. Mit Hilfe redundant vorhandener LWL-Phasern und einer entsprechenden Kabelauflegung im Patch-Feld der Verteiler ist man vielleicht in der Lage, das Problem zu lösen bzw. die gestellte Anforderung zu erfüllen. Wenn gar nichts mehr hilft, muß auch die LWL-Verkabelung im Backbone-Bereich erneuert werden. Man muß zum heutigen Zeitpunkt zunächst davon ausgehen, daß eine neue sternförmige Verkabelung auch in den nächsten 10 bis 15 Jahren noch Bestand haben wird und beim Umstieg auf eine neue Netzwerkinfrastruktur die Investition in die Verkabelung gesichert bleibt. Dies sind jedoch immer wieder Glaskugel-Argumente, die hoffentlich erfüllt werden; jedoch kann man nicht mit hundertprozentiger Sicherheit vorhersehen, welche neuen Techniken unter Umständen in den nächsten Jahren kommen werden.

Man ist sich dabei nur über eines im klaren – alles wird immer schneller und kleiner werden. Zudem werden die Innovationszyklen immer kürzer. Dies macht es ungeheuer schwer, den vollständigen Überblick zu behalten. Das liegt aber auch darin begründet, daß fast keine Woche vergeht, in der nicht in einer Fachzeitschrift zu lesen ist, daß Firma X von Firma Y aufgekauft worden ist.

12.3 Komponenten eines PC-Netzwerks

Ein lokales PC-Netz besteht nicht nur aus den Workstations, die mit Hilfe eines Kabels untereinander verbunden werden. Abbildung 12.1 soll die einzelnen Komponenten unter organisatorischen Gesichtspunkten genauer darstellen.

12.3.1 Das Transportsystem

Ein Transportsystem vereinigt die Komponenten, die zum reibungslosen Ablauf der Kommunikation in einem Netzwerk notwendig sind. Dies sind im einzelnen:

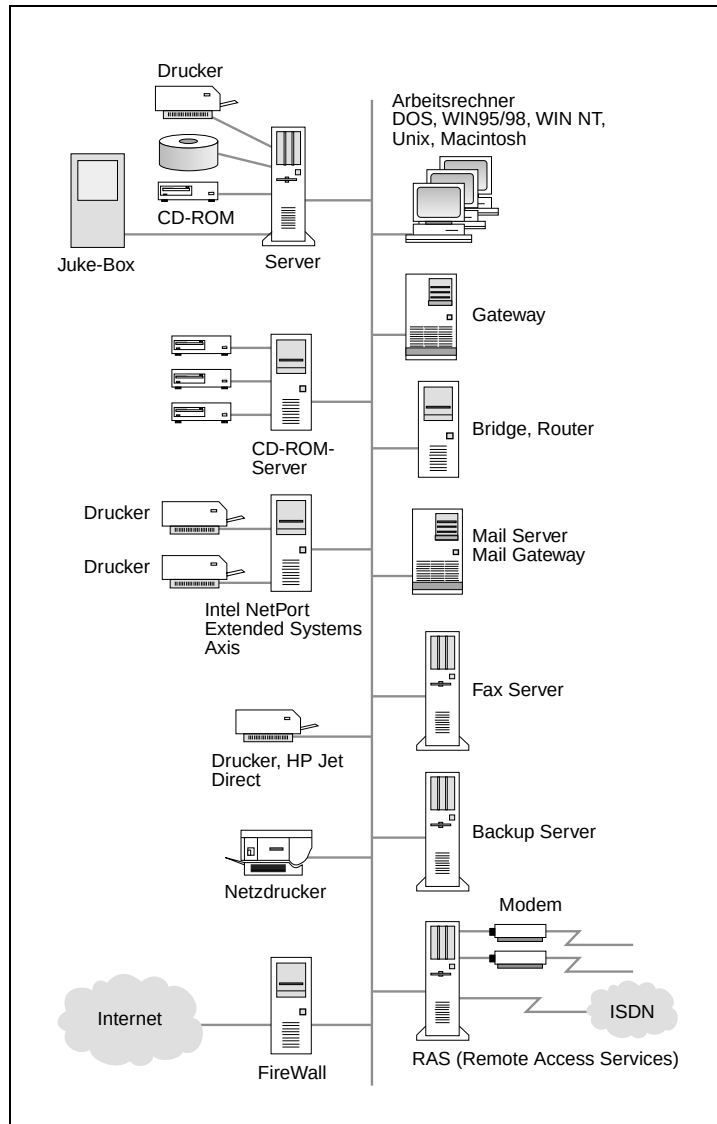
- *Netzwerkadapterkarte*

Mit den Karten und den darauf befindlichen Anschlüssen werden die einzelnen Workstations, Koppелеlemente, Server, Drucker etc. in das entsprechende Verkabelungssystem (Netzwerk) eingebunden. Die Netzwerkadapterkarten sind zuständig für die Datenübertragung und die Steuerung. Im ISO-OSI-Modell decken die Netzwerkkarten mit den entsprechenden Treibern die Ebenen 1 und 2 ab. Es ist darauf zu achten, daß für das jeweilige Netzwerk

12.3 Komponenten eines PC-Netzwerks

die passenden Karten eingesetzt werden. Dies klingt vielleicht etwas seltsam, aber es kommt immer wieder vor, daß jemand für Ethernet-Netzwerke Token-Ring-Karten bestellt. Man sollte in diesem Zusammenhang auch darauf achten, einen bekannten Hersteller zu nehmen, da man dann die Gewähr hat, bei Neuerungen die aktuellen Treiber zu bekommen. Das ist vor allem wichtig, wenn es zu einem Versionswechsel bei der Netzwerksoftware kommt oder gar die gesamte Treibersoftware geändert wird.

Abbildung 12.1
Netzkomponenten
im LAN



12 Lokale Netzwerke im PC-Bereich

■ *Anschlußeinheiten*

Hierunter sind die speziellen Einrichtungen zu verstehen, mit denen die Adapterkarten verbunden werden. Das kann zum Beispiel der Ringleitungsverteiler für Token-Ring sein oder ein FDDI-Concentrator für den Anschluß an ein FDDI-Netzwerk. In den vorherigen Kapiteln wurden diesbezüglich ausführliche Erläuterungen gegeben.

■ *Übertragungsmedium*

Das ist das Kabel, auf dem die eigentliche Datenübertragung stattfindet. Wie bereits besprochen, können mitunter Zwischenverstärker erforderlich sein. Je nach Netzwerk muß auch zwischen Koaxialkabelanschlüssen und Twisted-Pair-Anschlüssen für 100 bzw. 150 Ohm unterschieden werden. Wenn ein Netzwerk mehrere Anschlußtechniken unterstützt und diese auch von der Netzwerkkarte unterstützt werden, muß die Karte für den richtigen Anschluß konfiguriert werden, sofern sie keinen automatischen Erkennungsmechanismus enthält.

So gibt es zum Beispiel Ethernet-Karten als sogenannte Three-in-one-Karten. Diese Netzwerkkarte hat drei Anschlüsse für die drei von Ethernet verfügbaren Kabeltypen: Koaxial (BNC), Koaxial (Transceiver) und Twisted-Pair. Prüft die Karte beim Laden des Treibers nicht selbst, über welchen Anschluß die Verbindung zum Netz realisiert ist, muß entweder per Jumper oder per Software-Konfiguration der richtige Anschlußtyp eingestellt werden.

Der technische Aufbau der Verkabelung kann in einem kleineren Netz meist sehr schnell durchgeführt werden. In größeren Netzwerken sind jedoch sehr viele Umgebungsbedingungen abzuklären (Kabelschächte, äußere Störeinflüsse, Kabellängen, Mauerdurchbrüche etc.). Dies sollte genau geplant werden, um eine zügige Realisierung gewähren zu können. Sowohl die Realisierung eines kleinen als auch eines großen Netzwerks erfordert eine meist mehrtägige bis mehrwöchige (in manchen Fällen auch mehrmonatige) Netzwerkplanung.

12.3.2

Der Server

Der Server, auch File-Server genannt, ist das zentrale Betriebsmittel in einem Netzwerk. Die Bezeichnung File-Server ist historisch bedingt, als die Aufgabe dieses Systems hauptsächlich darin bestand, File-Services, d.h. Dateidienste, zur Verfügung zu stellen. Da die Aufgaben des File-Servers aber immer mehr erweitert worden sind, so daß er auch als Mail-Server, Print-Server oder auch Backup-Server dienen muß, spricht man seit längerem nur noch vom Server. Der Server ist neben den bereits erwähnten Diensten (Services) aber

12.3 Komponenten eines PC-Netzwerks

auch zuständig für die Überwachung des Systems, die Zugangsüberwachung, die Verwaltung von Daten, das Bereitstellen von Daten und viele andere Dinge mehr. Mit jeder neuen Version eines Netzwerkbetriebssystems werden die Aufgaben des Servers nochmals erweitert, verbessert und auch beschleunigt.

Da in einem Netzwerk sehr viele Workstations mit dem gleichen Material arbeiten, ist es notwendig, daß es sich bei diesem Gerät um eine sehr leistungsfähige Hardware handelt, so daß ein akzeptables Antwortzeitverhalten gewährleistet werden kann. Mit welchen Software-Konzepten Netzwerkbetriebssysteme zusätzlich ihre Leistung steigern können, werden wir bei der Behandlung von Novell NetWare bzw. Microsoft Windows NT Server erfahren. Auf dem Server muß also ein Betriebssystem, das sogenannte Netzwerkbetriebssystem installiert sein. Aufgabe des Netzwerkbetriebssystems ist es unter anderem, neben der Benutzerverwaltung und -überwachung auch die Bereitstellung der Ressourcen zu steuern.

12.3.3 Die Peripherie am Server bzw. direkt im Netzwerk

Die am Server angeschlossenen peripheren Einheiten stehen allen Netzwerkbenutzern zur Verfügung. In den meisten Fällen verwendet man dabei bessere und schnellere Geräte (Laserdrucker, Plattenlaufwerke, CD-ROMs, MO-Laufwerke etc.).

Man sollte bei der Auswahl der Peripherie darauf achten, daß der Durchsatz am Server wegen zu langsamer Geräte nicht herabgesetzt wird.

Zudem ist zu berücksichtigen, daß diese Peripherie nicht von einem Anwender allein beansprucht wird, sondern von allen. Man geht in der letzten Zeit jedoch immer mehr dazu über, die Peripherie, sofern dies möglich ist, nicht mehr am Server zu installieren, sondern sie direkt in das Netzwerk zu integrieren. Es gibt entsprechende Lösungen für Netzwerkdruker, CD-ROM-Laufwerke oder auch MO-Laufwerke.

Neben der direkten Anbindung spezieller peripherer Einheiten geht man sehr häufig dazu über, für ganz bestimmte Dienste eigene Server zu installieren (s.a. Abbildung 12.1). Damit versucht man zu vermeiden, daß alle Serverdienste auf ein und derselben Maschine laufen. Dies hat zum einen den Vorteil, daß der Server nicht so stark belastet wird, daß er nur noch sich selbst verwalten kann, und zum anderen ist von einem Ausfall oder einer dadurch bedingten Störung nicht der gesamte Server betroffen. Aus diesem Grund sollten die wichtigsten zusätzlichen Server-Dienste, die als eigene Server installiert werden können, nachfolgend näher beschrieben werden. Dabei kann man durchaus dazu übergehen, einige dieser Server, sinnvoll zusammen-

12 Lokale Netzwerke im PC-Bereich

gefaßt, auf ein und derselben Server-Plattform laufen zu lassen. Man sollte nicht plötzlich zu viele Server im Netzwerk haben, da diese auch ordnungsgemäß administriert werden müssen und dann unter Umständen der Aufwand im Netzwerk drastisch steigt. Die Ausfallsicherheit eines Servers kann jedoch nicht nur durch Mechanismen des Netzwerkbetriebssystems erreicht werden. Ein wesentlicher Aspekt hierbei ist der Anschluß des Servers an einer unterbrechungsfreien Stromversorgung, auch als USV bezeichnet. Eine USV übernimmt die Versorgung des Servers mit Strom für den Fall, daß ein Spannungsausfall erfolgen sollte. Damit der Server in diesem Fall nicht einfach stromlos ausfällt und dadurch die Gefahr eines Datenverlusts in Kauf genommen wird, schließt man den Server an einer USV an. Je nach Ausbaustufe kann eine USV den Server zwischen zehn Minuten und einer Stunde mit Spannung versorgen. Wichtig dabei sind zwei Aspekte:

- Die USV sollte auf alle Fälle über das Netzwerkbetriebssystem gesteuert werden. In diesem Fall wird die USV über ein Signalkabel mit dem Server verbunden. Entweder erfolgt der Anschluß der USV an der seriellen Schnittstelle oder über eine eigene Karte im Server (speziell für die USV). Nach dem Starten einer dazugehörigen Software überwacht die Software auf dem Server ständig den Zustand der USV. Sollte der Strom ausfallen, übernimmt die USV die Stromversorgung; über die Überwachungssoftware werden nicht nur alle aktiven Benutzer über den Zustand in Kenntnis gesetzt, sondern nach Ablauf der Zeit, die von der USV überbrückt werden kann, wird der Server ordnungsgemäß beendet und runtergefahren.
- Bei den USV-Anlagen ist zu unterscheiden zwischen Offline- und Online-USV-Anlagen. Bei einer Online-USV erfolgt die Spannungsversorgung permanent über den Akku, und der wird ständig geladen. Bei der Offline-USV ist der Akku ständig geladen, und der Server wird herkömmlich über die »Steckdose« gespeist, indem die Spannung über die USV durchgeschleift wird. Fällt der Strom aus, erfolgt mit einer kurzen Zeitverzögerung die Zuschaltung des Akkus, um den Server mit Spannung versorgen zu können.

Zu beachten ist auch, daß bei der Auswahl der USV ein System gewählt wird, das sich in das Netzwerkmanagement integrieren läßt. Auf diese Weise sind Sie in der Lage, den Zustand der USV über das Managementsystem zu überwachen und zu kontrollieren.

12.3 Komponenten eines PC-Netzwerks

CD-ROM-Server

Die Bedeutung der CD-ROM nimmt ständig zu. Anwendungen, Tools, Patches oder andere wichtige Informationsquellen werden immer öfter ausschließlich auf CD-ROM ausgeliefert. Es hat zwar fast jeder PC standardmäßig ein CD-ROM-Laufwerk zur Verfügung, aber wenn es darum geht, CD-ROMs allgemein für alle Teilnehmer im Netzwerk zur Verfügung zu stellen, kommt man um den Einsatz von CD-ROMs nicht mehr herum. Vor allem unter dem Aspekt, daß auch Dokumentationen auf CD-ROM ausgeliefert werden, gewinnt ein zentraler CD-ROM-Server sehr schnell an Bedeutung im Netzwerk. Es stellen zwar inzwischen alle Netzwerkbetriebssysteme Mechanismen zur Verfügung, um CD-ROM-Laufwerke als Ressource im Netzwerk verfügbar zu machen, jedoch erfordert der Wechsel von CD-ROMs einen direkten Zugriff zum Server. Wenn man die Verwaltung der CD-ROMs dezentralisieren will, dann sind externe Lösungen besser. Man kann sich hierzu entweder einen eigenen CD-ROM-Server, bestehend aus einem PC, entsprechender Software und eigener Administration, in das Netzwerk installieren, oder man nutzt Lösungen, die selbst über kleine externe, periphere Einheiten die Möglichkeit zur Verfügung stellen, an diese Peripherie CD-ROMs anzuschließen, und die gesamte Verwaltung (inkl. Zugriffsberechtigungen) wird über ein unter Windows eingesetztes Software-Programm durchgeführt.

Vor allem letztere Lösung ist sehr interessant, da die externe Peripherie nicht größer ist als eine herkömmliche Netzwerkkarte (nur etwas höher). Diese kleine externe Box besitzt eine SCSI-2 Schnittstelle, an der bis zu sieben CD-ROM-Laufwerke angeschlossen werden können. Nutzt man für den Anschluß auch noch die Möglichkeit, Mehrfachwechsler zu installieren, dann kann man eine große Anzahl von CDs verfügbar machen. Die Installation und Konfiguration dauert in der Regel nicht länger als zehn Minuten. Da diese externe Box einen direkten Netzwerkanschluß besitzt, kann sie auch direkt an der Stelle im Netzwerk positioniert werden, wo man sie benötigt. Man ist somit nicht darauf angewiesen, die CD-ROMs im Server-Raum zu platzieren, da man doch sehr häufig veranlaßt wird, neue CDs einzulegen. Derzeit bekannte Hersteller solcher externen CD-ROM-Server sind die Firmen Axis und Microtest.

Um einen herkömmlichen PC durch Einbau aller notwendigen CD-ROM-Laufwerke und der Installation der dazugehörigen Software zum externen CD-ROM-Server zu machen, kann z.B. ein Produkt der Firma Ornetix verwendet werden. Auch diese Hard- und Software-Lösung läßt sich innerhalb kürzester Zeit installieren, konfigurieren und im Netzwerk verfügbar machen.

12 Lokale Netzwerke im PC-Bereich

Die Aussagen, die hier für CD-ROM-Laufwerke getroffen worden sind, gelten im Prinzip auch für Jukebox-Systeme, wenn es darum geht, magnetooptische Laufwerke (wiederbeschreibbare optische Platten) in ein Netzwerk zu integrieren.

Da auch diese Produkte einer ständigen Verbesserung unterzogen werden, muß vor der Entscheidung für das eine oder andere Produkt der aktuelle Stand der Technik und der Software-Möglichkeiten überprüft werden.

Mail Server

Beim Einsatz von E-Mail-Systemen besteht die Aufgabe von Mail-Servern darin, die zu transportierenden Nachrichten vom Sender zum Empfänger weiterzuleiten. Auf dem Mail-Server können dann sogenannte Postoffices abgelegt sein, die benötigt werden, um die Nachrichten der E-Mail-Benutzer speichern zu können. Abhängig von der E-Mail-Lösung werden hierfür entweder eigene Server-Maschinen benötigt oder sie werden zusammen mit dem Netzwerkbetriebssystem auf der gleichen Server-Hardware eingesetzt. Werden zudem Übergänge zu anderen Mail-Systemen benötigt, dann sind auch noch Mail-Gateways notwendig. Da die Bedeutung der E-Mail-Systeme inzwischen immer größer wird, habe ich diesem Themenbereich ein eigenes Kapitel gewidmet.

Fax-Server

Eine ebenso wichtige Aufgabe wie E-Mail im Netz ist es inzwischen, Faxe bequem vom Arbeitsplatz nicht nur versenden zu können, sondern auch automatisch zu empfangen. Das Versenden ist dabei einfacher zu realisieren als das automatische Empfangen. In der Regel arbeiten die Fax-Server alle nach einem ähnlichen Prinzip. Ein zu versendendes Fax wird wie gehabt in der Textverarbeitung erstellt, statt es an einen Drucker auszugeben. Man wählt eine Option aus, die zwar auch Druckaufträge erzeugt, diese Druckaufträge jedoch in eine dafür eingerichtete spezielle Fax-Queue überträgt. Der auf dem Server aktive Fax-Server prüft die Fax-Queue in regelmäßigen Abständen, ob sich Fax-Aufträge darin befinden. Sobald der Fax-Server einen Faxeuftrag vorfindet, wird das Dokument über das am Fax-Server angeschlossene Modem an den Empfänger übertragen. Das Empfangen eines Faxes kann nur mit ISDN-Nebenstellenanlagen erreicht werden.

Man benötigt hierzu auch einen dazugehörigen Mail-Server, der es ermöglicht, eine am Fax-Server eingehende Faxmitteilung automatisch in die Mail-Box des Empfängers zu übertragen. Hierbei wird je-

12.3 Komponenten eines PC-Netzwerks

dem Benutzer auf dem Fax-Server eine Faxnummer hinterlegt. Dem Sender muß diese Nummer bekannt sein. Beim Eintreffen des Faxes am Fax-Server erkennt dieser die ISDN-Fax-Nachwahlnummer (d. h. die Faxnummer) und weiß somit durch die Konfiguration des Fax-Servers, welcher Anwender sich hinter dieser Faxnummer verbirgt. Statt das eingehende Fax auszudrucken, wird das Fax in die Mail-Box des Benutzers übertragen. Um den Durchsatz am Fax-Server entsprechend zu erhöhen, kann dieser mit mehreren Modems ausgestattet werden. Auch hier gilt, daß die Anzahl der Anbieter inzwischen so groß ist, daß eine genaue Untersuchung des Markts notwendig ist, um die Lösung zu finden, die den gestellten Anforderungen am ehesten gerecht wird. Die Einfachheit der Fax-Server zum Versenden wird dadurch erreicht, daß die Ausgabe des Faxes im Prinzip nicht anders erfolgt als die Ausgabe des Dokuments auf einen Drucker im Netzwerk, d. h., statt einer Print-Queue wird eine Fax-Queue verwendet.

Backup-Server

Um ein zentrales Backup im Netzwerk durchführen zu können, wird ein eigenes Backup-System benötigt. Es hängt auch hier wieder sehr stark von den bereits installierten Server-Komponenten ab, ob man dafür einen eigenen Backup-Server installieren will oder ob dieser Dienst auf eine bereits vorhandene Server-Maschine installiert werden soll. Die Erfahrung zeigt, daß es durchaus sinnvoll ist, für das Backup einen eigenen Server zu verwenden. Daneben ist zu prüfen, ob die Kapazitäten des Streamers bzw. der Bänder ausreichen, um einen Full Backup durchführen zu können. Darüber hinaus ist die Backup-Strategie von entscheidender Bedeutung. Man kann sich zum Beispiel dafür aussprechen, einmal einen Full Backup durchzuführen, um dann immer wieder mit einem Incremental Backup zu arbeiten. Da es für die einzelnen Netzwerkbetriebssysteme entsprechend viele Backup-Lösungen gibt, muß auch dieser Punkt vor einer Entscheidung sorgfältig untersucht werden. Da ein guter Backup sehr wichtig sein kann, sobald man auf ihn zurückgreifen muß, sollten auch die Bedienung und Handhabung relativ einfach gehalten werden.

Remote Access Services (RAS)

Beim Aufbau eines LAN bzw. für bereits im Betrieb befindliche Netzwerke werden die Forderungen immer wichtiger, Zugänge von und nach außen für jeden im Netzwerk verfügbar zu machen. Für den Zugriff nach außen, um zum Beispiel T-Online oder CompuServe zu nutzen, macht es im LAN wenig Sinn, jedem Anwender ein eigenes

12 Lokale Netzwerke im PC-Bereich

Modem lokal zu installieren. Zu diesem Zweck werden für das Netzwerk Remote Access Server zur Verfügung gestellt, die es erlauben, alle an diesem RAS angeschlossenen Modems und ISDN-Zugänge als Pool im Netzwerk zur Verfügung zu stellen. Entsprechende Sicherheitsmechanismen sorgen dafür, daß diese Modem- und ISDN-Pools nicht von jedem beliebigen Anwender im Netzwerk verwendet werden können, sondern nur berechtigten Personen Zugang gewährt wird.

Umgekehrt besteht für Außendienstmitarbeiter, Bedienungspersonal oder auch Home-Office-Anwendungen der Bedarf, von außen über Modem- oder ISDN-Anschlüsse den Zugang zum Netz zu ermöglichen. Um dabei den Sicherheitsanforderungen gerecht zu werden, muß eine Vielzahl von Sicherheitsvorkehrungen getroffen werden, unberechtigten Personen den Zugang zum Netzwerk zu verhindern. Das RAS kann entweder im Netzwerkbetriebssystem integriert sein (Windows NT Server), als Add-on für das Netzwerkbetriebssystem zur Verfügung gestellt (NetWare Connect) oder als eigenes System von einem Dritthersteller mit eigener Hard- und Software angeboten werden (NetBlazer von TeleBit). Entscheidend dabei ist in allen Fällen, ob analoge und digitale Verbindungen (Modem, ISDN) gleichzeitig unterstützt werden und wie groß die Anzahl der gleichzeitig unterstützten Verbindungen ist.

12.3.4 Das Gateway

Der Gateway-Rechner nimmt eine Sonderstellung im Netzwerk ein. Im Grunde handelt es sich bei dieser Maschine um einen speziellen Server, der nur dann benötigt wird, wenn ein PC im Netzwerk mit einem Netzwerk eines anderen Herstellers kommunizieren will.

Wenn die Netze sowohl von der Hardware als auch von der Software (Protokoll) her nicht zusammenpassen, übernimmt der Gateway-PC dabei die Umsetzung der Daten, die zwischen den beiden Systemen ausgetauscht werden sollen (Code-Konvertierung). Gleichzeitig ist der Gateway-Rechner für die Protokollumwandlung vom einen Netz in das andere zuständig. Dies kann zum Beispiel durch eine Terminalemulation mit eingebauten File-Transfer-Möglichkeiten geschehen oder durch den Einbau einer zweiten Netzwerkadapterkarte, die dann den Anschluß zum anderen Netz ausführt.

Der Gateway-Rechner stellt seine Leistung dem gesamten Netzwerk zur Verfügung, deshalb wird das Gateway auch oft Communication-Server genannt. Je nach Einsatzgebiet können die unterschiedlichsten Gateways eingesetzt werden:

12.3 Komponenten eines PC-Netzwerks

■ *Host-Gateway*

Je nachdem welcher Host (Großrechner) im Unternehmen zum Einsatz kommt, benötigt man ein Gateway für den Übergang zum IBM-Host, Siemens-Host oder auch Unix-Host. In Abhängigkeit der Anforderungen an dieses Gateway müssen die einzelnen Systeme der jeweiligen Hersteller näher auf Tauglichkeit und Einsatzfähigkeit im Netzwerk untersucht werden. Man kann kaum eine generelle Empfehlung geben, da jeder Hersteller mit den verschiedensten Mechanismen und Funktionen aufwartet.

■ *Mail-Gateway*

Beim Einsatz von Mailing-Systemen muß man immer das Problem im Hinterkopf haben, daß Übergänge zu anderen Mailing-Systemen benötigt werden. Es wurde bereits an anderer Stelle kurz darauf hingewiesen, daß es im Mailing-Bereich keinen einheitlichen Standard gibt, so daß in einer heterogenen Mail-Umgebung entsprechende Gateways benötigt werden. Die bekanntesten Gateways, die auch von jedem Mail-Software-Hersteller angeboten werden, sind für den Übergang zum Unix-SMTP-Protokoll und dem X.400-Protokoll verfügbar. Wer einen Zugang zum Internet haben möchte, benötigt auf alle Fälle ein SMTP-Gateway.

12.3.5 Bridge und Router

Bridge und Router haben die Aufgabe, Netzwerke miteinander zu koppeln. Wenn Sie an die Beschreibung des ISO/OSI-Modells zurückdenken, werden Sie sich erinnern, daß die Bridge bzw. der Router bei weitem nicht die Komplexität besitzt wie ein Gateway. Eine Bridge wird jedoch im allgemeinen dafür verwendet, zwei LANs (oder auch WANs) auf der ISO-Ebene 2 miteinander zu verbinden, und der Router dient dazu, diese Kopplung von LANs (oder auch WANs) auf Ebene 3 durchzuführen.

12.3.6 Arbeitsplatzrechner

Der Rechner, mit dem der Anwender im Netzwerk arbeitet, ist die eigentliche Schnittstelle zwischen Anwender und Netzwerk. Er stellt auch die letzte Komponente innerhalb eines Netzwerks dar. Zum Einsatz können dabei PCs jeder Ausbaustufe kommen (DOS/Windows-Rechner, WIN95-Rechner, Windows NT-Rechner, Macintosh-Rechner, Unix-Rechner). Nicht selten sind die Benutzerstationen mit zusätzlicher (redundanter) Peripherie ausgestattet (Festplatte, Drucker, Plotter). Ob diese Konstellation sinnvoll ist, muß aus den Bedürfnissen der Anwender im Zusammenhang mit den ablaufenden Programmen ersehen werden. Nach Möglichkeit sollte aber der ein-

12 Lokale Netzwerke im PC-Bereich

zelne Arbeitsplatzrechner nur noch mit Diskettenlaufwerk und Platte ausgestattet sein. Auf der lokalen Platte sollten nur das jeweilige Betriebssystem und die Auslagerungsdatei von Windows abgelegt sein. Ansonsten werden alle Datenbestände zentral auf dem Server abgespeichert und verwaltet. Sie vermeiden dadurch zum einen redundante Datenhaltung, zum anderen können Maßnahmen für Datenschutz und Datensicherheitsvorkehrungen zentral implementiert und verwaltet werden. Ein weiterer wichtiger Faktor ist die damit mögliche zentrale Datensicherung, da in der Regel die Platten der Workstations nicht gesichert werden.

Eine immer öfter geforderte Funktion ist die, daß Netzwerkbetriebssysteme Mechanismen zur Software-Distribution unterstützen. Man ist gerade dabei, entsprechende Unterstützung anzubieten, also Softwarelösungen bereitzustellen. Ziel soll es sein, die Konfiguration der Workstations zentral über den Server steuern zu können. Dies betrifft auch die Anpassungen und Änderungen notwendiger Konfigurationsdateien der Workstation. Im Zuge von immer komplexer werdenden Workstation-Betriebssystemen (man denke nur an die Komplexität von Windows 95/98 bzw. Windows NT) ist dies zwingend, damit alle verbundenen Konfigurationsänderungen von zentraler Stelle aus durchgeführt werden können. Man hat nicht mehr das Personal und die Zeit, daß man tage- und wochenlang von Workstation zu Workstation läuft, um die notwendigen Anpassungen durchführen zu können. Das Angebot von Software-Distribution-Produkten ist inzwischen so groß geworden, daß auch hier eine genaue Marktuntersuchung nötig ist, um das richtige und passende Produkt einzusetzen. Es gibt Produkte, die relativ leicht zu bedienen sind, wohingegen andere Systeme angeboten werden, mit denen man täglich arbeiten muß, um nicht zu vergessen, wie die eine oder andere Funktion anzuwenden ist und wie die einzelnen Optionen zu bedienen sind.

In diesem Zusammenhang tritt auch immer wieder die Frage auf, ob in einem Netzwerk Diskless Workstations aus Sicherheitsgründen eingesetzt werden sollen oder nicht. Dieses Problem ist immer in Abhängigkeit der eingesetzten Software und der zukünftigen Entwicklungen zu betrachten. Wenn Sie reine DOS-Arbeitsplätze einsetzen wollen und auch für die nächsten Jahre garantieren können, daß dies ausreicht, können Sie ohne Bedenken klassische Diskless Workstations einsetzen. Die Erfahrung der letzten Monate und Jahre zeigt jedoch, daß Windows 95/98 und Windows NT als Workstation-Betriebssystem immer mehr zum Einsatz kommen. Dabei ist es noch vertretbar, wenn DOS/Windows zentral auf dem Server und somit über das Netzwerk geladen wird. Die Performance für das Laden

12.3 Komponenten eines PC-Netzwerks

von Windows lässt sich durch Optimierung der Netzwerkinstallation von Windows sehr gut anpassen. Das im Vergleich zu Windows wesentlich mächtigere Betriebssystem Windows 95/98 zentral über den Server zu laden, ist zwar möglich, aber aufgrund der Komplexität nicht anzuraten. Da diese Betriebssysteme mit grafischer Oberfläche bekanntlich sehr viel Overhead erzeugen (Swap-Dateien), kann dies zu unvorhersehbaren Belastungen des Netzwerks und der I/O-Kanäle am Server führen. Aus diesem Grund ist der Einsatz einer lokalen Platte zu empfehlen und schon fast zwingend. Für die Betriebssysteme Windows NT und OS/2 bleibt im Prinzip gar keine andere Wahl mehr.

Um jedoch Datenschutz und Datensicherheit der lokalen Platten gewährleisten zu können, müssen andere Mechanismen eingesetzt werden. Die eine Möglichkeit besteht darin, das lokale Diskettenlaufwerk auszubauen und nur die lokale Platte in der Workstation zu betreiben oder spezielle Vorrichtungen zum Absperren der lokalen Diskettenlaufwerke zu nutzen. Andere Lösungen sind durch Software realisiert, wobei dann die Möglichkeit besteht, dem Anwender auf der Workstation den Zugriff auf das lokale Diskettenlaufwerk generell zu verbieten.

Einfacher ist es, wenn das BIOS im Rechner die Möglichkeit bietet, ein Systempaßwort für das BIOS zu vergeben, damit dort der Anwender selbst keine Konfiguration durchführen kann. Auf diese Weise kann das Diskettenlaufwerk deaktiviert und bei Bedarf vom Netzwerkverwalter wieder aktiviert werden, für den Fall, daß Konfigurationen über das Diskettenlaufwerk der Workstation installiert werden müssen.

Diese Forderungen werden vor allem deswegen immer häufiger gestellt, weil die Gefährdung der Daten durch Viren immer größer wird. In diesem Zusammenhang wird es auch notwendig, sich ein ausgereiftes und durchdachtes Datensicherungskonzept zu überlegen und konsequent durchzuführen.

Das Netzwerk sollte dabei aber auch so konfiguriert werden, daß auf dem Server ein Virenprüfprogramm ständig aktiv ist. Die Konfiguration sollte dabei so aussehen, daß alle eingehenden Daten durch das Virenprüfprogramm automatisch auf Viren untersucht werden. Für den Fall, daß eine eingehende Datei mit Viren behaftet ist, wird diese in der Regel in einen gesicherten Bereich geschrieben und der Administrator davon in Kenntnis gesetzt, wenn eine infizierte Datei entdeckt worden ist. Das Virenprogramm kann dabei auch so konfiguriert werden, daß die Virenprüfung zusätzlich zu einem bestimmten Zeitpunkt durchgeführt wird (z.B. um Mitternacht). Um auch Work-

12 Lokale Netzwerke im PC-Bereich

stations vor Viren zu schützen, kann ein zusätzlicher Mechanismus installiert werden, daß die Workstations bei jedem neuen Logon auf Viren überprüft werden, d.h., die lokale Platte bzw. die Platten werden untersucht. Ist es ein entsprechend leistungsfähiges Produkt, kann auch noch ein residentes Programm auf der Workstation gestartet werden (automatisch beim Logon), um jede Diskette, die in das Diskettenlaufwerk eingelegt wird, automatisch auf Viren zu untersuchen und entsprechende Meldungen auszugeben, für den Fall, daß ein Virus gefunden worden ist.

Exakte Analysen und Konzepte sind von Firma zu Firma verschieden, so daß hier nur auf die zu beachtenden Faktoren aufmerksam gemacht werden soll und Detaillösungen von Fall zu Fall entschieden werden müssen.

Inzwischen steigt die Nachfrage nach Sicherheitsuntersuchungen für Netzwerke. Dies betrifft sowohl die Installation der Server und Workstations als auch die Prüfung der Remote-Zugänge von und nach außen.

Zu beachten ist dabei, daß die meisten Virenschutzprogramme ein Virenpattern benötigen, um die aktuellen Viren erkennen zu können. Diese Virenpattern werden vom Hersteller meist monatlich aktualisiert und in der Regel auf der Mail-Box des Herstellers (BBS) oder vom Internet oder von CompuServe oder von AOL geholt. Diese Virenpattern sind kostenlos zu haben. Es gibt aber auch Hersteller, die einen kostenpflichtigen Update-Service anbieten. Dies kostet dann zwar ein paar Mark, aber man hat den Vorteil, daß man sich nicht mehr selbst darum kümmern muß.

12.3.7

Netzwerkdrucker

Der Anschluß von Netzwerkdruckern im LAN wird immer bequemer. Es gibt inzwischen eine Vielzahl von Möglichkeiten, Netzwerkdrucker dort einzusetzen, wo sie benötigt werden. Fast alle Netzwerkbetriebssystem-Hersteller unterstützen inzwischen nicht nur die Möglichkeit, Netzwerkdrucker am Server anzuschließen und somit allen Anwendern im Netzwerk zur Verfügung zu stellen, sondern auch die Möglichkeit, Drucker an Workstations anzuschließen und als Netzwerkdrucker zu konfigurieren. Dabei ist es meist möglich, DOS-, Windows-, Windows 95-, Windows 98-, Windows NT- und Windows 2000-Arbeitsplätze zu verwenden.

Eine andere Möglichkeit wird von Drittherrstellern angeboten. Entweder besteht für den Drucker selbst die Option, eine Netzwerkadapterkarte einzubauen, um den Drucker direkt in das Netzwerk zu integrieren, oder es wird eine Zusatzhardware angeboten, die direkt in das Netzwerk eingebunden werden kann. Daran sind wiederum

12.3 Komponenten eines PC-Netzwerks

mehrere Drucker anschließbar. Eine einfache, gute Möglichkeit ist es, auf den parallelen Port des Druckers einen sogenannten Pocket-Print-Server aufzustecken, der wiederum den direkten Anschluß im Netzwerk realisieren kann.

Alle aufgeführten Möglichkeiten dienen dazu, die Drucker im Netzwerk dort zu installieren, wo sie auch benötigt werden. Je nach Konfiguration und Umgebungsbedingung ist zu entscheiden, welcher der Alternativen der Vorzug zu geben ist. Wichtig ist, daß alle aufgeführten Optionen gut eingesetzt werden können und einfach zu handhaben sind.

Je nach Netzwerkbetriebssystem (z.B. Novell NetWare) kann man auch Drucker, die in unterschiedlichen Systemen konfiguriert sind, als Netzwerkdrucker allen Anwendern im System zur Verfügung stellen. So bietet z.B. Novell eine Option an, Drucker, die unter Unix konfiguriert sind, auch unter NetWare zu betreiben. Das heißt, ein Anwender unter NetWare kann seine Druckaufträge wie gehabt in eine NetWare-Print-Queue stellen, und ein spezieller Print-Server-Mechanismus übergibt die Druckaufträge an das LP-Spool-System der Unix-Maschine.

Umgekehrt ist es möglich, daß ein Unix-Anwender wie gewohnt seine Druckaufträge an das Unix-LP-Drucksystem weitergibt, und das speziell konfigurierte Unix-LP-Drucksystem übergibt die Druckaufträge an NetWare. Somit können Unix-Anwender auch auf Druckern ausdrucken, die unter NetWare konfiguriert sind.

Eine ähnliche Konfiguration bietet Novell für die SNA-Welt an. Ein NetWare-Drucker kann mit Zusatzsoftware (Host Print) so konfiguriert werden, daß zusammen mit dem NetWare for SAA Gateway von Novell ein 3270-Anwender seine Druckaufträge direkt an einen unter NetWare konfigurierten Drucker ausgeben kann.

Diese Möglichkeiten sind bei Bedarf von Hersteller zu Hersteller abzuklären, wenn Sie in Ihrer Netzwerkkonfiguration diese oder ähnliche Mechanismen nutzen möchten. Auch wenn sich dieses Buch nicht nur mit NetWare und den damit verbundenen Konzepten beschäftigt, ist es unmöglich, auf alle unterstützten Funktionen im Detail einzugehen. Zudem werden fast täglich neue Features angeboten, so daß gar nicht schnell genug reagiert werden könnte, wenn man sie alle beschreiben will. Die aufgeführten Konzepte sollen Ihnen jedoch einen umfassenden Überblick darüber geben, welche Leistungsfähigkeit und welche Funktionalitäten von heutigen Netzwerkbetriebssystemen unterstützt werden. In Abbildung 12.1 sind all die Möglichkeiten aufgezeigt, wie Sie Drucker als Netzwerkdrucker in das Netz integrieren können.

12 Lokale Netzwerke im PC-Bereich

Beachten sollte man bei diesen Produkten, daß die Software dieser Komponenten multiprotokollfähig ist, also die unterschiedlichen Netzwerkbetriebssysteme (Novell, Windows NT Server, Unix etc.) unterstützt werden, und dies auch noch parallel. Auf diese Weise ist es möglich, daß Netzwerkdrucker in einer heterogenen Umgebung gleichzeitig von den unterschiedlichen Netzwerkbetriebssystemen angesteuert werden können. Diese Komponenten fordern vom Netzwerkverwalter, regelmäßig von der Online-Datenbank des Herstellers, vom Internet, von CompuServe oder von AOL den aktuellsten Softwarestand zu holen.

12.3.8

Streamer

Der Streamer ist eines der wichtigsten Elemente, wenn es um den Aufbau von Netzwerken geht, und er sollte von Anfang an in das Konzept einbezogen und installiert werden. Ich stelle leider immer wieder fest, daß man der zentralen Datensicherung im Netzwerk zu wenig Bedeutung schenkt. Spätestens wenn man auf eine ordnungsgemäße Datensicherung zum Wiederherstellen von Daten angewiesen ist, sieht man, welche Vorteile ein richtiges und ordnungsgemäßes Datensicherungskonzept bietet. Man sollte aber nicht auf den Tag x warten, um zu dieser Einsicht zu kommen.

Da in der Regel alle Unternehmensdaten zentral auf dem oder den Servern abgespeichert werden – so sollte es zumindest sein –, würde ein Ausfall der zentralen Speicherkomponenten (Platte oder der Server selbst) zu Datenverlusten führen, die unter Umständen nur durch einen riesigen Aufwand und viel Zeit rekonstruiert werden könnten.

Aus diesem Grund muß im Netzwerk eine ausgereifte Datensicherung durchgeführt werden, deren Konzept gewährleisten kann, auch ältere Datenbestände bei Verlust wieder zu restaurieren. Schlug man sich früher mit Streamer-Kapazitäten von 100 Mbyte oder 250 Mbyte herum, so geht man heute bereits von Anfang an mit Streamerkapazitäten von 2, 4, 8 oder 40 Gbyte um. In speziellen Fällen werden auch Lösungen benötigt, die es erlauben, automatisch Kapazitäten von bis zu 1,98 Terabyte zu sichern. Das ist aber nur dann möglich, wenn man mit einem Bandwechsler arbeitet.

Wenn man sich die heutige Streamer-Technik ansieht, dann bringt man auf immer kleineren Bändern immer größere Datenkapazitäten unter. In speziellen Fällen wird auch gefordert, nicht häufig benötigte Daten statt auf Platte auf optischen Medien abzulegen bzw. zu archivieren, um dennoch bei Bedarf darauf zurückgreifen zu können. Zu unterscheiden sind dabei Streamer, die nach der DAT-Technik oder nach der DLT-Technik arbeiten. Die DAT-Technik kann der-

12.3 Komponenten eines PC-Netzwerks

zeit auf einem Band ca. 24 Gbyte speichern, hingegen können auf ein DLT-Band bis zu 70 Gbyte Daten gespeichert werden. Bei der DAT-Technik kommen 4-mm-Bänder zum Einsatz, in den DLT-Laufwerken werden die etwas größeren 8-mm-Bänder eingesetzt. Die DLT-Bänder zeichnen sich auch durch eine wesentlich höhere Lebensdauer aus, dies gilt übrigens auch für die DLT-Streamer.

Eine häufig gestellte Forderung ist dabei, daß die Datensicherung automatisch und ohne Eingriff des Administrators durchgeführt werden soll. Dies muß von der Streamer-Software erfüllt werden können. Wenn die Plattenkapazität so groß ist, daß die Daten nicht mehr auf ein einzelnes Band passen, muß unter Umständen ein System gewählt werden, das einen automatischen Bandwechsel durchführen kann. In solchen Fällen kommen Autoloader oder Stacker-Systeme zum Einsatz.

Bei der Auswahl der Streamer-Software ist nicht nur auf solche Funktionsleistungen Rücksicht zu nehmen, sondern es muß auch geklärt werden, ob die Streamer-Software für das jeweilige Netzwerkbetriebssystem tauglich ist. Fast alle Hersteller verwenden spezifische Security-Dateien, die nur von einer darauf abgestimmten Streamer-Software gesichert werden können. Ohne diese speziellen Systemdateien wäre es nicht mehr möglich, einen ordnungsgemäßen Restore von Daten durchzuführen.

Auf alle Fälle ist ein ausgefeiltes Datensicherungskonzept mit einem dazu passenden Auslagerungsverfahren erforderlich. Die Datensicherungsbänder sollten auf keinen Fall im gleichen Raum aufbewahrt werden, in dem sich auch der Server befindet. Sollte dort ein Feuer ausbrechen, wären auch die Sicherungsbänder gefährdet. Daher sollten die Bänder in einem feuersicheren Tresor aufbewahrt werden. Für das Auslagerungsverfahren muß geplant werden, in welchen Abständen Wochen-, Monats-, Quartals- oder auch Jahresbänder erstellt und in einer Bank oder einem ähnlich sicheren Ort aufbewahrt werden. Man sollte aber darüber hinaus einen Ort haben, der jederzeit zugänglich ist. Ich kenne bereits mehrere Fälle, wo es erforderlich war, auf Bänder zurückzugreifen, die in der Bank aufbewahrt wurden. Dies wäre noch nicht so schlimm gewesen, wenn es sich nicht gerade um ein Wochenende gehandelt hätte. Man hatte dann nach langem Suchen die zuständige Person der Bank gefunden, konnte aber nicht an den Tresor, da man es inzwischen in Banken mit Zeitschlössern zu tun hat, die man nicht mehr ohne weiteres umgehen kann. Der Aufwand, das Zeitschloß bei einer Bank zu öffnen, hätte wiederum das ganze Wochenende beansprucht. Somit konnte man gleich auf den Montag warten. Die Daten konnten also erst im Laufe des Montags zurückgesichert werden.

12 Lokale Netzwerke im PC-Bereich

Man sieht bereits an diesem kleinen, aber doch bedeutsamen Beispiel, daß es eine Vielzahl von Aspekten gibt, die beim Aufbau eines Netzwerks und der Inbetriebnahme von Servern, Server-Komponenten, Workstations und allen dazugehörigen Funktionen berücksichtigt werden müssen.

12.3.9 FireWall-System

Es wurde bereits mehrfach darauf hingewiesen, daß der Zugang zum Internet nicht ohne zusätzliche Schutzmechanismen erfolgen sollte. Zu diesem Zweck besteht die Möglichkeit, ein FireWall-System zu installieren. Die primäre Aufgabe des FireWall-Systems besteht darin, den Zugang vom Internet in das firmeneigene Netzwerk bzw. vom firmeneigenen Netzwerk zum Internet abzusichern. Auf diese Weise wird gewährleistet, daß nur die Benutzer die notwendigen und erforderlichen Zugänge erhalten, die auch berechtigt sind. Für den Aufbau und die Implementierung von FireWall-Systemen gibt es die unterschiedlichsten Lösungen einer Vielzahl von Herstellern. Mit der Implementierung des FireWall-Systems ist es jedoch nicht getan. Die vom FireWall-System geführten Protokolldateien müssen in regelmäßigen Abständen geprüft werden, um feststellen zu können, ob »Fremde« versucht haben, in Ihre Netzwerk einzudringen. Zudem sollte man sich für ein FireWall-System entscheiden, bei dem man die Gewähr hat, daß der Hersteller auch bestrebt ist, das System ständig zu verbessern. Da den Hackern immer wieder neue Methoden einfallen, um in ein System einzudringen und FireWall-Systeme unter Umständen zu umgehen, müssen die FireWall-Systeme (ähnlich den Virenschutzprogrammen) permanent an neue Begebenheiten angepaßt werden. Aufgrund der großen Bedeutung, die dem Internet und der Anbindung an das Internet zugemessen werden, ist dem Thema FireWall ein eigenes Kapitel gewidmet.

12.4 Die Phasen der Netzwerkinstallation

Wenn die Entscheidung für den Einsatz eines LAN getroffen worden ist, ergeben sich im weiteren Verlauf der Planung und der Realisierung für das Gesamtsystem in der Regel verschiedene Phasen für die Durchführung der Installation bis zur endgültigen Freigabe zum produktiven Betrieb. Die nachfolgend aufgeführten Planungsphasen sind nur als Vorschlag aufzufassen, der von Fall zu Fall variiert werden kann bzw. muß. Bei genauerer Betrachtung der einzelnen Schritte zur Durchführung derartiger Installationen lassen sich zehn Planungsphasen erkennen, die es von oben nach unten auszuführen gilt.

12.4 Die Phasen der Netzwerkinstallation

1. Erstellung eines Pflichtenhefts
2. Erstellung eines Systemkonzepts
3. Hardware-Entscheidungen
4. Spezifikation des Anwendungssystems (Verfeinerung des Pflichtenhefts)
5. Netzwerkkonzept erstellen
6. Netzwerkhardware und Netzwerkbetriebssystem auswählen
7. Netzwerkinstallation
8. Anwendersoftware installieren
9. Testen aller Komponenten
10. Übernahme in den produktiven Betrieb

Erläuterung der einzelnen Phasen

1. Schriftliche Fixierung der Zielvorgaben: Was soll mit dem neuen System durchgeführt werden können? Anforderungen, die das System auf alle Fälle erfüllen sollte bzw. muß. Daneben enthält das Pflichtenheft Wünsche, die nach Möglichkeit berücksichtigt werden sollen.
2. Auf Basis der vorbereitenden Analyse muß zuerst ein Konzept für das Gesamtsystem erstellt werden. Für dieses Konzept wird ein grober Anforderungskatalog erstellt, und daneben werden bereits die ersten Ansätze zur Modularisierung definiert. Damit werden bereits die ersten Komponenten der Anwendungssoftware festgelegt. Es kann sich dabei z.B. um Bausteine wie Angebotserstellung, Finanzbuchhaltung, Auftragsbearbeitung usw. handeln.
Schon hier werden im groben Rahmen die Hardware-Anforderungen festgelegt. Dies betrifft vor allem Angaben über den notwendigen Massenspeicherbedarf, Anzahl der Arbeitsplätze, Volumen des Druckaufkommens u.ä.
3. Aufgrund der Festlegungen in Phase 2, die bestimmte Hardware-Anforderungen genau vorgibt, kann in Phase 3 eine erste Entscheidung für eine ungefähre Hardware-Richtung eingeschlagen werden. Es werden hier die Alternativen bezüglich Einsatz eines Zentralrechners, einer Mittleren Datentechnik oder eines PC-Netzwerks gegeneinander abgewogen. Dies erfordert eine genaue Prüfung der einzelnen Möglichkeiten.
4. Das in Phase 1 erstellte Konzept wird hier genauer aufgeschlüsselt.
5. Die Informationen zur Erstellung des Netzwerkkonzepts stammen aus den Phasen 2 und 4. Im Netzwerkkonzept sollten folgende Fragestellungen enthalten sein:
 - Wie viele Arbeitsplätze werden insgesamt eingesetzt?
 - Wie groß ist die ungefähre Anzahl von Arbeitsplatzrechnern, die gleichzeitig aktiv sind?

12 Lokale Netzwerke im PC-Bereich

- Wie viele Workstations arbeiten mit zentralen Datenbeständen?
 - Auslegung der Server-Peripherie:
 - Plattenkapazität
 - Anzahl der Drucker
 - Geschwindigkeit der Drucker
 - Sicherungsmedium (Streamer zentral oder dezentral)
 - Gesamtausdehnung des Netzwerks, Integration in die Gebäudestruktur
 - Können Störeinflüsse von außen auftreten (Produktionsstätten, Spannungswandler etc.)?
 - Sollen bestehende EDV-Anlagen einbezogen werden (Gesamtumfeld der Endausbaustufe)?
6. Mit Hilfe dieser Überlegungen ist es nun möglich, sowohl die Hardware als auch die Software für das Netzwerk auszuwählen. Dabei ist jedoch mit besonderer Vorsicht vorzugehen, da auch eine Wahl der Arbeitsplatzrechner vorgenommen werden muß. Die Systeme sollen aufeinander abgestimmt sein. Es ist zum Beispiel zu beachten, daß beim Einsatz von DTP-Systemen eventuell 21-Zoll-Bildschirme eingesetzt werden und nicht die herkömmlichen 14- oder 17-Zoll-Schirme. Überlegt werden sollte auch, ob das Netzwerk bei dem einen Händler, Server- und Workstation-Hardware oder aber bei einer Zweit- oder Drittfirma beschafft werden. Aus eigener Erfahrung erscheint es von Vorteil, das gesamte Equipment aus einer Hand zu beziehen. Bei auftretenden Fehlern kann es Ihnen dann nicht passieren, daß der einzelne Händler das Problem auf die Hard- oder Software des anderen Händlers schiebt, dies vor allem dann, wenn der Fehler nicht eindeutig dem LAN, dem PC oder dem Server zuzuordnen ist.

Die richtige Wahl zu treffen ist nach wie vor eines der größten Probleme. Der bereits vorgestellte Kriterienkatalog soll Ihnen dabei eine kleine Hilfestellung geben. Dort sind allerdings nicht alle Fragen abgedeckt, da es von den einzelnen, individuellen Begebenheiten abhängt, welche Komponenten besser oder schlechter geeignet sind. Hilfreich sind in solchen Fällen auch Referenzkunden, die ein ähnliches Netzwerk der gleichen Größenordnung in Betrieb haben. Der Händler sollte Sie dabei so unterstützen, daß er Ihnen diese Referenzkunden nennt, damit Sie sich selbst vom Funktionieren dieser Netzwerke überzeugen können.

Neben dem Einsatz von standardisierter Hardware ist es auch notwendig, bei der Auswahl von Software darauf zu achten, ob es sich um spezielle Software für dieses spezielle Netzwerkbetriebssystem handelt oder ob die Software auf allen gängigen Systemen läuft. Weit verbreitet ist dabei in diesem Bereich derzeit

12.4 Die Phasen der Netzwerkinstallation

Novell NetWare auf Seite des Netzwerkbetriebssystems bzw. DOS/Windows 95/98 bzw. Windows NT als Workstation-Betriebssystem. Bei diesen Produkten haben Sie die Sicherheit für eine langfristige Funktionsfähigkeit des Gesamtsystems. Die Windows-NT-Server-Installationen und Windows-95/98- bzw. Windows-NT-Workstation-Installationen nehmen immer mehr zu.

7. Bevor die Fachabteilung mit der ausgewählten Software arbeiten kann, muß das Netzwerk auch installiert werden. Die Installation kann dabei in mehrere Phasen eingeteilt werden:

- *Verkabelung des Gebäudes*

Spätestens zu diesem Zeitpunkt ist zu überlegen, wie die Räume verkabelt werden, ob also der Platz in vorhandenen Kabelschächten reicht oder neue Schächte gelegt werden müssen. Es ist dabei zu beachten, ob eventuell zu einem späteren Zeitpunkt zusätzliche Kabel in die Schächte eingezogen werden können. Die Montage der Steckdosen in den Büros muß sorgfältig geplant werden, damit nicht der Fall eintritt, daß die Dose so platziert wird, daß ein Kabel durch den ganzen Raum gelegt werden muß, um den PC anschließen zu können. Ebenfalls muß überprüft werden, ob die Kabellängen der einzelnen Stränge nicht die vorgeschriebene Maximallänge überschreiten. Selten lassen sich Kabel direkt in die Räume verlegen, sondern sie müssen meistens verschlungen durch Decken und Keller gezogen werden. Gleichfalls sollte man überprüfen, ob in den Schächten oder in der Nähe von Schächten nicht andere Kabel liegen (Starkstrom etc.), die magnetische Abstrahlungen aufweisen und damit die Datenübertragung stören.

- *Installation von Server und Workstation*

Bei diesem Vorgang werden die entsprechenden Adapterkarten in den einzelnen Stationen eingebaut. Große Sorgfalt muß darauf gelegt werden, die Adapter so einzustellen, daß sie von der Hardware der Rechner akzeptiert werden (I/O-Adresse, Base-Memory-Adresse, Interrupt-Request müssen aufeinander abgestimmt sein).

Ganz wichtig ist hierbei, daß die Node-Adressen der einzelnen Rechner unterschiedlich eingestellt werden, da sonst das Netzwerk nicht richtig funktioniert und dieser Fehler nur schwer zu lokalisieren ist.

- *Einbau der Server-Peripherie*

Dies betrifft die Installation von Platten und Plattensubsystemen, Drucker oder Notstromversorgung. Es gilt dabei der gleiche Grundsatz wie oben, d.h., es ist darauf zu achten, daß die Peripherie mit der restlichen Hardware zusammenpaßt.

12 Lokale Netzwerke im PC-Bereich

– *Erster Test der Verkabelung und Hardware-Konfiguration*

Es gibt bei Novell NetWare zum Beispiel die Möglichkeit, die Hardware nach der Installation auf ihr korrektes Funktionieren zu überprüfen (Verkabelung, Server und Workstation). Dabei lassen sich leicht und schnell Fehler in den Hardware-Komponenten der Rechner (falsche Interrupts etc.) und der Verkabelung (Kabelbruch, defekter Stecker, defekter Active- oder Passive-Hub, nicht intakter Ringleitungsverteiler, kaputte Dose, doppelte Node-Adressen etc.) feststellen, erkennen und beseitigen.

Wenn solche Testmöglichkeiten zur Verfügung stehen, sollten sie auch genutzt werden, da man sich dabei eventuell lange Fehlersuchzeiten sparen kann.

– *Installation des Netzwerkbetriebssystems*

Dies muß nach den Installationsvorgaben des Herstellers erfolgen. Bevor Sie jedoch anfangen, das Betriebssystem zu installieren, sollten Sie vorher gründlich das Handbuch durchlesen. Sie vermeiden dadurch lange und unnötige Fehlversuche oder Falscheingaben.

8. Wenn diese Arbeiten erfolgreich durchgeführt worden sind, kann damit begonnen werden, die Anwendersoftware zu installieren. In den Installationsanweisungen sollten besonders die Anleitungen für eine Netzwerkinstallation beachtet werden, vorausgesetzt es handelt sich um netzwerkfähige Software. Im anderen Fall sind eventuell notwendige Änderungen zu überprüfen.

Nachdem die einzelnen Applikationen auf die Serverplatte gespielt worden sind, werden die Benutzer eingerichtet. Bei dieser Arbeit müssen unter anderem auch die notwendigen Berechtigungen vergeben werden. Für den Fall, daß der Endanwender über Menüs auf dem Server arbeitet, muß zu diesem Zeitpunkt auch das Anwendermenü erstellt werden.

9. *Testen aller Komponenten:* Bevor ein Netz für den produktiven Betrieb freigegeben wird, sollten alle Komponenten, Hardware und Software, sehr sorgfältig ausgetestet werden. Erst wenn alle Tests erfolgreich abgeschlossen sind, kann das System freigegeben werden. Parallel zu diesen Tests kann die Einweisung und Schulung der Endanwender durchgeführt werden. Wenn es als notwendig erachtet wird, kann, wie bei allen DV-Systemen, ein Parallelbetrieb aufrechterhalten werden. Dieser Parallelbetrieb sollte so lange wie möglich und so lange wie nötig durchgeführt werden, um alle Fehler frühzeitig aufdecken zu können.
10. *Produktionslauf:* Ab diesem Zeitpunkt sind die Arbeiten abgeschlossen. Nach Freigabe des Systems kann man nur hoffen, daß alles reibungslos funktioniert.

12.4 Die Phasen der Netzwerkinstallation

Diese zehn Projektphasen sind ein Anhaltspunkt dafür, wie der Aufbau eines LAN durchgeführt werden könnte. Sie sollten diese Phasen nicht als einen starren Plan zur Durchführung der Netzwerkinstallation ansehen. Es wird hier nur ein Überblick über die einzelnen Phasen gegeben.

Innerhalb dieser zehn Phasen wird die Notwendigkeit bestehen, entsprechende Schulungen durchzuführen, um mit den Möglichkeiten und der Bedienung, Wartung und Pflege des Systems vertraut zu werden. Sinnvoll ist es dabei, die Schulungen, vor allem für das jeweilige Netzwerkbetriebssystem, vor Beginn der logischen Implementierung des Netzwerks durchzuführen. Nur so kennen Sie alle Möglichkeiten, Restriktionen und Zusatzoptionen, die für das gewählte Netzwerkbetriebssystem zur Verfügung stehen.

Es hilft Ihnen relativ wenig, wenn Sie sich die schönsten Konzepte zur Implementierung der Netzwerkstruktur ausdenken und später bei der Umsetzung der Konzepte feststellen müssen, daß diese Möglichkeiten von der Software gar nicht unterstützt werden.

Achten Sie auch darauf, daß alle Phasen der Netzwerkinstallation durchgängig dokumentiert werden. Das beginnt bei der Verlegung der Kabel und hört bei der Dokumentation der Serverstrukturen und der Konfiguration der Workstations auf. In diesem Zusammenhang ist auch nach geeigneten Produkten zu suchen, die Ihnen die Erstellung der Dokumentation erleichtern. Das sind Entscheidungen und Konzepte, die in Zusammenhang mit dem Netzwerkmanagement zu betrachten sind.

Sie werden bei allen Produkten (unabhängig vom Netzwerkbereich) auf spezielle Anforderungen stoßen, die es nicht erlauben, sich an diesen Projektplan zu halten. Er ist als Anregung gedacht und soll auch als solche verstanden werden.

Bevor wir nun spezielle Netzwerkbetriebssysteme hinsichtlich ihrer Leistungsfähigkeit, ihrer unterschiedlichen Konzepte und Merkmale im Detail besprechen wollen, soll ein Vergleich von LAN und Mini-computer durchgeführt werden. Nach wie vor ist es eine Streitfrage, was besser ist – der Einsatz von LANs oder die Verwendung der Mittleren Datentechnik (z.B. Unix oder AS/400). Im nächsten Abschnitt versuche ich, näher auf diese Frage einzugehen. Es sei aber bereits an dieser Stelle bemerkt, daß es durchaus Anwendungsgebiete gibt, die durch den Einsatz von herkömmlichen Server-Systemen im LAN nicht abgedeckt werden können und wo der Einsatz eines MDT-Systems, in der Regel mit speziellen Branchensoftwarepaketen, effektiver ist. Oft wird aber auch beides im Netz eingesetzt.

12.5 Gegenüberstellung von LAN und MDT

Eine Bewertung dieser beiden Systeme, die Betrachtung der Vor- und Nachteile, gewinnt mehr und mehr an Bedeutung, da die Lokalen Netze in Bereiche vordringen, die bis vor kurzem noch eine reine Domäne der Minicomputer (MDT) waren.

Ein Lokales Netz und Minicomputersysteme repräsentieren im Grunde technologisch verschiedene Philosophien:

- Das LAN als Kommunikationsmedium
- Die MDT-Systeme als Rechner

In der Praxis werden diese beiden Begriffe für zwei mögliche Alternativen verwendet, wenn es um den Einsatz von Datenverarbeitungssystemen geht.

Wie bereits mehrfach besprochen, handelt es sich bei LANs in der Regel um Netzwerke mit verteilten PC-Arbeitsplätzen. Die Mittlere Datentechnik dagegen vertritt das Konzept der Host-Zentraleinheit, d.h., es wird ein gemeinsam genutztes Verarbeitungsnetzwerk verwendet, an dem Terminals ohne eigene Rechnerkapazität angeschlossen sind.

Es ist klar, daß ein Vergleich dieser Systeme nicht nur schwierig, sondern auch sehr vage sein muß. Letztendlich kommt es auf die Anwendungen an, mit der die Systeme eingesetzt werden sollen. Wenn Sie einen Sattelschlepper aussuchen wollen, vergleichen Sie den ja auch nicht mit einem PKW.

Soll ein Vergleich angestrebt werden, kann man sich auf drei Punkte konzentrieren:

1. Netzwerk:	zentrale oder dezentrale Verarbeitung
2. Server/Host:	PC oder Minicomputer
3. Arbeitsplatzrechner:	intelligente PCs oder unintelligente Terminals

Durch »SAA – das immer noch neue Konzept der IBM« zeichnet sich der Trend ab, daß sich die Datenverarbeitung und die Datenspeicherung immer mehr vom zentralen Großrechner lösen und in die einzelnen Abteilungen verlagert werden. Für diese Entwicklung werden verschiedene Bezeichnungen verwendet, wie zum Beispiel:

- Verarbeitung am Arbeitsplatz
- Verteilte Verarbeitung
- Verarbeitung auf Abteilungsebene
- Gleichrangige Netzwerkverarbeitung
- Individuelle Datenverarbeitung

12.5 Gegenüberstellung von LAN und MDT

Diese Tendenz hat mehrere Ursachen. Eine davon ist der sogenannte Anwenderstau, der sich im Lauf der Zeit seitens der Großrechner ergeben hat. Auf diese Problematik wird später noch näher eingegangen werden.

Eigentlich ist eine Abteilung nichts anderes als ein kleines Unternehmen. Dementsprechend müssen Systeme zur Verfügung stehen, mit denen die Datenverarbeitung durchgeführt werden kann. Wie in kleinen Unternehmen erfolgt die Datenverarbeitung vor Ort. Der Aufwand für den Großrechner und für die Datenübertragung (in Verbindung mit dem Host) wird geringer.

Deshalb werden verstärkt PCs eingesetzt und dann vernetzt. Die andere Alternative ist der Einsatz einer MDT-Anlage.

Minicomputersysteme kamen in den frühen siebziger Jahren zum Einsatz. Dies war der erste Schritt für die verteilte Verarbeitung. Faktoren, die eine zentrale Verarbeitung erzwungen haben, vor allem der Preis der Host-Systeme, verloren durch die ständig sinkenden Preise an Bedeutung. Damit lohnte es sich, im begrenzten Maße eine verteilte Datenverarbeitung einzuführen.

Betrachtet man die Architektur eines Minicomputersystems, so stellt man fest, daß es sich dabei im Grunde um einen Host im Kleinformat handelt. In beiden Fällen wird die Datenverarbeitung (Programmablauf, Steuerung der Terminals etc.) von diesen Rechnern übernommen. Die angeschlossenen Terminals besitzen dabei keine eigene Rechnerintelligenz, dies übernimmt der Host. Zum Zeitpunkt der Entwicklung dieser Systeme gab es noch keine andere Möglichkeit, um solche Arbeitsplatzrechner zur Verfügung zu stellen.

Fast ein Jahrzehnt lang entwickelte sich die verteilte Datenverarbeitung in dieser Form. Erst durch die Möglichkeiten der PCs, kurz darauf der Einsatz der ersten LANs, beschleunigte sich die Entwicklung hin zur verteilten Datenverarbeitung. Einerseits bieten MDTs die Funktionalität der Host-Terminal-Interaktion, andererseits ist das LAN (Verarbeitung am Arbeitsplatz – intelligentes Terminal) die natürliche Weiterentwicklung des Personalcomputers.

Hätte man zur damaligen Zeit einen Vergleich dieser beiden Technologien (LAN versus MDT) durchgeführt, dann wäre das LAN kläglich unterlegen. LANs waren damals nichts anderes als einfache Systeme zur gemeinsamen Nutzung von Peripheriegeräten (Disk-Server-Konzept der ersten LANs). Systeme der Mittleren Datentechnik hingegen boten Fähigkeiten zum Anschluß zahlreicher Bildschirmarbeitsplätze in Multi-User-Umgebung und die Möglichkeiten der Einbindung in Fernbereichsnetze (WAN).

12 Lokale Netzwerke im PC-Bereich

Inzwischen haben die LAN-Entwicklungen große Fortschritte gemacht; dies gilt vor allem für folgende Bereiche:

Festplattenverwaltung im File-Server

Die Schreib-/Lesefunktionen der Festplatte werden von der im File-Server ablaufenden Software gesteuert und verwaltet. Probleme, die mit der verteilten Plattenverwaltung entstehen, werden dadurch vermieden. Die Gewährleistung der Integrität der Daten im LAN erreicht deshalb einen Stand, wie er auch auf Großrechner- und Minicomputersystemen zu finden ist. Die Firma Novell hat 1983 als erster Hersteller für Netzwerkbetriebssysteme dieses Konzept verwendet. Es hat sich inzwischen zum De-facto-Industriestandard entwickelt. Wie aus den späteren Ausführungen zu sehen ist, hat sich sowohl Novell als auch Microsoft bemüht, durch stetige Weiterentwicklung auf diesem Gebiet allen Anforderungen gerecht zu werden.

Multi-User-Software

Es gibt mehrere Multi-User-Programme, die direkt von Großrechnerversionen und MDT-Versionen auf den PC-Bereich übertragen worden sind, so daß Funktionsumfang und Kompatibilität mit diesen Systemen erhalten geblieben sind.

Weitere Systeme sind speziell für den Einsatz in PC-LANs entwickelt worden. Alles in allem hat der Anwender eine reiche Auswahl an Software.

Datenübertragung

Über Gateways ist es möglich, den Zugang zum Großrechner oder MDT zu schaffen. Es können damit Dateien übertragen oder Online-Sitzungen durchgeführt werden. Der Arbeitsplatz wird dann zum Terminal des Host-Rechners oder der MDT-Anlage. Durch den Einsatz von Bridge-Rechnern werden transparente Verbindungen zu anderen LANs hergestellt. Über asynchrone Verbindungen oder Datex-P-Anschlüsse ist die Basis geschaffen, Fernnetze aufzubauen.

Fehlertoleranz

1986 führte Novell bei seinem LAN-Betriebssystem die fehlertolerante NetWare ein. Auch Microsoft hat im Zuge der Weiterentwicklung von Windows NT Server eine Vielzahl von Fehlertoleranzmechanismen eingebaut. Mit der Fehlertoleranz wird ein System vor Datenverlust und Ausfallzeiten geschützt, die sich durch den Ausfall einzelner Komponenten ergeben. Dies ist nur dann möglich, wenn

12.5 Gegenüberstellung von LAN und MDT

diese Komponenten redundant im System vorhanden sind (Sicherungseinrichtungen). Beim Ausfall einer Komponente wird sofort mit der Ersatzeinrichtung weitergearbeitet. Erst durch dieses fehlertolerante System wurde der Einsatz von LANs in vielen Unternehmen interessant.

Datenschutz und Datensicherheit

Auf dem Gebiet von Datenschutz und Datensicherheit werden ständig neue Methoden entwickelt und erforscht, um den unberechtigten Zugriff auf Datenbestände zu verhindern. Host-Systeme, MDT-Anlagen und LANs sind alle mit dem gleichen Problem konfrontiert. Auf ein und derselben Anlage arbeiten mehrere Anwender gleichzeitig. Jeder verwendet die gleichen Platten, um seine Daten zu speichern und zu bearbeiten. Es ist aber nicht gestattet bzw. sollte nicht gestattet sein, daß jeder die Daten des anderen einsehen kann.

Offensichtlich wird das Problem, wenn Sie sich überlegen, was es bedeuten würde, wenn Hinz und Kunz die Personalstammdateien lesen könnten. Jeder würde zum Beispiel herausfinden, welcher Mitarbeiter wieviel verdient. Der Problembereich ist sehr weit gespannt und muß dementsprechend abgesichert werden. Durch den Einsatz der PCs traten hier enorme Schwierigkeiten auf, da diese Systeme am Anfang ohne jeglichen Schutz auf den Schreibtischen der Mitarbeiter für jedermann zugänglich waren. Die besten Sicherheitsmechanismen sind hier auf den Großrechnern zu finden. Paßwortkontrolle, Zugangsberechtigungen, Audit-Trail und vieles mehr wird dort zum Schutz der Daten eingesetzt. Auf dem Gebiet der MDTs und LANs werden diese Methoden erst allmählich eingesetzt und weiter verbessert. Sowohl Novell als auch Microsoft realisieren Sicherheit in dem Maße, wie sie momentan nur auf Host-Systemen vorzufinden sind. Genauere Beschreibungen und Erklärungen hierzu werde ich bei der Beschreibung von Novell NetWare bzw. Windows NT Server anführen. In einem späteren Kapitel über Datenschutz und Datensicherheit werde ich auch noch grundsätzliche Strategien zum Schutz eines LAN- oder MDT-Systems besprechen: Schutz von außen, Schutz von innen und Schutz gegen Ausfall!

Aufgrund dieser Verbesserungen der LAN-Technologie konnten LAN-Systeme in Bereiche vordringen, die bisher nur den MDT-Anlagen vorbehalten waren.

Von einem pragmatischen Gesichtspunkt aus stehen LANs und MDTs nicht in Konkurrenz zueinander, sondern bilden eine Ergänzung. Betrachtet man die Entwicklung auf diesem Gebiet, stellt man fest, daß sowohl die LANs als auch die Mittlere Datentechnik dahingehend

12 Lokale Netzwerke im PC-Bereich

weiterentwickelt worden sind, daß beide Techniken miteinander verwendet werden können. Nicht nur, daß die Systeme innerhalb eines LANs miteinander existieren können, die MDT-Anlage kann sogar als File-Server für ein LAN eingesetzt werden (z.B. DEC VAX unter VMS mit dem Betriebssystem NetWare for VMS).

Damit können VAX-Rechner über das Netzwerk als Speicher- oder Rechenmedium eingesetzt und PCs im LAN als VAX-Terminals verwendet werden. Ähnliche Anschlußmöglichkeiten existieren auch für andere Computersysteme.

Zwei Faktoren sind für diese Entwicklung ausschlaggebend:

1. Die zunehmende Verbreitung von PCs und LANs. Auf dem Gebiet der Minicomputer ist dagegen kaum noch ein Wachstum zu verzeichnen.
2. Hersteller von MDT-Systemen erreichen eine Wertsteigerung für ihre Geräte, indem sie für die Anschlußmöglichkeiten zu diesem Wachstumsbereich der Datentechnik sorgen.

Für den LAN-Anwender hingegen ist die Möglichkeit des Anschlusses an den Minicomputer vorteilhaft. Damit erhalten die Benutzer von LANs und PCs Zugriff auf vorhandene Systeme und, damit verbunden, auf Datenbestände und Programme.

Dieses Einsatzgebiet ist allerdings nur dann sinnvoll, wenn es sich um bestehende Systeme handelt. Schutz der Investition sei hier als Stichwort angeführt. Bei völligen Neuinstallationen ist der Einsatz von PCs als File-Server eher anzuraten, da der PC der Mittleren Datentechnik im Leistungsverhalten in nichts mehr nachsteht. Zudem ist ein leistungsfähiger PC gegenüber einer MDT um einiges kostengünstiger.

Ein MDT-System ist im Gegensatz zum PC bzw. File-Server wesentlich aufwendiger zu warten und installieren. Für die meisten PC-LANs ist ein File-Server mit hoher Leistung von Bedeutung. Bewertet man das Preis-/Leistungsverhältnis, stellt man fest, daß ein PC mit 80586-Architektur eine bessere Lösung als ein Minicomputer ist.

12.5.1

Der Einsatz des PC als Arbeitsplatzrechner

Muß ein System für die Abteilung ausgewählt werden, spielen sehr viele Gesichtspunkte eine Rolle. Oft wird gewünscht, PCs als Arbeitsplatzrechner einzusetzen. Aus den Installationszahlen (steigende Tendenz seit Jahren) läßt sich ableiten, daß der PC mit zum zentralen Medium der Datenverarbeitung geworden ist bzw. sich dahin entwickelt. Die Anwendungen können dabei auf dem Schreibtisch des Anwenders abgearbeitet werden, was zu Kosteneinsparun-

12.5 Gegenüberstellung von LAN und MDT

gen bei der Datenübertragung und bei der Host-Verarbeitung führt. Auf Zusatzsysteme wie Host-Rechner, spezielle Peripherie, spezielle Server wird nur bei Bedarf zugegriffen.

Daneben bietet der Einsatz von PCs funktionelle und qualitative Eigenschaften, die ihm gegenüber anderen Systemen (Systemen mit Terminals) echte Produktivitätsvorteile bringen.

Terminalsysteme als Arbeitsplatzrechner wurden unter anderem deshalb entwickelt, um teure Rechen- und Speicherkapazität bzw. teure Peripherie gemeinsam nutzen zu können. Nachdem allerdings die Preise für Rechner, Speicher und Peripherie in letzter Zeit gefallen sind, ist es inzwischen finanziell vertretbar, jedem Benutzer diese Rechenleistung und die peripheren Einheiten in Form von PCs zur Verfügung zu stellen.

Der PC als Arbeitsplatzrechner bietet folgende Vorteile:

1. Verlässliche Antwortzeiten
2. Verbesserte Benutzerschnittstelle
3. Zuverlässigkeit
4. Benutzergesteuerte Anwendungsumgebung
5. Große Auswahl an Software-Produkten
6. Ständige Verfügbarkeit der Rechenleistung
7. Bessere Kontrolle der Daten
8. Spezielle auf PC zugeschnittene Anwendung, bessere Bedienung und Qualität (Leistungsumfang)

Das Antwortzeitverhalten der Terminals hängt von der Auslastung des MDT-Systems ab. Ist dieses überbeansprucht, muß der Endanwender entsprechend lange auf seine Ergebnisse am Bildschirm oder am Drucker warten. Fällt das Host-System aus, können die Terminals nicht mehr arbeiten; fällt in einem LAN der File-Server aus, können, wenn die Arbeitsplätze entsprechend gestaltet sind, diese dennoch einzeln benutzt werden.

Die Verarbeitungsgeschwindigkeit der Minicomputer hängt von der Belastung ab. Je mehr Terminals aktiv sind, um so geringer ist die Zeitspanne, in der das Terminal bedient werden kann. In einer LAN-Umgebung erbringt die Rechenleistung nach wie vor der einzelne PC (zentralisierte Datenverwaltung – dezentralisierte Rechenleistung). In eine Büroumgebung integriert, gewinnt der PC zudem an Bedeutung, da nicht nur teure Peripherie geteilt werden kann, sondern auch PC-Benutzer miteinander kommunizieren können.

Bei der Integration eines LAN in die Bürowelt handelt es sich um eine natürliche Erweiterung des PC. Die Verarbeitung bleibt im PC, und die MS-DOS-, Windows-, Windows-95/98-, Windows-NT- oder

12 Lokale Netzwerke im PC-Bereich

auch OS/2-Betriebsumgebung bleibt erhalten, d.h., Programme dieser Betriebssystemumgebungen können nach wie vor eingesetzt werden.

Durch die Verwendung von speziellen Applikationen für eine LAN-Umgebung kann die Funktionalität eines Mehrplatzsystems erreicht werden. Alle bisher gewohnten Eigenschaften werden wie in der vertrauten PC-Umgebung genutzt. Gemeinsame Datenbankzugriffe zum Beispiel stellen kein Problem mehr dar, da der File-Server des LAN die einzelnen Zugriffe steuert und Konflikte vermeidet, erkennt oder auflöst. Sollten PCs durch ein Minicomputersystem unterstützt werden, liegt das Problem unter anderem darin, wie zwei unterschiedliche Betriebssysteme in Einklang gebracht werden: Die MDT arbeitet unter einem bestimmten Betriebssystem, und der PC arbeitet zum Beispiel unter MS-DOS. Es gibt verschiedene Alternativen, um dies zu lösen.

1. Der PC emuliert ein nichtintelligentes Terminal der MDT-Anlage. Es können dann Applikationen auf der MDT ausgeführt werden. Die Vorteile des Arbeitsplatzrechners gehen dabei jedoch verloren, wie zum Beispiel hohe Prozessorleistung oder die Windows-Umgebung. Der Prozessor, der Speicher und die meisten Funktionen des PC werden bei dieser Variante nicht genutzt.
2. Der Minicomputer wird als »große Festplatte« verwendet. Er bietet eine VHS-Funktion (Virtual Host Storage) zur Abspeicherung von Dateien im DOS-Format. Zur Bearbeitung auf den PCs werden diese vom Mini heruntergeladen. Anwendungen auf dem Mini-Rechner können dann jedoch nicht mehr ausgeführt werden. Es verhält sich genau umgekehrt wie bei der ersten Lösung, d.h., Prozessor, Arbeitsspeicher und Funktionen der MDT werden nicht genutzt. Der Mini dient letztendlich als große und teure Festplatte, mit meist langsameren Übertragungsgeschwindigkeiten.
3. Man richtet auf dem Minicomputer eine DOS-kompatible Umgebung ein, die als Prozeß dieser Anlage unter dessen Betriebssystem abläuft. Damit können Single-User-Anwendungen unter DOS ausgeführt werden.

Da es sich bei diesen beiden Systemen um vollkommen unterschiedliche Architekturen bezüglich Zentraleinheit und Betriebssystem handelt, sind für die Übertragung der Daten und Informationen komplexe Übersetzungsvorgänge notwendig. Dies ist der Grund dafür, daß die Antwortzeiten wesentlich länger sind, als wenn man mit dem »originalen System« arbeiten würde. Allein das Laden von Anwendungen vom Mini auf den PC kann über die Norm weit hinausgehen; bei großen Datenbeständen oder sehr häufig auftretenden Ein- und Ausgabevorgängen macht sich dies besonders bemerkbar.

12.5 Gegenüberstellung von LAN und MDT

Bei der Durchführung obiger Alternativen ist immer zu entscheiden, welcher Zweck sich dahinter verbirgt. Bei reinen MDT-Systemen wäre es nicht sinnvoll, als Terminal einen PC zu verwenden, damit dieser nur in der Terminalemulation verwendet werden kann. Wenn jedoch Applikationen im Einsatz sind, die es sowohl auf PC-Ebene als auch auf MDT-Systemen gibt und die es erlauben, Datenbestände des einen oder anderen Systems zu verwenden, ist eine Kombination beider Welten durchaus sinnvoll einsetzbar.

12.5.2 Verteilte und zentrale Datenverarbeitung

Wie zu Beginn bereits erwähnt, waren Rechen- und Speicherkomponenten in den Anfängen der Datenverarbeitung sehr teure Betriebsmittel. Aus besagten Gründen wurden diese Betriebsmittel zentral angeordnet, um zum einen die Kosten zu senken und zum anderen die Auslastung zu erhöhen.

Dadurch wurde der Host-Rechner zum Dreh- und Angelpunkt der Datenverarbeitungssysteme. An diesen Host wurden bzw. werden Terminals angeschlossen, so daß er vielen Benutzern zur Verfügung steht, inklusive die verwalteten Betriebsmittel. Es entstand das Prinzip der gemeinsamen zentralen Verarbeitung.

Inzwischen sind die Kosten für Rechner- und Speicherkomponenten ständig gefallen. Aus betriebswirtschaftlichen Überlegungen ist es sinnvoll geworden, den einzelnen Benutzern eigene Rechner und eigene Speicherkapazität auf die Schreibtische zu stellen. Dieser Ansatz, Verlagerung von Rechenkapazität vom zentralen »Hobel« auf den Schreibtisch des Sachbearbeiters, wird als verteilte Verarbeitung bezeichnet.

Die zentrale Verarbeitung zeichnet sich dadurch aus, daß an der Spitze des Systems der Host angesiedelt ist. Alles, was am Terminal ausgeführt wird, läuft über den Großrechner, sei es eine Anforderung, die angesetzt wird, oder ein ganz einfacher Tastendruck.

Bei der verteilten Verarbeitung werden Übertragungskosten (Zeit) durch die horizontale Architektur reduziert. Der PC als Arbeitsplatzrechner wird zum Zentrum der Datenverarbeitung. Die meisten Vorgänge zur Verarbeitung von Daten werden innerhalb des PC durchgeführt. Auf spezielle Dienste wie Hochgeschwindigkeitsrechner, Übertragungs-Server, Print-Server, Communication-Server, File-Server wird nur zugegriffen, wenn diese Funktionen auch benötigt werden. Geräte für diesen Bereich können Großrechner, Minicomputer oder PCs sein.

12 Lokale Netzwerke im PC-Bereich

Der Host-Rechner stellt damit einen Netzwerkknoten dar, auf den nur zugegriffen wird, wenn er auch eingesetzt werden soll. Bei der verteilten Verarbeitung liegt in der Regel die Zahl der Übertragungsvorgänge wesentlich niedriger als bei der zentralen Verarbeitung.

Ein wesentlicher Unterschied zwischen LANs und Minicomputern liegt in der Form der Verarbeitung. Ein LAN beruht in aller Regel auf dem Prinzip der verteilten Verarbeitung, ein Minicomputer auf dem der zentralen Verarbeitung. Es gibt jedoch auch andere Ansätze. Windows NT Server und andere Systeme kombinieren diese beiden Welten.

Eine andere Variante der Mischung ist der Einsatz von Datenbank-Servern innerhalb eines LAN. In der Regel erbringt die Workstation die volle Rechenleistung, beim Einsatz von Datenbank-Servern wird die Verwaltungsaufgabe der Datenbank allerdings nicht von der Workstation zur Verfügung gestellt, sondern vom Datenbank-Server. Die Workstation überträgt dem Datenbank-Server nur noch die Aufgaben, die zu erledigen sind als Antwort erhält diese dann das Ergebnis.

In anderen Fällen kann die Anwendungsverarbeitung einen Arbeitsplatzrechner unter Umständen übermäßig lange binden. Mit Novell NetWare zum Beispiel können solche Anwendungen in Stapelrechnern durchgeführt werden – eine Form der gemeinsamen Nutzung von Netzwerkressourcen.

Der wichtigste Dienst in einem LAN ist der Dateidienst, der vom File-Server erbracht werden muß. Manche LAN-Strategien sind so strukturiert, daß auch alle zusätzlichen Dienste auf dem File-Server ablaufen (Print-Server, Gateway-Server, Communication-Server etc.). Der Verarbeitungsaufwand für den File-Server und für die anderen Dienste wird dadurch erhöht, und es kann zu einem Leistungsabfall bei allen beteiligten Server-Diensten kommen.

Aus diesem Grund ist eine Architektur vorzuziehen, die es erlaubt, Dienste als Prozesse anderer Hersteller laufen zu lassen. Über das auf Gleichrangigkeit arbeitende Netzwerkprotokoll kann ein Arbeitsplatzrechner direkt mit einem Dienst (Application-Server) kommunizieren, ohne daß der File-Server von diesem Geschehen etwas weiß. Notwendig hierfür ist der mögliche Einsatz von Peer-to-Peer-Protokollen (Netbios, APPC, LU 6.2).

Physikalisch gesehen können auch alle zusätzlichen Dienste in einen File-Server integriert werden. Zentraleinheit, Systembus und Speicher werden gemeinsam von allen verwalteten Diensten des Servers benutzt. Dies hat aber einen sehr großen Einfluß auf die Per-

12.5 Gegenüberstellung von LAN und MDT

formance des Systems. Es ist also angebracht, die einzelnen Dienstleistungen auf separate Rechner (Application-Server) zu verteilen. Sollte ein Server-System ausfallen, kann man zudem mit den noch vorhandenen Diensten arbeiten. Beim Ausfall des File-Servers kann beispielsweise mit dem Gateway-Server gearbeitet werden (z. B. Terminalemulation), da die Kommunikation zwischen Arbeitsplatzrechner und Application-Server unter Umgehung des File-Servers erfolgt.

12.5.3 Die Anwendungssoftware

Der Bereich der Anwendungssoftware ist sehr weit gespannt. Es gibt so ziemlich für alle Gebiete Softwaresysteme in den verschiedensten Leistungsklassen. Softwarepakete für eine MDT-Anlage sind nicht dieselben wie die für LANs. Dem Endanwender ist es gleichgültig, worin sie sich unterscheiden, aber derjenige, der zwischen LAN oder MDT die Entscheidung treffen muß, sollte sich auch mit diesem Problem befassen. Dabei sind Typ und Qualität der Software zu prüfen, die Existenz passender und ergänzender Software (sekundäre Applikationen), die Dauer der Einarbeitung (Komplexität, Bedienung, Benutzerführung etc.), der Wartungsaufwand und der Preis.

Da der Markt für MDT-Systeme bei weitem nicht so groß ist wie der von IBM-PCs und IBM-kompatiblen Systemen, wird Software für Minicomputer nur in beschränktem Umfang entwickelt. Für ein spezielles Minicomputersystem gibt es zum Beispiel nur ein paar wenige Textsysteme oder Kalkulationssysteme, zwischen denen man sich entscheiden kann. Vergleicht man dies mit dem PC-Bereich, dann stellt man fest, daß dort das Angebot schon fast wieder zu umfangreich ist, so daß die Entscheidung, welches Programm für welchen Einsatz sich am besten eignet, nicht gerade leichtfällt.

Dem Anwender eines PC-LAN steht somit die gesamte Bandbreite der PC-Systeme zur Verfügung. Darüber hinaus gibt es aber auch mehrere tausend netzwerkfähige Software-Produkte, die eingesetzt werden können. In Abhängigkeit von den Workstation-Betriebssystemen muß die Entscheidung für die jeweilige Anwendungssoftware getroffen werden.

Da der MDT-Markt begrenzt ist und eine andere Preispolitik verfolgt, sind dort Anwendungen in den meisten Fällen teurer als Anwendungen für den PC-LAN-Bereich.

In diesem Kapitel sind einige Punkte angesprochen worden, die beim Vergleich zwischen Minicomputersystemen und LANs eine Rolle spielen. Die Entscheidung für das eine oder andere System hängt jedoch meist davon ab, ob

12 Lokale Netzwerke im PC-Bereich

- vorhandene oder geplante PCs unterstützt werden,
- es bestimmte PC- oder Minicomputeranwendungen gibt, auf die man sich festlegen muß,
- die Notwendigkeit einer kostengünstigen, wirtschaftlichen und produktiven Lösung besteht.

Dienen PCs bereits als Arbeitsplatzrechner, oder ist es geplant, solche zu installieren, ist mit Sicherheit der Einsatz eines LAN die richtige Entscheidung. Nach den bisherigen und auch den folgenden Ausführungen sehen Sie, daß die Vorteile, nämlich die Leistung der intelligenten Arbeitsplätze, ständig verbessert und optimiert werden. Es bleibt einerseits die PC-Umgebung erhalten, andererseits wird die Nutzung fortschrittlicher. Dies betrifft sowohl die Übertragungsmöglichkeiten als auch die gemeinsame Nutzung von Betriebsmitteln.

Wird eine bestimmte Anwendung benötigt und existiert diese Anwendung nur auf einem der beiden Systeme, PC oder MDT, so wird sich die Entscheidung danach richten, auf welchem System die geforderte Anwendung lauffähig ist.

Beim letzten der obengenannten drei Punkte ist entscheidend, mit welchem System man am kostengünstigsten und am produktivsten eine Anwendung oder eine Reihe von Anwendungen betreiben kann.

Vergleicht man die Verkaufszahlen von MDT-Systemen mit denen von LANs, zeigt die Entwicklung auf diesem Gebiet, daß sich der Einsatz Lokaler Netze im Vergleich zu den MDTs rasant entwickelt.

12.5.4

Integration von LANs in die Minicomputer- und Mainframe-Welt

Im vorherigen Abschnitt haben wir einen Vergleich zwischen LANs und Minicomputern durchgeführt. Es stellt sich jedoch die Frage, ob und wie ein LAN in die bestehende DV-Welt integriert werden kann. Bei der Entwicklung der Datenverarbeitung bestand nicht selten das Problem, Großrechnersysteme oder MDT-Anlagen in die LAN-Umgebung mit einzubinden bzw. das LAN in bestehende Systeme. Ich werde versuchen, in diesem Abschnitt grundlegende Konzepte und Techniken dafür vorzustellen und gegeneinander abzuwägen.

Da MDTs und Großrechnersysteme in ihrer Architektur sehr ähnlich sind, werde ich im folgenden keinen Unterschied zwischen diesen beiden Systemen machen, sondern allgemein von Host-Rechnern oder Host-Systemen sprechen.

12.5 Gegenüberstellung von LAN und MDT

Inwieweit ist es sinnvoll, LANs und Host-Systeme miteinander zu koppeln? Soll die PC-Fähigkeit soweit erweitert werden, um auf den zentralen Host zuzugreifen? Wie stark ist die Belastung des Rechenzentrums durch den zusätzlichen Support-Aufwand? Ist es nicht sinnvoller, die Anwendungen auf dem Host zu belassen, mit Terminals an diesem System zu arbeiten und Probleme bezüglich Datenschutz und Datensicherheit dadurch zu vermeiden? Ein Benutzer, der nur mit seinem Terminal arbeitet, hat keine Möglichkeit, Datenbestände auf Diskette oder Platte zu kopieren. Beim Einsatz von LANs bzw. PCs als Terminalsystem ist es ein Leichtes, Daten zu kopieren und eventuell aus der Firma herauszutragen. Wer kann dies unterbinden?

Diese und ähnliche Fragen und Überlegungen beschäftigen immer wieder die einzelnen Abteilungen, DV-Leiter, Vorgesetzte und Cheftagen. Die Ankopplung von LANs (bzw. die der PCs in diesen LANs) kostet nicht nur Geld, Support und Personal, sondern sprengt auch das Sicherheitsgefüge. Es handelt sich dann nicht mehr um einen Closed-Shop-Betrieb. Würde ein Mitarbeiter aus dem Rechenzentrum – sofern er den Zutritt erhält – Aktenordner und Rechner heraustragen, fiel dies mit Sicherheit auf. Steckt er sich dagegen eine kleine 3.5-Zoll-Diskette mit kopierten Daten vom Host in die Jackentasche, bemerkt das normalerweise keiner. Welche Firma würde schon Leibesvisitationen durchführen?

Ich werde versuchen, Gründe für die Ankopplung zu erarbeiten und dabei auch auf das aufmerksam zu machen, was es zu beachten gilt.

Im Grunde gibt es drei wichtige Gründe für die Kopplung von LANs (PCs) an den Host:

- Zusätzliche Funktionen für den PC
- Datenintegrität und Datensicherheit im Unternehmen
- Verbesserung der Effektivität der Arbeit

12.5.5 Ausdehnung des PC zum multifunktionalen Arbeitsplatz

Nicht selten hat der Benutzer mehrere Systeme auf seinem Schreibtisch stehen. Dabei kann es sich unter anderem um das Host-Terminal handeln, den PC, Teletex-Anlage, Telex-Anlage, BTX-System und vielleicht noch um ein Telefax-Gerät.

Da diese Systeme nicht alle auf den Schreibtisch des Anwenders gestellt werden können, da er sonst keinen Platz mehr zum Arbeiten hätte, ist er gezwungen, ab und an den Schreibtisch zu verlassen. Wenn er Pech hat, sind diese Systeme nicht alle in seinem Büro, sondern auf der Etage verteilt. Es ist aber nicht gesagt, ob das benötigte

12 Lokale Netzwerke im PC-Bereich

System auch zur Verfügung steht, da vielleicht gerade ein anderer Mitarbeiter daran arbeitet. Inzwischen sind die Entwicklungen auf diesem Gebiet soweit fortgeschritten, daß alle diese Funktionen in ein und denselben PC (LAN) integriert werden können.

Wie bereits gesagt, geht der Trend hin zur dezentralen Datenverarbeitung. Mit den verfügbaren Software-Produkten für den PC-Bereich können wesentlich mehr Aufgaben, Auswertungen etc. durchgeführt werden als mit dem Host. Dies erfordert jedoch, daß auf dem PC die Daten des Großrechners zur Verfügung stehen.

Damit verbunden ist die Forderung: Wenn ein PC als Terminalemulation am Host Verwendung findet, dann nicht nur als intelligentes Terminal, sondern auch mit den Möglichkeiten des File-Transfers.

Dies ist der wichtigste Grund für eine PC-Host-Kopplung. Man unterscheidet beim File-Transfer zwischen der Übertragung vom PC zum Host (UP LOAD) und der Übertragung der Daten vom Host zum PC (DOWN LOAD).

Für die Verwendung der UP-LOAD-Funktion gibt es drei Gründe:

1. Einsatz des PC (LAN) als Datensammelstation: Die Erfassung von Daten wird am PC durchgeführt. Zu fest vorgegebenen Zeiten werden diese zum Host übertragen, der sie dann, meist durch Batch-Läufe, auf die entsprechenden Datenbanken überspielt. Datenerfassungen in Filialen und die folgende Übertragung zum Zentralrechner können als Beispiel angeführt werden.
2. Einsatz zur Vorverarbeitung von Daten: Daten werden vor Ort erfaßt und vorverarbeitet. Anschließend überträgt man diese Daten zum Host, oder dieser ruft die Daten ab.
3. Einsatz in der Bürokommunikation: Übertragung von fertigen Texten (inkl. Drucksteuerzeichen für den Host-Drucker) vom PC zum Hochleistungsdrucker.

Für die Nutzung der DOWN-LOAD-Funktion gibt es fünf mögliche Einsatzgebiete:

1. Auswertung von Datenmaterial von nationalen und internationalen Datenbanken (Online-Recherchen)
2. File-Transfer zwischen zwei PCs, der Host dient als Zwischenspeicher
3. Übertragen von Updates (neue Preise für Computerkassen zum Beispiel) vom Zentralrechner zu den Filialrechnern
4. Übertragung von Druck-Output
5. Übertragung von Datenmaterial für das Management, Aufbereitung vor Ort. Diese Daten werden zum Beispiel mit Grafikprogrammen weiterverarbeitet, um Präsentationen durchführen zu können.

12.5 Gegenüberstellung von LAN und MDT

Aus diesen und ähnlichen Gründen werden die Vorteile einer PC-Host-Anbindung – die mit dem Aufbau von LANs noch größer werden – immer mehr geschätzt. Da es sich beim PC-LAN um eine ganz andere Philosophie der Netzwerkstruktur handelt (Zugriffsverfahren, Protokollaufbau), kann der Anschluß eines LAN nur durch den Einsatz eines Gateways erfolgen, bis auf eine Ausnahme: bei Verwendung eines IBM-Token-Ring-Netzes.

Eine LAN-Host-Verbindung bietet mehrere Vorteile:

- Möglichkeiten der Host-Ankopplung (Terminalemulation, File-Transfer in beiden Richtungen).
- Jeder Anwender kann von einem beliebigen Arbeitsplatz aus, unter seiner Anmeldung, die Verbindung zum Großrechner herstellen.
- In den Arbeitsplatzrechnern muß nicht für jeden Anschluß eine Adapterkarte eingebaut werden. Durch die Verwendung eines Gateways haben alle Workstations die Möglichkeit, eine Host-Session herzustellen. Die Verbindung zum Host wird dann durch das Gateway kontrolliert und überwacht.

Eine Gefahr der PC-Host-Kopplung besteht darin, daß das Sicherheitssystem des Hosts geschwächt wird. Es ist leider noch nicht generell so, daß PCs vor unberechtigtem Zugriff geschützt werden. Meist werden zwar auf der Platte des PC Menüs mit Paßwortschutz installiert, dies hilft jedoch nichts, wenn sich der PC nach wie vor über die Diskettenstation ohne jeglichen Schutz booten läßt und damit die gesamte Festplatte frei zugänglich ist, also alle Daten gelesen, geändert oder gar auf andere Datenträger kopiert werden könnten.

Die Einbindung der Arbeitsplatzrechner über ein LAN in die Host-Umgebung spart nicht nur Geld und hat den Vorteil, daß unabhängig von der Workstation mit der eigenen Benutzerkennung die Verbindung zum Host aufgebaut werden kann, sondern bietet zudem erweiterte Möglichkeiten in puncto Datenschutz und Datensicherheit.

Der Zugang zum Großrechner und die Berechtigung, Daten von diesem zu lesen, regelt das Host-System selbst. Anders sieht es jedoch aus, wenn Daten mit DOWN-LOAD-Funktionen auf Platte gezogen werden. Der Host kann eine weitere Verwendung nicht mehr kontrollieren. Diese Aufgabe muß dann vom LAN-Betriebssystem übernommen werden. Um dies sinnvoll nutzen zu können, sollten zwei Punkte strikt befolgt werden:

12 Lokale Netzwerke im PC-Bereich

1. File-Transfer vom Host auf das LAN darf nur auf die File-Server-Platte erfolgen. Damit obliegt es dem Systemverantwortlichen, wie sicher die Zugangsschutzmechanismen aufgebaut werden, um den Zugriff Unberechtigter zu unterbinden. Der Transfer sollte auf Plattenbereiche erfolgen, auf die nur die Personen zugreifen können, die auch berechtigt sind.
2. Auch wenn Datenbestände auf die Platte des File-Servers verlagert werden und nur Berechtigte darauf zugreifen können, ist es immer noch möglich, daß diese Daten auf eine lokale Platte oder Diskette kopiert werden. Das kann auf zwei Arten unterbunden werden:
 - Der Einsatz von Diskless Workstations. In diesem Fall besteht der PC aus der notwendigen Hardware, um im Netz arbeiten zu können, es ist jedoch kein Platten- oder Diskettenlaufwerk eingebaut. Der Zugang zum File-Server wird mit sogenannten Boot-Proms realisiert. Aufgrund der zunehmenden Komplexität der Workstation-Betriebssysteme wird der Einsatz von Diskless Workstations immer seltener. Es wurde bereits an anderer Stelle darauf hingewiesen, wie dennoch eine ausreichende Sicherheit erzielt werden kann.
 - Wird aus bestimmten Gründen eine lokale Speicherperipherie benötigt, dann existiert bei einigen Netzwerkbetriebssystemen die Möglichkeit (z.B. Novell NetWare), bei einem bestimmten User-Login die lokalen Platten und Diskettenlaufwerke temporär »abzuhängen«. Das heißt, solange der User XY im Netz angemeldet ist, kann er mit seiner lokalen Speicherperipherie nicht arbeiten. Sobald er sich jedoch vom System abmeldet, kann er mit seinem PC als Standalone-System arbeiten.

Die Möglichkeiten der Ankopplung von LANs an Host- und MDT-Systeme werde ich in einem eigenen Kapitel behandeln. Bei der Darstellung der neuen Eigenschaften von Novell NetWare werde ich Ihnen zudem zeigen, mit welchen Funktionen und Möglichkeiten Novell die Ankopplung von LANs mit Hilfe des Communication-Servers realisieren will. Bevor ich jedoch auf diese speziellen Bereiche eingehen werde, sollen zuerst die wichtigsten Grundlagen von Novell NetWare aufgezeigt werden.

13

Die Entwicklungsgeschichte von Novell

Die Firma Novell wurde 1983 gegründet. Der Hauptsitz befindet sich in Utah, mit weiteren Niederlassungen unter anderem in Kalifornien und Texas. In Deutschland befindet sich die Niederlassung in Düsseldorf mit Geschäftsstellen unter anderem in München und Berlin.

Novell bemüht sich nicht nur um die Unterstützung und den Vertrieb von Netzwerkbetriebssystemen, sondern auch von Kommunikationsprodukten, Entwicklungs-Tools und Management-Tools, so daß Anwender alle Möglichkeiten haben, LANs, Großrechnersysteme und Anlagen der Mittleren Datentechnik nach den eigenen Vorstellungen zu integrieren. Durch die Erfahrungen, die Novell auf dem Gebiet der Anwendungssoftware gemacht hat, gab man sehr bald die Anstrengungen auf, WordPerfect oder auch UnixWare weiter unter dem Dach von Novell zu vermarkten. Durch den Verkauf von WordPerfect und UnixWare beschränkt man sich bei Novell wieder auf das Wesentliche: Netzwerkbetriebssysteme und die dafür notwendigen Zusatzkomponenten. Sie werden später mehr darüber erfahren, welche zukünftigen Entwicklungen Novell vorhat und in welche Richtung sich Novell weiterentwickeln wird. Da durch den Auf- und Verkauf keine klare Linie mehr zu erkennen war, ist es besonders wichtig, die neuen Entwicklungsrichtungen bei Novell deutlich zu machen.

Je nachdem, welchen Statistiken man Glauben schenken mag, liegt der weltweite Marktanteil von Novell im LAN-Bereich immer noch bei ca. 60%. Somit kann man mit Recht behaupten, daß Novell der Markt- und Technologieführer auf dem Gebiet der Lokalen Netzwerke ist.

Als Novell 1983 gegründet wurde, befand sich der LAN-Bereich im Entwicklungsstadium. Zu dieser Zeit wurde der Einsatz von LANs dazu benutzt, um mit Hilfe von PCs teure Peripheriegeräte gemeinsam zu nutzen. Es handelte sich dabei fast ausschließlich um Drucker- und Platteneinheiten. Netzwerkfähige Software gab es zu diesem Zeitpunkt noch kaum. Man darf in diesem Zusammenhang auch nicht vergessen, daß man zu dieser Zeit noch ca. 10.000 bis 15.000 DM für eine 10-Mbyte-Platte bezahlen mußte.

13 Die Entwicklungsgeschichte von Novell

Das LAN-Betriebssystem besaß auch noch keine Multi-User-Funktionen, d.h., Mechanismen wie Datei- oder Record-Locking wurden in den Verantwortungsbereich der Anwendungssoftware verlagert. Novell erkannte, daß auf dem PC basierende Netzwerke mit der Unterstützung des Distributed-Processing-Konzepts einen sehr großen Bedarf abdecken könnten.

Daher begann Novell mit der Entwicklung von Produkten für LANs mit dem Ziel, Datei-Sharing-Funktionen und die Einbindung von MDTs und Großrechneranlagen in ein PC-Netzwerk integrieren zu können. Seit dieser Zeit wurden ständig verbesserte und erweiterte LAN-Betriebssystemversionen von Novell auf den Markt gebracht, die sich auch an den ständig wachsenden Anforderungen der Technik, der Software-Technologie und vor allem der Anwender orientierten und sich an sie anpaßten.

Die ersten LAN-Betriebssysteme deckten den Bereich des Workgroup-Computing-Konzepts ab. Mit NetWare 3.11 und allen nachfolgenden Versionen orientierte sich Novell an dem Bereich des Network Computing. Mit der Entwicklung von NetWare 4 erfolgte dann der Sprung in Richtung Global Network Computing, d.h. von der Server-orientierten Sichtweise des Netzwerks hin zu einer netzwerkweiten Sichtweise. Auf den Unterschied dieser Konzepte werde ich später noch eingehen.

Betrachtet man die Entwicklung der PC-Hardware, dann stellt man fest, daß mit der Einführung neuer Technologien auch weitere Entwicklungen auf dem Gebiet der Software-Technologie stattgefunden haben und immer noch stattfinden. Ein Ende dieser Entwicklungen ist noch lange nicht in Sicht. Novell hat dem seit Einführung des LAN-Betriebssystems Novell NetWare durch Weiter- und Fortentwicklung des Betriebssystems Rechnung getragen.

Damit hat der Anwender vollkommene Wahlfreiheit, beginnend bei der Auswahl der Verkabelung bis hin zur Entscheidung für den Einsatz von Workstations, Workstation-Betriebssystemen und Protokollen. Es besteht die Möglichkeit, zu jedem Zeitpunkt das bereits installierte LAN – unter Novell NetWare – ständig an die neuen Entwicklungen anzupassen. Dies ist besonders wichtig! Kein Anwender wäre davon begeistert, sich alle paar Monate auf neue Hard- oder Software umstellen zu müssen. Das muß alles unter dem Aspekt »Schutz der Investition« betrachtet werden. Novell bietet Ihnen hierbei volle Unterstützung aufgrund der großen Flexibilität und Anpassungsfähigkeit.

Die Produkte von Novell sind durch folgende Eigenschaften gekennzeichnet:

■ *Hobe Performance*

Novell NetWare zählte von Anfang an zu den schnellsten LAN-Betriebssystemen. Dies ist darin begründet, daß Novell das Betriebssystem ständig an die neuen Hardware-Anforderungen anpaßt. Mit der Einführung von NetWare 3.11, 3.12, 3.2, Netware 4.x und NetWare 5 wurde ein Betriebssystem geschaffen, das bereits jetzt den Hardware-Entwicklungen im PC-Bereich weit voraus ist. Ich werde bei der Besprechung von NetWare (3.2, 4.11 und 5) noch genauer auf diesen Aspekt eingehen. Das Ziel von Novell ist aber, nicht nur das LAN-Betriebssystem NetWare, sondern auch alle weiteren Zusatzprodukte, die zum Aufbau von LANs und WANs angeboten werden, bezüglich der Geschwindigkeit zu optimieren.

■ *Zuverlässigkeit*

Das LAN-Betriebssystem NetWare zeichnet sich durch einen sehr hohen Grad an Zuverlässigkeit aus. Damit haben NetWare-Anwender die Gewähr, daß alle Daten hinsichtlich Datenintegrität und Datenkonsistenz optimal abgesichert sind. Hierbei geht es jedoch nicht nur um den Schutz bzw. das Abfangen von Software-Fehlern, sondern auch um die Möglichkeit, Hardware-Ausfälle (Netzwerkadapterkarten, Plattensubsysteme oder File-Server) abzufangen, um ein reibungsloses Arbeiten im Netzwerk gewährleisten zu können. Novell realisiert diese Sicherheitsmechanismen mit Hilfe unterschiedlicher Sicherheitsstufen, mit denen NetWare angeboten wird.

■ *Sicherheit*

Das Ziel von Novell ist, ein LAN-Betriebssystem anzubieten, das bezüglich Zugangsbeschränkungen, Rechtevergabe oder Zugriffsberechtigung auf einzelne Dateien optimal ausgerichtet ist. Die Sicherheitsmechanismen, die hierfür zur Verfügung stehen, wurden ständig verbessert und verfeinert. Es ist dabei nicht zu verkennen, daß man sich bei diesen Mechanismen eng an der Großrechnerwelt orientiert hat.

■ *Offene Architektur*

Um anderen Hard- und Software-Herstellern die Möglichkeit zu geben, Zusatzprodukte für NetWare zu entwickeln, legt Novell alle Hard- und Software-Schnittstellen offen dar.

■ *Unabhängigkeit*

NetWare unterstützt unterschiedliche Standards. Das bewirkt eine große Unabhängigkeit. Dadurch ist es möglich, mit den Novell-Produkten die Kopplung mit unterschiedlichen Systemen erfolgreich durchzuführen. Somit kann der Anwender selbst entschei-

13 Die Entwicklungsgeschichte von Novell

den, welche Systeme unter NetWare integriert werden sollen. Sie haben also kein Standalone-Netzwerk in Ihrer Firma, sondern ein System, das sich an fast alle gängigen Systeme anschließen läßt.

Ein weiterer wichtiger Aspekt in diesem Zusammenhang ist die intensive Zusammenarbeit von Novell mit anderen Herstellern. Anzuführen sind die Firmen Digital Equipment Corporation, Hewlett-Packard, IBM, Xerox oder Compaq. Damit ist gewährleistet, daß Novell seine Produkte ständig an die neuen Gegebenheiten anpassen kann, ohne dabei lange Verzögerungszeiten in Kauf nehmen zu müssen.

13.1 Die wichtigsten Entwicklungsphasen von Novell

Der Erfolg von Novell ist unter anderem in der konsequenten Strategie dieser Firma begründet. Hierbei legt Novell sehr großen Wert auf die Unterstützung der Industriestandards und die ständige Entwicklung neuer Strategien und Produkte zum Ausbau des Network-Computing-Konzepts. In Tabelle 13.1 ist eine kurze geschichtliche Zusammenfassung der technologischen Entwicklung dargestellt.

*Tabelle 13.1
Technologische
Entwicklung von
Novell*

1981	April:	Ankündigung des IBM-PC
1983	Januar:	Erste Auslieferung einer File-Server-Software von Novell
	Mai:	Novell kündigt Medienunabhängigkeit an
1985	März:	IBM liefert DOS 3.1 (Netzwerkunterstützung) und NetBios aus
	September:	Novell unterstützt als erstes unabhängiges Netzwerkunternehmen DOS 3.1 und NetBios
1986	Januar:	Novell liefert das erste Protected-Mode-LAN-Betriebssystem für 80286-Prozessoren aus. Novell bietet medienunabhängige Routing-Dienste
	März:	IBM liefert das Token-Ring-Netzwerk aus. Novell ist das erste unabhängige Netzwerkunternehmen, das IBM-Token-Ring unterstützt
	September:	Novell liefert die ersten fehlertoleranten LAN-Produkte aus
1987	September:	Novell kündigt die Open-Protocol-Technologie an
	Oktober:	IBM liefert die OS/2 Standard Edition aus
1988	September:	Novell liefert NetWare for VMS und den NetWare Requester für OS/2 aus

13.1 Die wichtigsten Entwicklungsphasen von Novell

	November: IBM liefert die OS/2 Extended Edition aus. Der Novell Requester für OS/2 unterstützt die OS/2 Extended Edition
	Dezember: Novell liefert die Apple-Macintosh-Unterstützung aus
1989	Februar: Novell führt Portable NetWare ein
	Mai: Novell führt NetWare Open Systems ein
	September: Novell liefert das erste 32-Bit-, 80386-basierende Netze werkbetriebssystem aus
1990	Januar: Novell liefert den ersten SNMP-basierenden Netzwerk- monitor aus
	April: Der erste strategische Partner, NCR, liefert Portable NetWare aus
	Juli: Novell liefert das protokollunabhängige Serverbe- triebssystem aus
1991	Februar: Novell liefert NetWare Name Service und Remote Ma- nagement Facility aus; Novell gibt die Vereinbarung zwischen Novell und IBM über Lizenzierung, Distribu- tion und Support von Novell-Produkten offiziell be- kannt
	Auslieferung der Produkte TCP/IP-, NFS-, Macintosh-, FTAM-, OSI-NetWare Loadable Modules; ebenso Aus- lieferung des Communication-Servers mit NetView- Unterstützung
	NetWare wird von IBM ausgeliefert und unterstützt
	Erste OSI- und US-GOSIP-Lösung verfügbar, NetWare FTAM
1992	NetWare NFS integriert Unix Workstations in ein Net- Ware-Netzwerk. DOS, MAC, OS/2 und Unix können somit gemeinsam NetWare-Dienste nutzen
	NetWare for SAA, NetWare-Anbindung an IBM Host und IBM AS/400
	NetWare Lite für kleine, einfache Netzwerke
	Auslieferung von UnixWare PE und AS
1993	Ankündigung und Auslieferung von NetWare 4, globa- les Network-Computing
	NetWare 4 für OS/2-Auslieferung
	Auslieferung NetWare 3.12
	Novell DOS 7 und Personal NetWare

13 Die Entwicklungsgeschichte von Novell

1994	UnixWare 1.1 Verstärkte Aktivitäten im Bereich AppWare Bekanntgabe der Multiprozessorstrategie für NetWare 4
1995	Apple unterzeichnet Abkommen für PIN auf PowerPC Beginn verstärkter Mailing-Aktivitäten durch Group-Wise-Einführung OEM-Version von SMP für Netware 4 wird ausgeliefert Immer mehr Produkte sind für NetWare 4 und NDS verfügbar Es zeichnen sich verstärkte Aktivitäten im Internetbereich ab
1996	Ankündigung von Green River, die weiterentwickelte Version von NetWare 4.1 NetWare Web Server wird ausgeliefert NetWare/IP 2.2 wird ausgeliefert Die neue Strategie Net2000 wird angekündigt Novell lizenziert Java von Sun Microsystems als neue Entwicklungsplattform
1997	Nach Einführung von NetWare 4.11 wird IntraNetWare for Small Business eingeführt NetWare 3.2 wird eingeführt – wegen Jahr-2000-Fähigkeit Die ersten Beta-Versionen von Moab kommen auf den Markt
1998	Es laufen alle Vorbereitungen für Jahr-2000-Umstellung Einführung von Z.E.N.works Einführung NDS4NT NetWare 5 wird eingeführt Fortführung der Open Solution Architecture Ankündigung Cluster-Technologie (Orion I und II)
1999	NDS4NT – Native-IP-Unterstützung Netware for SAA 4.0 NDS4Solaris ZENworks 2.0 Bordermanager 3.5

13.1 Die wichtigsten Entwicklungsphasen von Novell

Ich will Ihnen nachfolgend die wichtigsten strategischen Konzepte von Novell aufzeigen, durch die sich die LAN-Betriebssysteme NetWare von Novell auszeichnen. Das geschieht chronologisch, damit Sie sich einen Eindruck darüber verschaffen können, daß es von Anfang an das Ziel von Novell gewesen ist und auch immer noch ist, so schnell wie möglich alle notwendigen neuen technologischen Hard- und Software-Komponenten zu unterstützen. Dabei ist auch festzustellen, daß es Entwicklungsrichtungen gab, die von Novell eingeschlagen und nach einiger Zeit wieder aufgegeben worden sind, so wie zum Beispiel bei UnixWare. Dieser Bereich wurde durch den Verkauf an SCO wieder aufgegeben.

File-Service

1983, weniger als zwei Jahre nachdem IBM den ersten PC vertrieben hat, entwickelte und verkaufte Novell das erste LAN-Betriebssystem. Mit Hilfe der File-Server-Architektur wird die Multi-User-Funktion durch das Betriebssystem unterstützt – damit kann die netzwerkfähige Software einfacher und schneller entwickelt werden. Die notwendigen Sicherheitsmechanismen und die Datenintegrität werden durch den File-Server und das darauf laufende Betriebssystem unterstützt. Das Konzept der File-Server-Technologie besagt, daß auf dem File-Server das LAN-Betriebssystem läuft und auf jeder angeschlossenen Workstation das eigene Workstation-Betriebssystem eingesetzt wird, z.B. MS-DOS. Alle Programme und Daten werden von der Platte des File-Servers in den Hauptspeicher der Workstation geladen. Das heißt, die Applikation läuft auf der Workstation und nicht auf dem File-Server ab.

Unabhängigkeit des Mediums

Für den Aufbau von LANs werden seit jeher unterschiedliche Topologien angeboten. Sie können LANs zum Beispiel entweder unter Ethernet, Token-Ring oder ARCNET betreiben. Mit der Einführung von LAN-Betriebssystemen wurden diese zur damaligen Zeit von den Herstellern lauffähig auf bestimmten Topologien, gleichzeitig aber herstellerabhängig angeboten. Novell entschied sich damals bereits für eine offene Architektur und entwickelte ein Konzept, das es erlaubt, NetWare mit den unterschiedlichsten Topologien einzusetzen. Der Anwender hat damit die Wahlfreiheit, mit welcher LAN-Topologie NetWare eingesetzt werden soll, und ist nicht an bestimmte herstellerabhängige Hard- und Software-Produkte gebunden. Hierfür bietet NetWare LAN-Driver an. Auch Dritthersteller bieten LAN-Driver an, um NetWare mit deren Netzwerkkarten einsetzen zu können.

13 Die Entwicklungsgeschichte von Novell

Aufgrund der Unabhängigkeit von NetWare kann dieses System heute auf über 30 unterschiedlichen Netzwerktypen eingesetzt werden, und es werden derzeit LAN-Driver für über 100 Netzwerkkarten angeboten. Fast jeder Hersteller von LAN-Adapterkarten bietet gleichzeitig einen LAN-Driver für Novell NetWare an. Durch die Offenheit des Systems können auch die unterschiedlichsten Hardware-Systeme für den Server und die Workstation eingesetzt werden.

Routing-Services

Novell erweiterte das Konzept der Unabhängigkeit vom Medium für NetWare 1986 durch die Unterstützung der (mediumunabhängigen) Routing-Services. Auf diese Weise kann der Anwender mehrere Netzwerkkarten unterschiedlichen Typs in einen File-Server einbauen und betreiben. Das heißt, mit einem File-Server können bis zu vier LANs unterschiedlichen Typs betrieben werden. Der Anwender selbst hat den Eindruck, als würde es sich um ein einziges Netzwerk handeln. Man nennt diesen Mechanismus internes Routing. Mit zukünftigen Versionen wird auch das Routing-Verfahren von NetWare neu konzipiert werden. Novell geht weg von RIP und wendet sich einem herkömmlichen NetWare Link State Protocol zu. Dabei handelt es sich um ein Verfahren, das bereits von OSI als IS-IS-Protokoll bekannt ist bzw. für TCP/IP als OSPF verwendet wird. Der externe Router von Novell, Multiprotokoll-Router (MPR), wird als erster mit diesem Verfahren ausgestattet und ausgeliefert werden.

DOS-3.x- und NetBIOS-Unterstützung

Im März 1985 lieferte IBM das neue Betriebssystem PC-DOS 3.1 aus. In diesem Betriebssystem ist die Unterstützung der File-Server-Umgebung, der Netzwerke und der netzwerkfähigen Programme enthalten. DOS 3.1 bietet Schnittstellen zur Multi-User-Fähigkeit unter DOS. Mit der Einführung des LAN-Betriebssystems von IBM, IBM-PC-LAN, wurde auch ein neues Peer-to-Peer-Protokoll entwickelt. Es handelt sich dabei um NetBIOS. Diese NetBIOS-Schnittstelle erreichte sehr schnell einen gewissen Standard, nicht zuletzt durch die Vermarktung und Unterstützung von IBM. Um auch diese neuen Entwicklungen unter NetWare unterstützen zu können, lieferte Novell bereits im September 1985 entsprechende Software-Produkte aus, um DOS 3.x und NetBIOS unter NetWare einsetzen zu können.

Damit können sowohl die bestehenden Applikationen als auch Applikationen, die speziell für DOS 3.1 geschrieben worden sind, eingesetzt werden.

13.1 Die wichtigsten Entwicklungsphasen von Novell

Bislang hat Novell IPX/SPX als Kommunikationsprotokoll zwischen NetWare Clients und NetWare Servern verwendet. Da sich die heterogenen Netzwerke immer mehr am Markt durchsetzen, entwickelte Novell eine neue Schnittstelle, um ein Netzwerk einheitlich auf TCP/IP-Basis zu betreiben. Dieses Produkt ist als NetWare IP bekannt und muß separat zu einer Server-Lizenz gekauft werden. Dabei kann NetWare entweder ausschließlich mit TCP/IP oder gemischt mit IPX/SPX und TCP/IP konfiguriert werden.

80286-Protected-Mode-Betriebssystem

Mit der Einführung des AT von IBM wurde ein weiterer leistungsfähiger PC von IBM angeboten. Dieser Rechner typ arbeitet durch den Einsatz des Intel-80286-Prozessors nicht nur schneller, sondern kann mehr Hauptspeicher und Plattenkapazität als seine Vorgänger unterstützen. Damit kann dieser AT-Rechner hervorragend als File-Server eingesetzt werden. Die erweiterten Möglichkeiten des AT können nur durch die Ausnutzung des Protected Mode des 80286-Prozessors voll genutzt werden. Knapp ein Jahr nach der Auslieferung des ersten AT bot Novell die volle Unterstützung dieser neuen PC-Hardware mit einem neuen LAN-Betriebssystem an.

NetWare 286 war das erste Betriebssystem für LANs, das den Intel-80286-Prozessor in seinem vollen Funktionsumfang ausnutzen konnte. Es zählt somit zu den ersten 16-Bit-Netzwerkbetriebssystemen.

Der Erfolg von NetWare ist unter anderem darauf zurückzuführen, daß Novell immer innerhalb kürzester Zeit seine Produkte an die neuen Erfordernisse bezüglich der Hardware angepaßt hat.

Token-Ring-Netzwerkunterstützung

Als IBM im März 1986 das IBM-Token-Ring-Netzwerk auslieferte, demonstrierte Novell die schnelle Unterstützung von neuen Standards mehr denn je. Im gleichen Monat wurden bereits Programme zur Unterstützung des IBM-Token-Rings unter NetWare ausgeliefert. Novell war damit der erste unabhängige Netzwerkhersteller, der IBM-Token-Ring-Netzwerke unterstützte. Es wird geschätzt, daß etwa die Hälfte der derzeit installierten Token-Ring-Netzwerke unter Novell NetWare betrieben werden.

Im September 1986 setzte Novell einen weiteren Meilenstein auf dem Gebiet der LAN-Betriebssysteme. Zu diesem Zeitpunkt wurde NetWare um die System-Fault-Tolerant-Mechanismen (SFT-) erweitert. Hiermit werden Sicherheitsmechanismen angeboten, die zum

13 Die Entwicklungsgeschichte von Novell

Teil heute noch einzigartig für LAN-Betriebssysteme sind. Andere Hersteller von Netzwerkbetriebssystemen haben sich zwar bereits an diesen Mechanismen orientiert, aber dennoch hat Novell, vor allem durch die neue Version NetWare 4.x, einen Vorsprung vor allen anderen Herstellern von LAN-Betriebssystemen.

Open Protocol Technology

1987 kündigte Novell eine neue Strategie für NetWare an. Es handelt sich um die Protokollunabhängigkeit, von Novell als Open Protocol Technology (OPT) vermarktet. Die Unterstützung dieser neuen Technik wurde 1988 durch die Auslieferung von NetWare 286 v2.15 und NetWare for Macintosh realisiert. Bei NetWare for Macintosh handelt es sich um ein Zusatzprodukt für NetWare, um auf einem NetWare-File-Server das Apple Filing Protocol und das Apple Talk Protocol unterstützen zu können. Mit NetWare 3 und NetWare 4 werden diese Mechanismen noch weiter ausgebaut.

VMS- und OS/2-Unterstützung

Zur Unabhängigkeit von NetWare gehört auch die Unterstützung der unterschiedlichen Workstation-Betriebssysteme. Neben der Einbindungsmöglichkeit von Apple-Macintosh-Rechnern mit Hilfe von NetWare for Macintosh können auch OS/2-Arbeitsplätze unter NetWare betrieben werden. Dies geschieht durch den Einsatz des NetWare Requester für OS/2.

Der nächste Schritt in Richtung Network Computing, also die Einbindung unterschiedlichster Systeme unter NetWare, war die Einführung von NetWare for VMS. Damit kann die VAX sowohl als DEC-MDT-Anlage als auch als NetWare-File-Server eingesetzt werden.

NetWare – das offene System

Die Zielsetzung von Novell ist, Marktführer beim Übergang von Workgroup Computing zum Network Computing zu werden. Deshalb kündigte Novell 1989 das NetWare Open System an, die Architektur für Network Computing. Mit dieser offenen Architektur werden weitreichende Dienste für den Einsatz unterschiedlichster Plattformen festgelegt. Damit ist es für Software-Entwickler sehr einfach, netzwerkfähige Applikationen auf den Markt zu bringen. Durch die Implementierung dieser Komponenten und die Unterstützung anderer Technologien ist es möglich, daß NetWare Open System die Architektur sein kann, mit der es Novell gelingen wird, Netzwerklösungen für die neunziger Jahre anzubieten, die genauso effizient sind wie die Lösungen, die Novell in den achtziger Jahren zum Erfolg verholfen haben.

13.1 Die wichtigsten Entwicklungsphasen von Novell

NetWare-Ankündigungen

Die Ankündigung und Auslieferung von NetWare 3 und NetWare 4 hat eine ebenso große und positive Resonanz hervorgerufen, wie dies bei Einführung von NetWare 286 der Fall gewesen ist. Bei NetWare 3 handelt es sich um eine wesentlich verbesserte Version im Vergleich zu NetWare 286, wobei der Schwerpunkt nicht nur auf erhöhte Sicherheit, Zuverlässigkeit und Geschwindigkeit gelegt worden ist, vielmehr war auch angestrebt, einen großen Schritt in Richtung Network Computing zu gehen. Die gesamten Verwaltungs- und Funktionsmechanismen wurden mit NetWare 4 nochmals um wesentliche Aspekte erweitert – weg von der zentralen Ressourcenverwaltung, hin zur globalen Netzwerkverwaltung (unabhängig davon, wie viele Server im Netzwerk vorhanden sind).

Im nächsten Abschnitt werde ich Ihnen die wichtigsten strategischen Konzepte und Vorhaben von Novell etwas näher erläutern, um einen Eindruck über die Entwicklungstendenzen im LAN-Bereich zu geben.

UnixWare

Im Dezember 1992 wurde offiziell die erste Version von UnixWare Personal Edition und Application Server ausgeliefert. Novell unternimmt damit den Versuch, einen weiteren Markt zu erobern, den Unix-Markt. Mit den UnixWare-Produkten steht nicht nur ein neues Unix-System, System V Release 4.2, zur Verfügung, sondern auch eine Betriebssystemplattform, die es darüber hinaus gestattet, auch noch DOS- und Windows-Applikationen einzusetzen. Es überrascht nicht, daß UnixWare standardmäßig die Kommunikationsprotokolle IPX/SPX unterstützt und sich wie ein NCP Client den NetWare Servern gegenüber verhält. Um jedoch auch in einer bestehenden Unix-Welt eingesetzt werden zu können, unterstützt UnixWare auch die Mechanismen TCP/IP und NFS. Somit steht ein abgerundetes und flexibles Betriebssystem zur Verfügung. UnixWare wurde auch so konzipiert und entwickelt, daß Standard-Unix-Anwendungen eingesetzt werden können. Novell hat aufgrund neuer strategischer Richtlinien den Entschluß gefaßt, UnixWare nicht mehr selbst zu vertreiben und weiterzuentwickeln; die gesamte Produktentwicklung wurde an SCO abgegeben.

NetWare 4

Wenn vorher davon gesprochen wurde, daß NetWare 3 positive Resonanz hervorgerufen hat, dann trifft dies für NetWare 4 noch mehr zu. Am 10.3.93 wurde NetWare 4 in Wiesbaden offiziell angekündigt,

13 Die Entwicklungsgeschichte von Novell

und zwar weltweit mittels einer Satellitenübertragung von Amerika aus. Im Vergleich zu NetWare 3 handelt es sich bei NetWare 4 um eine vollständig überarbeitete NetWare mit dem Ziel, das Netzwerkbetriebssystem nicht nur noch sicherer und schneller zu machen, sondern auch die gesamte Administration zu verbessern. Wesentlicher Aspekt dabei ist, daß man sich von der bisher verwendeten Bindery löst, um Server-basierend Objekte im Netzwerk zu verwalten, und statt dessen eine globale Datenbank (NetWare Directory Services) verwendet, um ein gesamtes Netzwerk zu verwalten. Ich werde in diesem Buch ausführlicher auf NetWare 4 eingehen. Im Lauf der Zeit wird sich diesbezüglich noch eine Vielzahl von Neuerungen ergeben, die nur mit der Plattform von NetWare 4 erreicht werden können, z.B. Multiprocessing-Fähigkeit, Web-Server oder auch Processor Clustering.

13.2 Ein strategischer Überblick

Wenn man sich mit dem Einsatz von LANs auseinandersetzt, dann stellt man fest, daß in letzter Zeit sehr viele Diskussionen über Standards geführt werden. Dies beginnt beim Einsatz unterschiedlicher Topologien. Es geht hierbei um die Frage, ob sich Ethernet, Token-Ring oder ATM durchsetzen wird. Daneben geht es auch um die Frage, in welchen Fällen sich der Einsatz von ATM-Netzwerken lohnt. Kaum hat man sich für eine Entwicklungsrichtung entschieden, werden bereits neue Wege angekündigt und beschritten. So ist man derzeit dabei, eine Diskussion darüber zu führen, ob man sich im High-Speed-LAN-Bereich für Gigabit Ethernet oder ATM entscheiden soll. Ebenso ist die Frage zu klären, ob sich Fast Ethernet gegenüber ATM behaupten kann und wie es in Richtung High-Speed-WAN weitergehen wird.

Immer wieder kommt es vor, daß Firmen neue Entwicklungen bekanntgeben, die nur ein Ziel haben: höhere Leistung im LAN-Umfeld. Eine weitere Entwicklung, die in diesem Zusammenhang angeführt werden kann, ist unter dem Begriff »Switching« bekannt. So werden für Ethernet, Token-Ring und FDDI entsprechende Switching-Komponenten angeboten. Daß die Entwicklung von ATM ohne diese Technik nicht auskommt, wurde bereits an anderer Stelle ausführlich erläutert.

Sie werden auch Veröffentlichungen über SAA-konforme Applikationen, 32-Bit-Anwendungen, Windows NT, Windows 95/98, Windows NT Server, LAN-Server, NetWare 4 oder Client-Server-Konzepte finden. Dabei versucht jeder Hersteller, seine eigenen Konzepte und Strategien als den Standard darzustellen. In diesem Abschnitt werde

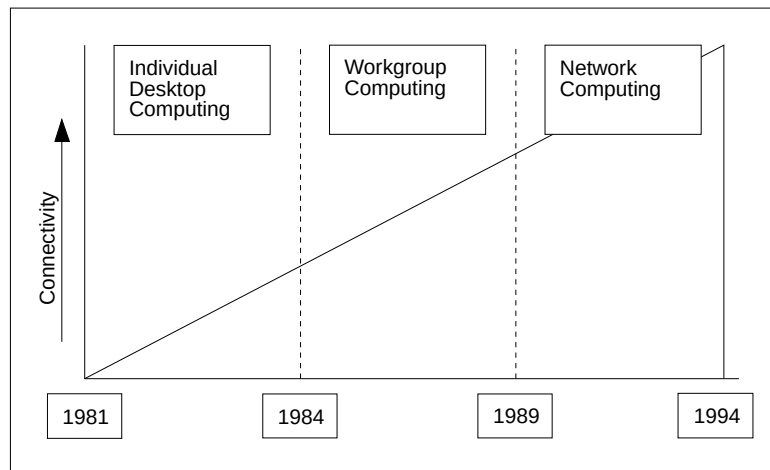
13.2 Ein strategischer Überblick

ich versuchen, Ihnen einen Teil dieser neuen Konzepte und Strategien zu erläutern und einen Einblick darüber verschaffen, wie Novell sich an diese Entwicklungen anpassen will.

13.2.1 Der LAN-Markt

Zu Beginn der Einführung von PCs, Anfang 1980, wurden diese ausschließlich als Standalone-Systeme eingesetzt. Sowohl die notwendigen PC-Dienste als auch Daten, die durch das eigene PC-Betriebssystem, meist PC-DOS, verwaltet wurden, waren nur isoliert und dediziert einem einzelnen Benutzer vorbehalten. Im Lauf der Zeit wurden in den Unternehmen immer mehr PCs eingesetzt, auf denen die individuellen Daten verwaltet und bearbeitet wurden.

Abbildung 13.1
Der Entwicklungs-
prozeß für LANs



Die Forderung nach Datenaustausch zwischen diesen PCs – also die Möglichkeit, Daten gemeinsam nutzen zu können – wurde immer größer. Diese Notwendigkeit beschleunigte den Prozeß der Evolution vom Standalone-PC zu »Workgroups« von PCs, die über Lokale Netzwerke miteinander verbunden sind. In Abbildung 13.1 ist der Entwicklungsprozeß dargestellt.

Workgroup Computing

Das Konzept Workgroup Computing erlaubt es den Anwendern, Ressourcen gemeinsam zu nutzen, indem die PCs in ein LAN integriert werden. Die Anwender haben damit den gemeinsamen Zugriff auf einen File-Server, also Zugriff auf Daten, Drucker und Platten-subsysteme. Auf dem File-Server übernimmt das Netzwerkbetriebs-

13 Die Entwicklungsgeschichte von Novell

system – nicht ein Workstation-Betriebssystem – die Kontrolle über die Hardware dieses Rechners. Das Netzwerkbetriebssystem muß auch die notwendigen Funktionen für Datensicherheit, Datenschutz, Zugriffsberechtigung etc. übernehmen. Der Anwender selbst merkt normalerweise nichts von der Existenz eines File-Servers. Er kann seinen PC so benutzen wie bisher, zuzüglich der erweiterten Ressourcen, die ihm der File-Server zur Verfügung stellt, d.h. größere Plattenkapazität, größere Druckleistung und dergleichen mehr.

Die ständige Anpassung der LAN-Betriebssysteme an die Bedürfnisse der Anwender und der schnelle Fall der Hardwarekosten haben dazu beigetragen, daß innerhalb kürzester Zeit die Anzahl der installierten LANs rapide angestiegen ist. Nicht selten wurden LAN-Installationen denen von MDTs vorgezogen. Diese Entwicklungstendenz, weg von Shared-Processing-Systemen (MDT) und hin zu Distributed-Processing-Systemen (LAN), bewirkt gleichzeitig eine Änderung bestimmter Unternehmensstrukturen.

Die organisatorische Struktur in einem Unternehmen ist in einem weit geringerem Maß als früher hierarchisch aufgegliedert und führt damit auch zu anderen Organisationsformen bei den Rechnerhierarchien. Aufgrund dieser Entwicklungstendenzen stieß das Prinzip des Workgroup Computing sehr schnell an seine Grenzen.

Die Einführung von LANs erzeugte unmittelbar den Bedarf, LANs in ein unternehmensweites EDV-Konzept einzubinden. Dies bedeutet, daß die Anbindung von LANs an Großrechner- oder MDT-Anlagen möglich sein muß. Somit sollen die Anwender den transparenten Zugriff auf die File-Server-Ressourcen und die Ressourcen des Hosts oder MDT erhalten. Mit diesem Konzept ist es notwendig, daß jeder Benutzer weiß, auf welchem Rechner (File-Server, Host oder MDT) seine einzelnen Ressourcen zur Verfügung stehen. Zudem wird durch dieses Konzept das Netzwerkmanagement wesentlich komplizierter. Das heißt, die Verwaltungsmöglichkeit der unterschiedlichen Rechnersysteme wird durch den Netzwerkverwalter mit Hilfe der unterschiedlichsten Software-Systeme wahrgenommen.

Durch diese Eigenschaften des Workgroup Computing wurde die nächste Entwicklungsphase im Netzwerkbereich eingeleitet. Es handelt sich um den Schritt in Richtung Network Computing.

Network Computing

Besteht das Ziel von Workgroup Computing darin, PCs in ein LAN zu integrieren, so wird mit dem Konzept des Network Computing eine unternehmensweite Integration von LANs und WANs verfolgt. Damit kann eine unternehmensweite Kommunikation mit den unterschied-

13.2 Ein strategischer Überblick

lichsten Systemen durchgeführt werden. Dieses Vorhaben verlangt vor allem von den LANs und den Netzbetriebssystemen eine sehr flexible Struktur, da diese meist in bestehende Großrechner- oder MDT-Systeme integriert werden müssen.

Die gängigsten Rechnersysteme und damit verbundenen Betriebssysteme, die zu einem Gesamtsystem zusammengeführt werden sollen, sind die Systeme von DEC unter VMS, IBM unter VM oder MVS, Unix und LAN-Systeme unter NetWare oder Windows NT. Auf den PCs muß die Integration von DOS, OS/2, Macintosh oder Unix möglich sein.

Mit dem Konzept des Network Computing kann ein Gesamtnetzwerk aufgebaut werden, das die Einbindung der oben aufgeführten Systeme erlaubt. Auf diese Weise haben die Anwender im Netzwerk Zugriff auf Großrechner-, MDT- und LAN-Server-Systeme. Durch den Aufbau von WANs besteht zudem die Möglichkeit, auf Rechnerressourcen an entfernt liegenden Orten zugreifen zu können.

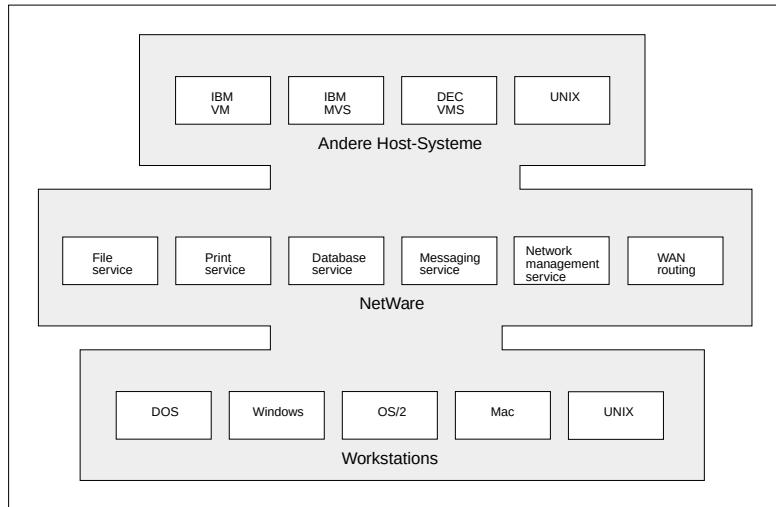
Network Computing verfolgt das Ziel, daß alle Benutzer im Netzwerk in einem Unternehmen auf Daten und Rechnerdienste transparent zugreifen können. Beim Workgroup Computing sind die Ressourcen und Dienste, die einem Benutzer zur Verfügung gestellt werden, in einem File-Server vereinigt. Beim Network Computing hingegen bildet das Netzwerk selbst die Plattform für die Bereitstellung der Netzwerkdienste. In Abbildung 13.2 ist ein solches Netzwerkkonzept dargestellt. Sie können daraus ersehen, daß die unterschiedlichsten Rechner- und Netzwerksysteme über einen gemeinsamen Backbone-Strang miteinander gekoppelt sind und jeder Benutzer somit Zugriff auf die einzelnen Rechnerressourcen hat.

Um das Prinzip des Network Computing nutzen zu können, reicht der Aufbau von heterogenen Netzwerken allein nicht aus. Es müssen Mechanismen zur Verfügung stehen, die nicht nur das Netzwerk als Transportmedium verwenden, sondern die es möglich machen, daß die einzelnen unterschiedlichen Systeme miteinander kommunizieren können. Dies stellt nicht nur bestimmte Anforderungen an die Netzbetriebssysteme, sondern auch an die einzelnen Applikationsprogramme auf den einzelnen Rechnern.

Diese Programme, die ursprünglich als Distributed Applications eingesetzt worden sind, erfordern die Mechanismen der Programm-zu-Programm-Kommunikation (Peer-to-Peer) mit der Funktion, über die Grenzen von speziellen Maschinentypen, Server-Betriebssystemen und Workstation-Betriebssystemen hinweg aufgerufen werden zu können. Um das realisieren zu können, werden folgende Anforderungen an das Network Computing gestellt:

13 Die Entwicklungsgeschichte von Novell

Abbildung 13.2
Das zukünftige
Konzept des Net-
work Computing



Aufgrund der Tatsache, daß die individuellen Server-basierenden Netzwerkbetriebssysteme für das Workgroup Computing ausgelegt sind, ist es notwendig, Netzwerkbetriebssysteme neu zu konzipieren. Ein Betriebssystem für die Unterstützung des Network Computing muß das Netzwerk, bestehend aus einzelnen unterschiedlichen Netzwerken, als ein Gesamtnetzwerk betrachten und verwalten können.

In der Vergangenheit, und zum Teil noch heute, wurde die Integration heterogener Systeme durch die Existenz unterschiedlicher Standards für den Aufbau von Netzwerken erschwert. Verschiedene Standards für das Übertragungsmedium, die Übertragungsprotokolle und eine Vielzahl von Host- und Workstation-Betriebssystemen erfordern zum Teil einen hohen Aufwand, um diese miteinander vereinen zu können. Den Anwendern kann der Nutzen des Network Computing erst bewußt werden, wenn Netzwerklösungen nicht nur die Unabhängigkeit von diesen unterschiedlichen Standards bieten, sondern auch die Unterstützung und Integration dieser Standards in einem Gesamtsystem zur Verfügung steht.

Aufgrund der Ausdehnung von Netzwerken auf unternehmensweite Konzepte und Lösungen ist es auch erforderlich, daß sich die hierfür entwickelten Netzwerkbetriebssysteme durch eine höhere Funktionalität und Geschwindigkeit auszeichnen. Dies gilt vor allem dann, wenn im Netzwerk zeitkritische Anwendungen zum Einsatz kommen. Eine weitere notwendige Forderung ist die Offenheit der Betriebssysteme für Entwickler und die Bereitstellung von geeigneten Entwicklungstools, um das Erstellen von Applikationen zur vereinfachen.

13.2 Ein strategischer Überblick

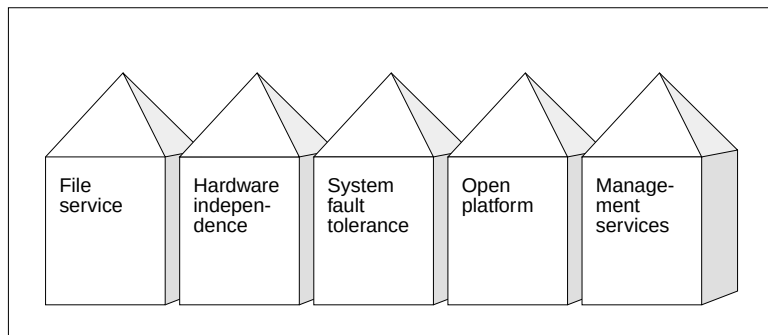
Durch die Integration mehrerer unterschiedlicher Netzwerke in ein Gesamtnetzwerk ist es auch erforderlich, daß der Netzwerkverantwortliche geeignete Management-Utilities zur Verfügung hat, um das Netzwerk zu überwachen und zu steuern.

13.2.2 Die fünf Meilensteine von Novell

Als Novell sein erstes Netzwerkbetriebssystem auf den Markt brachte, war das auch eine Workgroup-Computing-Lösung. Das heißt, DOS-Anwender hatten damit die Möglichkeit, Daten und Ressourcen gemeinsam zu benutzen. NetWare verbreitete sich so, weil es den Anwendern die Möglichkeit bot, Daten und Ressourcen in einer zuverlässigen, sehr schnellen und flexiblen Umgebung gemeinsam zu nutzen.

Die Funktionalitäten von NetWare sind das direkte Ergebnis von Novells Politik, auf die gestellten Anforderungen der Endanwender und die zukünftigen Bedürfnisse der Netzwerkbenutzer und Netzwerkverwalter einzugehen. Diese Entwicklungsschritte teilen sich in fünf Phasen auf, man spricht auch von fünf Meilensteinen bei der Entwicklung von Novell. In Abbildung 13.3 sind sie dargestellt.

Abbildung 13.3
Die fünf Meilensteine in der
Entwicklung von
Novell NetWare



Novell NetWare wird als Quasi-Standard für Netzwerkbetriebssysteme bezeichnet. Zur Zeit arbeiten ca. zehn Millionen Anwender mit NetWare bei mehreren hunderttausend installierten Systemen. Dieser Erfolg ist nicht nur auf die große Performance und unternehmensweite Integration von NetWare zurückzuführen, durch NetWare werden den PC-Anwendern Funktionen und Sicherheitsmechanismen zur Verfügung gestellt, die bisher nur auf Host- und MDT-Rechnern zu finden waren.

Außerdem wurde NetWare als ein vom Medium unabhängiges Betriebssystem auf dem Markt eingeführt. Durch die rasche Unterstüt-

13 Die Entwicklungsgeschichte von Novell

zung dieser Funktionalität kann NetWare heute auf über 30 unterschiedlichen Netzwerken eingesetzt werden, und für über 100 Netzwerkadapterkarten werden LAN-Driver angeboten. Damit ist NetWare auch auf einer Vielzahl von Servern und Workstations einsetzbar.

Ein weiterer Standard wurde von Novell durch die Einführung der System Fault Tolerant (SFT) NetWare auf dem LAN-Markt eingeführt. Damit läßt sich die Gefahr eines Ausfalls des Netzwerks minimieren. Ich werde bei der Behandlung von NetWare auf diese Mechanismen genauer eingehen.

Mit Einführung der Open Protocol Technology wurde NetWare protokollunabhängig. Damit wurde es möglich, NetWare problemlos in eine heterogene EDV-Welt einzubinden. Das heißt, es konnten als Workstations gleichzeitig DOS-, Windows-, Windows-95-, Windows-NT-, OS/2- und Apple-Computer eingesetzt werden. Weitere Pläne zielen auf die Unterstützung von Unix-Workstations. Die Einführung der NFS-Dienste (Unix-Services und Print-Services) erlaubt es, daß Unix-Anwender auf einen NetWare Server zugreifen können, so als würde es sich um ein Unix-Server-System handeln. Das wird durch die NFS-Dienste unter NetWare erreicht. Im Gegenzug wurde auch der umgekehrte Weg ermöglicht, so daß NetWare-Anwender transparent auf Unix-Dateisysteme zugreifen können. Durch die Unterstützung der LPR-Mechanismen kann auch transparent von Unix auf NetWare-Drucker und von NetWare- auf Unix-Drucker ausgegeben werden. Mit OPT wurde auch die Unterstützung weiterer Transportprotokolle angekündigt. Bislang unterstützt NetWare nur IPX/SPX. Mit OPT öffnet sich NetWare gegenüber den Transportprotokollen TCP/IP und OSI. Mit Einführung von NetWare 3 wurde damit begonnen, multiprotokollfähig zu sein. Mit NetWare 4 wurden diese Mechanismen konsequent weiterentwickelt.

Diese Entwicklungsschritte sind maßgeblich verantwortlich für den Übergang von Workgroup Computing zu Network Computing, um eine unternehmensweite Vernetzung aufbauen zu können. Die Integration von Macintosh durch die Unterstützung des Apple Filing Protocol (AFP) und die Ankündigung von NetWare for VMS und Portable NetWare sind große Schritte in Richtung Network Computing. Der letzte Schritt zur vollständigen Integration in ein Network-Computing-Konzept sind NetWare 3 bzw. NetWare 4 und die damit verbundenen Management Services.

Mit OPT wird die Protokollunabhängigkeit von NetWare ausgebaut. Management Services runden das Gesamtbild für Network Computing ab, da sich hierunter Konzepte der sogenannten Directory Services, System Management und Security-Mechanismen verbergen.

13.3 Die Server-Plattform für NetWare

Directory Services sind auch unter der Bezeichnung Naming Services bekannt. Dies bedeutet, daß Benutzer auf Ressourcen im Netzwerk zugreifen können, ohne wissen zu müssen, auf welchen Systemen sich diese Ressourcen befinden. Sowohl das Network Management als auch die zusätzlichen Sicherheitsmechanismen sind eng mit den neuen Naming-Service-Diensten gekoppelt. Dies ist notwendig, um unternehmensweite Netzwerke, basierend auf dem Konzept des Network Computing, besser verwalten zu können.

13.3 Die Server-Plattform für NetWare

Wenn Sie das Konzept des Network Computing betrachten, handelt es sich dabei letztlich um die Vernetzung der Datenverarbeitung, und zwar unterschiedlichster Systeme. Deshalb wird Network Computing auch sehr häufig als vernetzte Datenverarbeitung bezeichnet.

Die Entwicklung von Novell auf dem Gebiet der vernetzten Datenverarbeitung stützt sich auf eine Architektur, die als NetWare Open Systems bezeichnet wird.

Dabei werden die oben angesprochenen Meilensteine von Novell und andere Technologien und Strategien wie WANs und die offene Architektur miteinander vereint, so daß eine Basis für Network Computing geschaffen wird. Basisbestandteil dieser Entwicklung ist NetWare v3.11, ein Netzbetriebssystem für verteilte Systeme, das die Entwicklung von Novell bis in die neunziger Jahre bestimmen wird.

Die Strategien, die sich hinter NetWare Open Systems verbergen, können wie folgt zusammengefaßt werden:

- Anbieten von NetWare-Diensten auf ausbaubaren Server-Plattformen
- Unterstützung der Industriestandards, damit die Integration, Kommunikation und Kompatibilität mit Fremdprodukten aufrechterhalten werden kann und die Protokollunabhängigkeit ermöglicht wird
- Die Bereitstellung integrierter Routing- und WAN-Dienste
- Die Bereitstellung einer offenen Architektur mit einer leistungsfähigen Entwicklungsumgebung

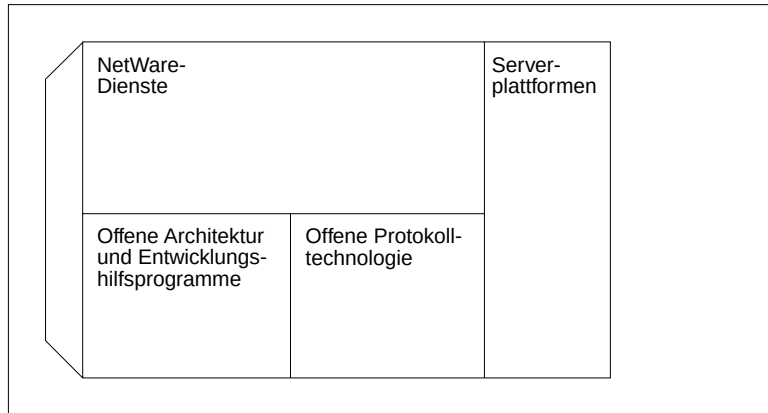
Die von Novell verfolgte Strategie wird im wesentlichen durch die Bereitstellung bzw. Unterstützung der Produkte auf vier Gebieten erreicht:

- Server-Plattformen
- Offene Architektur
- Offene Protokolltechnologie
- NetWare-Dienste

13 Die Entwicklungsgeschichte von Novell

In Abbildung 13.4 ist der Zusammenhang zwischen diesen vier Schlüsselbereichen dargestellt.

Abbildung 13.4
Die vier Schlüssel-
bereiche von Novell
NetWare



Durch die Kombination dieser vier Bereiche kann Novell eine weitreichende Lösung für das Network Computing, d.h. der vernetzten Datenverarbeitung, anbieten und realisieren. Die NetWare-Dienste wurden auf zwei wichtigen Server-Plattformen zur Verfügung gestellt: NetWare v3.11 und Portable NetWare.

Jede dieser Server-Plattformen zeichnet sich durch eine offene Architektur aus, die einen wichtigen Bestandteil für jede Komponente der NetWare Open Systems darstellt. Zudem werden geeignete Anwendungsschnittstellen für alle NetWare-Dienste bereitgestellt.

Somit haben verteilte Anwendungen auf allen Ebenen Zugriff auf das Netzwerk. Die Entwicklungs-Tools unterstützen den Anwender und Software-Hersteller bei der Entwicklung von verteilten Anwendungen und bieten große Flexibilität durch die offene Protokolltechnologie über unterschiedliche Industriestandards.

Mit der NetWare Open Systems entwickelt Novell die siebte Generation von NetWare-Produkten. Der Übergang von der Datenverarbeitung in Arbeitsgruppen (Workgroup Computing) zur vernetzten Datenverarbeitung (Network Computing) mit Hilfe von NetWare gewährleistet ein stabiles Wachstum auf der Grundlage einer markterprobten Technologie. Durch welche Konzepte und Funktionen sich NetWare v3.11 und Portable NetWare von anderen Netzwerkbetriebssystemen unterscheiden und inwieweit sich hierbei die NetWare-Open-System-Strategie widerspiegelt, wird an anderer Stelle näher erläutert.

13.3 Die Server-Plattform für NetWare

Um alle notwendigen Netzwerkoperationen durchführen zu können, ist es erforderlich, eine geeignete Server-Plattform einzusetzen. Dabei ist es vollkommen nebensächlich, ob dabei mit dem ursprünglichen Betriebssystem des Servers gearbeitet wird oder mit einem Host-Betriebssystem, wie zum Beispiel VMS von DEC. Das Dateisystem, die Speicherverwaltung und das Scheduling werden beispielsweise alle von den Server-Plattformen bereitgestellt.

Die richtige Auswahl der Server-Plattform, die in einem Netzwerk eingesetzt werden soll, hat auf viele Bereiche des Netzwerkbetriebs Auswirkungen. Von der Auswahl der Server-Plattform hängen die Leistung, Zuverlässigkeit und Sicherheit des gesamten Netzwerks ab. Anwendungen für das Netz können um so leichter entwickelt werden, wenn es sich dabei um eine offene Basis handelt.

Verständlicherweise kann eine Server-Plattform nicht alle Erfordernisse abdecken. Benutzer brauchen die Möglichkeit, den geeigneten Server aus einer Reihe von ausbaubaren Server-Plattformen auszuwählen. Für unterschiedliche Anwendungsbereiche lassen sich entweder spezialisierte Server wie NetWare Server oder Universalserver wie OS/2-Anwendungs-Server einsetzen, je nachdem welche am besten geeignet sind. Es gibt aber auch Fälle, in denen der Wunsch besteht, eine bereits existierende MDT-Anlage zusätzlich als Server einsetzen zu können, um damit die bestehende Hardware-Investition am besten nutzen zu können. Auf diese Weise könnten Betriebssysteme wie VMS oder Unix die Server-Funktion übernehmen.

Bei NetWare Open Systems gibt es zwei strategische Server-Plattformen: NetWare 3 bzw. NetWare 4 und Portable NetWare. Unter NetWare 3 bzw. NetWare 4 arbeiten die NetWare-Dienste mit Novell-Multitasking-Kern und -Dateisystem mit Echtzeitverarbeitung. Dieses Betriebssystem nutzt die 32-Bit-Umgebung des 80386- bzw. 80486-Prozessors voll aus (darüber später mehr).

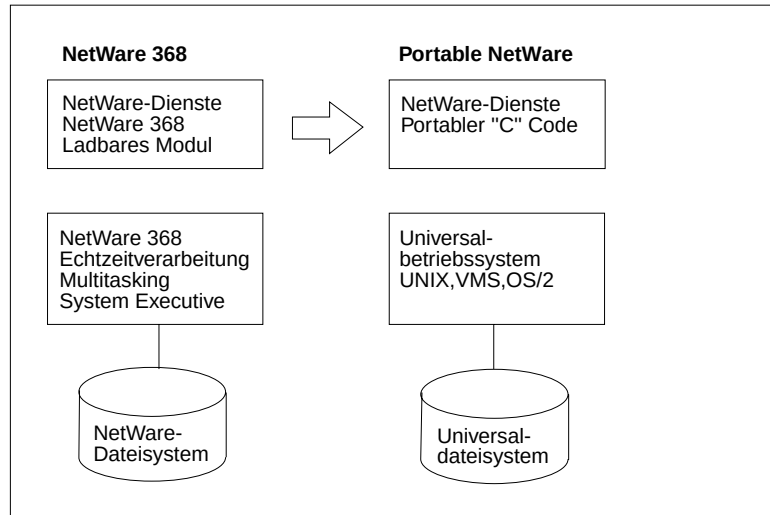
Portable NetWare ist eine weitere Version der NetWare-Dienste, die sich leicht auf andere Trägerbetriebssysteme adaptieren lässt. So ist es möglich, NetWare als Task auf einer VAX unter dem Betriebssystem VMS oder unter Unix einzusetzen. Der Zusammenhang zwischen NetWare 3 und Portable NetWare ist in Abbildung 13.5 dargestellt.

Durch die Verfügbarkeit unterschiedlicher Server-Plattformen und die Unterstützung von NetWare Open System wird dem Benutzer die Möglichkeit gegeben, sich den seinen Bedürfnissen angemessenen Netzwerkservers auszuwählen. Beide Serverumgebungen sind dabei voll interaktionsfähig und können auf der unterschiedlichsten Server-

13 Die Entwicklungsgeschichte von Novell

Hardware ablaufen. Dem Benutzer stehen also bei der Auswahl des Servers viele Optionen und Möglichkeiten zur Verfügung, um das Server-System zu finden, das seinen Bedürfnissen am besten entspricht.

Abbildung 13.5
NetWare 3 und
Portable NetWare
im Vergleich



Es sei erwähnt, daß es eine Weiterentwicklung der Portable NetWare bei Novell nicht mehr gibt. Zwar werden noch Versionen von NetWare 3 auf Basis von Unix angeboten, NetWare for Unix, jedoch sind dies noch NetWare-3-Implementierungen. Für NetWare 4 gibt es keine Produkte mehr in dieser Richtung. Als NetWare 4 angekündigt wurde, war auch die Rede von einer PIN-Version. Dabei sollte es sich um eine Processor Independent NetWare (PIN) handeln. Auch diese Entwicklungsrichtung wurde inzwischen aufgegeben. Zum Zeitpunkt der Erstellung dieses Buches war auch nichts Neues in dieser Richtung zu hören. So muß erst einmal davon ausgegangen werden, daß NetWare 5 bis auf weiteres nur auf Intel-Prozessoren eingesetzt werden kann. Eins steht bis heute bereits fest, daß es nämlich keine Weiterentwicklung von NetWare 3 geben wird. Damit ist NetWare 3.2 wahrscheinlich die letzte Version der NetWare-3-Serie, da die neue strategische Netzwerkbetriebssystem-Plattform ausschließlich durch NetWare 4 gebildet wird. Da es jedoch noch einen sehr großen Verbreitungsgrad von NetWare 3.2 gibt und auch bestimmte Funktionsmechanismen in die NetWare-4-Version übergegangen sind, werden in diesem Buch sowohl NetWare 3.2 als auch NetWare 4 näher beschrieben.

13.4 Global-Network-Strategie

Aus den bisherigen Ausführungen ist zu ersehen, daß Novell schon immer das Ziel verfolgt hat, schnell und zuverlässig auf die wachsenden Anforderungen des Markts zu reagieren. Dieses Kapitel soll zeigen, welche zukünftigen Entwicklungsrichtungen zu erwarten sind.

Diese Ausführungen werden auch zeigen, daß Novell sehr stark auf die NetWare Directory Services, so wie sie in NetWare 4 implementiert sind, setzt.

Die richtige Information zur richtigen Zeit am richtigen Ort zu haben ist eine der wichtigsten Forderungen, wenn es um Datenverarbeitung in der heutigen Zeit geht. Betrachtet man die Entwicklung der Computertechnologie der letzten 30 Jahre, so kann man eine dramatische Entwicklung feststellen. Dies hat auch nicht vor Netzwerken und Netzwerktechnologien halt gemacht. Da es fast keine Information mehr gibt, die nicht in elektronischer Form verfügbar gemacht werden kann, wird der universelle Zugriff auf »Smart Global Networks« das tägliche Arbeiten grundlegend ändern. Dies zeichnet sich bereits heute ab, wenn man Phänomene wie Internet, Intranet, Online-Dienste etc. betrachtet. Um diesen allgemeinen Anforderungen gerecht werden zu können, müssen auch die Netzwerkbetriebssysteme und die Workstation-Betriebssysteme entsprechend angepaßt, modifiziert und leistungsfähig gemacht werden. Das Ziel von Novell ist nun darin zu sehen, alle Anwender in einem globalen Netzwerk zu vereinen. Um dieses Ziel zu erreichen, hat Novell drei Anforderungen definiert:

1. Es müssen Smart Network Services zur Verfügung stehen. Über diese Dienste kann erkannt werden, wer sich im Netz anmeldet, von wo die Einbindung durchgeführt wird, was der Anwender benötigt und was für den Anwender getan werden kann. Das Netzwerk soll zu einem »intelligenten« Hilfsmittel werden, das Arbeiten erledigt, die ansonsten der Anwender selbst tun müßte.
2. Damit Millionen von Anwendern das Netzwerk nutzen können, muß man auf das Netzwerk zu jeder Zeit und von jedem Platz aus zugreifen können. Dabei sollen neben PCs auch andere intelligente Endgeräte integriert werden können – z.B. Telefone, Faxgeräte, TV, Pager und alles, in das ein Prozessor integriert ist.
3. Der Aufbau eines Netzwerks in dieser Form bedeutet aber auch, daß die unterschiedlichsten Komponenten der verschiedensten Hersteller eingesetzt werden. Das globale Netzwerk wird somit immer heterogen bleiben. Für alle, die darauf zugreifen wollen, muß es sich jedoch als einfaches Netzwerk darstellen, wenn es im Hintergrund auch eine komplexe physikalische Infrastruktur hat.

13 Die Entwicklungsgeschichte von Novell

Zum Aufbau der globalen Netzwerkinfrastruktur müssen Smart Network Services entwickelt werden, d. h. eine Sammlung von Software-Komponenten. Die Strategie von Novell, um Smart Network Services anbieten zu können, basiert auf vier wesentlichen Produkten und Technologien:

1. Das Smart Network hängt sowohl vom Netzwerkbetriebssystem als auch von den Kerntechnologien zum Aufbau von NetWare Distributed Services ab, so wie sie zum Beispiel von den NetWare Directory Services (NDS) angeboten werden. Diese beiden Komponenten stellen die Basis zur Verfügung, auf die alle anderen Komponenten im Netzwerk aufsetzen.
2. Das Smart Network hängt auch von erweiterten Client-Server-Lösungen und -Dienstleistungen ab. Hierzu zählen unter anderem das Management, E-Mail bzw. GroupWare-Mechanismen.
3. Um aus einer Vielzahl »kleiner« Workgroup- bzw. Enterprise-Netzwerke ein globales Netzwerk zu machen, müssen entsprechende Kopplungsmöglichkeiten zur Verfügung stehen. Durch die Entwicklung der NetWare Connect Services (NCS) will Novell Möglichkeiten bieten, über 2,5 Millionen NetWare-Netzwerke zu einem einzigen Netzwerk zusammenzuschalten, immer unter der Prämisse, die Performance, das einfache Management und die Sicherheit der einzelnen LANs zu erhalten.
4. All diese Aufgaben bedürfen aber auch des Zugangs zum Internet. Durch die Erweiterungen, die Novell zur Verfügung stellen kann – NetWare mit den erweiterten Diensten und NCS –, werden wesentliche Verbesserungen zur Verfügung gestellt, um den Zugriff, das einfache Management und die Funktionalität für das Internet zu ermöglichen.

Die von Novell angestrebten Ziele zeigen derzeit sehr starken Einfluß auf die Entwicklung von Netzwerkbetriebssystemen, Client-Software und anderen bereits verfügbaren oder in den nächsten Monaten und Jahren erhältlichen Produkten und Diensten. Um Ihnen einen Überblick zu geben, welche bereits jetzt existierenden Mechanismen und welche zukünftigen Entwicklungen hierfür zu erwarten sind, sollen nachfolgend die wichtigsten Aspekte aufgeführt werden.

Will man eine optimale Plattform für verteilte Dienste im Netzwerk erhalten, sind die folgenden Voraussetzungen zu erfüllen, die Novell mit NetWare, vor allem mit NetWare 4, bereits jetzt bietet.

■ *Performance*

NetWare ist aufgrund der 32-Bit-Architektur in der Lage, alle hierfür notwendigen Voraussetzungen zu schaffen. Die zusätzlich implementierten Mechanismen wie Disk-Caching, Directory-Caching oder auch Packet Burst Mode etc. werden in den späteren Ausführungen über NetWare 3 bzw. NetWare 4 näher erläutert.

13.4 Global-Network-Strategie

■ *Zuverlässigkeit*

Es war von Anfang an das Bestreben von Novell, mit NetWare immer die höchste Zuverlässigkeit zu gewähren. Dies wird nicht nur durch standardmäßig eingebaute Funktionen ermöglicht, sondern auch dadurch, daß man zwei vollständig gespiegelte Server aufbauen kann – dies ist auch unter dem Namen SFT III bekannt.

■ *Management*

Das Kapitel über Netzwerkmanagement hat bereits gezeigt, daß es in einer Netzwerkumgebung unerlässlich ist, entsprechende Netzwerkmanagementfunktionen und -mechanismen zu haben. In Verbindung mit ManageWise werden zum Beispiel über 250 Alerts unterstützt, die entsprechende Meldungen an die Managementconsole abgeben.

■ *Hardware-Optimierung*

Mit NetWare wird das Ziel verfolgt, die eingesetzte Hardware optimal zu nutzen. So werden entsprechende Implementierungen im Code des Betriebssystems durchgeführt, um diese Anforderungen erfüllen zu können.

■ *Skalierbarkeit*

Darunter werden Mechanismen verstanden, die es erlauben, die Anforderungen an den Server schrittweise zu steigern, sofern die Anzahl der Benutzer, die pro Server unterstützt werden sollen, dies erfordert. Mit NetWare 4 ist man inzwischen auch in der Lage, SMP (Symmetric Multiprocessing) zu unterstützen. Mit der Möglichkeit, pro Server bis zu 32 Prozessoren zu betreiben, bleiben keine Performance-Anforderungen mehr unerfüllt.

■ *Modularität*

Das Konzept der NLMs (NetWare Loadable Modules) erlaubt es, daß notwendige Module bei Bedarf im laufenden Betrieb geladen und auch wieder entladen werden. So kann das Netzwerkbetriebssystem entsprechend den notwendigen Diensten, die unterstützt werden sollen, dynamisch konfiguriert und betrieben werden. Die zusätzliche Unterstützung durch Dritthersteller nimmt ständig zu.

Durch die konsequente Weiterentwicklung der NetWare-Umgebung wird die Basis zur Schaffung einer Netzwerkbetriebssystem-Umgebung und komplexer und leistungsfähiger Distributed Network Services immer weiter verbessert. Bei Novell werden den folgenden Diensten für die Zukunft besondere Bedeutung beigemessen:

- NetWare Directory Services (NDS)
- NetWare Advanced File Services (NAFS)
- NetWare Distributed Print Services (NDPS)
- NetWare Security Services
- NetWare Database Services

13 Die Entwicklungsgeschichte von Novell

- NetWare Communication Services
- NetWare Licensing Services (NLS)
- NetWare Backup and Storage Services
- NetWare Mobile Services
- NetWare Telephony Services
- NetWare Host Connectivity Services
- NetWare Transaction Services

NetWare Directory Services

Wie später auch noch im Kapitel über die Beschreibung von NetWare 4 zu sehen sein wird, bildet die NDS das zentrale Verwaltungsschema in zukünftigen Netzwerkprodukten von Novell und Produkten von Drittherstellern. Mit der NDS steht eine globale, verteilte und replizierbare Datenbank zur Verfügung. Durch die einfache objektorientierte Verwaltung können Netzwerkstrukturen mit Zigtausenden von Objekten eingerichtet und administriert werden. Da es sich um eine dynamische Struktur handelt, können die internen NDS-Definitionen sowohl von Novell als auch von Drittherstellern bei Bedarf modifiziert werden. So sind diese Verfahren bereits von Intel oder auch Cheyenne bekannt, um eine optimale Integration in die NDS-Struktur zu ermöglichen. Novell selbst führt entsprechende Erweiterungen durch, um z.B. Internet-Web-Seiten besser verwalten und sicher aufbauen zu können. Durch die grafische Administration der NDS werden die Aufgaben für den Administrator nicht nur übersichtlicher, sondern auch einfacher und besser handhabbar. Die wesentlichen Vorteile der NDS liegen vor allem in folgenden Punkten:

- *X.500-Interoperabilität*
Die NDS ist ein Subset der X.500-Standards. Obwohl Novell mehr Funktionalitäten im Vergleich zum X.500-Standard eingebaut hat, bietet die NDS eine offene Architektur, damit andere Directory Services miteinander arbeiten und gemeinsam Directory-Informationen nutzen können, indem standardmäßige X.500-Protokolle verwendet werden (DAP und DSP). Die NDS erweitert die Funktionalität von X.500 durch leistungsfähige Verteilung, Replizierung, Synchronisation, Flexibilität, Performance, Erweiterbarkeit und die Möglichkeit der individuellen Anpassung.
- *Zentrale Administration*
Da es sich bei der NDS um mehr als einen einfachen Domain Name Service handelt, haben es Administratoren wesentlich leichter, auch große und komplexe Netzwerke damit zu verwalten. Die grafischen Oberflächen helfen hierbei sehr viel weiter, da im Prinzip über ein grafisches Tool alle administrativen Aufgaben erledigt werden können.

13.4 Global-Network-Strategie

■ *Net2000 Support*

Die NDS bietet derzeit eine Vielzahl von APIs, die es Entwicklern ermöglichen, vollen Zugriff auf die NDS-Funktionen und -Mechanismen zu erhalten. Anwendungen, die bestehende APIs verwenden, sind zur NDS vollständig kompatibel. Net2000 wird bestehende NDS-Schnittstellen vereinfachen und erweitern. Auf diese Weise wird die Entwicklung NDS-fähiger Anwendungen einfacher. Durch den Einsatz der Net2000-Schnittstellen sind Entwickler in der Lage, Anwendungen zu erstellen, die voll auf die NDS-Mechanismen aufsetzen, bei denen Anwendungsdienste von selbst in der NDS registriert werden und die Directory Informationen durch neue und einmalige Mechanismen verwaltet werden können.

NetWare Advanced File Services (NAFS)

Novell ist derzeit dabei, ein neues Dateisystem für NetWare zu entwickeln. Das bisherige, auf einer verbesserten FAT-Struktur basierende, Dateisystem genügt den zukünftigen Anforderungen nicht mehr. Da sich diese ändern – Mobile Computing, integrierte Dokumente, objektbasierende Verarbeitung, Imaging und andere Mechanismen – und immer mehr Informationen erstellt werden müssen, besteht die Notwendigkeit, die Leistungsfähigkeit des Dateisystems zu verbessern. Als zukünftiges, verteiltes Dateisystem ist NAFS nicht mehr auf einen bestimmten Server fixiert und kann somit über mehrere Server und Endgeräte verteilt werden. Mit NAFS ist der Anwender nicht mehr gezwungen, Laufwerksbuchstaben für ein bestimmtes Volume eines bestimmten Servers zu definieren, sondern er definiert Laufwerksbuchstaben für logische Volumes im Netzwerk. Das heißt, NAFS ist eine konsequente Weiterentwicklung der NDS-Funktionalitäten, da man durch die NDS-Verwaltung netzwerkweit auf alle Ressourcen zugreifen kann, ohne wissen zu müssen, wo diese Ressourcen physikalisch installiert sind. Nur bei den Volumes muß man derzeit noch wissen, an welchem Server diese angebunden sind, um wieder auf die Datenbestände zugreifen zu können. Die wesentlichen Vorteile von NAFS sind vor allem:

■ *Integrierte Dokumente*

Unter integrierten Dokumenten versteht man Dokumente, die mehrere integrierte oder über Links verbundene Objekte wie Dateien, Images, Texte und Sprachdaten enthalten.

■ *Globale Replizierung*

NAFS unterstützt File-Replizierung und File-Caching, um zu garantieren, daß der Benutzer immer auf die Informationen Zugriff haben, auch wenn er nur zeitweise mit dem Netzwerk verbunden ist. Wird die Verbindung zum Netzwerk wieder hergestellt, erfolgt eine automatische Resynchronisation für die Dateien und Objekte.

13 Die Entwicklungsgeschichte von Novell

■ *Große Kapazitäten*

Da es sich beim NAFS um ein 64-Bit-Dateisystem handelt, können sehr große Datenmengen verwaltet werden. Aufgehoben wird auch die Limitierung von 64 Volumes pro Server, da im Prinzip beliebig viele Volumes verwaltet werden können. Zudem können Dateien in Terabyte-Größe etliche Millionen Dateien, Directories und Objekte pro Volume verwaltet werden. Die Volume-Größe ist jetzt schon unter NetWare im Terabyte-Bereich zu sehen.

■ *Globale Dateinamen*

NAFS wird mit in die NDS integriert werden, um globale Namen für alle Dokumente, Objekte und Dateien für das gesamte Netzwerk bilden zu können. Informationen sind vollkommen unabhängig von der Lokation, und der Anwender muß davon keine Kenntnis haben. Zudem wird das Dateisystem administrierbar über NDS-fähige Mechanismen und die dazugehörenden Management-Tools.

■ *Net2000 Support*

Verteilte Anwendungen benötigen ein stabiles File-System, um damit die unterschiedlichsten Dateitypen und -informationen verwalten zu können. Die NAFS APIs sind darauf abgestimmt, allen diesen Anforderungen (die auch in den vorherigen Ausführungen dargestellt worden sind) gerecht zu werden.

NetWare Distributed Print Services (NDPS)

Mit NDPS setzt Novell einen neuen Standard, um vollkommen neue Print-Mechanismen zu realisieren. Novell entwickelte NDPS zusammen mit HP und Xerox, um das Drucken im Netzwerk nicht nur zu erleichtern, sondern auch eine höhere Intelligenz beim Drucken zu integrieren. Die wichtigsten Eigenschaften hierbei sind:

■ *Bidirektionale Kommunikation*

Ein NDPS-fähiger Drucker kann dem Anwender und der Anwendung ständig einen vollständigen Status über den Druckjob geben. Die Drucker können den Anwender automatisch darüber informieren, wenn der Toner leer ist, Fehler am Drucker aufgetreten sind oder andere Eingriffe am Drucker notwendig werden.

■ *Periphere Intelligenz*

Die oben aufgeführte Intelligenz kann aber nicht nur für Drucker, sondern auch für Kopierer, Scanner oder Faxgeräte implementiert werden. NDPS bietet eine offene Schnittstelle, um Hersteller in die Lage zu versetzen, jedes Endgerät mit einer CPU in das Netzwerk einzubinden. Dieser Entwicklungsschritt ist auch als NEST-Technologie bekannt.

13.4 Global-Network-Strategie

■ *Plug-and-Print*

NDPS werden durch NDPS direkt in das Netzwerk eingebunden. Durch die Plug-and-Print-Option werden die Treiber für die Anwendungen automatisch heruntergeladen, so daß Benutzer in der Lage sind, ohne weitere administrativen Eingriffe mit den aktuellsten Treibern zu arbeiten. Die Implementierung von SNMP ermöglicht zudem auch die Verwaltung über entsprechende Management-Systeme.

■ *Net2000 Support*

Net2000 wird NDPS-Schnittstellen enthalten, die es Entwicklern ermöglichen, leistungsfähige Anwendungen und Utilities zu entwickeln, um intelligente NDPS-Peripherie in zukünftige Netzwerke integrieren zu können.

NetWare Security Services

In Anbetracht der Global-Network-Strategie muß noch mehr darauf geachtet werden, daß Netzwerke nicht nur noch leichter administrierbar werden, sondern auch entsprechende leistungsfähige Mechanismen vorhanden sind, um Sicherheit zu gewährleisten. Novell setzt hierbei zum einen auf eine sichere Architektur für das Netzwerkbetriebssystem und die Client-Komponenten, zum anderen wird die C2/E2-Zertifizierung durchgeführt.

NetWare Database Services

Eine Vielzahl von Drittherstellern gewährleistet, daß die entsprechende Unterstützung für Datenbankdienste gegeben ist. Diese Unterstützung spiegelt sich in dem Vorhandensein von Schnittstellen wider, mit denen man Daten der NDS nicht nur exportieren, sondern auch importieren kann. So bietet Oracle in seiner neuesten Version eine vollständige NDS-Integration.

NetWare Communication Services

Die Netzwerkdienste und verteilten Anwendungen müssen in der Lage sein, zu kommunizieren und Informationen gemeinsam zu nutzen, unabhängig von der eingesetzten Plattform, Lokation und dem Kommunikationsprotokoll. Um diesen Anforderungen sowohl jetzt als auch künftig gerecht werden zu können, unterstützt NetWare die Protokolle TCP/IP, SNA, LAT, IPX/SPX und AppleTalk. Die neuen Mechanismen für ATM können ebenfalls integriert werden. Daß man die Client-Server-Kommunikation inzwischen neben IPX/SPX-Protokollen auch für TCP/IP konfigurieren kann, erleichtert das Arbeiten mit Netware. Hierzu bietet NetWare 4 einen zusätzlichen NetWare/IP an, mit dem der Server und der Client für das TCP/IP-Protokoll aus-

13 Die Entwicklungsgeschichte von Novell

gestattet werden können. NetWare/IP ist ein Zusatz für NetWare, TCP/IP selbst wird standardmäßig mit NetWare ausgeliefert. Ab NetWare 5 kann auch Native-IP eingesetzt werden.

NetWare Licensing Services (NLS)

In künftigen Versionen von NetWare sind Module und Verwaltungsprogramme eingebaut, die es erlauben, Software-Lizenzüberwachung durchzuführen. Interessant ist dabei, daß sich die Mechanismen alle vollständig in die NDS integrieren lassen. Über diesen Weg sind Software-Hersteller in der Lage, Anwendungen bereits bei der Installation unter NetWare 4 automatisch lizenzieren zu lassen, indem entsprechende NDS-Objekte eingefügt werden.

NetWare Backup und Storage Services

Bereits vor Jahren hat Novell damit begonnen, zur Datensicherung einen neuen Mechanismus zu entwickeln, der unter der Bezeichnung SMS bekannt ist. Durch SMS hat Novell eine offene Architektur entwickelt, die Dritthersteller nutzen können, um die jeweiligen Backup-Systeme darauf aufsetzen zu können.

NetWare Mobile Services

Der Bedarf, flexibel und bequem von unterwegs in das Netzwerk eingebunden werden zu können, wird immer größer. Aus diesem Grund müssen Hard- und Software-Komponenten zur Verfügung stehen, die entsprechende Mechanismen anbieten. So bietet Novell selbst mit NetWare Connect ein Produkt an, mit dem Dial-in- und Dial-out-Funktionen realisiert werden können. Durch die vollständige Integration in die NDS werden auch alle notwendigen Sicherheitsmechanismen und -funktionen unterstützt, die über die NDS zur Verfügung gestellt werden. Zusätzliche Mechanismen innerhalb des NetWare-Connect-Produkts erweitern die entsprechenden Sicherheitsmechanismen. Durch den NetWare Mobile Client werden die Funktionen für Remote-Zugriffe um weitere Funktionen verbessert. Mit diesem Produkt geht es nicht nur darum, den Remote-Zugriff auf das Netzwerk zu realisieren. Es sind weitere Funktionen eingebaut, die es erlauben, bestimmte Datenbereiche vom Server auf die Workstation zu laden. Es kann dann mit diesen Daten weitergearbeitet werden, und beim erneuten Verbindungsaufbau zum Netz kann eine Resynchronisation der Daten auf dem Server erfolgen. Damit auf dem Remote-PC nicht jeder mit den Daten, die vom Server geladen worden sind, arbeiten kann, werden zusätzlich die Sicherheitsmechanismen und -funktionen von NetWare unterstützt. Das heißt, der Zugriff auf die transferierten Daten auf diesem PC kann nur dann er-

13.5 Internet Services

folgen, wenn man sich ordnungsgemäß auf diesem PC angemeldet hat. Der Remote-Client stellt also alle Sicherheitsfunktionen zur Verfügung, die notwendig sind, Daten auf dem PC so zu bearbeiten, als würden sie sich auf dem Server befinden.

NetWare Telephony Services

Es wird immer deutlicher die Tendenz sichtbar, eine Vielzahl von Diensten über das Netzwerk abzuwickeln. Man hat auch nicht davor haltgemacht, die Telefondienste ebenfalls in das Netzwerk zu integrieren. Eine Vielzahl von Funktionen, die mit der Telefonanlage und dem Telefonieren verbunden sind, lassen sich dabei nicht nur überwachen, sondern auch steuern. Das Ziel von Novell ist auch darin zu sehen, daß die NDS als Basis zum Aufbau eines Telefonbuchs genutzt wird, in dem bereits entsprechende Einträge gemacht werden können. Hierzu müssen auf dem NetWare Server notwendige Module installiert und über einen passenden Kommunikationsadapter muß die Verbindung zur Telefonanlage hergestellt werden.

NetWare Host Connectivity Services

Wenn es darum geht, heterogene Netzwerke zu realisieren, dann muß auch die Einbindung von Host-Systemen unterstützt werden. Die am weitesten verbreiteten und am meisten benötigten Mechanismen sind die Integration der IBM-Welt (Großrechner und AS/400) und die Integration der DEC- und Unix-Welt. Dabei besteht die Produktfamilie zur Einbindung in die IBM-Welt aus NetWare for SAA, NetWare HostPrint und NetWare HostPrint/400. Das Produkt NetWare for DEC dient zur Integration in die DEC-Welt, so daß gemeinsam auf Dateien und andere Ressourcen zugegriffen werden kann. Über die NetWare NFS Services werden der bidirektionale Zugriff auf Dateien und das bidirektionale Drucken ermöglicht. Durch die vollständige Integration in die NDS-Umgebung wird das Verwalten und Einrichten wesentlich vereinfacht.

13.5 Internet Services

Das Internet bietet für alle Anwender, die darauf Zugriff haben, eine Vielzahl von Informationen und Diensten. Neben den Möglichkeiten, Informationen zu holen und anzubieten (über entsprechende Web-Seiten bzw. das World Wide Web) wird das Internet hauptsächlich dazu verwendet, E-Mails zu versenden. Aufgrund der rasanten Verbreitung, die das Internet in der letzten Zeit erfahren hat, wächst auch der Bedarf, einfach und schnell die Dienste im Internet nutzen zu können. Die Hersteller sind bestrebt, eine breite Palette an Pro-

13 Die Entwicklungsgeschichte von Novell

dukten dafür anzubieten. Es muß dabei nur darauf geachtet werden, daß die Einbindung in das Netzwerk, d.h. die Kompatibilität zum Netzwerkbetriebssystem bzw. zum Client, gewährleistet ist. Dies ist vor allem beim Einsatz von Web-Browsern, Web-Servern und Publisher-Programmen zu berücksichtigen. Um dem auch gerecht werden zu können, bietet Novell TCP/IP-Unterstützung für Clients und Server, Unix Services bzw. NetWare/IP mit der Unterstützung von DNS-Server und NIS-Server, Web-Server mit vollständiger NDS-Integration und passende Publisher-Software-Integration.

Ein weiterer Meilenstein in dieser Richtung ist die Lizenzierung von Sun Microsystems Java-Plattform durch Novell. Novell hat in einem Abkommen mit Sun Microsystem die Java-Plattform erworben. Somit ist Novell in der Lage, Entwicklern und Kunden den Zugang zu Java zu bieten.

Java – ebenfalls ein Schlagwort, das man in letzter Zeit immer häufiger zu hören bekommt. Was steckt eigentlich dahinter?

Java ist ursprünglich eine Programmiersprache zur Erstellung von Anwendungen im Internet – vor allem für die Erstellung von World-Wide-Web-Seiten. Java war die erste Programmiersprache, mit deren Hilfe gleichzeitig Musik und Animation in eine Web-Seite eingebunden werden können. Bei der Entwicklung der Programmiersprache Java wurde großer Wert darauf gelegt, eine einfache, objektorientierte, robuste und architekturunabhängige Plattform bereitzustellen.

Mit der Java-Technologie unter NetWare wird Novell also eine neue Programmierungsumgebung für NetWare Server zur Verfügung stellen. Durch diese Technologie wird es möglich sein, auf Java-Applikationen zuzugreifen, unabhängig von der Client-Plattform. Dies gilt sowohl für das Internet als auch für das Intranet.

Intranet – ebenfalls ein häufig verwendeter Begriff. Das Intranet ist im Prinzip das Internet für ein Unternehmen. Auf diese Weise stellt man Internetmechanismen und -möglichkeiten für ein einzelnes Unternehmen zur Verfügung. Wird der Zugang zum weltweiten Internet geschaffen, verbindet sich das Intranet mit dem Internet. Alle neuen Entwicklungen, die sich für das Internet ergeben, werden auch für das Intranet zur Verfügung stehen und umgekehrt.

Durch das Lizenzabkommen kann Novell den gesamten Java-Funktionsumfang an Software-Entwickler weitergeben. Durch die Einbettung der Java Virtual Machine in NetWare sind Entwickler damit in der Lage, Java-Anwendungen für NetWare zu erstellen. Damit wird sich eine neue Entwicklungsrichtung und -umgebung ergeben. Auf diese Weise wird Java die Applikationsumgebung der nächsten Generation und andererseits NetWare die nächste große Anwendungs-

13.6 Open Solutions Architecture

plattform für Java werden. Durch die Java Virtual Machine und die notwendigen Class Libraries in NetWare verfolgt Novell das Ziel, NetWare zur Quelle aller Java-Funktionen zu machen.

Novell wird in diesem Zusammenhang auch die Java-Anwendungen in die NDS integrieren. Damit werden Client-Netzwerk-Architekturen unterstützt, in der Anwendungen oder Objekte über Intranets oder das Internet verteilt werden können. Bei den vorherigen Ausführungen wurde bereits mehrfach der Begriff Net2000 verwendet. Net2000 ist der momentane Code-Name von Novell, mit dem Novell diese Initiative verfolgt. Abschließend sollen deshalb diese Schlüsselfunktionen der Net2000-Initiative dargestellt werden:

1. Component Management Services nutzen die Möglichkeiten der NetWare Directory Services (NDS). Sie konzentrieren sich auf die Verteilung, gemeinsame Nutzung, Zugriff, Sicherheit und Management von Komponenten über das Netzwerk.
2. Einfacher Zugriff auf NetWare-Dienste durch standardisierte Schnittstellen. Hierzu gehören OLE Control (OCX), Visual Basic Control (VBX), Delphi Control (VCL) und Java Class Libraries. Durch diese Mechanismen können Administratoren und Entwickler einfach und schnell Anwendungen erstellen, mit denen man auch auf die Vielzahl der Netzwerkdienste zugreifen kann. Hierzu zählen u. a. die wesentlichen Dienste, die mit der NDS verbunden sind.
3. Erweiterung der NetWare-Entwickler-Plattform durch die Lizenzierung der Java-Plattform. NetWare soll dadurch nicht mehr länger als File- und Print-Service-Plattform gesehen, sondern immer mehr in Richtung Applikations-Server genutzt werden. Hierzu sollen leistungsfähige Anwendungen für das Intranet und das Internet bereitgestellt werden.

Als letzte Entwicklungsrichtung zur weiteren und stetigen Verbesserung der NetWare-Umgebung hat Novell die Open Solutions Architecture (OSA) eingeführt. Der Inhalt und die Strategie von OSA sollen nachfolgend näher erläutert werden.

13.6 Open Solutions Architecture

Novell Open Solution Architecture (OSA) ist eine neue Entwicklerstrategie von Novell zum Aufbau von Directory-basierenden Anwendungen für das Internet. Zur zentralen Aufgabe von Novell, um das Netzwerk Directory-fähig zu machen, gehört auch, Anwendungen und Lösungen ebenfalls Directory-fähig und für die Installation, das Management, die Lizenzierung, die Entwicklung, die Überwachung und den Einsatz über das Netzwerk einfacher zu machen. OSA setzt

13 Die Entwicklungsgeschichte von Novell

dabei auf Internet-Standards und offene Schnittstellen, um den Entwicklern einfache Werkzeuge zur Verfügung zu stellen. Hierzu gehört auch die Verfügbarkeit einer großen Anzahl von APIs und Netzwerkdiensten, um netzwerkfähige, internetfähige und realisierbare Lösungen erstellen zu können. Entwickler haben dabei die Wahlmöglichkeit, serverbasierende Anwendungen in C (NLM-Technik), Java (Java Class Libraries, JavaBeans und Enterprise JavaBeans) und Script-Sprachen (JavaScript, Perl und NetBasic) zu erstellen. Die Schnittstellen für die Clients, z.B. ActiveX Controls oder C-APIs, sind ebenfalls verfügbar, um Client/Server-Anwendungen zu entwickeln.

Zu den generellen APIs, Frameworks und Infrastrukturen, die in OSA enthalten sind, gehören:

- *Java/CORBA-Runtime-Umgebung*
Java Virtual Machine (JVM) – Java Developer's Kit (JDK), JIT Compiler, Java CORBA Object Request Broker (ORB)
- *Java-Application-Server-Umgebung*
Weblogic Tengah Java Application Server, Database Access (JDBC), JavaBeans, RMI, Servlets, Java Naming und Directory Interface, Java Networking Service Interface, Enterprise JavaBeans und vieles mehr.
- *Internet-Web/Database-Development-Umgebung*
Netscape Fastrack & Enterprise Web Server, CGI, JavaScript, Perl, NetBasic (Visual Basic Scripts), ODBC- und JDBC-Schnittstellen und vieles mehr.
- *Tools und Entwickler-Umgebung*
Symantec Visual Café, IBM Visual Age, Inprise Jbuilder und vieles mehr.
- *Management- und Entwicklungs-Umgebung*
Common Console Framework (ConsoleOne), Common Installation, Licensing, Metering und vieles mehr.

Für die Entwicklung von OSA sind die Anforderungen der Benutzer, Planer und Strategen verantwortlich, um den Einsatz und die Verwaltung von Netzwerken immer einfacher, schneller und leistungsfähiger zu gestalten. Den Entwicklern sollen jedoch auch Werkzeuge und Entwicklungsplattformen an die Hand gegeben werden, die es erlauben, diese Anforderungen auch schnell und unproblematisch umzusetzen und einzusetzen.

Novell definiert OSA wie folgt:

„Open Solutions Architecture integrates existing Novell architecture, technologies and products. It builds on the vision that everything is connected through the network, where heterogeneous systems must be integrated to provide solutions to everyday problems. Open Solu-

13.6 Open Solutions Architecture

tions Architecture is not the killer application or service. It is the standards and infrastructure that enable the heterogeneous systems to come together in the network workplace.“

Da die Systeme in einem Netzwerk nicht nur heterogen sind, sondern auch zukünftig heterogen bleiben und noch heterogener werden, wird eine Vielzahl von Architekturen existieren, die wiederum das Ziel erfüllen müssen, daß eine Kommunikation zwischen diesen Systemen möglich ist. Ebenso wird gefordert, daß eine vernünftige und – wenn möglich – einheitliche Handhabbarkeit existieren soll. So basiert zum Beispiel eine typische Anwendung auf der NCA (Network Computing Architecture) von Oracle, kommuniziert mit dem Fastrack Web Server von Netscape und fügt alle Komponenten mit Hilfe von ActiveX Controls von Microsoft zusammen. Open Solutions Architecture beabsichtigt, die notwendigen Tools und die Infrastruktur zur Verfügung zu stellen, um die notwendige Integration dieser unterschiedlichen Technologien und Umgebungen in einer einheitlichen Lösung zu erreichen. OSA integriert deshalb auch die bereits existierenden Produkte und Architekturen und bietet zudem den Einstieg für zukünftige Architekturen. In Abbildung 13.6 ist dargestellt, wie man sich die Architektur von OSA vorzustellen hat.

Es ist zu ersehen, daß Java eine sehr wichtige Rolle bei dieser Architektur spielt. So unterstützen die Directory Services derzeit Java noch nicht direkt. Wenn Novell die Unterstützung für die Java-Ausführung erweitert, dann werden einige oder alle Komponenten der Directory Services für die Java-Unterstützung umgestellt werden. Novell wird sowohl selbst als auch mit Partnern entsprechende und notwendige Tools zur Verfügung stellen, um eine problemlose Entwicklung auf Basis der OSA durchführen zu können.

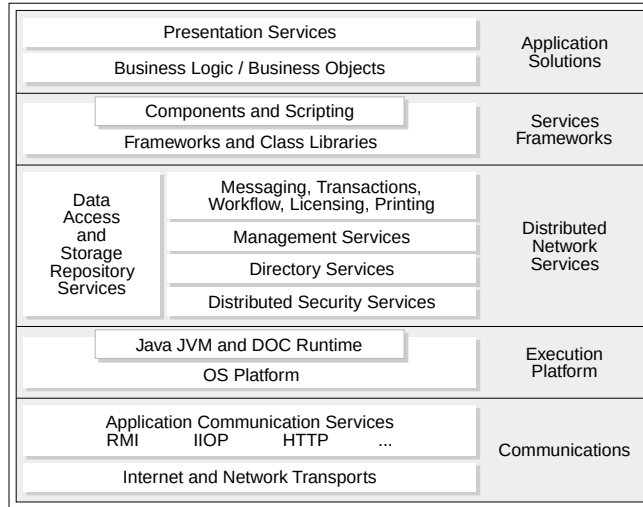
Es ist nicht zu verkennen, daß Novell bereits mit den heutigen Entwicklungen ein hohes Maß an Sicherheit, Stabilität und Leistungsfähigkeit zur Verfügung gestellt hat. Dies wird durch die sehr leistungsfähige Serverplattform erreicht, auf die alle Clients zugreifen können; dies beginnt bei DOS, OS/2, Windows NT, Windows 95/98, WfW, Unix und hört bei Apple-Macintosh-Rechnern auf.

Die Basis dieser gesamten Entwicklung bildet deshalb die Serverplattform (siehe auch die nachfolgenden Kapitel und Beschreibungen), d.h. das Serverbetriebssystem, der Client und die Anwendungen auf Basis einer Client-Server-Architektur.

Zu den bisherigen Serverbetriebssystemen ist zu sagen, daß Novell schon immer versucht hat, die bestehende Hardware-Plattform optimal zu nutzen.

13 Die Entwicklungsgeschichte von Novell

Abbildung 13.6
OSA-Architektur



Man war schon immer bestrebt, ein dediziertes Netzwerkbetriebssystem zur Verfügung zu stellen, das ausschließlich die Serverfunktion übernimmt und nicht zusätzlich als Workstation dienen kann. Nur so ist man in der Lage, ein optimal gestaltetes NOS (Network Operation System) zu entwickeln. Das Kernstück bildet dabei der Kernel, der inzwischen auch als Multiprozessor-Kernel zur Verfügung steht. Das ursprünglich und inzwischen legendäre IPX-Protokoll für die Kommunikation der Workstations mit dem Server wird mit Einführung von NetWare 5 durch Native-IP abgelöst. IPX wird zwar immer noch als Protokoll unterstützt, bildet aber nicht mehr den primären Protokoll-Charakter. Die klassischen Services am Server werden über das NetWare Core Protocol (NCP) abgewickelt. Prägnant für den Serverbetrieb ist auch der Einsatz von NLMs (NetWare Loadable Modules), um den NetWare Kernel um weitere zusätzliche Funktionen erweitern zu können, mit der Möglichkeit, NLMs im laufenden Betrieb zu laden und zu entladen. Die Änderungen im Netzwerkbetriebssystem, so wie diese mit NetWare 5 eingeführt werden, unterstützt OSA ebenso wie die traditionellen Funktionen.

Auch der Client hat in den letzten Jahren eine enorme Entwicklung erlebt. Typischerweise besteht ein Client aus einem Redirector, einem Requester und einem Sicherheitsmodul. Der Redirector fängt lokale Betriebssystemaufrufe ab und konvertiert diese in Service Requests für den Server. Auf ähnliche Art und Weise werden die Ergebnisse des Servers, die zum Client zurückgeschickt werden, zurückkonvertiert in lokale Betriebssystemfunktionen. Der Redirector verwendet normalerweise einen Requester – ein Modul, das mit dem

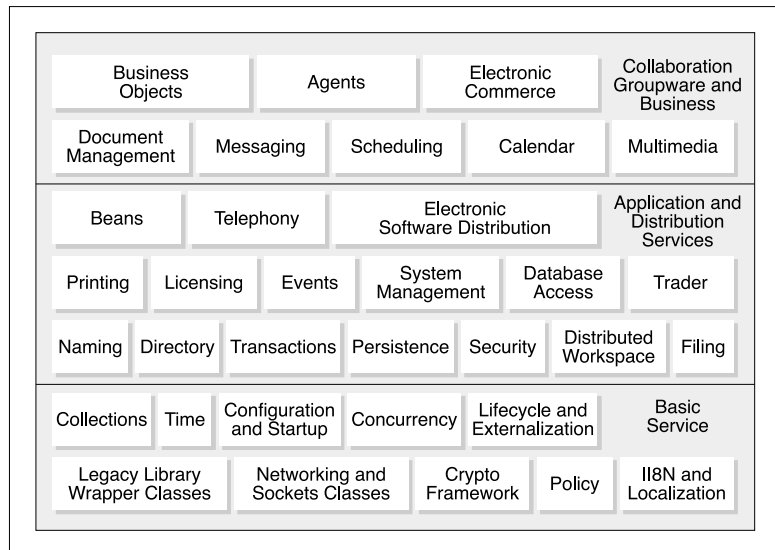
13 Die Entwicklungsgeschichte von Novell

In Abbildung 13.7 ist dargestellt, wie man sich die Verbindungen zwischen den einzelnen Kommunikationsbereichen vorstellen muß. Daraus ist auch zu erkennen, daß OSA in Zusammenarbeit mit dem Industriestandard eingesetzt werden kann, um damit die Integration und Kommunikation untereinander gewährleisten zu können. Nicht übersehen werden darf, daß De-facto-Standards, die ebenso wichtig sind, unterstützt werden. So ist zum Beispiel RMI (Remote Method Invocation) ein De-facto-Standard für Java, und die Unterstützung für die sogenannten Connectivity-Standards IIOP und LDAP sind ebenso gegeben.

Neben den sogenannten Connectivity-Mechanismen bietet OSA eine vollständige Palette von Diensten, die aus dem Netzwerk das machen, was man braucht und erwartet. In Abbildung 13.8 ist der Aufbau dieser Architektur zu sehen, die sich in drei Bereiche aufteilt:

- Basic Services
- Application und Distribution Services
- Collaboration, Groupware und Business

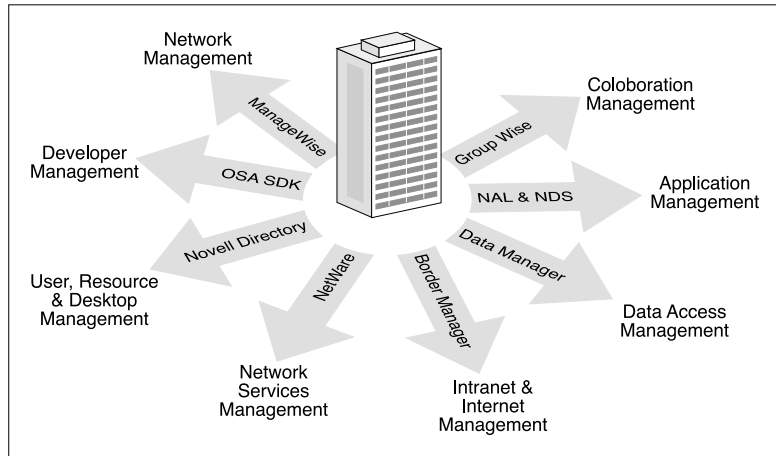
Abbildung 13.8
Architekturaufbau



Die OSA-Architektur wird weiterentwickelt zum sogenannten Universal Component System, um damit noch leistungsfähiger werden zu können. Abschließend sei aufgezeigt, welches Ziel Novell verfolgt, um ein vollständiges Management des Unternehmens realisieren zu können. Hierzu ist in Abbildung 13.9 dargestellt, welche einzelnen Bereiche dafür von Novell abgedeckt werden.

13.6 Open Solutions Architecture

Abbildung 13.9
Management des
gesamten Unter-
nehmens



Aus diesen Ausführungen ist zu ersehen, daß Novell sehr großen Wert darauf legt, eine leistungsfähige und erweiterbare Basis für den Aufbau sowohl kleiner als auch großer Netzwerkumgebungen zu schaffen. Es wird aber auch klar, daß die zukünftige Entwicklung immer mehr in Richtung NDS unter NetWare 4 und NetWare 5 geht. Ebenso ist zu erkennen, daß Java ein strategisches Element für zukünftige Entwicklungen sein wird. Bei den Ausführungen über NetWare 5 werden Sie darüber noch mehr erfahren. Es stellt sich dabei aber auch die Frage, wie die Entwicklung bei Microsoft aussieht. Im folgenden sollen deshalb die unterschiedlichen Plattformen dargestellt werden, die Novell und Microsoft zur Verfügung stellen. Es geht darum, wie sich diese beiden Plattformen voneinander unterscheiden und wo deren Vor- und Nachteile zu sehen sind.

14

Netzwerkbetriebssysteme

Neben der richtigen Wahl der Hardware-Ausstattung eines LAN ist es ebenso wichtig, sich für das geeignete Netzwerkbetriebssystem zu entscheiden, um die notwendigen Aufgaben und Funktionen in einem LAN ausführen zu können. In diesem Kapitel will ich Ihnen die wichtigsten Aspekte aufzeigen.

Im nächsten Kapitel werden die Netzwerkbetriebssysteme von Novell und ihre Funktionalität näher erläutert.

Auf die wichtigsten Aufgaben der LANs bin ich bereits im einzelnen eingegangen. Bei Auswahl von Netzwerkbetriebssystemen sind unter anderem zu beachten:

- Betriebssystemarchitektur
- Server-Plattform
- Protokollunterstützung
- Performance
- Zuverlässigkeit
- Unterstützte Standards

14.1 Betriebssystemarchitektur

Wenn es um die Auswahl von Netzwerkbetriebssystemen geht, können vier Komponenten unterschieden werden:

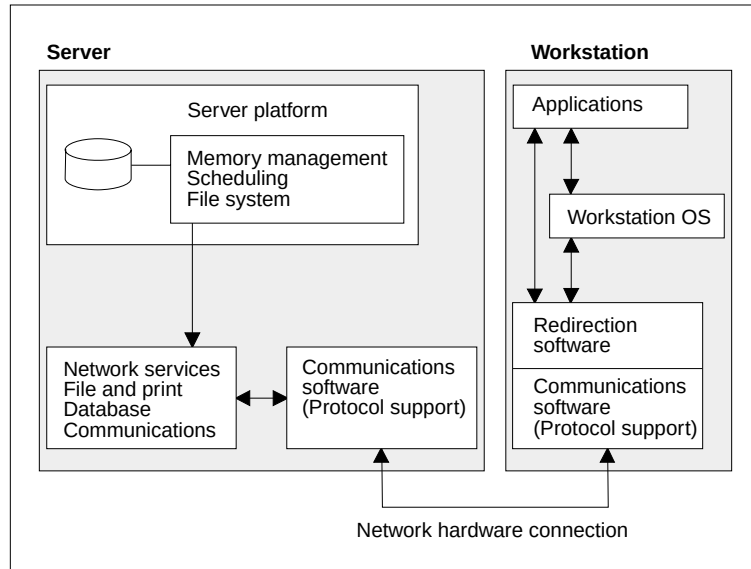
- Server-Plattform
- Unterstützte Netzwerkdienste
- Redirection-Software
- Kommunikationssoftware

Diese Komponenten beeinflussen im wesentlichen die Funktionsfähigkeit und Flexibilität eines Netzwerks. In Abhängigkeit davon können Sie die Leistungsfähigkeit des Gesamtsystems bewerten. Der Zusammenhang dieser Teilbereiche ist in Abbildung 14.1 dargestellt.

Wie bereits besprochen, stellt die Auswahl der richtigen Server-Plattform das Kernstück eines Netzwerkbetriebssystems dar und ist somit entscheidend, was die Leistungsfähigkeit und Ausbaufähigkeit eines Netzwerks betrifft. Auf dieser Server-Plattform läuft das Netzwerkbetriebssystem und stellt in Zusammenarbeit mit dem Betriebssystem alle notwendigen Funktionen zur Verfügung.

14 Netzbetriebssysteme

Abbildung 14.1
Wie Server und
Workstation mit-
einander kommu-
nizieren



Die Unterstützung des Dateisystems, das Memory Management oder auch das Scheduling (Verwalten) der Prozessortasks werden maßgeblich von dieser Server-Plattform bestimmt. Wenn in den folgenden Kapiteln auf NetWare 5, NetWare 4 und NetWare 3.2 eingegangen wird, werden Sie besser verstehen, in welcher Beziehung diese Faktoren zueinander stehen.

Die Netzwerkdienste auf der Server-Plattform sind verantwortlich für die Unterstützung weiterer wichtiger Netzwerkdienste, wie zum Beispiel File- und Record-Locking. Es kann sich dabei aber auch um wesentlich komplexere Angelegenheiten handeln, wenn zum Beispiel auf der Server-Plattform ein SQL-Server abläuft und dieser für die Verwaltung von verteilten Datenbanken zuständig ist bzw. SQL-Abfragen erledigen muß. Es handelt sich dabei um eine typische Anwendung von verteilter Verarbeitung; ein Schlagwort dafür ist inzwischen das Client-Server-Prinzip geworden.

Auf irgendeine Art und Weise muß in einem Netzwerk eine Verbindung zwischen dem Workstation-Betriebssystem und dem Netzbetriebssystem hergestellt werden. Die reine Verkabelung der einzelnen Komponenten reicht dabei noch nicht aus. Die Systeme müssen auch in der Lage sein, das zu verstehen, was ihnen der andere Partner erzählt. Dieser Teil der Kommunikation wird von der Netzwerkkommunikations-Software abgedeckt. Sie ist in der Lage, eine logische Verbindung mit Hilfe der physikalischen Verkabelung zwischen den im Netzwerk beteiligten Stationen aufzubauen.

14.1 Betriebssystemarchitektur

Die Kommunikationssoftware unterstützt ein oder mehrere Kommunikationsprotokolle, um Anfragen (Requests) bzw. Antworten (Replies) über das Netzwerk empfangen und versenden zu können. Ein Bindeglied auf der Workstation zwischen der Anwendung und der Kommunikationssoftware ist die sogenannte Redirection-Software, sehr oft auch als Shell bezeichnet. Deren Aufgabe ist es, zu entscheiden, ob eine formulierte Anfrage vom eigenen Workstation-Betriebssystem oder vom Netzwerkbetriebssystem zu erledigen ist. Ein typischer Anwendungsfall ist zum Beispiel der Zugriff auf die lokale Festplatte zum Lesen einer Datei (dies muß vom Workstation-Betriebssystem erledigt werden) oder das Lesen einer Datei von der File-Server-Platte (dies muß von der Redirection-Software zum File-Server übertragen werden).

Wie bei NetWare 3.2 zu sehen sein wird, kann auf die Redirection-Software unter bestimmten Voraussetzungen verzichtet werden, zumindest was die besondere Anpassung an die NetWare-Umgebung anbelangt.

In den letzten Ausführungen habe ich Ihnen bereits grundlegende Aspekte in bezug auf die möglichen Server-Plattformen aufgezeigt. Wie Sie daraus ersehen können, lassen sich zwei Plattformen herausfiltern:

- Native Server (»spezielle« Server)
- Host-basierende Server (»allgemeine« Server)

Mit beiden Server-Typen kann eine breite Palette von Netzwerkdiensten abgedeckt werden. Eine Server-basierende Datenbankapplikation kann zum Beispiel in Verbindung mit den Netzwerkdatei- und Druckdiensten laufen.

Native Server zeichnen sich dadurch aus, daß sie für ganz spezielle Aufgaben im Netzwerk konzipiert werden bzw. das Betriebssystem die Funktionalitäten auf diesen Servern voll ausnutzen kann. Ein Dedicated NetWare Server zum Beispiel ist optimiert für die Unterstützung von Datei- und Druckdiensten im Netzwerk. Da die Native Server auf die Abarbeitung spezieller Jobs zugeschnitten sind, können von ihnen bestimmte Funktionen, Leistungssteigerungen und Zuverlässigkeitsaspekte unterstützt werden, wie sie nicht unbedingt von Host-basierenden Servern angeboten werden können. Native Server werden vor allem dann eingesetzt, wenn sehr großer Wert auf Zuverlässigkeit, Sicherheit, Geschwindigkeit, Funktionalität und Flexibilität gelegt wird.

In den meisten Fällen basieren Native Server auf 80486-, 80586- oder Pentium-Prozessoren, da sie bezüglich der Leistungsfähigkeit eine Vielzahl von Netzwerkdiensten innerhalb eines Serversystems ab-

14 Netzwerkbetriebssysteme

decken und hohe Leistungsfähigkeit zur Verfügung stellen können. Server mit 80386-Prozessoren sind inzwischen aufgrund der geringeren Leistungsfähigkeit in diesen Punkten beschränkt einsetzbar und werden in der Regel nur noch als Testsysteme verwendet – wenn überhaupt. Ausschlaggebend hierbei ist auch der Einsatz des richtigen Netzwerkbetriebssystems, damit dieses die Prozessorleistung voll ausnutzen kann. Hierbei unterscheiden sich auch die Konzepte von NetWare und NT Server. Inzwischen ist man soweit, daß man bei der Neubeschaffung eines Servers sowieso darauf abzielt, den aktuell besten Prozessor zu nutzen. Ausschlaggebend für die Ausstattung des Servers ist dann im wesentlichen nur noch die Frage des Hauptspeicherbedarfs. Da sich auch hierin NetWare und NT Server voneinander unterscheiden, stehen für das jeweilige Netzwerkbetriebssystem Berechnungsformeln zur Verfügung, um den aktuellen und zukünftigen Speicherausbau (in Abhängigkeit der eingesetzten Anwendungen) ermitteln zu können.

Host-basierende Server stützen sich auf Betriebssysteme wie OS/2, Unix, VMS, MVS oder OS-AS400. Es muß genau untersucht werden, für welche Einsatzgebiete diese Server geeignet sind. Sehr oft geht es auch um effektive Kopplung unterschiedlicher Netzwerksysteme. Diese Server werden auf unterschiedlichen Hardware-Plattformen angeboten, die sich zum Teil in ihren Funktionen, Geschwindigkeiten, flexiblen Ausrichtungen und ihrer Leistungsfähigkeit wesentlich unterscheiden. Da diese Host-basierenden Server nicht dediziert eingesetzt werden, können bei deren Einsatz unter Umständen Kosten eingespart werden. Die Kosteneinsparung bedeutet aber nicht selten auch eine Verminderung der Zuverlässigkeit oder Leistungsfähigkeit. Das hängt jedoch stark von der eingesetzten Hardware-Plattform ab.

14.2 Die wichtigsten Anforderungen an Netzwerkbetriebssysteme

Um die nachfolgenden Ausführungen über die unterschiedlichen Netzwerkbetriebssysteme besser verständlich zu machen, werde ich in diesem Abschnitt die wichtigsten Anforderungen, die ein Netzwerkbetriebssystem erfüllen muß oder sollte, kurz darstellen. Wie Sie bei den unterschiedlichen Netzwerkbetriebssystemkonzepten von Novell anschließend sehen werden, unterscheiden sich diese durch die Erfüllung der einzelnen Faktoren mehr oder weniger stark. Sie können die hier aufgeführten Faktoren auch heranziehen, um einen Vergleich unterschiedlicher Netzwerkkonzepte durchführen zu können.

14.2 Die wichtigsten Anforderungen an Netzwerkbetriebssysteme

14.2.1 Leistungsfähigkeit

Dies ist die häufigste Anforderung, die an Netzwerkbetriebssysteme gestellt wird. Da Netzwerke immer größer werden – Netzwerke mit mehreren hundert Endstationen sind keine Seltenheit mehr –, bekommt dieser Faktor vor allem im Zusammenhang mit den Network Computing immer größere Bedeutung. Deshalb benötigen immer mehr Benutzer Netzwerkdienste des File-Servers. Dazu ist aber nicht nur ein ausgefeiltes Netzwerkbetriebssystem am File-Server notwendig, sondern es sollte auch großer Wert auf die Verkabelung des gesamten Systems gelegt werden. Was nützt Ihnen das leistungsfähigste Netzwerkbetriebssystem, wenn gleichzeitig das Verkabelungssystem, d.h. die Topologie des Netzwerks, nicht in der Lage ist, das Datenvolumen, das über das Netzwerk transportiert werden muß, schnell genug zu übertragen. Entscheidend ist aber nicht nur der Einsatz der richtigen Netzwerktopologie, sondern auch der Einsatz leistungsfähiger Netzwerkkarten. Dieser Faktor wird leider bei der Auswahl von Netzwerken sehr oft unterschätzt, da nur das Augenmerk auf die Leistungsfähigkeit des File-Servers gelegt wird. Was nützt Ihnen jedoch der schnellste File-Server und das leistungsfähigste Netzwerkbetriebssystem, wenn über das Verkabelungssystem die Daten nicht schnell genug transportiert werden können.

Berücksichtigen Sie deshalb bei der Auswahl von Netzwerken auch diese Faktoren, um sich nicht bereits bei der Verkabelung und den Netzwerkkarten einen Flaschenhals einzubauen. Beachten Sie immer den Grundsatz: Das Gesamtsystem ist nur so gut wie das schwächste Glied in der Kette. Bei der Auswahl der File-Server-Komponente können Sie sich zwischen Native Servern (z.B. PCs) und Host-basierenden Servern entscheiden. Dann sind auch noch die Kosten für diese Server-Plattform zu berücksichtigen.

14.2.2 Zuverlässigkeit

In jedem Netzwerk wird sehr großer Wert auf die Zuverlässigkeit der Netzwerkinstallation gelegt. Dieser Faktor bekommt eine um so größere Bedeutung, je mehr kritische Anwendungen über das Netzwerk abgewickelt werden und je größer die Abhängigkeit der Benutzer vom Funktionieren des Netzwerks ist. Der Ausfall eines Netzwerks über längere Zeit hinweg kann unter Umständen die Existenz eines Unternehmens aufs Spiel setzen. Deshalb muß sowohl von der Hardware als auch vom Netzwerkbetriebssystem her ein gewisses Maß an Zuverlässigkeit gegeben sein, um alle kritischen Faktoren eines Ausfalls abfangen zu können.

14.2.3 Sicherheit

Da die Benutzer im Netzwerk auf immer mehr Ressourcen Zugriff haben (dies gilt vor allem für die vernetzte Datenverarbeitung), muß ein immer größeres Augenmerk auf die Sicherheit im Netzwerk gelegt werden. Es muß gewährleistet sein, daß die Benutzer nur auf die Daten und Ressourcen Zugriff haben, die sie unbedingt für die Arbeit benötigen. Die dafür notwendigen Sicherheitsmechanismen können in folgende Bereiche aufgeteilt werden:

- Accounting-Sicherheit
- Paßwortsicherheit
- Directory-Sicherheit
- Dateisicherheit
- Internetwork-Sicherheit
- File-Server-Sicherheit

Die am Markt befindlichen Netzwerkbetriebssysteme variieren in ihrer Flexibilität, diese Sicherheitsmechanismen mehr oder weniger abdecken zu können. Die Unterstützung solcher Mechanismen ist zum Teil auch abhängig von der eingesetzten Server-Plattform. Auf die einzelnen Aspekte werde ich bei der Besprechung der von Novell angebotenen Netzwerkbetriebssysteme näher eingehen.

14.2.4 Workstation-Unterstützung

Vor einigen Jahren konnte noch ohne Bedenken behauptet werden, daß DOS als Workstation-Betriebssystem den Markt beherrscht. Dies hat sich auch durch den Einsatz von Windows und Windows for Workgroups nicht geändert. Heute sieht die Situation bereits ganz anders aus. Wenn man den Markt näher betrachtet, kann man vier Standardbetriebssysteme für Workstations unterscheiden: DOS, OS/2, Windows 95/98, Windows NT, Macintosh und Unix. Es besteht deshalb die Anforderung, diese unterschiedlichen Workstation-Betriebssysteme auf Arbeitsplatzrechnern im Netzwerk einzusetzen. Es ist aber leider nicht so, daß man jedes beliebige Betriebssystem auf den Workstations einsetzen kann, um damit auf dem File-Server arbeiten zu können. Wenn Sie Abbildung 14.1 ansehen, stellen Sie fest, daß dazu die notwendigen Software-Schnittstellen und Programme zur Verfügung stehen müssen, damit sie in ein Netzwerkkonzept eingebunden werden können.

Jedes Betriebssystem verwendet dabei sein eigenes Dateisystem, das mit den anderen Dateisystemen nicht kompatibel ist. Damit der Anwender im Netzwerk nicht auf ein bestimmtes Betriebssystem für die Workstation beschränkt ist (Novell spricht von »the users' freedom to choose the workstation operating system«), muß das Netzwerkbetriebssystem

14.2 Die wichtigsten Anforderungen an Netzwerkbetriebssysteme

triebssystem den Einsatz unterschiedlicher Workstation-Betriebssysteme unterstützen, entweder durch spezielle Funktionen am File-Server (siehe NetWare 3 oder NetWare 4) oder durch spezielle Software auf der Workstation in Verbindung mit einer dazugehörigen Server-Unterstützung, wenn es auch darum geht, die Native-Dateiformate zu unterstützen. Man geht jedoch dazu über, die Funktionalität eines sogenannten Multi-Protokoll-Stacks auf die Server-Plattform zu verlagern, um flexibler zu bleiben und Workstations in der gewohnten Umgebung zu belassen, d.h., so wie sie sind, was sie können und wie sie bislang zum Einsatz gekommen sind. Betrachtet man die Entwicklung von Novell oder Microsoft, so stellt man fest, daß beide Hersteller bestrebt sind, die Unterstützungsmechanismen zu implementieren, um allen Anforderungen, die zukünftig zu erwarten sind, gerecht werden zu können.

Das Problem liegt aber nicht nur in den unterschiedlichen Dateisystemen, sondern auch in den unterschiedlich eingesetzten Protokollen, die nicht miteinander kompatibel sind, wenn es darum geht, Anfragen zum File-Server zu übertragen bzw. Antworten des File-Servers verstehen zu können. Deshalb ist die Forderung nach Protokollunabhängigkeit seitens des Netzwerkbetriebssystems eine unabdingbare Forderung. Mit NetWare und NT Server wird dem Rechnung getragen.

14.2.5 Standards

Neben der unterstützten Architektur, der Leistungsfähigkeit, der Zuverlässigkeit und Sicherheit des File-Servers ist auch noch die Unterstützung von Industriestandards durch das Netzwerkbetriebssystem von entscheidender Bedeutung. Die Unterstützung unterschiedlicher Standards gewährt die Einbindung in ein heterogenes System, vor allem dann, wenn es um Network Computing geht. Somit wird die Effektivität und Leistungsfähigkeit eines Netzwerks wesentlich verbessert. Sie sind also nicht auf eine vorgegebene Hard- und Softwareplattform festgelegt, sondern können ein flexibles und leistungsfähiges Netzwerk aufbauen.

Mit der Einführung und Entwicklung von Netzwerken haben sich leider auch unterschiedliche Standards entwickelt. Die für den Betrieb von Netzwerken notwendigen Standards können aufgeteilt werden in Anwendungsstandards und Kommunikationsprotokollstandards.

Anwendungsstandards

Generell können drei Klassen von Netzwerkprogrammen unterschieden werden: reine Netzwerkprogramme, Client-basierende und Server-basierende Applikationen. In der Vergangenheit waren fast alle netzwerkfähigen Programme sogenannte Workstation-basierende Programme, d. h., diese Programme liefen ausschließlich auf der Workstation im Netzwerk ab.

Anwendungen dieses Typs stützen sich auf das Dateisystem und sind abhängig von dem speziellen Workstation-Betriebssystem, wo diese Applikation eingesetzt wird. Die Anwendungen können entweder für DOS-, OS/2-, Windows-, Windows-95/98-, Windows-NT-, Macintosh- oder Unix-Umgebung geschrieben sein. Im Abschnitt über die Workstation-Unterstützung wurde bereits darauf hingewiesen, daß in einem Netzwerkbetriebssystem für den Einsatz unterschiedlicher Workstation-Betriebssysteme nicht nur die dazugehörigen Kommunikationsprotokolle, sondern auch die unterschiedlichen Dateisysteme unterstützt werden.

Während bestimmte Applikationen Workstation-basierend bleiben werden, gibt es für andere Anwendungsfälle gute Gründe, diese nach dem Client-Server-Prinzip zu entwickeln und einzusetzen. Hierbei läuft ein Teil der Applikation als Server-basierendes Programm auf dem File-Server ab, der andere Teil der Applikation läuft als Workstation-basierendes Programm in der Workstation im Netzwerk ab. Bei Applikationen, die nach dem Client-Server-Prinzip arbeiten, wird im Netzwerk eine Peer-to-Peer-Verbindung zwischen dem Client- und Server-Prozeß aufgebaut. Damit kann die Applikation nicht unabhängig vom Netzwerk-Server arbeiten.

Diese Client-Server-Applikationen werden häufig auch als Distributed Applications oder verteilte Anwendungen bezeichnet. Um verteilte Anwendungen im Netzwerk effektiv in einem unternehmensweiten Konzept unterstützen zu können, muß das Netzwerkbetriebssystem eine Vielzahl von sowohl Server- als auch Client-Plattformen unterstützen. Hierbei sind als Client-Plattform DOS, OS/2, Windows, Windows 95/98, Windows NT, Macintosh-OS und Unix zu nennen. Als Server-Plattform können unter anderem OS/2, VMS oder andere Server-Plattformen dienen. Zu diesen Plattformen zählen aber auch NetWare und NT Server. Auch NetWare kann als Server-Plattform eingesetzt werden. Mit der neuen Net2000- bzw. OSA-Strategie und der Implementierung der Java-Server-Plattform wird Novell diesen Entwicklungsschritt immer weiter ausbauen. Es gibt bereits eine Vielzahl von Anwendungen, die als Client-Server-Mechanismus für NetWare entwickelt worden sind. Die Ausführungen über NetWare 5

14.2 Die wichtigsten Anforderungen an Netzwerkbetriebssysteme

werden zeigen, daß sich auch die Anwendungen, basierend auf Java, direkt am Server starten lassen. So haben die ersten Versuche mit NetWare 5 gezeigt, daß man sich aus dem Internet eine beliebige Java-Anwendung holen kann und diese dann auf einem NetWare 5 Server startet. Dies alles funktioniert und arbeitet problemlos. So ist zum Beispiel die Entwicklung von ConsoleOne nur ein kleines Beispiel dafür, wie man eine einmal entwickelte Java-Anwendung auf unterschiedlichen System einsetzen kann. Die für NetWare 5 entwickelte Java-Anwendung ConsoleOne kann sowohl auf dem NetWare Server als auch auf einer herkömmlichen Workstation mit Java-Unterstützung gestartet und eingesetzt werden. Wie bereits erwähnt bildet Java die strategische Ausrichtung der neuen NetWare 5 mit dem Ziel, NetWare auch als klassischen Applikations-Server einzusetzen. Bei den Ausführungen über NetWare 5 werde ich noch detaillierte Informationen geben.

Unabhängig von der eingesetzten Server- und Client-Plattform verwenden Server-basierende Anwendungen sogenannte Interprocess-Communications-Protokolle (IPC), um eine logische Verbindung zwischen dem Client- und dem Server-Prozeß aufzubauen. Auf dem Markt existieren unterschiedliche Interprocess-Kommunikationen. Um auch die Flexibilität für den File-Server in bezug auf den Einsatz von Client-Server-Anwendungen im Netzwerk zu gewährleisten, sollte das Netzwerkbetriebssystem unterschiedliche IPC-Mechanismen unterstützen. Derzeitige IPC-Standards sind Novells SPX, IBMs NetBIOS und APPC, Microsofts Named Pipes und das Transport Library Interface (TLI) von AT&T. Diese gängigen Standards sollten von einem Netzwerkbetriebssystem unterstützt werden.

Protokollstandards

Zum Einsatz von Netzwerken gehören nicht nur Verkabelung, Netzwerkadapterkarten, Netzwerkbetriebssystem und netzwerkfähige Software, sondern auch die Unterstützung eines geeigneten Kommunikationsprotokolls. Die Protokolle für LANs können in drei Gruppen eingeteilt werden: Medienprotokolle, Transportprotokolle und Client-Server-Protokolle. Jeder Protokolltyp unterstützt dabei unterschiedliche Dienste, um dem Benutzer den Zugriff auf gemeinsame Ressourcen gewähren zu können. Für jedes dieser notwendigen Protokolle gibt es aber auch mehrere Standards am Markt.

Das Medienprotokoll bestimmt die Art und Weise der physikalischen Verbindung im Netzwerk. Wenn eine hardwaremäßige Verbindung zwischen den Stationen im Netzwerk hergestellt ist, wird ein Transportprotokoll benötigt, um Datenpakete zwischen den Stationen transportieren zu können.

14 Netzwerkbetriebssysteme

Wenn sowohl die Hardware-Verbindung als auch der Transport von Datenpaketen im Netzwerk geregelt ist, dann benötigt man noch ein Client-Server-Protokoll, um auf die Dienste des File-Servers zurückgreifen zu können. Das Client-Server-Protokoll bestimmt die Art und Weise, wie eine Workstation Netzwerkdienste anfordern kann und wie der File-Server die Antworten zur Workstation zurückgibt.

Alle diese Protokolle arbeiten zusammen, um den Benutzern im Netzwerk die Möglichkeit zur Verfügung zu stellen, Daten und Dienste von Servern (z.B. File-Server) im Netzwerk zu erhalten. Zum Beispiel wird die Anforderung zum Öffnen einer Datei normalerweise innerhalb einer Applikation abgesetzt. Diese Anforderung wird von der Netzwerksoftware, die auf der Workstation läuft, aufgenommen und gemäß dem Client-Server-Protokoll aufbereitet. Die Anforderung wird dann durch den Einsatz des Transport- und Medienprotokolls zum File-Server übertragen. Auf dem File-Server wird das Datenpaket entgegengenommen, da dieser das gleiche Client-Server-Protokoll unterstützt. Dieser verarbeitet die Anfrage, bereitet die Antwort gemäß dem Client-Server-Protokoll auf und überträgt dieses Datenpaket zur Workstation. Dies geschieht auch wieder über den Einsatz des Transport- und Medienprotokolls. Die Kombination dieser Protokolle wird sehr oft als Protocol-Stack oder Protocol-Suite bezeichnet. Diese Bezeichnungen spiegeln die Abhängigkeit der einzelnen Protokollschichten wider.

Solange Sie in einem Netzwerk immer nur die gleichen Medien-, Transport- und Client-Server-Protokolle einsetzen, ist es relativ unproblematisch, einheitliche Komponenten einzusetzen. Anders sieht es aus, wenn Sie bereits mit unterschiedlichen LAN-Topologien, wie Ethernet, Token-Ring oder ARCNET, arbeiten müssen.

Daneben existiert eine Vielzahl von Transportprotokollen, wie zum Beispiel Novells IPX, IBMs NetBEUI/DLC oder TCP/IP. Client-Server-Protokolle werden meist für eine bestimmte Workstation-Umgebung entwickelt. Das Client-Server-Protokoll AFP (Apple Filing Protocol) wurde ausschließlich für den Einsatz in einer Macintosh-Umgebung entwickelt. Sun Microsystems NFS (Network File System) wurde für die Unix-Umgebung konzipiert und IBMs SMB (Server Message Blocks) für OS/2-LAN-Server. Die SMB-Mechanismen werden aber auch unter NT Server eingesetzt.

Das ISO-Gremium versucht zwar, hier eine gewisse Standardisierung zu entwickeln, bis dies jedoch vereinheitlicht ist, werden noch Jahre vergehen. Solange können Sie allerdings nicht warten, um heterogene Netzwerke aufzubauen. Es ist erforderlich, daß leistungsfähige Netzwerkbetriebssysteme (zum Einsatz in einem heterogenen Umfeld oder für den Einsatz des Network Computing) nicht nur einen

14.3 Das Client-Server-Prinzip

Protokollstandard unterstützen, sondern ausbaufähig für den Einsatz der unterschiedlichsten Protokollstandards sind und entsprechend erweitert werden können. Somit kann auch der Weg offengehalten werden, wenn zukünftige Protokolle eingebunden werden sollen, die heute noch gar nicht existieren, z.B. OSI-Protokolle.

Diese Ansätze werden von vielen Herstellern angeboten und mehr oder weniger befriedigend unterstützt. Um ein für die Zukunft offenes System zu installieren, muß auf diese Tendenzen und Funktionen geachtet werden. Es ist schließlich kaum möglich, jedes Jahr ein neues Netzwerk zu installieren, um auf die neuen Entwicklungen zurückgreifen zu können.

Die Netzwerke und Netzwerkbetriebssysteme der Zukunft müssen flexibel und ausbaufähig sein, damit zukünftige Entwicklungen problemlos integrierbar sind, ohne komplette Server-Plattformen austauschen zu müssen.

14.3 Das Client-Server-Prinzip

Was unterscheidet ein herkömmliches Programm von verteilten Anwendungen (Distributed Applications), die nach dem Client-Server-Prinzip arbeiten? Diese Frage soll in diesem Kapitel näher beleuchtet werden. Wenn man die Arbeitsweise von Applikationen im Netzwerk betrachtet, können drei Arten unterschieden werden:

- Lokale Netze mit Single-User-Anwendungen
- File-Sharing: Lokale Netze mit netzwerkfähiger Software
- Processor-Sharing: Lokale Netze mit Einsatz von netzwerkfähiger Software und der Unterstützung des Client-Server-Modells

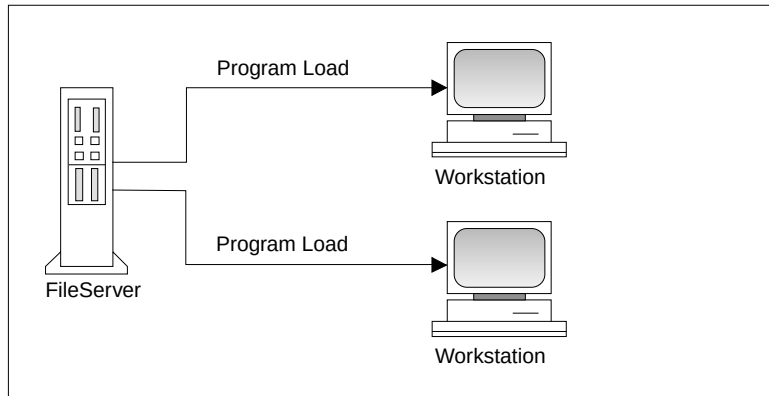
14.3.1 Lokale Netze mit Single-User-Anwendungen

Die Arbeitsweise dieser Anwendungen ist in Abbildung 14.2 dargestellt.

Der File-Server wird nur dazu verwendet, um das Programm oder Daten von der Platte des File-Servers zu laden bzw. Daten auf dieser zu aktualisieren oder zu löschen. Es besteht keine Möglichkeit, daß mehrere Benutzer gleichzeitig auf den gleichen Datenbestand zugreifen können, da ansonsten die Konsistenz und Integrität der Daten nicht mehr gewährleistet werden kann. Es handelt sich schließlich auch um eine Einplatzversion. Zudem dient das Netzwerk dazu, allen Benutzern im Netzwerk die Peripherie am File-Server (Platten, Drucker etc.) zur Verfügung zu stellen. Auch können allen Benutzern die Sicherheitsvorkehrungen des Netzwerks zur Verfügung gestellt werden.

14 Netzwerkbetriebssysteme

Abbildung 14.2
Standalone-Pro-
gramme im LAN



14.3.2

File-Sharing: Lokale Netze mit netzwerkfähiger Software

Bei dieser Variante kann das Programm von mehreren Benutzern im Netzwerk gleichzeitig benutzt werden. Zudem werden von diesen Programmen Mechanismen unterstützt, mit denen man File- oder Record-Locking für gemeinsame Zugriffe koordinieren kann. Das ist notwendig, damit die Integrität von Daten, auf die gleichzeitig von mehreren Benutzern zugegriffen wird, erhalten bleibt. Beispiele hierfür sind mehrplatzfähige Datenbanksysteme, Druck-Spool-Programme oder Textverarbeitungssysteme. Die Programme laufen jedoch, wie im obigen Beispiel, alle im Hauptspeicher der Workstation ab, von der das Programm geladen wird. Man spricht in diesem Fall auch von einer zentralen Datenverarbeitung und einer dezentralen Rechenleistung. Das Programm wird von der Platte des File-Servers in den Hauptspeicher der Workstation geladen und auf dieser gestartet. Die Synchronisation für gemeinsame Datenzugriffe wird von der netzwerkfähigen Software unter Einbeziehung der entsprechenden Schnittstellen zum Netzwerkbetriebssystem durchgeführt. Das heißt, in diesen Fällen wird auf die netzwerkfähige Unterstützung des File-Servers zurückgegriffen.

14.3.3

Processor-Sharing: Lokale Netze mit Einsatz von netzwerkfähiger Software und Unterstützung des Client-Server-Modells

Diese Methode der Kommunikation in einem Netzwerk ist für PC-LANs neu und revolutionär. Das Konzept der Abarbeitung von Programmen wird entweder als verteilte Anwendung oder Client-Server-Applikation bezeichnet. Bei diesem Verfahren stellt der Client (Work-

14.3 Das Client-Server-Prinzip

station) eine Anfrage an den Server und erhält von diesem das gewünschte Resultat. Man bezeichnet solche Programme auch als Workstation-Based (Client) und Server-Based (Server) Applications. Das Workstation-Programm (Client) muß sich nicht mehr darum kümmern, wie es die Daten vom File-Server erhält. Es ist auch kein unnötiger Datentransfer über das Netzwerk mehr nötig, da nur noch die Daten vom Server übertragen werden, die von der Workstation benötigt werden. Damit erspart man sich den gesamten Overhead der Datenübertragung. In Abbildung 14.4 ist das Verfahren dargestellt.

Abbildung 14.3
Netzwerkfähige
Programme im
LAN

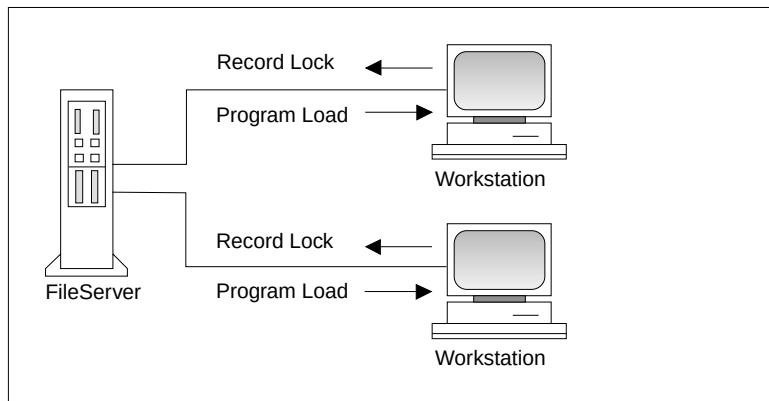
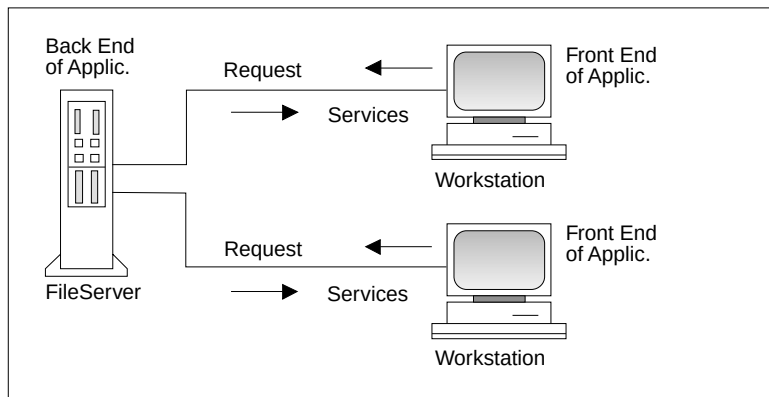


Abbildung 14.4
Distributed
Applications



Beim Einsatz von Server-Based-Applications werden die zugrundeliegenden Programme in zwei Bereiche unterteilt, das Server-Programm und das Client-Programm. Zusammen ergeben die beiden Programmteile eine vollständige Applikation. Beide Programmteile laufen dabei auf unterschiedlichen Maschinen, also Prozessoren, ab.

14 Netzwerkbetriebssysteme

Durch die Aufteilung der Programme wird die Leistung so verteilt, daß eine optimale Ausnutzung beider Maschinen erreicht werden kann.

Da beide Programme gleichzeitig ablaufen, kann die Synchronisation beider Prozesse nur durch die Kommunikation zwischen dem Server- und dem Client-Prozeß durchgeführt werden.

In einem Netzwerk laufen der Client- und der Server-Prozeß auf unterschiedlichen Maschinen. Der Server-Prozeß sollte dabei auf einem schnellen Rechner mit genügend peripherem Speicher ablaufen. Der Client-Prozeß hingegen wird auf einer beliebigen Workstation im Netzwerk gestartet. Der Server wird häufig auch als Back-End-Process und der Client als Front-End-Process bezeichnet.

Das Front-End ist der Teil, den der Benutzer zu sehen bekommt, das Back-End arbeitet für den Benutzer im Verborgenen, d.h., er muß davon überhaupt nichts wissen. Das Front-End führt jedoch die Hauptaufgaben für die Applikation durch. Die Front-End-Software wird vom Benutzer bedient und stellt diesem u.a. Bildschirmmasken, Ein- und Ausgaben zur Verfügung. Das Back-End hingegen aktualisiert Daten, sucht nach bestimmten Datensätzen oder speichert notwendige Informationen ab.

Wie Sie aus den bisherigen Ausführungen ersehen können, muß sich der Software-Hersteller bei der Entwicklung von Client-Server-Applikationen entscheiden, für welches Netzwerk diese Applikationen erstellt werden sollen. Da unterschiedliche Netzwerke auch unterschiedliche Protokolle unterstützen, muß dies bei der Entwicklung solcher Distributed Applications berücksichtigt werden. Die Adaptierung der gleichen Software für ein anderes Netzwerksystem bedeutet für den Entwickler die Anpassung der Software an das andere Protokoll für dieses Netzwerk.

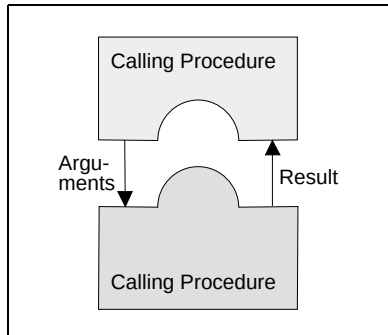
Um Software-Herstellern hierfür eine größere Flexibilität zur Verfügung zu stellen, wird von Netwise eine sogenannte RPC-Unterstützung angeboten. Auf diese Weise können bereits bestehende Distributed Applications ohne größeren Aufwand an die Umgebung anderer Netzwerke angepaßt werden, ohne die komplette Software neu konzipieren zu müssen. Wie wird diese Aufgabe durch die RPC-Software gelöst?

Das RPC-Modul (Remote Procedure Call) stützt sich auf die Schnittstelle der Kommunikation der Software zwischen den Computern im Netzwerk. Das Konzept geht davon aus, daß der herkömmliche Prozeduraufrufprozeß erweitert werden kann, so daß die aufrufende Prozedur und die aufgerufene Prozedur auf unterschiedlichen Maschinen im Netzwerk sein können. Unter einem herkömmlichen Pro-

14.3 Das Client-Server-Prinzip

zeduraufruf ist dabei folgendes zu verstehen: Die aufrufende Prozedur übergibt ein Argument an die aufgerufene Prozedur und erhält von dieser das benötigte Ergebnis. Abbildung 14.5 zeigt diesen Vorgang.

Abbildung 14.5
Herkömmlicher
lokaler Prozedur-
aufruf



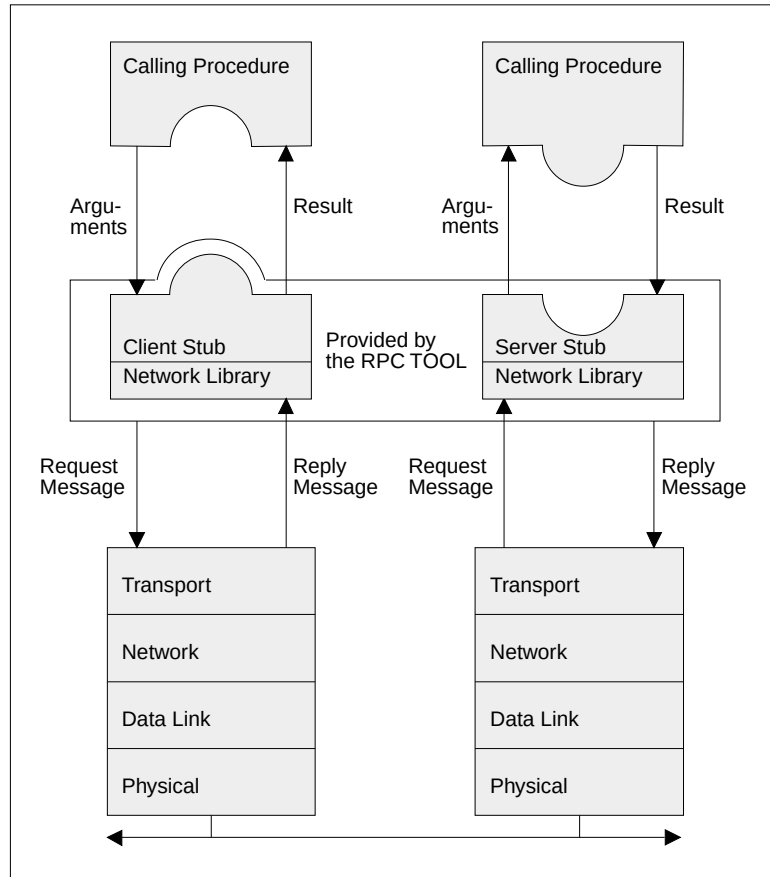
Mit Hilfe der RPC-Tools können einfach und schnell Distributed Applications entwickelt werden. Die mit Hilfe der RPC-Tools entwickelte Applikation überträgt anschließend nur noch die Daten über das Netzwerk, die von der Workstation angefordert worden sind. Auf diese Weise lassen sich Distributed Applications entwickeln. Die Einbindung und der Ablauf von Client-Server-Programmen, die mit Hilfe der RPC-Tools entwickelt werden, sind in Abbildung 14.6 dargestellt.

Die Netwise-RPC-Tools bestehen unter anderem aus einem Source Code Compiler, der die entsprechende netzwerkfähige Client-Server-Applikation erzeugt. Die RPC-Tools unterstützen zum Beispiel die Transportprotokolle von NetWare (SPX), IBM (NetBIOS), TCP/IP, DECnet und SNA/APPN. Die Netwise Tools und die damit erzeugte Applikation können auf allen herkömmlichen PCs, VAX Minis, Sun-Unix-Rechnern, Crays, IBM-Host-Rechnern oder auch Unisys-Rechnern eingesetzt werden. Die unterstützten Betriebssysteme sind unter anderem MS-DOS, OS/2, VMS, Ultrix, Unix oder NetWare.

Es wurde von Netwise auch die Unterstützung der RPC-Tools für IBM-MVS-Großrechner und Apple-Macintosh-Computer freigegeben. Somit unterstützt Netwise inzwischen über 50 Plattformen für die Entwicklung und den Einsatz von Distributed Applications. Dies reicht vom Großrechner bis hin zu DOS-basierenden Anwendungen. Es ist somit möglich, durch Austausch der RPC-Schnittstelle die Distributed Application schnell und einfach an andere Netzwerke und Betriebssysteme anzupassen.

14 Netzwerkbetriebssysteme

Abbildung 14.6
Konzept der
Remote-Procedure-
Call-Architektur



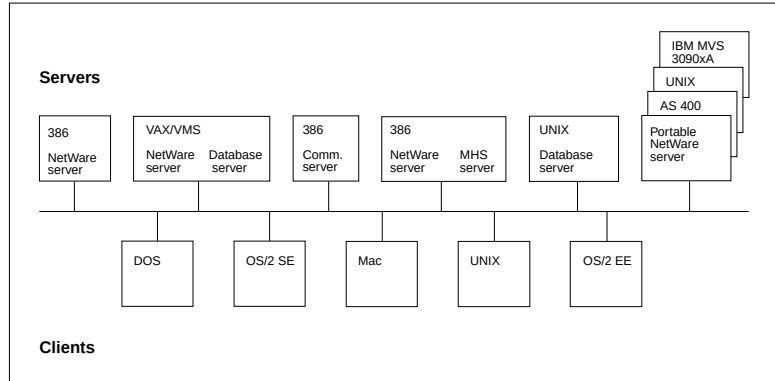
Wenn ich Ihnen die E-Mail-Systeme vorstelle, wird bei der Behandlung des Mail Exchanger von Microsoft zu sehen sein, daß auch hier RPC-Mechanismen eingesetzt werden, um damit klassische Client-Server-Systeme aufzubauen.

14.4 Die Server-Strategie von Novell

Die meisten Netzwerkbetriebssysteme sind für den Einsatz auf bestimmten Workstation-Umgebungen konzipiert. Da Novell kein Vertrieber von Workstation-Betriebssystemen ist, wird ein besonderes Augenmerk auf die Unterstützung aller gängigen Workstations und Workstation-Betriebssysteme gelegt. Somit kann die Einbindung in ein heterogenes Netzwerkkonzept realisiert werden.

14.4 Die Server-Strategie von Novell

Abbildung 14.7
Die Hardware-
und Protokoll-
unabhängigkeit
von NetWare



Zu beachten ist dabei, daß NetWare kein Trägerbetriebssystem verwendet, so wie dies zum Beispiel beim LAN-Server von IBM der Fall ist (benötigt OS/2). NetWare setzt im Prinzip direkt auf der Hardware des Systems auf, allerdings immer Intel-Prozessor-Technik vorausgesetzt. Dies ist aber nicht mehr so relevant, da ähnliches inzwischen auch für den Windows NT Server von Microsoft gilt, nachdem sich fast alle Entwicklungen auf die Intel-Plattform konzentrieren, obwohl der NT Server aufgrund der HAL-Technik prozessorunabhängig eingesetzt werden kann – vorausgesetzt man entwickelt die dazugehörige HAL.

Dadurch wird erreicht, daß NetWare sowohl von der Hardware als auch vom Protokoll unabhängig ist, und somit Netzwerke, wie sie in Abbildung 14.7 dargestellt sind, aufgebaut werden können.

Innerhalb dieser heterogenen Welt will Novell die unterschiedlichsten Anwendungen unterstützen. Hierbei ist vor allem an die Unterstützung von bestehenden Client-basierenden und netzwerkfähigen Applikationen gedacht, um auch zukünftige Entwicklungen integrierbar zu machen. Zusätzlich wird durch dieses heterogene Umfeld ein Client-Server-Modell aufgebaut, das aus einer Vielzahl von Client- und Server-Plattformen besteht. Novell ist bestrebt, für alle gängigen Client-Server-Anwendungen in diesen heterogenen Netzen volle Unterstützung bieten zu können. Dies kennzeichnet einmal mehr die Strategie, Netzwerkbetriebssysteme für Network Computing zu entwickeln. Novell stellt zudem allen Entwicklern Tools zur Verfügung, um einfach und schnell netzwerkfähige bzw. Client-Server-Applikationen erstellen zu können. Durch den starken Einsatz der Java-Technik wird dieses Ziel noch weiter ausgebaut, verbessert und beschleunigt.

14 Netzwerkbetriebssysteme

Diese strategischen Ziele erlauben es Novell, eine Umgebung aufzubauen, die für den Benutzer von wirklichem Nutzen ist. Es handelt sich dabei um eine Umgebung, die sich durch ein Maximum an Flexibilität in Implementierung und Ausbau auszeichnet. Der Anwender kann aus einer großen Anzahl von Server-Plattformen auswählen und mit diesen die Standard-Workstation-Umgebungen einsetzen – alles unter dem Gesichtspunkt, welche Anforderungen der Anwender an dieses Netzwerksystem stellt.

In Anbetracht der bisherigen Ausführungen über Server-Plattformen, Client-Server-Applikationen, Protokollstandards, zukünftigen Strategien oder Auswahlkriterien für LANs und Netzwerkbetriebssysteme will ich Ihnen in den nächsten Kapiteln die Funktionsweisen und Leistungskriterien von NetWare 3.2, NetWare 4 und NetWare 5 im Detail aufzeigen.

Um einen Vergleich mit anderen Netzwerk-Betriebssystemkonzepten zu erhalten, will ich Ihnen nach der Darstellung von NetWare 3, NetWare 4 und NetWare 5 das System von Microsoft vorstellen.

14.5 Multiprozessorfähigkeit

Mit Einführung von NetWare 4.11 ist das Netzwerkbetriebssystem standardmäßig multiprozessorfähig, sofern die eingesetzte Hardware die entsprechende Unterstützung bietet und sich an die dazugehörigen Spezifikationen hält. Während der Installation von NetWare 4.11 wird automatisch die Prüfung mehrerer Prozessoren durchgeführt und ein Vorschlag gemacht, die entsprechenden Treiber hierfür zu installieren. Bei der Lizenzierung von NetWare 4.11 müssen die regulären Connections-Lizenzen unterschieden werden, die in den Abstufungen 5, 10, 25, 50, 100, 250, 500 und 1000 zur Verfügung stehen. Hinzu kommt dann noch die Lizenz für SMP, d.h. eine SMP-Lizenz. Die Grundlizenz von NetWare (siehe oben) unterstützt standardmäßig bis zu vier Prozessoren. Sollen unter NetWare 4.11 mehr als vier Prozessoren eingesetzt werden, dann muß eine zusätzliche SMP-Prozessor-Lizenz gekauft werden. Jede SMP-Prozessor-Lizenz unterstützt dann wieder bis zu vier weitere Prozessoren. Wird somit ein System mit weniger als vier Prozessoren eingesetzt, dann reicht die herkömmliche Connection-Lizenz für den Betrieb aus. Wird ein System mit acht Prozessoren eingesetzt, dann benötigt man eine Connections-Lizenz (inklusive der ersten vier Prozessoren) und eine zusätzliche SMP-Prozessor-Lizenz.

14.5 Multiprozessorfähigkeit

Beim Einsatz von SMP sind die folgenden Aspekte zu berücksichtigen:

1. NetWare 4.11 SMP bringt keine Verbesserung der File-System-Performance, außer auf dem Server läuft ein Datenbank-System mit einem proprietären Datei-System-Interface. Bei der momentanen SMP-Version für NetWare 4.11 laufen alle Dateisystem-Zugriffe immer noch ausschließlich über den Prozessor 0. Ebenso ist der Kernel von NetWare 4.11 noch nicht SMP-fähig und wird es auch nicht mehr werden, da man diese Erweiterung und auch die Verbesserung für das Dateisystem bezüglich SMP-Fähigkeit in NetWare 5 implementiert hat. Für den Kernel bedeutet dies zum Beispiel auch, daß bei Ausfall von Prozessor 0 der Server steht und keine Arbeit mehr verrichten kann.
2. Verbesserungen ergeben sich beim Einsatz von SMP jedoch für die Performance im LAN. Die LAN-Support-Module in NetWare 4.11 SMP sind multiprozessorfähig und nutzen somit die Vorteile jedes zusätzlichen Prozessors voll aus. Sollte ein Server Performance-Engpässe in der LAN-Kommunikation aufweisen, dann kann der Einsatz von SMP deutliche Verbesserungen bringen.

Einen Schritt weiter zur Verbesserung der Performance geht Novell nicht nur mit der Entwicklung von NetWare 5 (siehe spätere Ausführungen), indem hier die Multiprozessorfähigkeit auf das gesamte System ausgeweitet wird, sondern auch durch die Entwicklung der Cluster-Technologie.

In einem Cluster wird eine Gruppe von Servern, Mono- und auch Multiprozessorsysteme, als eine einheitliche Ressource betrachtet. Damit kann ein Server Aufgaben an einen anderen Server übertragen, wenn dieser weniger stark ausgelastet ist. Zudem bietet Clustering die Möglichkeit, I/O-Vorgänge und Ressourcen auf die Server eines Netzwerks zu verteilen, um dadurch generelle Engpässe zu vermeiden. Die gesamte Server-Hardware wird somit im Netzwerk wesentlich effektiver genutzt, da auch weniger stark beanspruchte Systeme (Server) besser ausgelastet werden können.

Auf die von Novell angestrebte Cluster-Technologie werde ich an anderer Stelle näher eingehen.

Festzuhalten ist an dieser Stelle somit, daß Netware 4.11 SMP nur eingeschränkte Möglichkeiten bietet, wohingegen die volle Leistungsfähigkeit von SMP mit NetWare 5 zur Verfügung gestellt wird.

Entgegen allen Ankündigungen von Novell wird es in nächster Zeit drei Netzwerkbetriebssysteme für die unterschiedlichen Einsatzgebiete geben. Es handelt sich hierbei um

14 Netze**rk**betrie**bs**systeme

- NetWare 3.2
- NetWare 4.2
- NetWare 5

In den nächsten Kapiteln soll deshalb aufgezeigt werden, worin sich diese Systeme unterscheiden, welche Möglichkeiten damit verbunden sind und wie die weiteren Entwicklungen aussehen werden.

15

Novell NetWare 3.2

Nachdem ich Ihnen in den letzten Kapiteln sehr viel über Netzwerkkonzepte, Network Computing, Workgroup Computing, Internet oder auch Intranet erzählt habe, will ich Ihnen in den nun folgenden Kapiteln aufzeigen, auf welche Weise diese Konzepte von Novell NetWare abgedeckt werden. Es sollen Ihnen dabei der funktionelle Aufbau der NetWare, die Zuverlässigkeit, Sicherheitsmechanismen und im Überblick die Bedienung des Systems nähergebracht werden.

1997 hat Novell eine überarbeitete Version von NetWare 3.12 auf den Markt gebracht. Man vergab die neue Versionsnummer 3.2, eine bereinigte NetWare-3.12-Version, die sich nur durch einige neue Zusätze von der Vorgängerversion unterscheidet. Da sich die eingebauten Zusätze nur sehr schwer geordnet in die nachfolgende Beschreibung aufnehmen lassen, vor allem, wenn es darum geht, die Unterschiede zu NetWare 3.12 erkennen zu können, sollen die Modifikationen am Ende dieses Kapitels zusammengefaßt dargestellt werden.

Das Wichtigste soll jedoch bereits jetzt für NetWare 3.2 erläutert werden:

Aufgrund der starken Verbreitung und immer noch sehr großen Beliebtheit von NetWare 3 hat Novell beschlossen, einen Update NetWare 3.2 auf den Markt zu bringen. Der wesentliche Aspekt von NetWare 3.2 ist, daß es sich um eine leicht verbesserte NetWare 3.12 handelt, die eine vollständige Jahr-2000-Fähigkeit gewährleistet und eine grafische Administrationsoberfläche zur Verfügung stellt. Ansonsten haben sich keine großen funktionellen Änderungen zur Netware 3.12 ergeben. Da es sich um einen »kleinen« Update handelt, bekommt man für die Umstellung auf NetWare 3.2 ein sogenanntes Enhancement Pack zur Verfügung gestellt. In diesem Enhancement Pack sind dann alle Änderungen enthalten, die notwendig sind, vor allem, um mit NetWare 3.2 problemlos in das Jahr 2000 wechseln zu können.

Das neueste strategische Produkt von Novell heißt entweder NetWare 4 oder NetWare 5. Da es sich hierbei um ein noch leistungsfähigeres Netzwerkbetriebssystem handelt, werde ich Ihnen im Anschluß an die Beschreibung von NetWare 3.2 auch diese Betriebssysteme vorstellen. Da ein Teil der Grundfunktionen von NetWare 4 (mit NetWare 5 zum Teil) mit denen von NetWare 3.2 vergleichbar sind, werde ich mich bei der Beschreibung von NetWare 4 bzw. Net-

15 Novell NetWare 3.2

Ware 5 nur auf die wesentlichen Unterschiede beschränken. Diese sind jedoch umfassend genug. Zum Zeitpunkt der Erstellung dieses Buchs war NetWare 4.2 die aktuelle 4er-Version, und NetWare 5 wird ausgeliefert. Man hat in der 4er- und der 5er-Version noch mehr Wert darauf gelegt, die Administration und die damit verbundenen Möglichkeiten weiter zu verbessern.

Es sei schon hier darauf hingewiesen, daß diese Beschreibungen nicht als Installationsanweisungen gedacht sind, sondern sich an den Konzepten und Funktionen orientieren.

Bei jeder Überarbeitung dieses Buchs war zu erkennen, daß sich innerhalb kürzester Zeit gravierende Veränderungen auf dem Netzwerksektor und auf dem Gebiet der Netzwerkbetriebssysteme ergeben hatten. Nach Bekanntwerden von neuen Versionen hatte man immer den Eindruck, es könne eigentlich jetzt nichts wesentlich Neues mehr hinzukommen. Es zeigt sich aber immer wieder, daß es nicht nur neue Techniken, sondern auch neue Funktionen und Mechanismen sind, durch die sich Netzwerkbetriebssysteme mit jeder neuen Version auszeichnen. Deshalb wird auch mit den nachfolgenden Ausführungen versucht, den aktuellen Stand zu beschreiben, so wie dieser zum Zeitpunkt der Erstellung dieses Buchs bekannt war. Dabei kann es durchaus sein, daß sich beim Lesen der einzelnen Abschnitte bereits neue Ankündigungen ergeben, die dann zusätzlich in diese Ausführungen von Ihrer Seite eingebunden werden müssen.

Man kann zum Teil gar nicht so schnell schreiben, wie sich neue Entwicklungen ergeben. Ebenso aufwendig ist die Entscheidung, welche neuen Konzepte in eine neue Auflage übernommen werden sollen.

Somit werde ich mich im ersten Teil mit NetWare 3.2 beschäftigen, Ihnen anschließend NetWare 4 bzw. NetWare 5 vorstellen und vergleichend dazu das Konzept von Windows NT Server, ebenfalls in den Versionen Windows NT Server 4.0 und Windows NT Server 5.0, erläutern.

Das Netzwerkbetriebssystem Novell NetWare zählt zu den besten und leistungsstärksten Betriebssystemen für PC-LANs. Das erste Betriebssystem dieser Art wurde bereits 1983 zur Verfügung gestellt und seither den laufenden Entwicklungen auf dem Hard- und Software-Markt angepaßt.

Novell NetWare basiert auf dem Prinzip des Servers (File-Server, Print-Server, Communication-Server etc., wobei alle diese Server-Dienste auf der gleichen Maschine eingesetzt werden können). Im Gegensatz zu anderen Systemen – wie PC-LAN von IBM oder MS-NET von Microsoft, die als Trägerbetriebssystem MS-DOS verwendet

haben, NT Server, die NT als Trägerbetriebssystem verwenden, bzw. IBM-LAN-Server, die als Trägerbetriebssystem OS/2 verwenden – setzt Novell NetWare 3.2/4.11/5 direkt auf der Hardware, sprich auf der 80486 bzw. 80586-Architektur, auf. Nicht zu vergessen ist auch die Unterstützung des neuen Intel-Pentium-Pro-Prozessors und der MMX-Technologie. Dies bedeutet, genauso wie bei OS/2 bzw. Windows NT, die fast vollständige Ausnutzung der Leistungsfähigkeit dieser Prozessortypen. Für den Benutzer sind die zusätzlichen Leistungen und Ressourcen im Netzwerk nur Erweiterungen der vorhandenen Umgebung. Das Konzept, das dabei zugrunde liegt, bedeutet, die Netzwerkleistung auf das PC-Betriebssystem zuzuschneiden und nicht etwa umgekehrt. Novell prägte hierfür den Begriff »PC-Zentralität«. Durch diese Struktur erscheinen dem Benutzer die Netzwerkkomponenten, die Dienste und die Ressourcen, die zur Verfügung stehen, als eine Einheit. Der Kern des Netzwerks, eine Kombination aus Netzwerkkomponenten, die auf die Erfordernisse des Benutzers abgestimmt sind, bleibt unsichtbar. Es können zum Beispiel neue Komponenten, Technologien, Protokolle oder Hardware in das Netzwerk integriert oder auch wieder aus diesem entfernt werden, ohne daß dies negative Auswirkungen hat. Darüber hinaus ist es möglich, durch den modularen Aufbau des Netzwerkbetriebssystems ein bereits installiertes Netz schrittweise zu erweitern.

Novell NetWare hat sich im Lauf der Jahre zu einem mächtigen und leistungsstarken Betriebssystem für Lokale Netze weiterentwickelt, das seinesgleichen sucht. Mit NetWare 4 und NetWare 5 ist es Novell gelungen, ein Betriebssystem zu entwickeln, das schon lange geforderte Mechanismen beinhaltet und das Einrichten und Verwalten von Multi-Server-Netzwerken wesentlich verbessert und erleichtert. NetWare 5 wird in den nächsten Jahren den vollständigen Ersatz für NetWare 3.2 und NetWare 4 bilden, und es wird als solches auch bereits vermarktet. Es ist bis jetzt jedoch noch kein Time-Scale bekannt, wann dies erfolgen wird. Man wird sich noch lange zwischen drei Systemen entscheiden können. Man sollte sich deshalb bei der Neuinstallation eines Netzwerks gleich für NetWare 5 entscheiden, statt noch mit NetWare 3.2 bzw. NetWare 4 zu beginnen. Jedoch werden die Entscheidungen gegen die aktuellste Version immer dann getroffen, wenn man der Meinung ist, daß man nicht das High-End-Produkt haben muß, da eine kleinere Version auch reicht. Man sollte sich aber immer überlegen, ob es nicht sinnvoller ist, vor einer Umstellung von NetWare 3.12 auf NetWare 3.2 gleich auf NetWare 4 oder NetWare 5 umzusteigen. Novell selbst bietet inzwischen eine Vielzahl von Produkten an, die nur noch auf NetWare 4 bzw. NetWare 5 aufgesetzt werden können, da hierfür die vollständige NDS-Unterstützung gegeben ist.

Durch das Konzept, ein Netzwerkbetriebssystem zu entwickeln, das ohne darunterliegendes Trägersystem arbeitet, also direkt auf die Hardware abgestimmt ist, ist es auch möglich, allen Overhead, mit dem Trägerbetriebssysteme zwangsläufig behaftet sind, zu vermeiden. Da Trägerbetriebssysteme wie OS/2, Windows NT oder Unix auch noch für den Einsatz kommerzieller Software entwickelt wurden, sind darin auch noch andere Techniken enthalten, die ein Netzwerkbetriebssystem nicht unbedingt benötigt. Das heißt, daß die anderen Konzepte unter Umständen an der Trägheit der Basis, auf der aufgesetzt wird, zu leiden haben.

15.1 Allgemeiner Überblick über Novell NetWare 3.2

File-Server, die unter Netware 3.2, NetWare 4 oder NetWare 5 betrieben werden, stehen unter der Kontrolle des Betriebssystems, das für Datensicherheit, Zugriffsverwaltung, Datei- und Verzeichnisverwaltung und Übermittlung von Nachrichten Sorge trägt. Im NetWare File-Service Core Protocol (NCP) sind an die 200 Dienstleistungsauf-rufe verankert, die über das Betriebssystem einer vernetzten Workstation abgesetzt werden können. Diese Schnittstelle dient der Kommunikation der Workstation-Shell mit dem Netz, damit lokale Anwendungen Dienste des Netzes in Anspruch nehmen können.

Mit Hilfe der Schnittstellenkonzeption des NCP können unterschiedliche PC-Betriebssysteme ohne Probleme an die Dienste und Ressourcen unter NetWare angebunden werden. Diese Anbindung wird mit Hilfe der Shell realisiert. Die Funktion des Betriebssystems auf der Workstation wird erweitert, und es wird die Integration in die Netzwerkumgebung ermöglicht.

Außerdem erlaubt Novell NetWare, Hardware-Netzwerkkomponenten auf mehrere Stellen im Netz zu verteilen. File-Server, Dienste, Anwendungen und Betriebsmittel jeglicher Art können zentral, verteilt und/oder spezifisch genutzt und zur Verfügung gestellt werden. NetWare koordiniert den transparenten Zugriff auf diese heterogenen Netzwerkkomponenten sowie die notwendigen Sicherheitsmaßnahmen. Der Benutzer hat den Eindruck, als handle es sich um ein einziges System.

Die offene Architektur gestattet es den Entwicklern, File-Server, Netzdienstleistungen und Anwendungen anderer Hersteller in die erweiterte Arbeitsumgebung der Benutzer zu integrieren. Sowohl File-Server als auch Dienste anderer Hersteller lassen sich dadurch in

15.2 Übertragungseinrichtungen von Novell NetWare 3.2

eine Netzwerkumgebung einpassen, und einzelne Dienstleistungen im Netz lassen sich ergänzen oder ersetzen. Beispiele hierfür können sein:

Druck-Server, Communication-Server, Stapeljob-Server, Archivierungs-Server oder Datenbank-Server. Diese Funktionen können in Workstations (non-dedicated), auf eigenen Rechnern (dedicated) oder auf einem File-Server integriert werden.

Durch dieses Synergiekonzept von File-Services in Zusammenhang mit offener Architektur, Systemfehlertoleranz und der Möglichkeit, Netzdienstleistungen zu dezentralisieren oder über das gesamte Netzwerk zu verteilen, erreicht Novell NetWare ein Leistungsspektrum, das bisher nur von MDT-Systemen oder Host-Systemen bekannt war.

15.2 Übertragungseinrichtungen von Novell NetWare 3.2

Technologische Innovationen betreffen nicht nur Hardware, sondern auch Software. Auf dem Gebiet der Kommunikationstechniken und Netzwerkarchitekturen werden Protokolle ständig verbessert oder gar neu entwickelt. Deshalb wurde Novell NetWare so konzipiert, daß mit allen gängigen Protokollen und Architekturen zusammengearbeitet werden kann. Durch die Systemarchitektur bereitet es keine Probleme, NetWare-Produkte an neue sich entwickelnde Standards anzupassen. Dieses weitsichtige Konzept ist entscheidend dafür, daß Novell auf dem Gebiet der Integration von Systemen, die eine Kombination aus Produkten verschiedener Hersteller sind, weiterhin am Markt ganz vorne dabei sein wird.

Das ISO/OSI-Modell für offene Kommunikation haben wir bereits ausführlich behandelt. Jetzt soll gezeigt werden, wie Novell im LAN-Bereich hier einzuordnen ist. Das Schichtenmodell läßt zwei verschiedene Übertragungstechniken in einer Netzwerkumgebung zu: die formelle und die informelle Methode.

Die *informelle Methode* ist eine der ältesten und einfachsten Techniken. Ein übertragenes Paket wird wie eine geschlossene Einheit behandelt. Jedes Paket enthält deshalb die Zieladresse und kann mit dieser transportiert und zugeteilt werden, ohne daß vorher eine Absprache zwischen Sender und Empfänger getroffen wird. Pakete dieser Art werden Datagramme genannt. Die informelle Methode wird deshalb in der Literatur auch als Datagrammtechnik bezeichnet.

15 Novell NetWare 3.2

Folgende Protokolle basieren auf dieser Übertragungstechnik:

- UDP, The Department of Defense's User Datagram Protocol
- IPX, Internet Packet Exchange von Novell
- PEP, Packet Exchange Protocol von Xerox
- DDP, Datagram Delivery Protocol von Apple

Gegenüber anderen Methoden hat diese Übertragungstechnik folgende Vorteile:

1. Es wird unnötiger Verbindungsaufwand für die Implementierung von Station-Netzwerk-Shells, Brücken und Servereinheiten vermieden.
2. Ein informelles Paket kann problemlos an viele Zielgruppen verschickt werden (Broadcast).
3. Es ist nicht erforderlich, daß Absender und Empfänger gleichzeitig sende- und empfangsbereit sind.

Dies macht die informelle Methode zu einer leistungsstarken Lösung für Paketübertragungsnetze.

Bei der *formellen Methode* wird vor dem Datentransfer eine logische Verbindung zwischen Sender und Empfänger aufgebaut. Zunächst wird ein Verbindungsanforderungspaket an die Zielstation geschickt. Damit wird diese zum Aufbau der logischen Verbindung aufgefordert. Akzeptiert die Zielstation die Verbindung, sendet sie eine Nachricht – »Verbindung akzeptiert« – zurück. Die Verbindung ist somit aufgebaut, und der Datentransfer kann beginnen. Solange der Transfer andauert, kann das formale System Funktionen wie Flußsteuerung, Überwachung der korrekten Reihenfolge des Datenflusses und die Fehlerüberwachung übernehmen. Bei Beendigung des Datentransfers erhält die Sendestation eine Quittierung.

Protokolle, die die formelle Methode anwenden, sind:

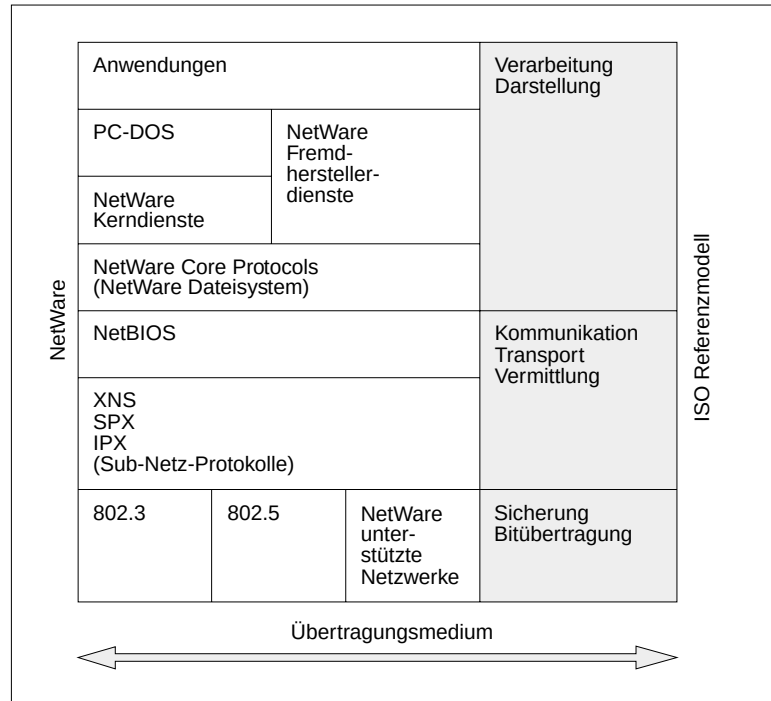
1. TCP (Transmission Control Protocol vom DoD)
2. SPP (Sequenced Packet Protocol von Xerox)
3. ATP (AppleTalk Transaction Protocol von Apple)

Die formelle Methode ist zwar sicherer als die informelle Methode, erfordert aber einen gewissen Mehraufwand. Die informelle Übertragung ist in der Praxis meist effektiver unter der Voraussetzung, daß Sender und Empfänger für eine korrekte Fehlerbehandlung Sorge tragen.

Novell basiert auf der informellen Methode. Formelle Dienstleistungen können durch zusätzliche Dienste über diese gelegt werden. Anwendungen, die solche Dienste anfordern, können diesen zusätzlichen Dienst in Anspruch nehmen.

15.2 Übertragungseinrichtungen von Novell NetWare 3.2

Abbildung 15.1
Einordnung von
Novell NetWare in
das ISO/OSI-
Schichtenmodell



Damit Entwickler eine flexible Netzwerkkumgebung vorfinden, ist NetWare mit vier unterschiedlichen Netzschnittstellen ausgestattet:

- Datagrammschnittstelle
- Schnittstelle für virtuelle Verbindungen
- Kommunikationssteuerungs-Schnittstelle
- Station-Shell-Schnittstelle

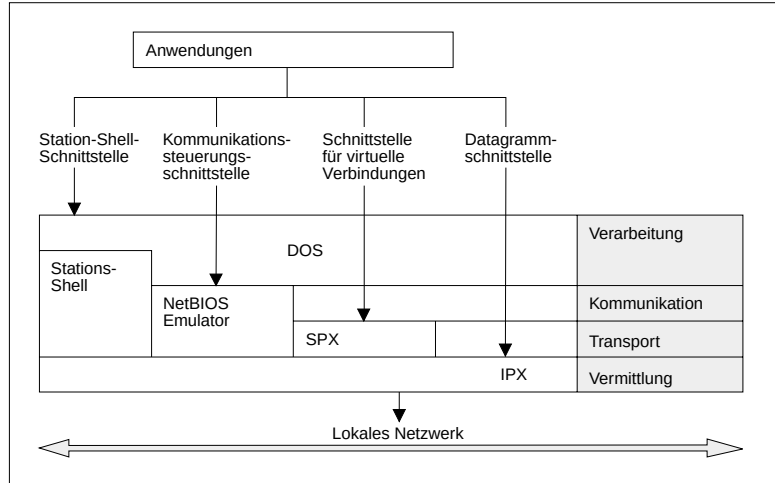
In Abbildung 15.1 ist eine Einordnung von Novell und dem Schichtenmodell aufgezeigt, und in Abbildung 15.2 sind die vier Schnittstellen dem Schichtenmodell gegenübergestellt.

Die Datagrammschnittstelle sorgt für schnelle und unkomplizierte Datagrammdienste (informelle Methode), denn diese kommt ohne die erhöhten Aufwendungen für Initialisierung und Aufrechterhalten der Verbindung aus, wie dies bei den höheren Transport- und Kommunikationssteuerungsprotokollen der Fall ist.

Die Datagrammschnittstelle eignet sich deshalb besonders für Anwendungen und Dienste, die selbst eine Zustellungsprüfung vornehmen. Dies sind zum Beispiel Anwendungen, die auf Master/Slave-Beziehungen basieren.

15 Novell NetWare 3.2

Abbildung 15.2
Die vier NetWare-
Schnittstellen



Auf der Datagrammschnittstelle setzt die Schnittstelle für virtuelle Verbindungen auf; diese garantiert und bestätigt die Zustellung der Pakete, da nach erfolgreicher Zustellung eine positive Quittierung erfolgt. Diese Schnittstelle garantiert optimale Übertragungsleistung.

Über der Datagrammschnittstelle liegt die Schnittstelle für Kommunikationssteuerung. Mit Hilfe dieser Schnittstelle können zum Beispiel Anwendungen im Netz, die für NETBIOS konzipiert worden sind, unter NetWare ablaufen. Eine Anpassung der Anwendung ist somit nicht erforderlich.

Die Station-Shell-Schnittstelle ist mit dem DOS-Dateiservice kompatibel. Auch diese liegt über der Datagrammschnittstelle. Die Station-Shell ordnet einer DOS-Anfrage einen Unterprogrammaufruf des entsprechenden NetWare-Diensts zu. Für DOS ist dies vollkommen transparent. Durch diesen Mechanismus können Standardanwendungen Zugriff auf NetWare-Ressourcen ausführen und von den Dienstleistungen der NetWare profitieren. Zum Beispiel erkennt die Shell, ob der Zugriff auf die lokale Festplatte eines PC ausgeführt wird oder ob der Zugriff auf die File-Server-Platte umgeleitet werden muß. »Erweiterung der PC-Umgebung« sei hier nochmals als Stichwort angeführt, alles unter dem Gesichtspunkt, daß der Anwender davon nichts merkt; er arbeitet ganz normal unter seiner gewohnten DOS-Umgebung.

Bereits zu Beginn dieses Buchs habe ich darauf hingewiesen, daß LANs nicht als Insellösungen in einer Abteilung, Firma oder einem Büro eingesetzt werden, vielmehr wird eine Einbindung in die bestehende DV-Welt angestrebt. Hierbei kann es sich um Host-Systeme

15.3 NetWare 3.2 – eine offene Systemarchitektur

oder MDT-Anlagen auf dem Firmengelände handeln. Auch die Verbindung zu entfernt liegenden Systemen außerhalb des Grundstücks oder in einer anderen Stadt bzw. in einem anderen Land soll hergestellt werden. Aus einem LAN wird dann ein WAN (Wide Area Network). Dem Benutzer eröffnen sich damit wesentlich höhere und flexiblere Arbeitstechniken und -möglichkeiten. Eine Vielzahl von Ressourcen auf der ganzen Welt kann verwendet werden. Die NetWare-Architektur deckt die vier Übertragungsschnittstellen ab, die mit den gängigsten Übertragungsprotokollen und -medien zusammenarbeiten:

- IBM-kompatible Schnittstelle
- IBM-Gateway-Schnittstelle
- Asynchrone Service-Schnittstelle

Durch Dritthersteller werden diese Bereiche zusätzlich ergänzt und erweitert. Wir werden bei der detaillierten Besprechung von Gateways auf dieses Thema noch näher eingehen.

Dieses Konzept ist bereits von früheren NetWare-Versionen bekannt. Mit NetWare 3.2 und NetWare 4 ist man jedoch nicht mehr daran gebunden, für den NetWare Server ausschließlich IPX-Protokolle zu verankern. NetWare 3.2 und Netware 4.x bieten eine wesentlich offenere Systemarchitektur. Diese will ich Ihnen näher erläutern. Anzumerken ist, daß mit Einführung von NetWare 5 TCP/IP das Standardprotokoll von NetWare 5 ist, d.h., NetWare unterstützt für die Client/Server-Kommunikation Native-IP; das IPX-Protokoll kann aus Kompatibilitätsgründen noch optional installiert und konfiguriert werden.

15.3 NetWare 3.2 – eine offene Systemarchitektur

Wenn man das Konzept und den Aufbau der Architektur von NetWare 3.2 näher betrachtet, fällt auf, daß NetWare 3.2 im Design wesentlich verbessert worden ist – es handelt sich um eine offene Systemarchitektur.

Die Verbesserungen betreffen die Unterstützung von Transport/Client-Server-Protokollen, das Datei- und Directory-System, Dateinamenskonventionen, LAN-Driver und andere zusätzliche NetWare-Dienste. Durch die offene Server-Plattform kann der Systemverantwortliche ohne Probleme zusätzliche Dienste oder NetWare-Module am File-Server laden oder auch wieder entfernen.

15 Novell NetWare 3.2

Dies beginnt bereits bei der Installation von NetWare. NetWare 3.2 lässt sich relativ einfach und schnell installieren. Auch nachträgliche Erweiterungen oder Anpassungen des File-Server-Systems sind viel schneller durchzuführen. Diese Vorgänge werden jedoch in den Nachfolgeversionen NetWare 4 und NetWare 5 nochmals verbessert. Die Krönung hierbei ist, daß NetWare 5 eine vollständige auf Java-basierende, grafische Installation zur Verfügung stellt. Ab diesem Zeitpunkt besteht dann auch die Notwendigkeit, den Server mit einer Maus auszustatten. Für NetWare 3.2 und NetWare 4 ist dies noch nicht notwendig, da die Installation hier immer noch mit textbasierenden Menüfenstern abläuft.

Durch die Unterstützung von zusätzlichen Transport- und Client-Server-Protokollen (dies alles unter dem Gesichtspunkt eines offenen Systems) wird eine wichtige Grundlage für NetWare als Server-Plattform des Network Computing geschaffen. NetWare 3.2 ist nicht mehr auf ein Transportprotokoll und ein Client-Server-Protokoll beschränkt. Durch die Entwicklung von NetWare/IP von Novell ist man sogar in der Lage, TCP/IP als Standardprotokoll einzusetzen, um somit vollständig auf die IPX-Mechanismen verzichten zu können. Dies bedeutet jedoch, daß zusätzliche NetWare/IP-Software-Komponenten und ein eigener NetWare/IP-Client installiert werden müssen.

Neben dem standardmäßig von Novell unterstützten Transportprotokoll IPX und dem Client-Server-Protokoll NCP kann NetWare 3.2 um zusätzliche Transport- und Client-Server-Protokolle erweitert werden.

Darüber hinaus ist NetWare 3.2 nicht mehr auf eine Datei- und Directory-Namenskonvention beschränkt. Durch zusätzliche Module kann ein sogenannter Name Space Support geladen werden. Damit ist es möglich, daß der File-Server unter NetWare 3.2 neben den Datei- und Directory-Konventionen von DOS auch Macintosh-, OS/2-, Windows-NT-, Windows-95/98- oder Unix-Datei- und -Directory-Konventionen unterstützen kann.

Auf diese Weise wird erreicht, daß jede Workstation mit ihrem eigenen Betriebssystem unter NetWare 3.2 eingesetzt werden und jedes Workstation-Betriebssystem mit seinen eigenen Datei- und Directory-Konventionen seine Dateien und Directories am File-Server ablegen und pflegen kann.

Die offene Systemarchitektur von NetWare 3.2 besteht im wesentlichen aus drei Komponenten:

■ *NetWare 3.2 Loadable Modules (NLMs)*

Der File-Server wird beim Einsatz von NetWare 3.2 zum größten Teil aus NLMs aufgebaut. Der Kernel von NetWare wird durch das Programm SERVER.EXE unter DOS gestartet. Nachdem dieses Pro-

15.3 NetWare 3.2 – eine offene Systemarchitektur

gramm geladen ist (es handelt sich hierbei um die System-Executive), werden alle anderen notwendigen File-Server-Komponenten nacheinander geladen. Bei all diesen Modulen handelt es sich um NLMs.

Durch das Laden von NLMs wird die System-Executive um zusätzliche Komponenten erweitert. Diese NLMs können im laufenden File-Server-Betrieb geladen und auch wieder entladen werden. Außer der System-Executive (SERVER.EXE) handelt es sich bei allen anderen Komponenten um NLMs. Dies gilt unter anderem für LAN-Driver, Disk-Driver, Installationsprogramm, Datenbank-Server, Print-Server, Server-Utilities, Kommunikationsdienste und dergleichen mehr.

■ *Open Data Link Interface*

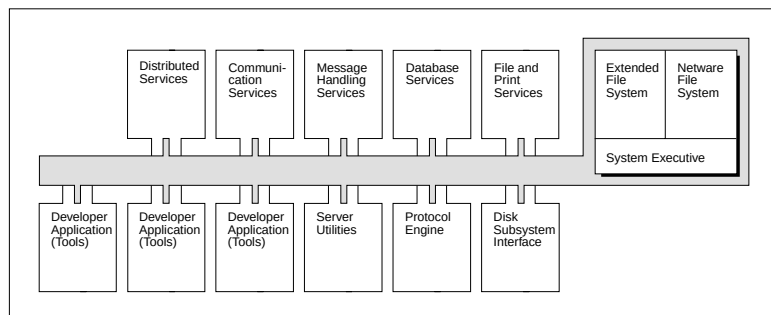
Hierbei handelt es sich um eine Menge von Spezifikationen, die NetWare 3.2 zu einer offenen Server-Plattform machen, auf der sogenannte Multiple Link Interface Driver, d.h. spezielle NLMs, aufbauen. Durch diese Spezifikationen ist es möglich, daß sich mehrere Transportprotokolle (Communication Protocols), wie zum Beispiel IPX/SPX, TCP/IP oder AppleTalk, den gleichen LAN-Driver und den gleichen Netzwerkadapter teilen. Das heißt, diese Protokolle können über ein und denselben Netzwerkadapter bearbeitet werden.

■ *Streams Interface*

Diese Schnittstelle ist notwendig, damit mehrere Client-Server-Protokolle innerhalb eines File-Servers abgearbeitet und verstanden werden können, so daß NetWare 3.2 zu einer offenen Server-Plattform wird.

In Abbildung 15.3 ist der prinzipielle Aufbau von NetWare 3.2 dargestellt. In den nachfolgenden Beschreibungen soll auf diese einzelnen Komponenten und Funktionen von NetWare 3.2 näher eingegangen werden.

Abbildung 15.3
Der Aufbau von
NetWare 3.2



15 Novell NetWare 3.2

NetWare 3.2 unterstützt standardmäßig die System Fault Tolerant Stufe II (SFT II). Seit Ende 1992 steht auch zusätzlich die SFT III zur Verfügung, allerdings nur noch für NetWare 4.10, eine Entwicklungsrichtung, die allerdings durch den Einsatz der Cluster-Technologie für NetWare 4.11 und NetWare 5 in dieser Form nicht mehr weiter entwickelt wird. Mit SFT III ist es möglich, gesamte Server zu spiegeln. Die genauen Unterschiede zwischen SFT I, II und III sollen in einem späteren Abschnitt erläutert werden.

Aufgrund der vollen Ausnutzung des 80386- bzw. 80486-Prozessors, inklusive Pentium-Technologie, zeichnet sich NetWare 3.2 durch folgende grundlegenden Eigenschaften aus:

- Integration von LAN- und WAN-Technologie
- Unterstützung einer unternehmensweiten Vernetzung
- Unterstützung der unterschiedlichsten Workstations und Workstation-Betriebssysteme
- Unterstützung von Workstation- und Host-Anbindung und deren Verträglichkeit
- Protected-Mode-Unterstützung
- 32-Bit-Instruktionen
- 32-Bit-Datenpfad
- Keine Speichersegmentierung mehr
- 4 Gbyte physikalisch adressierbarer Hauptspeicher
- 32 Tbyte periphere Plattenkapazität
- 250 gleichzeitige Benutzer pro File-Server
- 100.000 gleichzeitig geöffnete Dateien am File-Server
- Dynamische Hauptspeicherkonfiguration am File-Server
- 64 Volumes pro File-Server, wobei ein Volume über 32 Festplatten verteilt sein kann (Spanned Volumes)
- 16.777.216 Bindery-Objekte und -Properties pro File-Server möglich
- 1024 Festplatten können pro File-Server unterstützt werden
- Sparse Files werden unterstützt
- Unterstützung der NetView-Management-Schnittstelle von IBM
- Einfache Installation über CD-ROM

Da NetWare 3.2 als Netzwerkbetriebssystem für Network Computing konzipiert worden ist, beinhaltet NetWare 3.2 Funktionalitäten, die genau auf diese Systemanforderungen zugeschnitten sind. Mit NetWare 3.2 hat der Systemverwalter Wahlfreiheit für die einzusetzenden Workstations. Somit können DOS, Windows, Windows 95/98, Windows NT, OS/2, Macintosh-OS oder auch Unix-Rechner als Arbeitsplatzrechner eingesetzt werden. Die neue Architektur ist modular aufgebaut, so daß es möglich ist, zusätzliche Netzwerkbetriebssystem-Komponenten im laufenden Betrieb am File-Server zu laden

15.4 Leistungskomponenten von Novell NetWare 3.2

und zu entladen. Die Verwaltung und Überwachung des File-Servers unter NetWare 3.2 ist damit wesentlich flexibler und einfacher als bei anderen Netzwerkbetriebssystemen. Mit NetWare 4 bzw. NetWare 5 wird diese Funktionalität nochmals verbessert, da man von der serverorientierten Verwaltung Abschied nimmt und eine netzwerkorientierte Verwaltung aufgebaut hat. Wesentlichen Einfluß hat der Einsatz der NDS im Vergleich zu den Bindery-Mechanismen, so wie sie in NetWare 3.2 verankert sind.

Die zentrale Komponente von NetWare 3.2 ist das Real-Time-Betriebssystem, d.h. der Kernel von NetWare 3.2. Der Kernel ist neben den erwähnten Funktionen unter anderem zuständig für das Zuweisen von Hauptspeicher, für das Überprüfen der Zugangsberechtigungen und für die Freigabe der Dateien und Directories für den Benutzer und für das Verwalten der einzelnen Tasks (gestartete Prozesse) am File-Server.

Aufgrund der 80386- bzw. 80486- und Pentium-Prozessor-Unterstützung zeichnet sich NetWare 3.2 durch wesentlich höhere Verarbeitungsgeschwindigkeiten im Vergleich zu früheren Versionen aus.

15.4 Leistungskomponenten von Novell NetWare 3.2

Ein Netzwerkbetriebssystem erfordert ein Konzept, das Leistungsfähigkeit und Sicherheit in den Vordergrund stellt. Die Probleme der Leistungsengpässe sind nur allzu bekannt, wenn man den Bereich der Mittleren Datentechnik betrachtet. In einem LAN erbringt zwar die Workstation die Rechenleistung, aber der File-Server ist verantwortlich dafür, wie schnell die Anforderung der Workstation (Datei lesen, Datei schreiben etc.) erledigt werden kann.

Da NetWare auch noch Funktionen zur Verfügung stellt, um zusätzliche Server-Dienste auf ein und derselben Maschine zu implementieren (Print-Server, Communication Server, Router etc.), muß noch mehr darauf geachtet werden, leistungsfähig zu sein und zu bleiben. In diesem Abschnitt wollen wir zeigen, mit welchen Mechanismen Novell diesen Bereich abdeckt.

Novell wollte ein spezialisiertes Betriebssystem entwerfen und untersuchte die Bedingungen für verteilte Verarbeitung. Eine Liste grundlegender Charakteristika und möglicher Engpässe wurde zusammengestellt, inklusive der Anforderung spezieller notwendiger Dienste, die ein solches System abdecken muß. Dieser Entwurf ergab ein System umgebungsspezifischer Anforderungen, die zur Realisierung eines LAN-Betriebssystems mit verteilter Verarbeitung notwendig sind.

15.4.1 Grundlegende Eigenschaften

1. Da die Forderung gestellt wurde, ein System zu entwickeln, das es gestattet, Arbeitsplätze mit den unterschiedlichsten Betriebssystemen zu unterstützen, mußte die File-Service-Umgebung so spezifiziert werden, daß sie eine breite Palette von Unterprogrammaufrufen zur Verfügung stellt, damit Datenzugriffe und Datennutzung synchronisiert werden können.

Damit können die Dateianforderungen von allen Benutzern an die File-Service-Dienste des Netzwerks weitergeleitet werden.

2. Das Antwortzeitverhalten der angeschlossenen PCs muß besser, zumindest gleich denen von Standalone-PCs sein.
3. Der Entwurf eines neuen Betriebssystems bot die Gelegenheit, Dienste zu implementieren, die bisher von PC-Betriebssystemen noch nicht angeboten worden sind.

15.4.2 Mögliche Engpässe bezüglich Geschwindigkeit und Leistung innerhalb eines LAN

Die Leistungsfähigkeit eines LAN hängt von mehreren Faktoren innerhalb des Netzwerks ab. Ein solcher Engpaß kann neben der Netzwerkadapterkarte und Übertragungsrate des Netzes das Betriebssystem selbst sein. Es kommt dabei vor allem auf die interne Struktur, d.h. auf die Verarbeitungsweise des Betriebssystems an, um entsprechend effizient und schnell arbeiten zu können. Die Steuerung des Prozessors, der Taskwechsel in der CPU und die Hauptspeicherverwaltung sind nur einige dieser Faktoren. Da ankommende Anforderungen die momentane Bearbeitung eines Prozesses unterbrechen können, muß dieser Wechsel bzw. das Umschalten auf einen anderen Prozeß sehr schnell erfolgen.

Sind der Aufwand für einen Task-Wechsel und die Steuerung der Prozesse zu hoch, kann es so weit kommen, daß die CPU bereits bei sehr wenigen parallelen Aktivitäten nur noch damit beschäftigt ist, von einem Task auf den nächsten umzuschalten, und deswegen keine Anforderungen mehr erledigen kann. Man sagt in solchen Fällen auch, das Betriebssystem ist mit der eigenen Verwaltung voll ausgelastet und kann deshalb nichts anderes mehr erledigen. In Fachkreisen wird dies als »thrashing« (Überlastung) bezeichnet. Dagegen schränken unnötige Operationen der CPU im File-Server die Leistungsfähigkeit des Netzwerks erheblich ein.

Da der File-Server von allen angeschlossenen und aktiven Stationen zum Laden und Abspeichern von Daten und Programmen verwendet wird, ist es für den Durchsatz auch entscheidend, wie schnell die

15.5 Der Betriebssystemkern (Nukleus)

Übertragungs- und Plattenkanäle sind. Dies kann einen weiteren Engpaß auf dem File-Server bilden. Entscheidend für den Durchsatz des Plattenkanals ist die eingesetzte Hardware im File-Server. Die Plattenkanäle arbeiten – wie alle peripheren Einheiten eines Computers – im Vergleich zur CPU wesentlich langsamer. Hierbei kann ein Faktor von 100 durchaus erreicht werden. Novell hat es sich beim Erstellen des Konzepts für ein LAN-Betriebssystem zum Grundsatz gemacht, eine Reihe von Verbesserungen dahingehend mit einzubeziehen. Im folgenden Abschnitt werden wir diese Konzepte und Möglichkeiten näher untersuchen.

Folgende Netzwerkdienste und -leistungen sind laut Novell entscheidend für die Architektur eines LAN-Betriebssystems.

1. Unterstützung aller File-Services für PCs und die hierfür eingesetzten unterschiedlichen Betriebssysteme
2. Hohe Leistung
3. Kompatibilität zu allen anerkannten Übertragungsstandards
4. Transparenter Zugriff auf Ressourcen beim Einsatz von »Internetworking« mit dynamischer Wegwahl (Routing)
5. Fehlertoleranz in mehreren Ausbaustufen
6. Verwendung von Transaktionsfortschreibung, damit die Integrität und Konsistenz von Datenbeständen erhalten bleibt
7. Einsatz eines modularen Internetwork-Konzepts, damit dieses schrittweise ausgebaut werden kann
8. Offene Architektur, um damit anderen Herstellern die Integration von zusätzlichen Diensten zu ermöglichen

Sie werden feststellen, daß dies für Novell nicht nur Schlagwörter sind.

Das Betriebssystem von Novell stellt eine elegante Lösung für verteilte PC-Netzwerke dar. Der Nukleus, der Übertragungskanal und der Plattenkanal wurden so konzipiert, daß sie Dienste in einer Multi-User-Umgebung mit verteilter Verarbeitung bieten und koordinieren können.

15.5 Der Betriebssystemkern (Nukleus)

Der Nukleus oder Kernel eines Betriebssystems entscheidet darüber, wie schnell oder wie langsam Arbeiten erledigt werden. Wird die CPU ständig durch andere Prozesse zur Freigabe aufgefordert, damit diese abgearbeitet werden können, kann kein Prozeß vernünftig und kontinuierlich abgearbeitet werden. Novell hat sich deshalb dafür entschieden, daß laufende Verarbeitungsprozesse die CPU von sich aus freigeben, z.B., wenn auf das Lesen von Daten von der Fest-

platte gewartet werden muß. Dies bedeutet, daß ankommende Prozesse warten, bis der gerade laufende Prozeß endet oder dieser die CPU freigibt. Ein Wechsel der CPU von einem Prozeß zum anderen erfolgt also nur, wenn es unbedingt notwendig ist. Der entstehende Overhead für Prozeßwechsel und damit verbunden die Prozessorsteuerung werden auf ein Minimum reduziert.

Ankommende Pakete haben alle die gleiche Priorität und den gleichen Anspruch auf Dienstleistungen. Ankommende Anforderungen müssen somit warten und können nicht einfach den laufenden Prozeß unterbrechen. Dies ergänzt das oben ausgeführte Prinzip.

Aufgrund dieser Voraussetzungen konnte der Programmcode für den Nukleus entsprechend reduziert werden, was wiederum dazu beiträgt, daß die Abarbeitungsgeschwindigkeit um einiges höher wird und die Leistung des Betriebssystems zunimmt.

15.5.1 **Ablauf der Kommunikation zwischen File-Server und Workstation**

Damit die erweiterten Funktionen des Netzwerks auch genutzt werden können (Datenmanipulation, Zugriffsschutz, Zugriffssynchronisation etc.), die vom File-Server geboten werden, muß eine Schnittstelle zwischen der Applikation, die in der Workstation läuft, und dem File-Server geschaffen werden. Die Aufgabe der Koordination übernimmt die Workstation-Shell bzw. der NetWare Requester auf der Workstation.

Bei der Shell bzw. dem Requester handelt es sich um mehrere residente Programme, die auf der Workstation im Hintergrund laufen. Die Funktionen des Betriebssystems auf der Workstation (es kann sich um DOS, Windows, Windows 95/98, Windows NT oder OS/2 handeln) werden um zusätzliche Dienste, die der File-Server zur Verfügung stellt, erweitert. Es wird praktisch ein »Fenster zum Netzwerk« eröffnet, über dem gearbeitet werden kann. Durch die Unterstützung unterschiedlicher Protokollwelten ist es möglich, Workstations in ihrer Native-Form zu integrieren (Apple, Unix). Dazu werden Funktionen auf dem Server installiert, die einem Apple-Rechner den NetWare Server wie einen AppleShare Server erscheinen lassen oder einer Unix-Maschine den Eindruck vermitteln, es würde sich beim NetWare Server um einen Unix-Server handeln. Das betrifft auch die Unterstützung der spezifischen Dateinamenskonventionen: NetWare unterstützt die Mechanismen der Name-Space-Module, die zusätzlich für das jeweilige Client-Betriebssystem aktiviert werden können.

15.5 Der Betriebssystemkern (Nukleus)

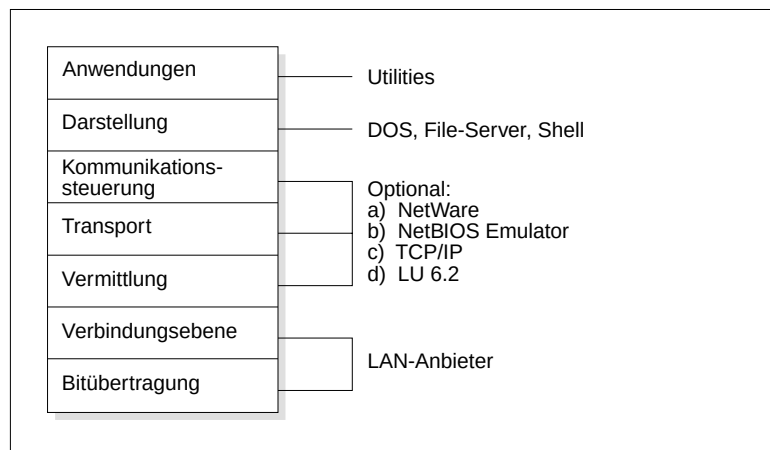
Für die Einbindung von Macintosh-Rechnern oder Unix-Systemen werden zusätzliche Mechanismen am Server installiert, um entsprechende Protocol Stacks unterstützen zu können. Wie noch zu sehen ist, kann auch eine Workstation so eingerichtet werden, daß sie mit mehreren Protocol Stacks arbeiten kann. Das ist unter anderem dann erforderlich, wenn neben IPX/SPX-Protokollen auch TCP/IP-Protokolle notwendig sind, um gleichzeitig an einer Unix-Anlage über Telnet oder FTP arbeiten zu können. Aber dazu später mehr.

15.5.2 Die Funktionsweise der Shell

Wird die Station-Shell aktiviert, wird sie automatisch von DOS als Standard-DOS-Anwendung geladen. Wenn die Steuerung an die Shell abgegeben wird, paßt sich diese an die DOS-Umgebung an, bevor sie endet. Durch die Shell wird der DOS-Interrupt 21H im unteren Bereich mit Adressen, die in den Adreßbereich der Shell zurückweisen, überschrieben. Die Shell übernimmt somit die Steuerung aller DOS-Funktionsaufrufe, die über den Interrupt 21H ausgeführt werden, und ordnet die Systemaufrufe den Netzwerkdiensten zu. Schließlich beendet sich die Shell selbst, bleibt jedoch resident im Speicher und wartet erneut auf Anforderungen der Applikation.

In Abbildung 15.4 ist die Eingliederung der Software-Schnittstellen in das ISO/OSI-Modell beim Einsatz von Novell NetWare dargestellt.

Abbildung 15.4
Einordnung der
Protokolle unter
NetWare im ISO/
OSI-Modell



15 Novell NetWare 3.2

Damit NetWare in der Lage ist, all diese Funktionen in der Performance zu unterstützen, wird von jeher sehr viel Wert auf die optimale Ausnutzung des Hauptspeichers gelegt und diese auch realisiert. Ein großer Hauptspeicher ist tatsächlich – wie immer wieder behauptet wird – gut für die Performance. Die nachfolgenden Ausführungen sollen Ihnen helfen zu verstehen, warum dies so ist.

Mit der Einführung von NetWare 4 hat Novell eine vollkommen neue Workstation-Umgebung entwickelt: den 32-Bit-Client. Diese Umgebung wurde inzwischen auch für NetWare 3.2 eingeführt. Es ist jedoch nach wie vor möglich, sowohl mit dem neuen Requestor als auch mit der alten Shell-Umgebung am NetWare Server zu arbeiten. Während der Entwicklung von NetWare 5 hat man bereits im Vorfeld den sogenannten Z.E.N.works-Client freigegeben. Hierbei handelt es sich ebenfalls um den 32-Bit-Client, der weitere wesentliche Verbesserungen für DOS/Windows, Windows 95/98 und Windows NT zur Verfügung stellt.

Arbeitet man aus historischen Gründen noch mit der ganz alten Shell, die nicht NDS-fähig ist, bedeutet dies jedoch, daß Sie dann nur im Bindery-Modus arbeiten können. Langfristig gesehen sollte die Workstation-Umgebung generell mit dem neuen Requestor ausgestattet werden. Die Vorteile der Requester-Umgebung werden bei der technischen Beschreibung von NetWare 3.2 näher behandelt.

Im Zuge der Windows-95-Einführung hat Novell eine neue Workstation-Umgebung entwickelt, die NIOS heißt. Dabei handelt es sich um die neue 32-Bit-Treiberumgebung für DOS/Windows und Windows 95, eine nochmalige Verbesserung der VLM-Umgebung. Eine Entwicklung für Windows NT ist inzwischen auch abgeschlossen. Neben dem wesentlich geringeren Speicherbedarf besteht ein Vorteil der neuen 32-Bit-Umgebung darin, daß ein Login direkt unter Windows bzw. Windows 95/98 durchgeführt werden kann, ein Mechanismus, der bislang nicht so ohne weiteres möglich gewesen ist, da dann keine Login-Scripts ausgeführt worden sind und somit alle Laufwerkszuordnungen gefehlt haben. Kaum hat man sich an die neue 32-Bit-Umgebung gewöhnt, ergeben sich durch die Einführung von Z.E.N.works nochmals Verbesserungen. Bei der Darstellung von NetWare 4 bzw. NetWare 5 soll etwas näher auf diese neue 32-Bit-Umgebung eingegangen werden.

15.6 Hauptspeichervoraussetzung

Will man NetWare 3.2 starten, muß der File-Server zuerst mit DOS gebootet werden. Unter DOS wird anschließend das Programm SERVER.EXE geladen, um die System-Executive von NetWare 3.2 zu aktivieren. Sobald die System-Executive gestartet ist, wird DOS auf dem File-Server »schlafen« gelegt. DOS belegt dann zwar noch den Hauptspeicher, kann aber nicht mehr benutzt werden. NetWare 3.2 läßt sich nur als dedizierter File-Server einsetzen. Um den Speicher, den DOS im Hauptspeicher belegt, zusätzlich für NetWare zur Verfügung zu stellen, kann DOS aus dem Hauptspeicher entfernt werden. Für NetWare 4.x ist der Startvorgang gleich. NetWare 3.2/4.x ist somit nicht im Besitz eines eigenen Bootstrap-Loaders und muß deshalb auf DOS als Mittel zum Zweck zurückgreifen können. Meinen Sie jetzt aber bitte nicht, daß NetWare unter DOS läuft, DOS wird nur als Starthilfe benötigt.

Nach dem Starten von NetWare wird der Hauptspeicher also unterteilt für DOS, für das NetWare-3.2-Betriebssystem und für Einheiten von Cache-Puffern. Diese Cache-Puffer werden benötigt, um File-Caching, Directory-Caching und Directory-Hashing durchführen zu können. Werden zusätzliche Module (NLMs) am File-Server geladen, werden aus den Cache-Puffer-Bereichen Hauptspeicherplätze entnommen. Zu Beginn der Ausführungen über NetWare 3.2 wurde bereits erwähnt, daß die Hauptspeicherverwaltung unter NetWare 3.2 dynamisch erfolgt.

Um NetWare 3.2 einsetzen zu können, sind neben einem 80386-, 80486 oder 80586-Rechner mindestens 4 Mbyte Hauptspeicher erforderlich. Je nachdem wie groß Ihre gesamte Platte ist, müssen Sie eventuell mehr Hauptspeicher im File-Server einbauen, um NetWare starten zu können. Die Erfahrung zeigt, daß auch bei kleinen Netzwerken mit mindestens 32 Mbyte Hauptspeicher begonnen werden sollte, wenn es sich um einen Server mit 4 Gbyte Plattenkapazität, herkömmlichen Anwendungen und einer passenden Datensicherung handelt. Von welchen weiteren Faktoren der Speicherbedarf abhängt, werde ich Ihnen an anderer Stelle noch zeigen. Durch das dynamische Hauptspeichermanagement erhalten Sie automatisch eine Mitteilung an der Server-Console, wenn das Betriebssystem feststellt, daß mehr Hauptspeicher erforderlich ist. Der File-Server läuft in diesem Fall zwar ohne Probleme weiter, aber aufgrund des zu geringen Hauptspeichers und der dynamischen Hauptspeicherverwaltung leidet die Performance des File-Servers, da ständig Hauptspeicher zwischen den einzelnen aktiven Tasks hin- und hergeschaufelt werden muß.

15 Novell NetWare 3.2

Der Hauptspeicher des File-Servers wird unter NetWare in Cache-Puffer-Bereiche eingeteilt. Einen Teil des Hauptspeichers belegt das Netzwerkbetriebssystem (System-Executive), der verbleibende Rest wird von den zusätzlich geladenen NLMs belegt. Daneben benötigt NetWare noch Hauptspeicher zum Ablegen der FAT-Tabellen für jedes einzelne Volume, für das Directory-Caching, für das Einrichten der Directory-Hashing-Tabellen und das File-Caching.

Generell gilt, daß der nicht belegte Cache-Puffer-Bereich für das File-Caching bereitgestellt wird. Wird nun ein neues NLM geladen oder benötigt ein geladenes NLM zusätzlichen Hauptspeicher, wird dieser entweder einem anderen Prozeß entzogen, wenn dieser den Cache-Puffer-Bereich freigeben kann, oder aus dem File-Cache-Puffer-Bereich entnommen. Dabei ist jedoch gewährleistet, daß unter anderem für File-Caching, Directory-Caching und Directory-Hashing eine Mindestzahl von Cache-Puffern reserviert wird, die nicht von anderen Prozessen oder NLMs benutzt werden dürfen.

Sie sehen, daß NetWare 3.2 mit den gleichen Komponenten zur Leistungssteigerung am File-Server arbeitet, wie dies bereits von früheren NetWare-Versionen bekannt ist. Dieser Prozeß ist jedoch dynamisch.

Durch die dynamische Hauptspeicherverwaltung unter NetWare 3.2 muß man sich über die Parameterwerte zur Aufteilung des Hauptspeichers zu Beginn der Installation keine Gedanken mehr machen, da NetWare 3.2 diese selbst bei Bedarf vergrößert. Es muß nur beachtet werden, daß während des Betriebs die möglichen Maximalwerte nicht überschritten werden. So ist es zum Beispiel nicht möglich, auf ein Volume unter NetWare 3.2 mehr als 2.097.152 Directory-Einträge zu schreiben oder mehr als 100.000 Dateien am File-Server gleichzeitig geöffnet zu haben. Hierbei handelt es sich allerdings um Grenzwerte, die von kaum einer Installation erreicht werden dürften.

Die Default-Cache-Puffer-Größe unter NetWare 3.2 beträgt 4 Kbyte. Beim Starten des File-Servers kann unter NetWare 3.2 festgelegt werden, mit welcher Cache-Puffer-Größe der Hauptspeicher eingerichtet werden soll. Es steht hierbei die Einteilung von 4 Kbyte, 8 Kbyte oder 16 Kbyte zur Verfügung. Durch eine Vergrößerung der Cache-Puffer-Größe kann die Geschwindigkeit des File-Servers erhöht werden. Am File-Server werden Cache-Puffer zu folgenden Zwecken verwendet:

- Der Server leiht sich Cache-Puffer, wenn NetWare Loadable Modules, wie zum Beispiel LAN-Driver, Disk-Driver, das INSTALL-Utility, das Monitor-Programm, andere Management NLMs etc. ge-

15.7 Dynamische Speicherkonfiguration

laden werden. Wird das NLM wieder entladen, dann wird der freiwerdende Hauptspeicher wieder zum Cache-Puffer-Bereich zurückgegeben.

- Der Server legt sich genügend Cache-Puffer an, um die FAT eines jeden Volumes in den Hauptspeicher laden zu können.
- Der Server legt sich Cache-Puffer an, um Teile der Directory-Tabellen eines jeden Volume in den Hauptspeicher laden zu können. Es ist also nicht so, daß die gesamte Directory-Struktur eines Volume in den Hauptspeicher geladen wurde, vielmehr ist es hier nur der Teil, der am häufigsten bzw. momentan im Zugriff ist.
- Der Server benutzt den verbleibenden Cache-Puffer-Bereich, um alle im Zugriff befindlichen Dateien im Hauptspeicher des File-Servers zwischenspeichern zu können.
- Der Server belegt Cache-Puffer, um Hash-Tabellen für alle Directory-Einträge anlegen zu können.
- Der Server legt sich Cache-Puffer an, um Turbo FATs einrichten zu können. Diese Turbo FATs werden automatisch eingerichtet, wenn Dateien als Random-Access-Dateien im Zugriff sind und mehr als 64 FAT-Einträge besitzen. Die Datei selbst muß nicht mehr mit dem Dateiattribut *Indexed* versehen werden, wie dies unter früheren NetWare-Versionen der Fall war.

Die Hauptspeicherauslastung sollte jedoch in regelmäßigen Abständen geprüft werden, um feststellen zu können, ob sich der Server in einer optimalen Konfiguration befindet. Bei Bedarf können die Parameterwerte am Server geändert werden, um Einfluß auf die Verteilung des Speichers und damit auf die Performance nehmen zu können. Dies muß jedoch mit äußerster Vorsicht geschehen, damit nicht versehentlich das genaue Gegenteil bewirkt wird.

15.7 Dynamische Speicherkonfiguration

Beim Einsatz von NetWare 3.2 muß sich der Systemverantwortliche keine Gedanken mehr machen, wieviel Speicherbereich für bestimmte Systemressourcen am File-Server zugewiesen werden muß. Wenn die System-Executive geladen ist, überwacht sie die richtige Speicherzuordnung für Cache-Speicher, Directory-Caching und Hashing, NLMs etc. Jedesmal, wenn ein Netzwerkdienst zusätzlichen Speicher benötigt, wird dieser von der System-Executive zugewiesen. Die Zuordnung geschieht jedoch immer in Abhängigkeit des zur Verfügung stehenden Gesamtspeichers. Die dynamische Speicherkonfiguration – Novell spricht hier von der sogenannten Dynamic Resource Configuration – erfolgt für:

15 Novell NetWare 3.2

- Directory Cache-Buffer
- File Service Processes
- Turbo FAT Index Tables
- FAT Tables
- Routing Buffers
- Disk Elevator Size
- Directory Hash Tables
- Router/Server Advertising Memory
- Maximum Number of Open Files
- File Locks
- Kernel Processes
- Kernel Semaphores
- TTS Transactions
- Memory for Loadable Modules

Um jedoch unnötige Speicherzuordnungen zu vermeiden, die aufgrund plötzlicher, unregelmäßiger Spitzen von Serveraktivitäten auftreten könnten, wartet der Server ein paar Sekunden, nachdem die Speicheranforderung beim File-Server eingetroffen ist. Kann die Speicheranforderung von einem anderen Prozeß abgedeckt werden, muß kein Speicher aus dem Cache-Puffer entnommen werden.

Die dynamische Speicherkonfiguration kann auf fünf Arten erfolgen. Die beiden ersten Arten werden als Nonreturnable und die anderen drei als Returnable bezeichnet.

15.7.1 Nonreturnable Memory

Nonreturnable Memory wird nicht mehr an den File-Cache-Puffer-Bereich zurückgegeben, nachdem dieser von einem Prozeß einmal angelegt und dann wieder von ihm freigegeben wird. Dieser Cache-Puffer wird nur dann wieder freigesetzt und an den File-Cache-Puffer zurückgegeben, wenn der File-Server runtergefahren wird. Der einmal belegte Puffer-Bereich für Nonreturnable Memory wird anschließend nur noch an den Memory-Pool zurückgegeben, von dem er angelegt worden ist. Dies gilt nicht für den sogenannten Permanent Memory Alloc Pool. Für den Nonreturnable-Memory-Bereich sind zu unterscheiden:

- *Alloc Pool*
 - Speicher wird schnell und effizient angelegt.
 - Legt Speicher in kleineren Bereichen als 4-Kbyte-Cache-Block-Größe an.
 - Legt Speicher an, wenn dieser nur kurze Zeit benötigt wird.
 - Legt den Speicher in genau der Größe an, in der er benötigt wird.

15.7 Dynamische Speicherkonfiguration

- Der Speicher wird nicht an den File-Cache-Puffer zurückgegeben.
- Der Speicher wird an den Memory-Pool zurückgegeben.
- Der Speicher wird nicht verschoben.
- *Permanent Memory Alloc Pool*
 - Legt Speicher in beliebigen Größen an.
 - Legt den Speicher in genau der Größe an, in der er benötigt wird.
 - Der angelegte Speicher wird nicht mehr an den File-Cache-Puffer zurückgegeben (NLMS können diesen Speichermechanismus nicht benutzen).
 - Der Speicher wird auch nicht mehr an den Memory-Pool zurückgegeben.
 - Der Speicher wird nicht verschoben.
- *Permanent Returnable*
 - Der Speicher wird in kleineren Größen als der eines 4-Kbyte-Blocks angelegt.
 - Dieser Speicher wird angelegt, wenn er für längere Zeit benötigt wird.
 - Der Speicher wird in genau der angeforderten Größe angelegt.
 - Der Speicher wird nicht mehr an den File-Cache-Puffer zurückgegeben.
 - Der Speicher wird an den Memory-Pool zurückgegeben.
 - Der Speicher wird nicht verschoben.

15.7.2 Returnable Memory

Ein Prozeß, der Speicher als »returnable« angelegt hat, gibt ihn wieder an den File-Cache-Puffer zurück, wenn er vom Prozeß freigegeben wird. Das gesamte Returnable Memory wird an den Memory-Pool nach seiner Freigabe zurückgegeben. Für diese Hauptspeicherklassen sind zu unterscheiden:

- *Nonmoveable Memory (von NLMS benutzt)*
 - Legt Speicher in den Cache-Block-Größen von 4 Kbyte, 8 Kbyte oder 16 Kbyte an.
 - Legt den Speicher für kurze oder längere Zeitperioden an.
 - Der Speicher wird wieder an den File-Cache-Puffer-Bereich zurückgegeben.
 - Der Speicher wird an den Memory-Pool zurückgegeben.
 - Der Speicher wird nicht verschoben.
- *Moveable Memory*
 - Der Speicher wird in großen Cache-Block-Größen von 4 Kbyte, 8 Kbyte oder 16 Kbyte angelegt, wenn dieser Bereich

15 Novell NetWare 3.2

wachsen kann, z.B. wenn Systemtabellen angelegt werden und diese aufgrund der dynamischen Konfiguration größer werden können.

- Der Speicher kann sowohl kurzfristig als auch langfristig angelegt werden.
- Der Speicher wird an den File-Cache-Puffer-Pool zurückgegeben.
- Der Speicher wird an den Memory-Pool zurückgegeben.
- Der Speicher kann verschoben werden. Es gibt Prozesse, die in der Lage sein müssen, Pointer für diesen Speicherbereich anzupassen.
- Es wird keine Fragmentierung des Cache-Puffer-Bereichs verursacht.

Diese Speicherverwaltung sieht nicht nur schön aus, sondern bietet auch Vorteile, schließlich kann sie auch mehr Leistung aus dem System holen. Im Lauf der Zeit stellte man allerdings fest, daß durch diese Speicherverwaltung auch Nachteile entstehen können. Durch häufiges Laden und Entladen von NLMs zum Beispiel ist es durchaus möglich, daß der Hauptspeicher so fragmentiert ist, daß kein NLM mehr geladen werden kann, obwohl eigentlich genügend Hauptspeicher zur Verfügung steht, dieser jedoch nicht zusammenhängend ist. Beim Laden von NLMs wird immer noch einem in der Größe notwendigen zusammenhängenden Speicher gesucht.

Es gibt auch belegte Speicherbereiche, die nach dem einmaligen Anlegen nicht mehr an den Disk-Cache-Bereich zurückgegeben werden, auch wenn der belegte Speicher von dieser Anwendung nicht mehr benötigt wird. Dies betrifft unter anderem zur Spitzenlast angelegte Packet Receive Buffers oder Directory Cache Buffers, die im Alloc-Pool behalten werden, auch wenn deren Gebrauch nicht mehr notwendig wäre. Mit NetWare 4.x wird auch dieses Problem gelöst sein, da es dann nur noch einen einzigen Memory-Pool geben wird.

15.8 Unterstützung der Netzwerkadapterkarten

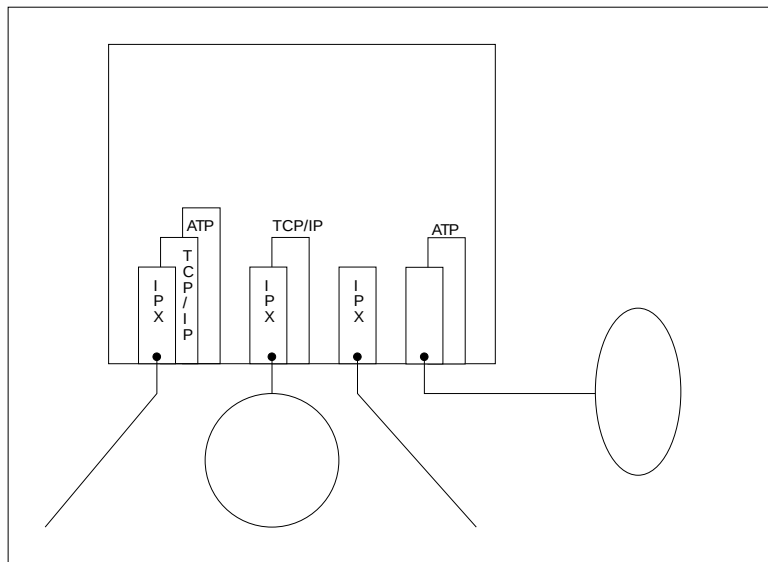
NetWare arbeitet unabhängig von physischen Medien und Zugriffsprotokollen. In jedem File-Server eines Netzes können theoretisch bis zu 16 Netzwerkkarten eingebaut werden. Es kann sich dabei um homogene oder heterogene Karten handeln. Somit besteht die Möglichkeit, mit einem File-Server mehrere physisch getrennte Netze zu betreiben, wobei alle Workstations der gekoppelten Netzwerke mit ein und demselben File-Server zusammenarbeiten und Stationen in LAN A auch Dienste, die in LAN B installiert sind, nutzen können.

15.8 Unterstützung der Netzwerk-adapterkarten

Alle können den gleichen Datenbestand verwenden und untereinander Nachrichten austauschen sowie gemeinsame Ressourcen benutzen. Dieser Mechanismus ist in Abbildung 15.5 dargestellt.

NetWare fungiert als interner Router, um Datenpakete innerhalb dieser LANs über den Router-Mechanismus von NetWare transportieren zu können. Dies funktioniert vor allem auch deshalb, weil das NetWare-IPX-Protokoll, wie auch IP und ATP, als Routing-fähiges Protokoll konzipiert ist. Dies unterscheidet das IPX- deutlich vom NetBEUI-Protokoll, da NetBEUI nicht Routing-fähig ist.

*Abbildung 15.5
Physikalisch eine
Karte, logisch wird
für jeden Protokoll-
Header eine eigene
Karte verwaltet,
zugleich ist auch
internes Routing
aktiv*



Bei den erwähnten theoretischen 16-LAN-Adaptoren pro Server ist zu beachten, daß jeder zusätzliche Protokoll-Header, den eine LAN-Karte unterstützen kann, unter NetWare jeweils eine eigene logische Netzwerkadapterkarte darstellt. Das heißt, wenn Sie eine physikalische Netzwerkkarte im Server installiert haben, z.B. eine Ethernet-Karte, und diese Karte sowohl Ethernet 802.3 als auch Ethernet II unterstützen kann, verwaltet der Server intern zwei logische Adapterkarten. Führen Sie das Beispiel fort, und Sie installieren vier Ethernet-Karten, und jede unterstützt die maximalen vier Protokoll-Header (Ethernet 802.3, Ethernet II, Ethernet 802.2, Ethernet SNAP), dann haben Sie Ihre 16 logischen Netzwerkkarten im Server bereits installiert.

Über die Arbeitsweise dieser Mechanismen und die Unterstützung der Protokoll-Stacks wird noch berichtet werden.

15.9 Verbesserte Plattenkanalausnutzung

Tests in LANs haben gezeigt, daß die meisten Anforderungen an den File-Server das Lesen oder Schreiben auf die Festplatte(n) betreffen. Zudem zwingen die unterschiedlichen Geschwindigkeiten zwischen File-Server-CPU und Plattenlaufwerk dazu, eine Optimierung des Datentransports durchzuführen. Der Ausdruck »Plattenkanal« soll dabei die Software und die Hardware bezeichnen, die für einen erfolgreichen Lese- oder Schreibzugriff auf die Festplatte erforderlich sind.

Vergleicht man die Geschwindigkeit zwischen CPU und Plattenkanal, stellt man fest, daß während einer Plattenoperation die CPU zwischen 50.000 und 100.000 Befehle ausführen könnte, je nachdem welcher Prozessor mit welchem Taktzyklus für diesen Vergleich verwendet wird.

Die Hardware des Plattenkanals und die File-Server-CPU arbeiten asynchron zueinander. Somit wäre es am besten, die Hardware des Plattenkanals mit höchster Geschwindigkeit arbeiten zu lassen, während die CPU andere Tätigkeiten ausführt (ein weiterer Grund für das Multi-Tasking von Novell). Noch einfacher und schneller wäre es, wenn es gelingen würde, den Plattenkanal völlig zu umgehen. Um diese Optimierungen einsetzen zu können, arbeitet Novell NetWare mit einem Mehrpfad-Plattenprozeß und verschiedenen Cache-Methoden, so daß sich die Geschwindigkeit des Plattenkanals erhöht und sich in vielen Fällen die Hardware des Plattenkanals ganz umgehen läßt. In Abbildung 15.6 sind alle von Novell eingesetzten Techniken zur Plattenkanaloptimierung aufgezeigt.

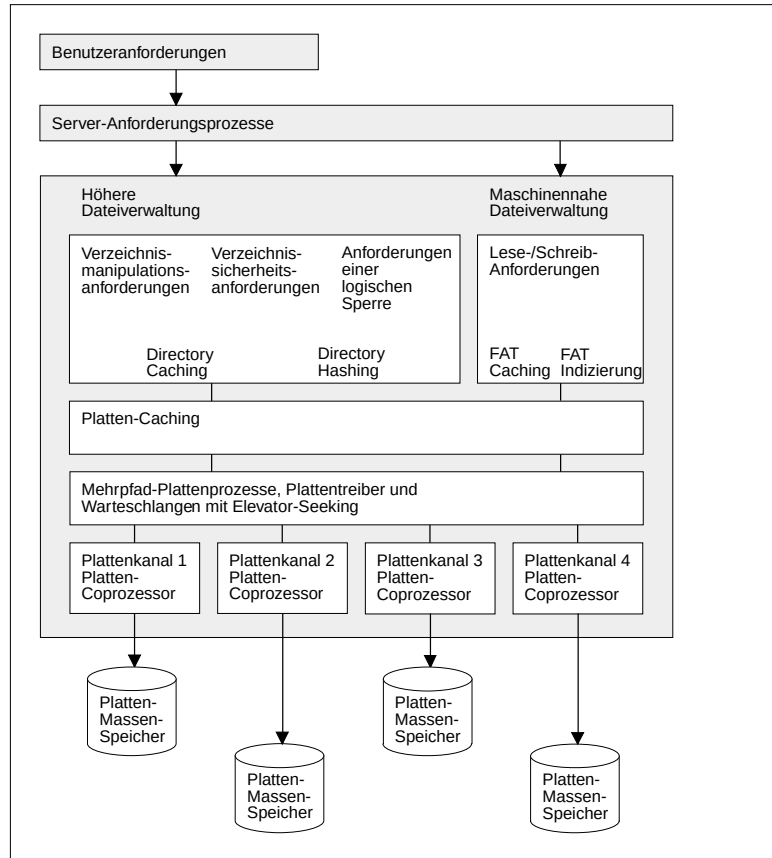
Wenn Sie auf einer Festplatte DOS, OS/2 oder Unix einrichten bzw. diese unter einem der genannten Betriebssysteme einsetzen möchten, muß vorher auf der Platte eine DOS-, OS/2- oder Unix-Partition eingerichtet werden. Dies ist auch der Fall, wenn eine Platte unter NetWare eingesetzt werden soll. Hierzu muß die Platte bei der Installation mit einer NetWare-Partition versehen werden. Diese NetWare-Partition kann man nun wiederum in Teilbereiche einteilen. Man bezeichnet sie als Volumes. Sie können eine NetWare-Partition in mehrere Volumes aufteilen, wobei auf einer Partition jedoch nicht mehr als acht Volumes eingerichtet sein dürfen. Die Größe des Volume unter NetWare 3.2/4x kann maximal 32 Tbyte betragen. Der File-Server kann bis zu 64 Volumes verwalten.

Mit NetWare 3.2 haben Sie auch die Möglichkeit, CD-ROM-Laufwerke an Standard-SCSI-Controllern zu installieren und als Volume zu mounten. Dann können alle Anwender im Netzwerk auf die CD-ROM-Laufwerke zugreifen.

15.10 Festplatten- und Volume-Verwaltung

NetWare 3.2 bietet aber bezüglich der Festplattenunterstützung und Performance-Steigerung noch eine Vielzahl weiterer Mechanismen.

Abbildung 15.6
Plattenverwaltung
unter NetWare



15.10 Festplatten- und Volume-Verwaltung

Bei der Verwaltung von Festplatten unter NetWare 3.2 muß beachtet werden, daß diese in Partitions, Volume-Segmente und Volumes aufgeteilt werden. In diesem Abschnitt will ich die unterschiedlichen Mechanismen, die Organisation und das Format von NetWare-3.2-Festplatten genauer aufzeigen.

Es geht dabei um:

- NetWare Partitions
- Volumes
- Disk-I/O
- Disk Allocation Block Size

- FATs und Turbo FATs
- Theoretische Hauptspeicher- und Plattenkapazität

15.10.1 NetWare Partitions

Um Festplatten unter NetWare einsetzen zu können, müssen diese zuerst in NetWare Partitions eingeteilt werden. Wird der File-Server unter NetWare eingesetzt, kann jede Platte ausschließlich mit einer NetWare-Partition eingerichtet werden.

Auf der internen Platte des File-Servers – das ist die Platte, die am internen Platten-Controller angeschlossen ist und von der aus der File-Server gebootet wird – muß neben der NetWare-Partition eine zusätzliche kleine DOS-Partition eingerichtet werden. Auf diese Weise kann der File-Server mit DOS von der Platte booten und über die AUTOEXEC.BAT automatisch SERVER.EXE aufrufen.

Auf jeder Festplatte können zwar mehrere Partitions vorhanden sein, aber auf jeder Platte kann nur eine NetWare-Partition eingerichtet sein. Die NetWare-Partition wird aufgeteilt in eine Hot Fix Redirection Area und den NetWare-Datenbereich. Die Hot Fix Redirection Area wird verwendet, um den Mechanismus der »Read after Write Verification« und den damit verbundenen Mechanismus der Fehlererkennung, wie später bei SFT Level I beschrieben, abzudecken.

Jede NetWare-Partition verfügt über vier Kopien einer Volume-Definitionstabelle. Die Kopien sind auf den Sektoren 32, 64, 96 und 128 abgelegt. Diese 512 Byte große Tabelle beschreibt den Rest der NetWare-Partition, beginnend bei Sektor 160 bis zum Ende der Partition. Jede Partition kann in ein bis maximal acht Volumes bzw. Volume-Segmente eingeteilt werden. Jedes Volume-Segment kann dabei zu einem anderen Volume gehören.

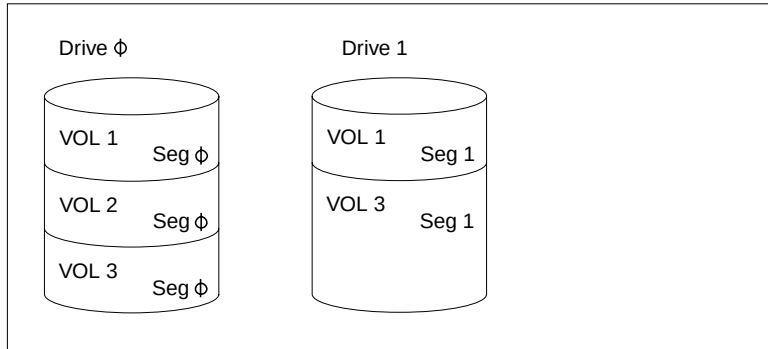
15.10.2 Volumes unter NetWare 3.2

Ein File-Server unter NetWare 3.2 kann bis zu 64 Volumes verwalten. Ein NetWare Volume ist dabei eine logische Einheit, die aus mindestens einem bis maximal 32 Volume-Segmenten besteht. Ein Volume unter NetWare 3.2 kann maximal 32 Tbyte groß sein. Jedes Volume-Segment kann entweder die ganze NetWare-Partition der Platte oder auch nur einen Teil der NetWare-Partition belegen. Ein Volume kann sich über mehr als eine Festplatte, also NetWare-Partition, erstrecken. Ein Volume-Segment hingegen ist immer auf eine NetWare-Partition beschränkt, d.h., es kann sich nicht über mehrere Platten erstrecken.

15.10 Festplatten- und Volume-Verwaltung

Durch diesen Mechanismus ist es leicht möglich, ein bestehendes Volume im laufenden File-Server-Betrieb zu vergrößern. Man fügt zum bestehenden Volume ein neues Volume-Segment hinzu und hat damit das Volume um die Größe des Segments erweitert. In Abbildung 15.7 ist eine mögliche Plattenaufteilung unter NetWare 3.2 dargestellt.

Abbildung 15.7
Verteilung der
Volume-Segmente
unter NetWare 3.2



Die Erweiterung eines Volume kann ohne Probleme im laufenden Betrieb durchgeführt werden, also auch während andere am File-Server arbeiten.

15.10.3 Disk-I/O

Mit NetWare 3.2 werden der Anschluß von Platten an den File-Server über SCSI-Controller und die damit verbundenen Vorteile noch besser ausgenutzt. Ein SCSI-Disk-Driver (Small Computer Systems Interface) ist verantwortlich für den I/O mit den Festplatten. Auf früheren NetWare-Servern wurde eine Art Hand-Shake-Verfahren beim Platten-I/O durchgeführt, d.h., es wurde der Platte die I/O-Anforderung mitgeteilt. Daraufhin wartete der Driver-Prozeß, bis die Platte bereit war, die Anforderung zu erledigen. Anschließend wurde der I/O mit der Platte durchgeführt. Dieser Mechanismus wurde bei jedem Platten-I/O erneut durchgeführt. Es ist leicht einsichtig, daß diese Methode nicht unbedingt die schnellste ist, vor allem dann nicht, wenn man bedenkt, daß sich die SCSI-Driver-Spezifikation diesbezüglich wesentlich besser ausnutzen läßt.

Diese Disk-I/O-Methode ist deshalb ineffizient, weil der SCSI-Driver-Prozeß untätig bleibt und wartet, bis die Platte den Disk-I/O durchgeführt hat oder bis sie bereit ist, ihn durchzuführen. Da NetWare 3.2 den sogenannten SCSI-Disconnect-Mechanismus für neuere SCSI-Controller unterstützt, gibt es diesen Nachteil nicht mehr.

15 Novell NetWare 3.2

Durch die Unterstützung des SCSI-Disconnect-Mechanismus sendet der SCSI-Driver-Prozeß eine Nachricht zur Platte, daß Daten auf die Platte geschrieben oder von der Platte gelesen werden sollen. Ist die Platte zur Bearbeitung dieser Anforderung bereit, muß sie eine entsprechende Meldung an den SCSI-Driver-Prozeß zurückschicken, um ihm mitzuteilen, daß die Anforderung durchgeführt werden kann. Dies alles geschieht, bevor der SCSI-Driver-Prozeß mit dem I/O auf die Platte beginnt.

Der Vorteil von SCSI Disconnect ist, daß der SCSI-Driver-Prozeß nicht mehr warten muß, bis die Platte bereit ist, den Disk-I/O durchzuführen. Während auf die Ready-Meldung der einen Platte gewartet wird, kann der SCSI-Driver-Prozeß bereits an eine andere Platte die Meldung senden, daß auch hier I/Os durchzuführen sind, oder der SCSI-Driver-Prozeß kann den I/O auf einer anderen Platte durchführen.

Da das Lesen von und das Schreiben auf Platten über Disk-Driver erfolgt, kann der Server nur eine bestimmte Anzahl von Disk-I/Os pro Sekunde durchführen. Dieser Engpaß kann vermieden werden, wenn die Volumes über zwei, drei oder mehr Platten verteilt werden. Sind diese Platten auch noch an unterschiedlichen Platten-Controllern angeschlossen, ist ein zusätzlicher, verbesserter Durchsatz beim Lesen bzw. Schreiben zu verzeichnen.

Ist ein Volume über mehrere Platten verteilt, d.h., die Platte besteht aus mehreren Volume-Segmenten, dann füllt NetWare 3.2 beim Schreiben nicht zuerst das erste Segment des Volume und dann das nächste Segment und so weiter, sondern verteilt die Daten gleichmäßig über die einzelnen Volume-Segmente. Aufgrund dieser Technik ist die Wahrscheinlichkeit sehr groß, daß von den Anwendern im Netz Daten gelesen und geändert werden, die sich zwar auf dem gleichen Volume befinden, aber aufgrund der Aufteilung des Volume in Segmente auf unterschiedlichen Platten abgelegt sind.

Dieses Verfahren birgt allerdings auch eine gewisse Gefahr in sich, wenn man nicht besondere Sicherheitsmaßnahmen einsetzt. Da viele der Dateien eines Volume über mehrere Volume-Segmente verteilt und somit über mehrere Platten verteilt sein können, bedeutet der Ausfall einer Platte den Verlust dieser Dateien. In diesen Fällen gilt der Grundsatz:

Werden Volumes über mehrere Platten verteilt, sollten diese immer gespiegelt werden. Das bedeutet entweder den Einsatz von Disk Mirroring oder Disk Duplexing. Möglich machen das die SFT-II-Mechanismen von NetWare 3.2.

15.10 Festplatten- und Volume-Verwaltung

An dieser Stelle sei auch noch erwähnt, daß sich ein Volume im laufenden Betrieb zwar problemlos vergrößern läßt, aber ein Verkleinern des Volume, d.h. das Entfernen eines Volume-Segments, nicht möglich ist. Soll ein Volume verkleinert werden, kann das nur dadurch geschehen, daß man dieses Volume löscht und anschließend wieder neu anlegt. Dann darf die Datensicherung des Volume nicht vergessen werden, da sonst alle Daten des Volume verloren sind.

15.10.4 Disk Allocation Blocks

Wenn Sie Daten auf der Platte des File-Servers abspeichern, müssen diese organisatorisch so abgelegt werden, daß sie später auch wieder gefunden werden. Zum Wiederauffinden der Datei dient zum einen der Directory-Eintrag, zum anderen die Verknüpfung der Datei mit der File Allocation Table (FAT). Dieses Prinzip wird auch von MS-DOS verwendet. Nun ist es aber nicht so, daß Dateien sektorenweise auf der Platte abgelegt werden. Um die Effizienz des Speicherns und Lesens besser nutzen zu können, werden die Daten unter MS-DOS immer in Clustern abgelegt. NetWare speichert die Daten in Blöcken ab, wobei ein Block in der Regel 4 Kbyte groß ist.

Unter NetWare 3.2 können Sie beim Einrichten eines Volume festlegen, mit welcher Blockgröße dieses Volume arbeiten soll. Sie müssen zwischen 4-Kbyte-, 8-Kbyte-, 16-Kbyte-, 32-Kbyte- oder 64-Kbyte-Blocks wählen. Sie können dabei für jedes Volume eine andere Blockungsgröße verwenden. Die Disk Allocation Block Size legt die kleinste Einheit fest, mit der Daten auf dem Volume abgelegt werden.

Angenommen, Sie haben für ein Volume eine Blockungsgröße von 4 Kbyte gewählt. Wenn Sie eine Datei abspeichern, die von einem Byte bis 4095 Byte groß ist, belegt diese physikalisch auf der Platte einen Block von 4 Kbyte. Legen Sie eine Datei ab, die 4097 Byte bis 8010 Byte groß ist, dann belegt diese Datei physikalisch auf der Platte zwei 4-Kbyte-Blöcke.

Um ein Optimum an Effizienz zu erzielen, ist es sinnvoll, Volumes entsprechend der Verwendung zum Abspeichern von Daten mit unterschiedlichen Blockungsgrößen einzurichten. Sie müssen dabei abwägen, wie groß Ihre Dateien sind oder werden, die auf den Volumes abzulegen sind. Für große Dateien wählen Sie dann einen höheren Blockungsfaktor, für kleine Dateien benutzen Sie für das Volume einen kleineren Blockungsfaktor. Sie dürfen nicht vergessen, daß NetWare Datenbestände immer blockweise, in Abhängigkeit von der Disk Allocation Block Size, von der Platte liest.

Denken Sie aber auch daran, daß Sie beim Abspeichern einer 5 Kbyte großen Datei auf einem Volume mit einer Disk-Allocation-Block-Größe von 64 Kbyte auf dem Volume 59 Kbyte auf der Platte verschwenden, da die kleine Datei trotzdem einen ganzen Block auf der Platte belegt.

15.10.5 File Allocation Tables (FATs)

Auf jedem Volume befindet sich ein Abschnitt, der als File Allocation Table (FAT) bezeichnet wird. Für das Abspeichern und Wiederauffinden von Daten auf den File-Server-Platten verwendet Novell NetWare, genauso wie MS-DOS, eine FAT.

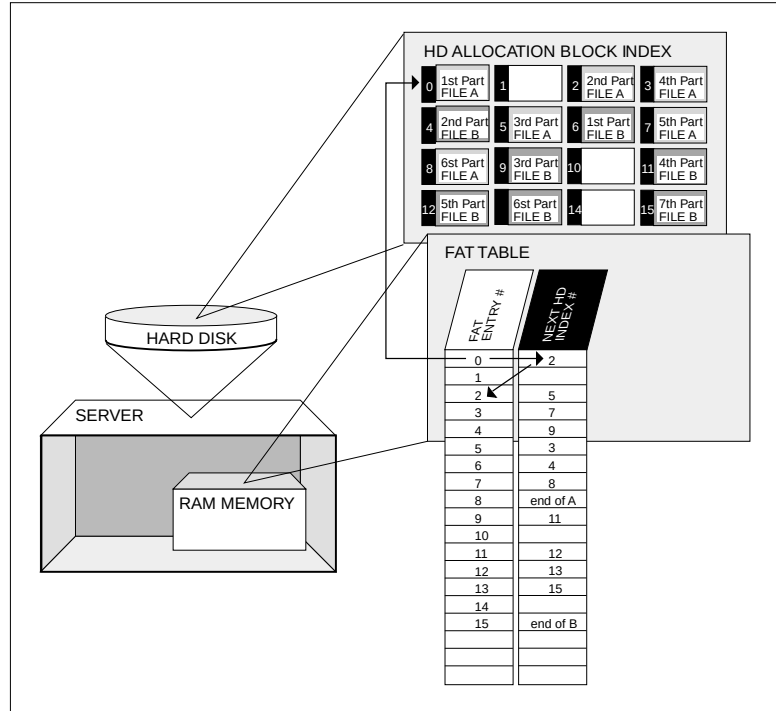
Die FAT ist eine einfach verknüpfte Liste von Pointern, die je nach definierter Disk Allocation Block Size auf Plattenbereiche von 4, 8, 16, 32 oder 64 Kbyte verweisen und den Daten einer bestimmten Datei entsprechen. Das Betriebssystem durchsucht diese Liste und findet so heraus, wo sich die angeforderten Daten auf der Platte befinden. Jede Datei hat ihre eigene FAT-Liste, die definiert, wo die Daten der Datei gespeichert sind. Soll zum Beispiel ein Datensatz einer Datei gelesen werden, der bei 20 Kbyte in der Datei beginnt, dann sucht das Betriebssystem in der FAT nach dem fünften Eintrag, und dieser Wert des fünften Eintrags ist dem entsprechenden Plattensektor zugeordnet. Der Datensatz kann jetzt gelesen werden.

Bei der FAT handelt es sich also um einen Index auf einem oder mehreren Disk Allocation Blocks, auf denen die Dateien abgespeichert werden. NetWare 3.2 liest die gesamte FAT eines Volume in den Hauptspeicher des File-Servers, wenn es das Mounten des Volume durchführt. Auf diese Weise kann NetWare die Dateien wesentlich schneller finden, weil der Zugriff auf die FAT auf der Platte beim Lesen einer Datei nicht durchgeführt werden muß – diese ist komplett im Hauptspeicher abgelegt. Änderungen der FAT, die im Hauptspeicher durchgeführt werden, schreibt NetWare sofort auf das Volume zurück. Über eine Verkettung der FAT-Einträge kann NetWare feststellen, auf welchen Blöcken die Datei auf dem Volume abgespeichert ist. In Abbildung 15.8 ist der Zusammenhang zwischen einer Datei und der FAT dargestellt.

Jeder FAT-Eintrag belegt im Hauptspeicher des File-Servers 8 Byte. Wenn Sie nun wissen wollen, wieviel Hauptspeicher Sie für die FAT benötigen, müssen Sie nur wissen, wie viele Blöcke ein Volume besitzt. Sie addieren anschließend die Anzahl Blöcke pro Volume und multiplizieren die Summe mit 8, dann erhalten Sie den Speicherbedarf für die FAT in Byte. Dividieren Sie diesen Wert durch 1024, und Sie haben die Menge der Kbyte. Eine zweite Division durch 1024 ergibt den Mbyte-Wert.

15.10 Festplatten- und Volume-Verwaltung

Abbildung 15.8
Prinzip der FAT-
Verarbeitung



Angenommen Sie haben ein Volume mit 300 Mbyte Kapazität, dann haben Sie auf diesem 76800 Blöcke bei einer Disk Allocation Block Size von 4 Kbyte. Dies ergibt $76800 \cdot 8 = 614400$ Byte bzw. 600 Kbyte Hauptspeicherbedarf zum Ablegen der FAT. Haben Sie 2 Volumes à 300 Mbyte, dann benötigen Sie in diesem Fall bereits fast 1,2 Mbyte Hauptspeicher für die FAT.

15.10.6 Turbo File Allocation Table (Turbo FAT)

Für einen rein sequentiellen Zugriff auf Dateien ist diese Organisation des Zugriffs auf die FAT sehr geeignet. Das Betriebssystem braucht die FAT nur der Reihe nach abzuarbeiten, um die Ein- und Ausgabeanforderungen zu erledigen. Der Speicherplatz des letzten FAT-Zugriffs wird gespeichert, damit nachfolgende Operationen an dieser Stelle wieder aufsetzen können und das sequentielle Lesen fortgesetzt werden kann.

Wesentlich ineffizienter ist diese Technik jedoch, wenn die Verarbeitung einer Datei nicht sequentiell, sondern im sogenannten »wahl-freien Zugriff« erfolgt, zum Beispiel Random Access in Reinstform für

15 Novell NetWare 3.2

Datenbankanwendungen. In den nächsten Beispielen wird davon ausgegangen, daß ein Blockungsfaktor von 4 Kbyte für das Datenvolumen verwendet worden ist.

Wurde zum Beispiel die letzte Anforderung für den Plattenbereich 100 durchgeführt (das entspricht 400 Kbyte weit in der Datei), und der nächste Satz, der gelesen werden soll, liegt auf Plattenbereich 1000, dann müßte das Betriebssystem 900 FAT-Einträge überlesen, bis der Plattenplatz für Block 1000 gelesen werden kann. Da sich das Betriebssystem den letzten Einsprung (100) merkt, müssen nur noch 900 Einträge gelesen werden. Gilt die nächste Anforderung für Block 900, müßte das Betriebssystem zum Anfang der FAT-Liste zurückspringen, um den Speicherplatz für Block 900 zu finden, der letzte Einsprung in unserem Beispiel ist ja 1000. Da es sich bei der FAT um eine einfach verkettete Liste handelt, die nur vorwärts durchsucht werden kann, läßt sich dies nicht anders lösen.

Diese Verarbeitungsweise zum Auffinden von Datenblöcken ist für ein Netzwerkbetriebssystem zu langsam. Die Zeit für das Durchsuchen eines Eintrags in der FAT dauert etwa fünf Mikrosekunden, da sich die FAT immer im Hauptspeicher befindet, sonst wäre es noch zeitraubender. Um 1000 Einträge zu durchsuchen, muß mit einer Verarbeitungszeit von ca. fünf Millisekunden gerechnet werden. Beträgt die Größe einer Datei 32 Mbyte, so belegt diese 8.192 FAT-Einträge. Ein Durchsuchen der gesamten FAT von Anfang bis Ende würde ca. 40 Mikrosekunden dauern. Bedenkt man dabei, daß das Lesen eines Cache-Speichers normalerweise weniger als eine Millisekunde dauert, ist es durchaus sinnvoll, die Zeit zum Durchsuchen der FAT bei großen Dateien zu optimieren.

Deshalb erlaubt es Novell NetWare, daß eine Datei als »*indexed*« gekennzeichnet wird (das erledigt NetWare 3.2/4.x nach bestimmten Regeln automatisch).

Wird eine Datei von mehreren Stationen geöffnet, so teilen sich diese denselben FAT-Index. Auch wenn alle Stationen diese Datei schließen, bleibt der FAT-Index im Hauptspeicher erhalten, bis die Anzahl gekennzeichneteter Dateien größer wird als die Anzahl konfigurierter FAT-Indizes. Wird eine Datei geöffnet und es existiert bereits eine Turbo FAT im Hauptspeicher des File-Servers, so wird diese benutzt, ohne daß eine neue Turbo FAT erstellt werden muß.

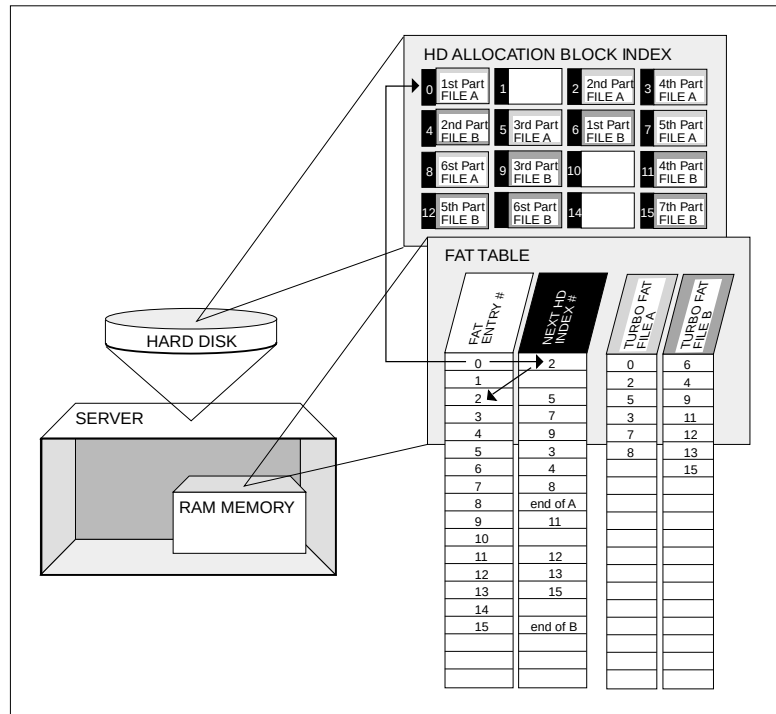
Beim Einsatz von NetWare 3.2 müssen Sie weder bei der Installation angeben, wie viele Turbo FATs angelegt werden sollen, noch Dateien mit dem Attribut *Indexed* versehen. Ich habe bereits alle Bereiche aufgezählt, für die NetWare das dynamische Memory Management einsetzt. In diesen Bereich fällt auch die Zuordnung der Turbo

15.10 Festplatten- und Volume-Verwaltung

FATs. NetWare 3.2 geht dabei so vor, daß für jede Datei, die mehr als 64 FAT-Einträge belegt, automatisch eine Turbo FAT eingerichtet wird.

Hat eine Datei mehr als 1024 FAT-Einträge, dann wird nicht mehr jeder FAT-Eintrag in die Turbo FAT übernommen. In Abbildung 15.9 ist das Prinzip der Turbo FATs dargestellt.

Abbildung 15.9
Einsatz der
Turbo FAT



15.10.7 Theoretische Hauptspeicher- und Plattenkapazität

Die gesamte Plattenkapazität, die unter NetWare 3.2 verwaltet werden kann, wird von drei Faktoren bestimmt:

- Größe eines FAT-Eintrags im Hauptspeicher (8 Byte)
- 4 Gbyte Hauptspeicher, die unter NetWare 3.2 verwaltet werden können
- Die größte erlaubte Disk Allocation Block Size (64 Kbyte)

Rein theoretisch können auf dem NetWare-3.2-File-Server bis zu 536.870.912 FAT-Einträge verwaltet werden. Dies ergibt sich aus der maximalen Hauptspeicherkapazität dividiert durch 8 Byte (pro FAT-Eintrag).

15 Novell NetWare 3.2

Mit jedem FAT-Eintrag kann ein Block mit 64 Kbyte auf der Platte adressiert werden, wenn Sie mit der maximalen Disk Allocation Block Size arbeiten. Wenn Sie die theoretische Anzahl von FAT-Einträgen, die im Hauptspeicher verwaltet werden können, mit 64 Kbyte Blockgröße multiplizieren, erhalten Sie die maximale Plattenkapazität von 32 Tbyte. Um auf diese Plattenkapazität zu kommen, müßten Sie ca. 220.000 Festplatten à 155 Mbyte Kapazität anschließen.

NetWare 3.2 unterstützt derzeit maximal 2048 Platten. Dies ergibt sich daraus, daß NetWare bis zu 64 Volumes verwalten kann, wobei jedes Volume über 32 Platten verteilt sein kann ($64 * 32 = 2048$).

15.10.8 Directory-Hashing in Kombination mit Directory-Caching

Die Festplattenlaufwerke eines File-Servers können unter Novell NetWare in mehrere Volumes aufgeteilt werden. Beim Zugriff auf Dateien werden nur Teile dieser Directory-Struktur in den Hauptspeicher des Servers geladen.

Der Zugriff auf eine Datei des entsprechenden Volume erfolgt dann nur noch über die Directory Entry Table, die sich im Hauptspeicher des File-Servers befindet, und nicht mehr über das Volume. Nur Änderungen innerhalb des Directory werden auf die Platte zurückgeschrieben. Directory-Blöcke, die sich im Hauptspeicher befinden, werden bei Bedarf wieder freigegeben und durch neue Blöcke überschrieben. Ein einmal angelegter Directory-Cache-Block wird nicht mehr an den File-Cache-Buffer zurückgegeben.

Zusätzlich zum Caching-Verfahren verwendet NetWare zwei verschiedene Arten von Hashing-Tabellen, um den Zugriff auf die Verzeichnisse und die Dateien innerhalb der Verzeichnisse zu optimieren. Ein rein sequentielles Durchlesen der Directory-Struktur zum Auffinden einer Datei, die gelesen werden soll, wie es zum Beispiel unter MS-DOS der Fall ist, wäre für den File-Server viel zu langsam. Wie bereits erwähnt, wird das Directory-Caching bei der Initialisierung des Servers individuell für jedes Volume durchgeführt. Im Gegensatz dazu erfolgt das Directory-Hashing auf zweierlei Arten.

Die erste Möglichkeit ist die Verwendung eines Hash-Algorithmus, um die Verzeichnisstrukturen eines jeden Verzeichnisbereichs zu indizieren; die zweite Möglichkeit ist die Verwendung eines Hash-Algorithmus, um die Dateien nach Verzeichnisbereichen und Unterverzeichnissen zu indizieren. Dieser Algorithmus ist leistungsfähiger, wenn nach Dateinamen mit Globalzeichen gesucht wird.

15.10 Festplatten- und Volume-Verwaltung

Abbildung 15.10
Das Prinzip des
Directory-Caching

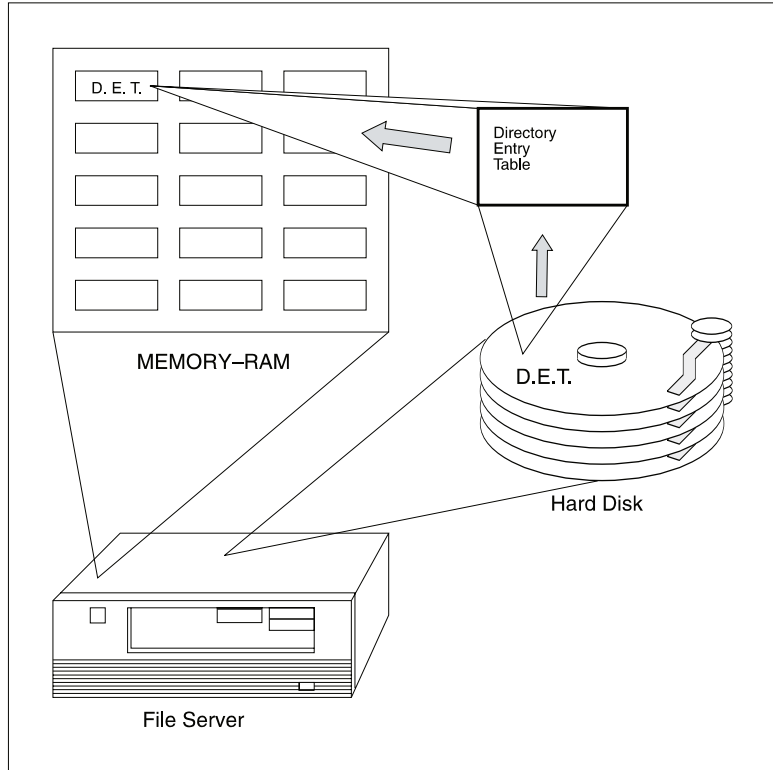
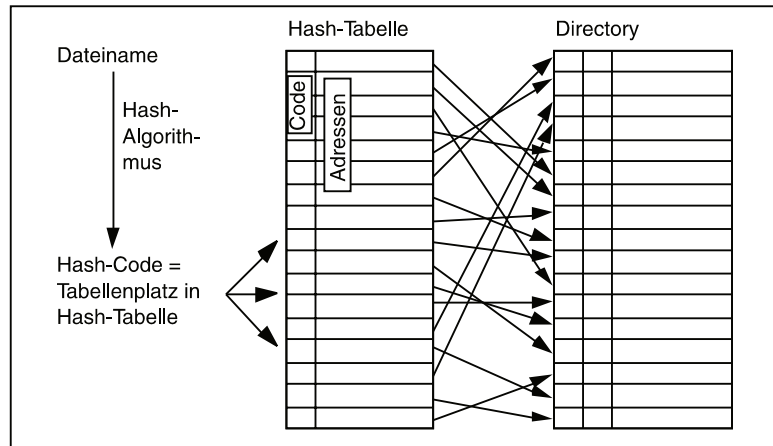


Abbildung 15.11
Das Prinzip des
Directory-Hashing



15 Novell NetWare 3.2

Das Directory-Caching macht physikalische Plattenzugriffe überflüssig, wenn Dateien im Directory gesucht werden, also gelesen werden sollen. Die beiden Directory-Hashing-Algorithmen optimieren zusätzlich den Plattenkanal, indem die Anzahl der Zugriffe auf ein Verzeichnis reduziert wird, wenn eine Datei im Verzeichnis gefunden werden soll. In Abbildung 15.10 und Abbildung 15.11 ist die Wirkungsweise von Directory-Caching bzw. Directory-Hashing aufgezeigt.

15.10.9 File-Caching unter NetWare 3.2

Ein weiterer Mechanismus, den NetWare zur Leistungssteigerung verwendet, ist das Prinzip des File-Caching. File-Caching beschreibt das Verfahren zum Speichern von Daten im Hauptspeicher des File-Servers. Caching ist ein wesentlicher Bestandteil von NetWare, da die Leistung des File-Servers dadurch entscheidend verbessert wird. Der Plattenprozeß von NetWare ist so programmiert, daß immer ganze x-Kbyte-Blöcke von der File-Server-Platte (in Abhängigkeit von der Disk Block Size) gelesen werden. Eine Benutzeranforderung dagegen ist vielleicht nur 1 Kbyte oder 2 Kbyte groß. Bei einer ankommenden Leseanforderung wird also immer ein 4-Kbyte-Plattenblock eingelesen. Bevor die Anforderung, d.h. der Datensatz, an den Benutzer weitergereicht wird, führt NetWare ein Caching des gesamten Plattenblocks durch. Damit werden mehr Daten in den Hauptspeicher gelesen als angefordert. Nach der LRU-Strategie (Least Recently Used) wird der Hauptspeicherbereich mit einem neuen Cache-Block überschrieben, der die längste Zeit nicht mehr benutzt worden ist, falls der Hauptspeicher für den Cache-Mechanismus bereits voll ist.

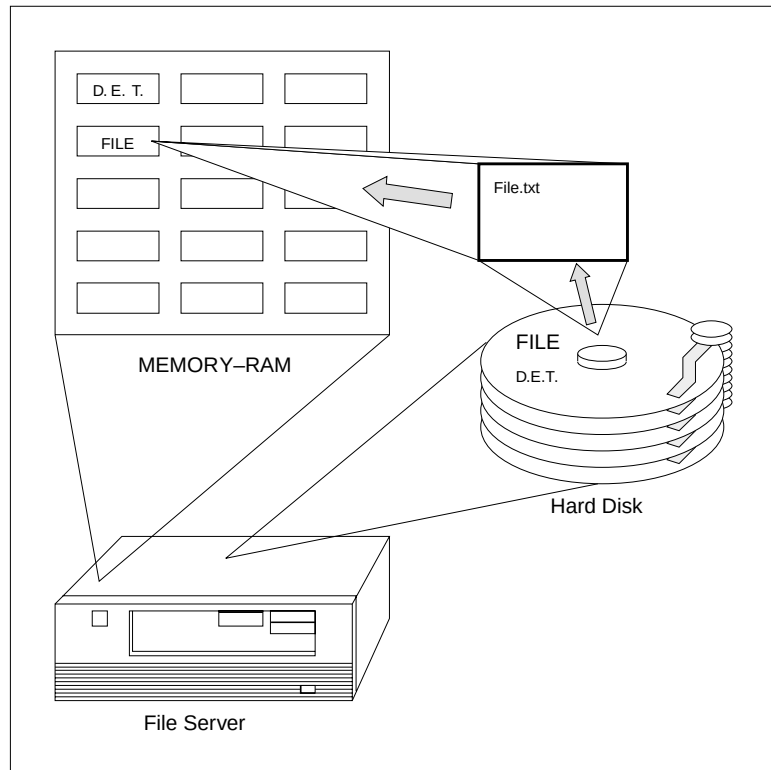
Das Prinzip des File-Caching verbessert die Leistung des File-Servers entscheidend. Die Übertragung von großen Datenmengen wird schneller, da die Festplatte in ganzen Abschnitten gelesen wird. Kleine sequentielle Anforderungen werden schneller, da Zugriffe auf den Hauptspeicher schneller sind als Plattenzugriffe.

Auch beim Schreiben von Daten wird das Caching verwendet. Trifft die Schreiboperation eines Benutzers beim File-Server ein, werden die Daten in den Cache-Speicher geschrieben, und es wird bereits eine positive Quittierung zurück an den Benutzer übertragen. Dadurch ist es möglich, daß der File-Server zusätzlich optimiert wird. Kleine Schreib Anforderungen werden zu größeren zusammengefaßt, bevor sie physisch auf die Platte zurückgeschrieben werden. Der Benutzer muß somit nicht warten, bis die Daten physisch auf der Platte stehen, sondern nur so lange, bis sie beim File-Server angekommen sind. Der File-Server koordiniert dann die Schreibzugriffe auf die Platte, ohne damit die Leistung der Station zu beeinflussen.

15.10 Festplatten- und Volume-Verwaltung

Da alle bisherigen Methoden im Hauptspeicher des File-Servers ablaufen, um Geschwindigkeitsvorteile zu erzielen, ist es unabdingbar, den File-Server mit soviel Hauptspeicher wie möglich auszustatten. Dann können die gesamten Mechanismen optimal genutzt werden. In Abbildung 15.12 ist das Prinzip des File-Caching aufgezeigt.

Abbildung 15.12
Die Arbeitsweise
des File-Caching



15.10.10 Optimierung der Plattenzugriffe durch Elevator-Seeking

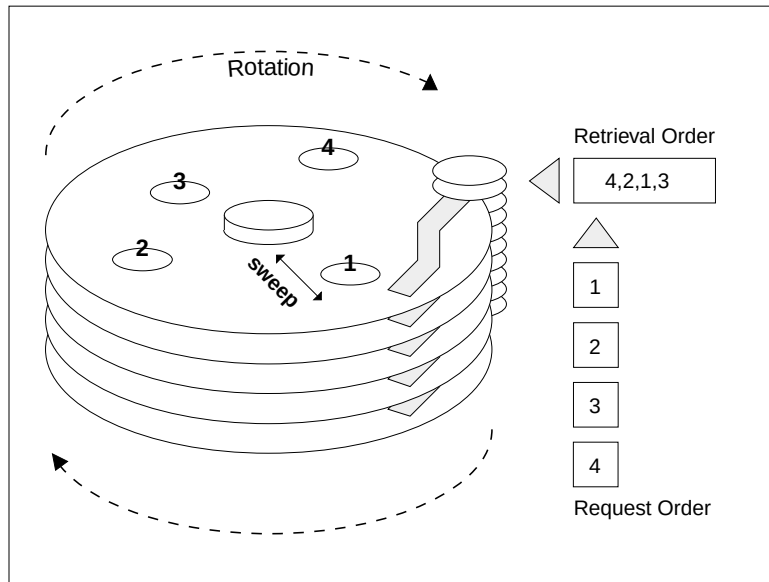
Die Verwendung dieser Methode für Zugriffe auf die Plattenlaufwerke des Servers stellt eine hochmoderne Technik dar, die es bisher bei keinem anderen File-Server-System gibt. Das Lesen von Dateien wird durch dieses Prinzip optimal organisiert. In Abbildung 15.13 ist die Funktionsweise dieses Mechanismus aufgeführt.

Gemeinsam genutzte Platten und der dazugehörige Kanal können durch die vermehrten und stark voneinander abweichenden Anforderungen und Operationen innerhalb eines LAN sehr schnell überlastet sein. Durch das Elevator-Seeking wird ein Auftreten solcher

15 Novell NetWare 3.2

Überlastungen vermieden, da die Plattenoperationen in eine logische Ordnung gebracht werden, bevor sie als Lese- oder Schreiboperation vom Server ausgeführt werden.

Abbildung 15.13
Der Mechanismus
des Elevator-
Seeking



Der Elevator-Seeking-Algorithmus optimiert durch den Einsatz einer heuristischen Prozedur den Zugriff auf die Festplatten des File-Servers. Für den Plattentreiber innerhalb des File-Servers wird eine Warteschlange gepflegt. Die Lese- und Schreiboperationen, die in die Warteschlange eines bestimmten Laufwerks eingereiht werden, werden vom Betriebssystem so geordnet, daß der Plattenkanal nicht unnötig belastet wird.

Der Plattentreiber bedient die Warteschlange so, daß nachfolgende Anforderungen entweder vor oder hinter die letzte Anforderung eingefügt werden. Der Schreib-/Lesekopf der Platte bewegt sich deshalb in Schwingbewegungen von einem Ende der Platte zum anderen. Die Suchzeiten auf der Platte werden dadurch reduziert, und die Belastung des Laufwerks wird durch unnötige Positionierungen der Köpfe vermieden. Das Elevator-Seeking ist vergleichbar mit der Funktionsweise eines Aufzugs, daher auch die Bezeichnung (elevator=Aufzug). Wenn in einem Hochhaus der Aufzug zuerst im 5. Stock, dann im 3. Stock und anschließend im 2. Stock angefordert wird, dann fährt der Aufzug auch nicht in der Reihenfolge der Anforderung die einzelnen Etagen ab, sondern bleibt beim Auf- und Abfahren auf den entsprechenden Stockwerken stehen.

15.10.11 Einsatz von mehreren Plattenkanälen

Die meisten PC-Entwürfe sind so ausgelegt, daß sie nur einen Plattenkanal verwenden. Schreib- und Leseoperationen werden nur über diesen einen Kanal ausgeführt. Novell hat deshalb zusätzliche Hardware entworfen, die es erlaubt, noch bis zu vier weitere Plattenkanäle im File-Server zu verwenden, da Zugriffe auf die Platte die Hauptfunktion des File-Servers ist. Mit dem Einsatz des internen ATA-Platten-Controllers (bzw. IDE, EIDE oder SCSI) stehen somit insgesamt fünf Plattenkanäle zur Verfügung.

Novell NetWare kann dafür, wie oben gesehen, mit unterschiedlichen Platten-Controllern installiert werden. Man geht jedoch immer mehr dazu über, die leistungsfähigen SCSI-Karten einzusetzen. Arbeiten zum Beispiel zwei verschiedene Abteilungen mit einem gemeinsamen File-Server, wäre es sinnvoll, die beiden Datenbereiche dieser Abteilungen auf getrennten Platten zu speichern und jede Platte an einem SCSI-Board anzuschließen. Da beide Plattenkanäle unabhängig voneinander sind und parallel arbeiten können, kann der Durchsatz hierfür verdoppelt werden. Bei der Behandlung der Sicherheitsmechanismen unter Novell NetWare werden wir noch genauer auf diese Variante zu sprechen kommen.

15.11 Dateien und Directories unter NetWare 3.2

Dateien werden auf den Volumes des File-Servers abgelegt. Wie unter MS-DOS unterteilt man diese meist in Directories, um auch eine sinnvolle Directory-Struktur auf den Volumes zu erzielen. Die Möglichkeiten, die Ihnen dazu von NetWare 3.2 geboten werden, unterscheiden sich sowohl von MS-DOS als auch von anderen Betriebssystemen. Die zur Verfügung stehenden Funktionen und Möglichkeiten beziehen sich auf die Bereiche:

- Directory-Tabellen
- Multiple Name Space Support
- Sparse Files
- Salvageable Dateien (wiederherstellbare Dateien)

15.11.1 Directory-Tabellen

Auf jedem Volume befindet sich ein Bereich, in dem Directory-Einträge, d.h. Dateien und Subdirectories, gespeichert werden. Die Directory-Einträge belegen dabei mehrere Blöcke auf dem Volume. Unabhängig von der gewählten Disk Allocation Block Size für das

15 Novell NetWare 3.2

Volume werden die Directory-Blöcke immer in 4-Kbyte-Blockgrößen angelegt. NetWare 3.2 reserviert sich zuerst einen kleinen Bereich von Blöcken für die Directory-Einträge. Wenn NetWare einen neuen Directory-Block benötigt, wird dieser auf dem Volume einfach angelegt. Ein einmal angelegter Directory-Block wird nicht mehr freigegeben. Das heißt, wenn Sie für die bestehenden Directory-Einträge z.B. zehn Blöcke auf dem Volume belegt haben und alle Dateien von diesem Volume löschen, bleiben diese Directory-Blöcke erhalten. In einem 4-Kbyte-Directory-Block können 32 Einträge mit je 128 Byte Länge angelegt werden.

Auf einem Volume können jedoch nicht beliebig viele Directory-Blöcke eingerichtet werden. Die maximale Anzahl Directory-Einträge pro Volume ist auf 2.097.152 beschränkt, da auf einem Volume nicht mehr als 65.536 Directory-Blöcke à 32 Einträge angelegt werden können.

In einem Directory-Block können die unterschiedlichsten Arten von Einträgen stehen:

- Dateieinträge für unterschiedliche Workstation-Betriebssysteme
- Directory-Einträge für unterschiedliche Workstation-Betriebssysteme
- Datei-Trustee-Einträge
- Directory-Trustee-Einträge
- Freie Einträge

In jedem Eintrag werden Informationen über Dateien, Directories, Datei-Trustees, Directory-Trustees etc. abgelegt. Das Volume SYS wird zu Beginn mit sechs Directory-Blöcken angelegt. Jedes andere Volume wird mit zwei Directory-Blöcken eingerichtet. Wenn auf dem Volume während des Betriebs zusätzliche Directory-Blöcke benötigt werden, legt NetWare diese dynamisch auf dem Volume an.

15.11.2 Multiple Name Space Support

Es wurde bereits mehrfach erwähnt, daß NetWare 3.2 speziell für den Bereich des Network Computing entwickelt worden ist. Da ein solches Netzwerkbetriebssystem die Möglichkeit bieten muß, unterschiedliche Workstations und Workstation-Betriebssysteme einzubinden, sind damit natürlich auch gewisse zusätzliche Forderungen zu erfüllen.

Jedes Workstation-Betriebssystem zeichnet sich durch andere Funktionalitäten und Dateikonventionen aus. Wenn Sie zum Beispiel mit MS-DOS arbeiten, dürfen Ihre Datei- und Directory-Namen nur aus acht Stellen bestehen und die Extension aus drei Stellen. Arbeiten Sie hingegen mit einem Apple-Macintosh-Betriebssystem oder Unix,

15.11 Dateien und Directories unter NetWare 3.2

können die Dateinamen bis zu 32 Stellen haben, unter OS/2 mit High-Performance-File-System sind 255 Stellen für den Dateinamen erlaubt. Windows NT und Windows 95/98 unterstützen ebenfalls 255-stellige Verzeichnis- und Dateinamen.

NetWare 3.2 unterstützt bei der Einbindung unterschiedlicher Arbeitsplatzrechner und deren Betriebssysteme diese im sogenannten Native Mode, d.h., der File-Server unterstützt Dateikonventionen und Dateiformat so, wie es Ihnen vom Workstation-Betriebssystem angeboten wird. Man muß sich also nicht auf einen gemeinsamen Nenner für Dateiformat und Dateikonvention einigen, vielmehr steht der File-Server jedes unterstützten Workstation-Betriebssystems in seinem vollen Leistungsumfang zur Verfügung.

Dies wird durch die Einführung des Multiple Name Space Support erreicht und realisiert. Wenn Sie unter MS-DOS eine Datei am File-Server abspeichern, wird hierfür ein Dateiname vergeben. Dieser Dateiname belegt einen Directory-Eintrag in der Directory-Tabelle des File-Servers. In diesem Directory-Eintrag werden neben dem Dateinamen auch noch die Länge des Dateinamens (1 Byte), Dateiattribute, der Eigentümer, Erstellungsdatum und -uhrzeit und die Verbindung zur Datei-Trustee-Liste abgelegt.

Die Dateikonventionen einzelner Workstation-Betriebssysteme können sich hinsichtlich der Länge des Dateinamens, erlaubter Zeichen im Dateinamen, Data und Resource Fork etc. unterscheiden. Damit all diese Unterschiede am File-Server unterstützt werden, muß für das entsprechende Workstation-Betriebssystem ein Name Space Module am File-Server geladen werden. Dies ist jedoch nur unter NetWare 3.2 und NetWare 4.x möglich.

Multiple-Name-Space-Unterstützung bedeutet das Vorhandensein mehrerer Dateieinträge. Ist Ihr File-Server zum Beispiel so eingerichtet, daß sowohl DOS- als auch Macintosh-Name-Space-Unterstützung für ein Volume festgelegt ist, dann werden für jede Datei, die Sie am File-Server ablegen, zwei 128-Byte-Datei-Einträge generiert. In einem Dateieintrag sind die Dateiattribute, Eigentümer, Erstellungszeit und -datum, DOS-Dateiname etc. abgelegt. Im anderen Dateieintrag werden der Macintosh-Dateiname und die Macintosh-Finder-Information abgelegt. Unterstützt ein File-Server Multiple Name Space, dann wird für jede Datei ein Datei-/Directory-Eintrag für jeden unterstützten Name Space Support eingerichtet.

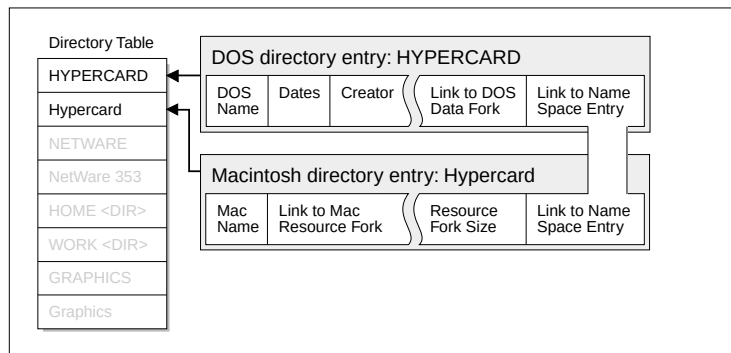
Beim Anlegen von Directory-Namen wird genauso verfahren. Die Unterstützung der DOS-, OS/2-, Windows-95- und Windows-NT-Konvention ist standardmäßig im Netzwerkbetriebssystem enthalten, d.h., hierfür muß kein separater Name Space geladen werden. Zu

15 Novell NetWare 3.2

beachten ist dabei, daß der Name Space Support für jedes Volume einzeln festgelegt wird, d.h., es können Volumes installiert sein, für die Sie unterschiedliche Name-Space-Unterstützung festgelegt haben. In Abbildung 15.14 ist die Aufteilung der Directory-Tabellen beim Einsatz von Multiple Name Space dargestellt.

Wenn Sie für ein Volume einen zusätzlichen Name Space Support festgelegt haben, benötigt der File-Server den doppelten, dreifachen etc. Hauptspeicherplatz, um die Directory-Einträge ablegen zu können, je nachdem, ob Sie zwei, drei etc. Name-Space-Support-Module geladen haben.

Abbildung 15.14
Name Space
Support unter
NetWare 3.2



NetWare 3.2 unterstützt auch sogenannte Multiple-Byte Characters für Dateien, Directories und Bindery-Einträge. Dies ist notwendig, weil es Workstation-Betriebssysteme gibt, die zwei Byte benötigen, um ein Zeichen darstellen zu können. Da NetWare 3.2 eine maximale Dateigröße von 4 Gbyte unterstützt und sich Volumes über mehrere Platten erstrecken können, ist es auch möglich, daß sich Dateien über mehrere Platten erstrecken (Spanned Files).

15.12 Sparse Files

Unter NetWare 3.2 werden auch sogenannte Sparse Files unterstützt. Solche Dateien werden sehr oft von Datenbanksystemen erzeugt. Wie Sie bereits wissen, werden Dateien auf der Platte des File-Servers immer blockweise abgespeichert. Unter einem Sparse File versteht man eine Datei, bei der mindestens ein Block leer ist; dieser Block enthält also noch keine Informationen. NetWare 3.2 schreibt den Block nicht mehr auf die Platte, wenn er leer ist. Befindet sich im Block auch nur ein Byte Information, wird er auf die Platte geschrieben.

15.13 Salvageable Dateien (wiederherstellbare Dateien)

Folgendes Beispiel macht Ihnen das Prinzip verständlicher:

Angenommen, Sie legen auf dem Volume DATEN, das mit einer Disk Allocation Block Size von 4 Kbyte eingerichtet worden ist, Ihre Datenbankdateien ab. Außerdem gehen wir davon aus, daß von der Datenbank eine neue Datei geöffnet wird, auf die Byte-Stelle 1.048.576 in der Datei 5-Byte-Daten geschrieben werden sollen und anschließend die Datei wieder geschlossen wird. Ein nicht optimal arbeitender Server würde in diesem Fall die gesamte Datei auf dem File-Server abspeichern (d.h. 256 Blöcke, die mit Null gefüllt sind – das erste Mbyte – und anschließend einen weiteren Block mit 5-Byte-Daten und 4091 Nullen).

Auf diese Weise verschwenden Sie auf der Platte 1 Mbyte der Plattenkapazität. NetWare 3.2 schreibt das erste Megabyte, gefüllt mit Nullen, nicht auf die Platte des File-Servers. NetWare 3.2 schreibt nur den letzten Block auf die Platte. Versucht nun das Datenbanksystem, Informationen vom ersten Megabyte der Platte zu lesen, dann werden vom Server Nullen generiert und an das Datenbankprogramm zurückgegeben.

15.13 Salvageable Dateien (wiederherstellbare Dateien)

Wem ist das noch nicht passiert? Sie arbeiten auf Ihrem PC und wollen Dateien löschen. In der Annahme, daß Sie sich im richtigen Directory befinden, geben Sie den Befehl `DEL *.*` ein. Auf die Anfrage von MS-DOS, ob auch wirklich alle Dateien gelöscht werden sollen, antworten Sie selbstbewußt mit Yes. Kaum haben Sie bestätigt, ist es auch schon passiert. Sie stellen fest, daß Sie sich im falschen Directory befunden und soeben die verkehrten Dateien gelöscht haben. In diesem Fall müssen Sie unter MS-DOS auf Utilities wie NORTON oder PC-TOOLS zurückgreifen, um alle gelöschten Dateien restaurieren zu können.

Die Möglichkeit des Wiederherstellens von gelöschten Dateien wird von NetWare 3.2 in einer sehr komfortablen Art und Weise angeboten.

Unter NetWare 3.2, NetWare 4.x und NetWare 5 werden alle gelöschten Dateien in ihrem ursprünglichen Directory erhalten. Erst wenn auf dem Volume kein Platz mehr vorhanden ist, wird begonnen, die bereits am längsten gelöschten Dateien zu überschreiben. Der Benutzer kann aber auch jederzeit bestimmen, daß wiederherstellbare Dateien vollständig von der Platte entfernt werden sollen. Man

15 Novell NetWare 3.2

spricht in diesem Fall davon, daß ein PURGE auf die Datei durchgeführt wird. Was passiert jedoch, wenn Sie ein komplettes Directory von der Platte löschen? Wie oben beschrieben, werden gelöschte Dateien im ursprünglichen Directory aufbewahrt.

Wenn Sie komplette Directories löschen, werden alle Dateien des Directory in einem hierfür speziell eingerichteten Directory angelegt. Das heißt, alle gelöschten Dateien von gelöschten Directories werden im DELETED.SAV-Directory abgelegt. Dieses spezielle Directory befindet sich automatisch auf jedem Volume. Solange wiederherstellbare Dateien nicht explizit durch PURGE oder durch Überschreiben der gelöschten Datei von der Platte entfernt werden (weil die Platte voll ist), können sie jederzeit restauriert werden.

Neben allen anderen notwendigen Informationen für diese gelöschte Datei wird zusätzlich ausgewiesen, wann und von wem die Datei gelöscht worden ist. Das Wiederherstellen von gelöschten Dateien wird durch das SALVAGE-Menüsystem durchgeführt. Für den Fall, daß Sie eine Datei restaurieren wollen, deren Dateiname inzwischen bereits für eine neue Datei in diesem Directory verwendet worden ist, fragt das SALVAGE-Menüsystem nach, unter welchem Namen die Datei restauriert werden soll.

Mit dem SALVAGE-Menüsystem können Sie auf einer oder auf mehreren Dateien einen PURGE durchführen. Soll es für Dateien nach dem Löschen unmöglich gemacht werden, sie wiederherzustellen, haben Sie hierfür drei Möglichkeiten.

1. Sie vergeben für die Datei das Attribut PURGE. Damit legen Sie fest, daß diese Datei nach dem Löschen sofort von der Platte entfernt wird, also nicht mehr wiederherstellbar ist.
2. Sie vergeben für das Directory das Attribut PURGE. Hiermit legen Sie fest, daß jede Datei in diesem Directory nach dem Löschen nicht mehr wiederhergestellt werden kann.
3. Sie setzen am File-Server den Parameter *Immediate Purge of Deleted Files=ON*. Hiermit wird für jede gelöschte Datei ein PURGE durchgeführt, wenn diese auf der Platte des File-Servers gelöscht wird. Damit erhöhen Sie zwar auch die Performance des File-Servers, aber mit dem Nachteil, daß Sie über die Funktion zum Wiederherstellen von gelöschten Dateien nicht mehr verfügen. Wenn Sie diesen Parameter verwenden, gilt der Mechanismus für alle Volumes des File-Servers, d.h., er kann nicht auf ein bestimmtes Volume beschränkt werden.

15.14 **Datensicherheit unter Novell NetWare 3.2**

Die Datensicherheit eines Netzwerks muß zwei Seiten abdecken. Zum einen geht es unmittelbar um die Sicherheit der Daten, d.h., es müssen Mechanismen vorhanden sein, die es unterbinden, daß jemand das Netz benutzen kann, der gar nicht berechtigt ist, und daß jeder die Daten des anderen einsehen kann. Zum anderen geht es um die Hardware-Sicherheit: Was kann getan werden, damit das System vor Ausfällen geschützt ist?

In diesem Abschnitt werden wir uns mit dem ersten Problem beschäftigen; der nächste Abschnitt wird dann die Methoden aufzeigen, die Novell bietet, um das Netz vor Ausfällen zu sichern. Die Daten- und Ressourcensicherheit gewinnt bei der Vernetzung immer mehr an Bedeutung. Diese Probleme sind bei den Großrechnersystemen schon seit langem gelöst. Im PC-Bereich liegt dieser Bereich eher noch brach. Im PC-LAN-Bereich bietet Novell hierfür hervorragende Lösungen an.

Novell NetWare stellt Entwicklern und Systemverwaltern eine Reihe leistungsstarker Sicherheitsmechanismen zur Verfügung, wenn Datensicherheit im LAN gefordert wird. Eine zentrale Sicherheitseinrichtung steuert ein System von alternativen Sicherheitseinrichtungen, das aus folgenden Punkten besteht:

- Sicherheit auf Abrechnungsebene
- Sicherheit auf Paßwortebene
- Sicherheit auf Verzeichnisebene
- Sicherheit auf Dateiebene
- Sicherheit auf Internet-Ebene

Dem Verantwortlichen stehen eine Reihe von Utilities zur Verfügung, mit deren Hilfe die oben genannten Sicherheitsmechanismen aktiviert und definiert werden können. Inwieweit die einzelnen Methoden verwendet und umgesetzt werden, obliegt dem Systemverantwortlichen.

Mit Hilfe des ausgereiften Sicherheitssystems von NetWare 3.2 wird festgelegt,

- wer am File-Server arbeiten darf,
- welche Ressourcen der Benutzer am File-Server verwenden darf (Directories, Dateien, Print-Queues etc.),
- was der Benutzer mit diesen Ressourcen machen darf (z. B. nur lesen, lesen und schreiben, ändern etc.) und
- wer Programme (Tasks) am File-Server starten darf.

Das zentrale Sicherheitsmedium für die Realisierung dieser Mechanismen wird durch die Bindery, dem zentralen Sicherheitssystem von NetWare 3.2, aufrechterhalten.

15.14.1 Die Bindery – zentrale Sicherheitseinrichtung

Bei der Bindery handelt es sich um eine Datenbank, mit der alle notwendigen Sicherheitsbereiche des File-Servers überwacht und gesteuert werden. In der Bindery werden Informationen über die Ressourcen, wie zum Beispiel File-Server, Print-Server, Datenbank-Server, abgelegt, und zwar zusammen mit den Angaben, welche Benutzer mit welchen Berechtigungen auf diese Ressourcen Zugriff haben. Wenn zum Beispiel ein Print-Server die Dienste für ein gesamtes Internetwork als Ressource zur Verfügung stellt, dann wird dieser Print-Server mit einem Namen und einer Internetwork-Adresse in der Bindery eines jeden File-Servers in diesem Internetwork verwaltet. Die Bindery kann als Resource Directory betrachtet werden, von dem sich die Benutzer (Clients) eine Auflistung aller Ressourcen, die im Netzwerk zur Verfügung stehen, ausgeben lassen können.

In der Bindery werden zudem für jeden Benutzer alle Informationen abgespeichert, die als Basis zum Aufbau der Login-Sicherheit unter NetWare 3.2 notwendig sind. Dies betrifft unter anderem den Paßwortschutz, Accounting des Benutzers, Benutzerrestriktionen, Trustee-Rechte etc. Ich werde Ihnen das Prinzip und die Arbeitsweise der Bindery in drei Abschnitten erklären:

- Bindery-Dateien
- Bindery-Komponenten
- Bindery-Sicherheit

Bindery-Dateien

Die Bindery unter NetWare 3.2 teilt sich in drei Dateien auf. Diese drei Bindery-Dateien werden auf dem NetWare-System-Volumen SYS:SYSTEM abgelegt und gepflegt. Diese können von Benutzern nicht gelöscht oder kopiert werden – nicht einmal vom Supervisor.

Eine Modifikation der Bindery ist nur durch entsprechende NetWare-Utilities möglich und erlaubt. Es handelt sich hierbei um die Dateien:

- NET\$OBJ.SYS Verwalten der Bindery-Objekte
- NET\$PROP.SYS Verwalten der Bindery-Properties
- NET\$VAL.SYS Verwalten der Bindery-Data-Sets

In der Bindery können bis zu 16.777.216 Objekte und 16.777.216 Properties gespeichert und verwaltet werden. Ein Bindery-Objektname kann bis zu 48 Byte lang sein, ein Byte-Längengeld, gefolgt von

15.14 Datensicherheit unter Novell NetWare 3.2

1 bis 47 Byte für den Objektnamen. Wie bereits für Dateien und Directories besprochen, unterstützt die Bindery unter NetWare 3.2 auch Multiple-Byte-Characters.

Komponenten der Bindery

Die Bindery setzt sich aus Objekten und Properties zusammen. Ein Objekt kann ein Benutzer, eine Benutzergruppe, ein File-Server, ein Print-Server oder jedes andere logische oder physikalische Objekt in einem Netzwerk sein, dem ein Name gegeben wird. Jedem Objekt werden sogenannte Properties zugewiesen, wobei jedes Property einen Property-Wert besitzt.

Property-Werte wiederum werden in zwei Bereiche aufgeteilt: SET Properties oder ITEM Properties. Ein Property SET besitzt eine Liste oder ein Set von Objekt-IDs, die als Property-Wert eingetragen sind.

Ein Property ITEM hingegen besitzt einen Property-Wert, der wiederum jeden beliebigen Datenwert besitzen kann. Typischerweise handelt es sich dabei um numerische Werte, einen String oder eine Struktur. Jedem Objekt können mehrere Properties zugewiesen werden. Zum Beispiel kann dem Objekt-Benutzer als Property ein Paßwort, eine Account-Balance oder eine Liste von Gruppen zugewiesen werden, in denen der Benutzer Mitglied ist. Ein Server hingegen wird nur ein Property haben; es handelt sich dabei um die Netzwerkadresse.

Der Property-Wert enthält den momentan aktuellen Wert, der diesem Property zugewiesen ist. Das Paßwort eines Benutzers wird zum Beispiel im Property-Wert abgelegt, der für das Property-Paßwort vergeben worden ist. Obwohl ein Property nur einen Wert haben kann, kann dieser Wert mehrere Segmente enthalten, wobei jedes Segment 128 Byte groß sein kann.

Bindery-Sicherheit

Die Sicherheitsmaßnahmen des File-Servers werden unter NetWare von der Bindery abgedeckt. Streng genommen sind die Sicherheitsvorkehrungen der Bindery und die Dateisystemsicherheit unabhängig voneinander. In der Bindery werden keinerlei Trustee-Informationen gespeichert (Datei- und Directory-Trustee-Rechte). Alle Directory- und Datei-Trustee-Informationen werden im Directory-Eintrag abgespeichert. Der einzige Zusammenhang zwischen der Bindery und dem Dateisystem besteht darin, daß im Dateisystem alle Informationen von Directory- und Datei-Trustee-Rechten mit Hilfe der Objekt-ID abgespeichert sind. Wird also einem Benutzer ein Tru-

15 Novell NetWare 3.2

stee-Recht für ein Directory zugewiesen, dann legt NetWare für dieses Directory in einem weiteren Directory-Eintrag die User-Objekt-ID und die dazugehörigen Rechte ab.

Die Bindery stellt eine flexible, aber sichere Betriebssystemumgebung durch eine Vielzahl von Sicherheitsmechanismen zur Verfügung. Es handelt sich dabei um:

- Security Access Levels (Sicherheitsstufen)
- Privileges
- Encrypted Passwords

Sicherheitsstufen

Jedem Objekt und jedem Property in der Bindery wird eine Sicherheitsstufe zugewiesen, welche den Lese- und Schreibzugriff auf ein Bindery-Objekt und deren Properties überwacht. Die Objekt-Sicherheit und die Property-Sicherheit werden in zwei Halbbytes festgelegt. Das niederwertige Halbbyte steuert die Sicherheit für das Lesen und das höherwertige Halbbyte die Sicherheit für das Schreiben. Für jedes Halbbyte werden folgende Werte benutzt.

Hex	Binär	Zugriff	Beschreibung
0	0000	Anyone	Der Zugriff wird allen Clients erlaubt, auch wenn er nicht am File-Server angemeldet ist.
1	0001	Logged	Der Zugriff wird nur den Clients erlaubt, die sich erfolgreich am File-Server angemeldet haben.
2	0010	Object	Der Zugriff wird nur erlaubt, wenn der Benutzer, der auf dieses Objekt zugreifen will, am Server als dieses Objekt angemeldet ist.
3	0011	Supervisor	Der Zugriff wird nur Clients erlaubt, die sich als Supervisor oder Supervisor-Equivalent am File-Server angemeldet haben.
4	0100	NetWare	Der Zugriff wird nur dem NetWare-Betriebssystem gewährt.

Privileges

Die Sicherheit unter NetWare 3.2 mit Hilfe der Bindery wird durch zusätzliche Privileges erhöht: Supervisors, Workgroup-Managers, Benutzer.

15.14 Datensicherheit unter Novell NetWare 3.2

Nach der Installation von NetWare auf dem File-Server existiert unabhängig von der Art des File-Servers automatisch ein Benutzer. Es handelt sich dabei um den Benutzer *Supervisor*. Der Supervisor hat alle notwendigen administrativen Aufgaben im Netzwerk zu erledigen, d.h. das Einrichten von Benutzern, das Einrichten von Gruppen, die Vergabe von Directory- und Dateirechten oder die Vergabe von Account Restrictions etc. Sie haben auch die Möglichkeit, für einen Benutzer Security-Equivalence-Funktionen zu vergeben. Das heißt, der Benutzer erhält die gleichen Rechte wie das Objekt, über das dieser Security-Equivalence-Rechte besitzt.

Die Definition von Security-Equivalence-Funktionen ist sehr hilfreich beim Einrichten und Benutzen von Gruppendefinitionen. Man faßt bestimmte Rechte in einer Gruppe zusammen und erteilt einem Benutzer die Security-Equivalence-Funktion für diese Gruppe. Damit erhält der Benutzer die gleichen Rechte wie die Gruppe selbst. Mit dieser Funktion ist es auch möglich, den Benutzer A zum Security Equivalence von Benutzer B zu machen. Somit hat Benutzer A die gleichen Rechte wie Benutzer B. Wenn Sie einen Benutzer zum Security-Equivalence-Supervisor machen, dann hat dieser Benutzer die gleichen Rechte wie der Supervisor.

Mit NetWare 3.2 werden zwei neue Properties unterstützt. Es handelt sich dabei um WG_MANAGER und OBJ_SUPERVISOR. Diese beiden Properties werden benötigt, um das neue Workgroup-Manager-Konzept von NetWare 3.2 unterstützen zu können. Was versteht man nun unter einem Workgroup-Manager?

Wenn es um die Verwaltung eines Netzwerks unter NetWare geht, existiert ein Benutzer oder Benutzer-Equivalence, der die gesamte Verantwortung und Kontrolle darüber hat. Dies ist der Supervisor. Er ist unter anderem für das Einrichten von Benutzern, Vergabe von Zugriffsrechten, Einrichten von Gruppen, Festlegen von Account Restrictions, Einrichten von Applikationen etc. verantwortlich. Da Netzwerke jedoch immer größer werden, wachsen damit natürlich auch die Aufgaben, die von diesem Supervisor zu erfüllen sind. Mit Hilfe des Workgroup-Manager-Konzepts ist es möglich, diese Art Aufgaben auf mehrere Benutzer zu verteilen. Das heißt, Sie legen einen oder mehrere Benutzer fest, die Workgroup-Manager-Status besitzen, und ermöglichen somit, daß dieser Workgroup-Manager für das Einrichten, die Vergabe von Rechten etc. selbst verantwortlich ist. Die Oberhand behält immer noch der Supervisor, er legt auch fest, wer diesen Status erhält. Er kann jedoch administrative Aufgaben im Netzwerk verteilen.

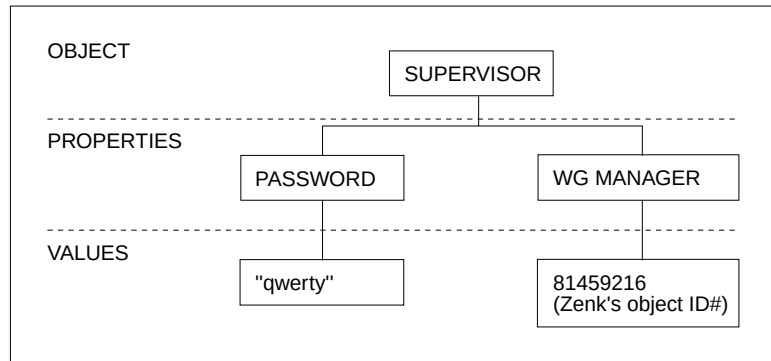
WG_MANAGER ist ein Property Set, das mit dem Objekt Supervisor verbunden ist. Der Supervisor vergibt dieses Property für einen Be-

15 Novell NetWare 3.2

nutzer oder eine Gruppe beim Einrichten mit Hilfe des Menüs *Sys-con*. Er vergibt also eingeschränkte Supervisor-Privilegien an einzelne Benutzer oder Gruppen, die so zum Workgroup-Manager werden.

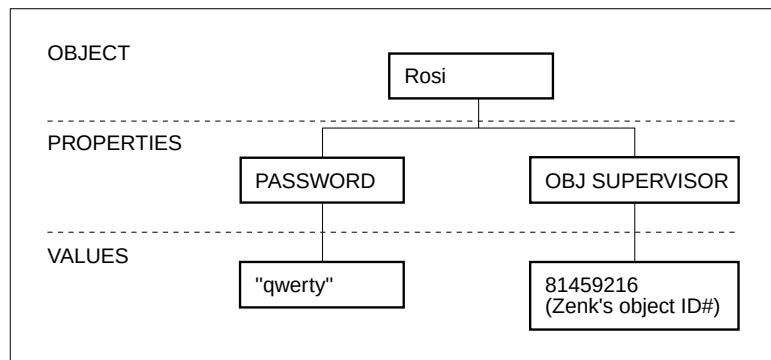
Wird eine Objekt-ID im WG_MANAGER Data Set eingetragen, kann dieses Objekt neue Bindery-Objekte einrichten. In Abbildung 15.15 ist dargestellt, wie dieser Zusammenhang aussieht, wenn Sie den Benutzer als Objekt-ID in den WG_MANAGER Data Set eintragen.

Abbildung 15.15
Aufbau der Work-
group-Manager-
Beziehung



Jedem Objekt, das von einem Workgroup-Manager eingerichtet wird, wird das Property Set OBJ_SUPERVISOR zugewiesen, in dem die Objekt-ID des Workgroup-Managers eingetragen wird, der dieses Objekt in der Bindery eingerichtet hat. Wenn zum Beispiel der Workgroup-Manager Zenk den Benutzer Rosi eingerichtet hat, dann wird im Property Set OBJ_SUPERVISOR die Objekt-ID von Benutzer Zenk eingetragen. In Abbildung 15.16 ist dieser Zusammenhang dargestellt.

Abbildung 15.16
Eintrag der Bin-
dery, wenn der Be-
nutzer von einem
Workgroup-Mana-
ger eingerichtet
wird



15.14 Datensicherheit unter Novell NetWare 3.2

Beachten Sie: Wenn die Objekt-ID von Benutzer Zenk im OBJ_-SUPERVISOR Property Set von Objekt Rosi eingetragen ist, dann hat Objekt Zenk alle Rechte über das Objekt Rosi, egal ob die Objekt-ID von Zenk im SUPERVISOR WG_MANAGER Data Set eingetragen ist oder nicht. Auf diese Weise können Sie einen beliebigen Benutzer zum User-Account-Manager eines anderen Benutzers definieren. Der hat dann alle Rechte über diesen Benutzer.

Encrypted Password

Zusätzlich zu den neuen Sicherheitsmechanismen in bezug auf Workgroup-Manager und User-Account-Manager bietet die Bindery auch noch weitere Sicherheitsfunktionen hinsichtlich der Login-Sicherheit in Verbindung mit dem Property-Paßwort. Mit NetWare 3.2 wird das Paßwort eines Benutzers nicht nur verschlüsselt in der Bindery abgelegt, sondern es wird auch noch verschlüsselt über die Netzwerkleitung übertragen. Auf diese Weise ist es nicht möglich, mit Hilfe eines LAN-Analysers ein übertragenes Paßwort von der Workstation zum File-Server abzuhören. Arbeitet man unter Umständen noch mit älteren Netzwerkkomponenten, z.B. externen Print-Servern, die diesen Mechanismus zur Einbindung in das Netzwerk nicht unterstützen, ist es möglich, im gemischten Netzwerkbetrieb am NetWare-3.2-File-Server festzulegen, daß auch nicht verschlüsselte Paßwörter akzeptiert werden. Dies dürfte jedoch inzwischen nur noch ganz selten vorkommen.

Im nächsten Abschnitt will ich Ihnen zeigen, wie das Sicherheitssystem von NetWare 3.2 mit Hilfe der Bindery aufgebaut und realisiert wird. In der Einleitung von Abschnitt 15.14. habe ich bereits darauf hingewiesen, daß sich die Sicherheit von NetWare 3.2 über die folgenden Bereiche erstreckt:

- Login-Sicherheit
- Rechte-Sicherheit
- Attribut-Sicherheit
- File-Server-Sicherheit

Diese sollen näher betrachtet werden. Ich will Ihnen auch weiterführende Informationen über die Accounting-Services von NetWare 3.2 geben.

15.14.2 Sicherheitsgruppen und Äquivalenzdefinitionen

Ein wesentliches Merkmal von NetWare ist die Möglichkeit, Objekte zu Gruppen zusammenzufassen. Sind am File-Server mehrere Benutzer mit ihren Benutzer-IDs definiert, können diese eine Gruppe bilden. Andere Benutzer können zu einer anderen Gruppe zusammen-

15 Novell NetWare 3.2

gefaßt werden. Jeder Gruppe können entsprechende Rechte zugewiesen werden, die sich danach richten, welche Berechtigungen die Gruppe für die Erfüllung ihrer Arbeit benötigt (Festlegung von Zugriffsrechten).

Eine Gruppe wird durch ihren Namen gekennzeichnet. Wird für diese Gruppe zum Beispiel Schreib- und Lesezugriff auf ein bestimmtes Subdirectory erteilt, aber kein Recht, Dateien daraus zu löschen, kann ein Mitglied dieser Gruppe an diesen Definitionen nichts ändern. Die Vergabe von Rechten obliegt ausschließlich dem Supervisor oder dem Supervisor-Equivalence. Durch diesen Mechanismus ist es für den Systemverantwortlichen sehr einfach, die Kontrolle und den Überblick über das Netzwerk mit all seinen Benutzern zu behalten.

Existieren für bestimmte Objekte bereits vorgegebene Sicherheitsdefinitionen und die gleichen Definitionen werden für ein anderes Objekt auch benötigt, so können sogenannte Äquivalenzen vergeben werden. Novell bezeichnet diese Art der Definition als Security Equivalence. Ein Benutzer A mit Äquivalenzrechten von Benutzer B besitzt die gleichen Zugriffsrechte wie Benutzer B, ohne daß zusätzliche Definitionen angegeben werden müssen.

Meldet sich ein Benutzer am File-Server korrekt an, sammelt dieser alle Gruppenzugehörigkeiten und Äquivalenzinformationen über den Benutzer.

Werden Zugriffsberechtigungen für einen Benutzer durch den Netzwerkadministrator durchgeführt, während er noch angemeldet ist, sind diese für den Benutzer sofort wirksam, ohne daß er sich neu anmelden müßte.

Nach der Installation des Netzwerkbetriebssystems existiert standardmäßig bereits ein Benutzer mit dem Namen Supervisor. Der User Supervisor ist verantwortlich für die Vergabe von Rechten, Festlegung der Benutzer und Gruppendefinitionen, die Vergabe von Directory-Rechten und der File-Attribute und vieler Dinge mehr, wie wir später noch sehen werden. Dem Supervisor können keine Rechte entzogen werden; er hat ausschließliche Privilegien und kann als Benutzer auch nicht gelöscht werden. Ohne Supervisor bzw. ohne Benutzer mit Supervisor-Equivalence-Rechten kann am Filer-Server nichts mehr definiert und kontrolliert werden. Daher sollte mit dieser Benutzerkennung äußerst vorsichtig umgegangen werden.

15.15 Die Accounting-Dienste von NetWare 3.2

Um die Definition und Anwendung der Sicherheitseinrichtungen für den Systemverwalter so einfach wie möglich zu gestalten, bietet NetWare 3.2 eine Vielzahl von Mechanismen an, die es gestatten, für die Benutzer im Netzwerk genau festzulegen, auf welche Ressourcen sie Zugriff haben. Mit dem Accounting-System von NetWare 3.2 ist es möglich, für die Benutzung von Server-Diensten Gebühren zu verrechnen. So könnte es zum Beispiel sein, daß man bei einem Datenbank-Server festlegt, wie hoch die Gebührensätze für das Lesen von Datenbanksätzen, das Schreiben von Datenbanksätzen, die Verbindungszeit zum Datenbank-Server etc. sein sollen. Bei einem Print-Server können Sie die Gebührensätze in Abhängigkeit von den gedruckten Seiten festlegen. Der Supervisor für den File-Server bestimmt, für welche Bereiche Gebührensätze in welcher Höhe verrechnet werden sollen.

Die Information darüber, für welchen Server in welcher Höhe Gebührensätze berechnet werden sollen, wird in der Bindery des File-Servers abgelegt. In der Bindery wird auch abgelegt, wie groß zum einen der Kontostand des einzelnen Benutzers und wie hoch das Kreditlimit eines Benutzers ist. Sobald ein Server als Accounting-Server in der Bindery eingetragen und aktiv ist, können folgende Aufgaben durchgeführt werden:

- Abbuchen von Gebührensätzen vom Konto des Benutzers.
- Das Account eines Benutzers auf HOLD stellen, wenn das Konto aufgebraucht ist.
- Den Account-Status eines Benutzers abfragen.
- Accounting-Informationen in einem Audit-File, der Accounting-Protokolldatei, abspeichern.

Da die Accounting-Dienste ebenso durch die Bindery verwaltet werden, benötigt NetWare auch dazu besondere Properties. Hierzu stehen in der Bindery drei Properties zur Verfügung, um sowohl die Objekt-IDs aller festgelegten Accounting-Server als auch alle Informationen über das Account des bzw. der Benutzer (Clients) zu verwalten. Es handelt sich hierbei um die Properties ACCOUNT_SERVERS, ACCOUNT_BALANCE, ACCOUNT_HOLDS. Die Aufgabe dieser drei Properties soll anschließend etwas näher betrachtet werden.

15.15.1 Property ACCOUNT_SERVERS

Wird für einen Server, egal ob File-Server, Print-Server oder auch Datenbank-Server, das Accounting eingerichtet, muß für jeden Server eine ACCOUNT_SERVER-Property eingerichtet werden. Dieser Property-Eintrag enthält die Objekt-ID eines jeden Servers, der die Berechtigung besitzt, Accounting-Daten zu übertragen. Bevor zum Beispiel der Print-Server PS-SERVER Accounting-Abrechnungsdaten zum File-Server FS1 übertragen kann, muß die Objekt-ID von PS-SERVER in der Property ACCOUNT_SERVERS in der Bindery von File-Server FS1 eingetragen sein.

Dies gilt auch für jedes Objekt, das Security-äquivalent zu einem Objekt ist, das in der ACCOUNT_PROPERTY eingetragen ist.

15.15.2 Property ACCOUNT_BALANCE

Jedes Objekt, das sich am File-Server anmelden kann, d.h. ein Property Password hat, besitzt eine ACCOUNT_BALANCE Property. Die Account Balance (Kontostand) des Objekts und das Kreditlimit für das Objekt werden im Property ACCOUNT_BALANCE gespeichert. Besitzt ein Objekt diese Property nicht, kann der Zugang zum File-Server verwehrt werden. Wenn das Kreditlimit eines Objekts erreicht ist, wird der Zugang zum entsprechenden Server verweigert, falls dieser Accounting-Daten erzeugt.

15.15.3 Property ACCOUNT_HOLD

Ein berechtigter Server kann das Account eines Benutzers auf HOLD stellen, also außer Kraft setzen, den Status des Benutzer-Accounts abfragen oder einen Gebührensatz für den Benutzer in Rechnung stellen. Jedes Objekt, das sich am Server anmelden kann, ist in der Lage, ein Property ACCOUNT_HOLD zu besitzen. Dieser Property-Eintrag erfolgt nur dann, wenn das Accounting des Benutzers abgelaufen ist, temporär deaktiviert wird oder das Konto des Benutzers aufgebraucht ist. Wird das Account eines Benutzers wieder freigegeben, dann wird dieser Eintrag für das Objekt gelöscht.

Die Einrichtung des Accounting-Systems ist unter NetWare 3.2 optional. Nach der Installation des Accounting-Systems wird Protokoll darüber geführt, wann sich ein Benutzer von welcher Station aus am File-Server angemeldet und wieder abgemeldet hat. Außerdem wird registriert, welche Accounting-Beträge für das Lesen von Daten, das Schreiben von Daten etc. in dieser Login-Zeitperiode am File-Server von den Benutzern in Anspruch genommen worden sind.

15.15 Die Accounting-Dienste von NetWare 3.2

Mit der Installation des Accounting-Systems können zusätzlich für einzelne Ressourcen Gebührensätze festgelegt werden. Diese Gebührensätze können für jeden Tag und in 30-Minuten-Intervallen unterschiedlich gestaffelt werden. Für die Benutzung der Ressourcen müssen nur sogenannte Charge Rates (Kontobelastungen) definiert werden. Folgende Optionen stehen dabei zur Verfügung:

- *Verrechnung von Gebührensätzen für jeden Benutzer*
Der Supervisor legt fest, welcher Server (File-Server, Print-Server, Datenbank-Server, Communication-Server etc.) die Berechtigung erhält, für die Inanspruchnahme seiner Ressourcen Charge Rates zu verrechnen.
- *Welche Ressourcen verrechnet werden sollen*
Der Supervisor entscheidet, welche Dienste des Servers verrechnet werden. Je nach Anwendung können einzelne Möglichkeiten eingesetzt werden, andere hingegen, die nicht notwendig erscheinen, müssen nicht aktiviert sein.

Für folgende Bereiche können Charge Rates definiert werden:

- *Blocks Read*
Die Festlegung dieses Gebührensatzes bestimmt, welcher Betrag vom Konto des Benutzers abgebucht wird, wenn dieser Blöcke von der Platte des Servers liest. Der Gebührensatz wird pro gelesenen Datenblock festgelegt. Ein Datenblock entspricht dabei der entsprechenden Disk Allocation Block Size des Volume, von dem die Daten gelesen werden.
- *Blocks Written*
Mit dieser Festlegung wird ein Gebührensatz für jeden Datenblock, der auf die Platte des File-Servers abgespeichert wird, bestimmt. Ein Datenblock entspricht dabei der entsprechenden Disk Allocation Block Size des Volume, auf das die Daten geschrieben werden.
- *Connect Time*
Mit dieser Charge Rate wird bestimmt, wieviel ein Benutzer für die Dauer des Logins am File-Server bezahlen muß. Die Charge Rate wird dabei pro Minute berechnet.
- *Disk Storage*
Diese Option erlaubt die Bestimmung einer Charge Rate für jeden Block, der auf der Platte für einen Tag abgespeichert ist. Die Charge Rate wird durch die Bestimmung Blöcke/Tag festgelegt (Anzahl der Blöcke an einem Tag).
- *Service Requests*
Diese Option erlaubt die Bestimmung der Charge Rate für jeden Server-Dienst (Anfrage an den File-Server), den der Benutzer in Anspruch nimmt. Die Charge Rate wird für jeden Request vom Konto des Benutzers abgebucht.

15.16 Die Login-Sicherheit

Mit dieser Funktion wird überwacht, ob der Benutzer die Berechtigung besitzt, sich am File-Server anzumelden, und mit welchen Rechten er am File-Server arbeiten darf. Es wird festgelegt und kontrolliert, welcher Benutzer am File-Server arbeiten kann, wann er am File-Server arbeiten kann, auf welchen Workstations er sich am File-Server anmelden kann und auf welche Ressourcen er Zugriff hat. Diese Festlegungen werden vom Supervisor bzw. Workgroup-Manager beim Einrichten des Benutzers definiert. Sie können jederzeit wieder geändert werden.

Jeder Benutzer besitzt nach dem Einrichten ein User Account. Dieses User Account stellt einen weiteren Teil der Möglichkeiten zur Festlegung von Sicherheitsmechanismen dar. Einige der Optionen werden automatisch beim Einrichten des Benutzers angelegt, andere hingegen müssen explizit eingerichtet und zugewiesen werden. Sie können wahlweise verwendet werden. Im Folgenden sollen diese User-Account-Optionen der Reihe nach angesprochen werden.

15.16.1 Benutzername

Ein Benutzer kann am File-Server den Login erst dann durchführen, wenn er zumindest in der Bindery als Objekt eingetragen ist. Der Benutzername kann 1 bis 47 Zeichen lang sein. Dem Benutzer werden dann zusätzliche Properties, Property Sets und Werte zugewiesen.

Mitgliedschaft einer Gruppe

Als Supervisor oder Workgroup-Manager haben Sie die Möglichkeit, neue Gruppen zu definieren, die Rechte für diese Gruppe festzulegen und zu bestimmen, welcher Benutzer Mitglied in diesen Gruppen sein soll.

Trustee- Assignments

Damit ein Benutzer auf Directories und Dateien am File-Server Zugriff hat, muß ihm der Supervisor oder Workgroup-Manager auch den Zugriff auf Directories und Dateien gewähren. Die Berechtigung hierzu erhält der Benutzer durch die Festlegung von Trustee-Assignments. In den Trustee Assignments wird bestimmt, mit welchen Berechtigungen der Benutzer auf Directories und Dateien zugreifen kann. Der Benutzer hat keine Berechtigung, auf sie zuzugreifen, solange diese Trustee Assignments fehlen. Die Festlegung von Trustee-Rechten kann entweder direkt für den Benutzer selbst oder in einer Gruppendefinition erfolgen, wobei der Benutzer dann Mitglied dieser Gruppe sein muß. Auf die Möglichkeiten, die Ihnen NetWare 3.2 hierfür zur Verfügung stellt, werde ich in einem eigenen Kapitel noch zu sprechen kommen.

15.16 Die Login-Sicherheit**Security
Equivalences**

Durch die Festlegung der Security Equivalences können an den Benutzer die gleichen Berechtigungen vergeben werden, die ein anderer Benutzer oder eine andere Gruppe besitzt. Wenn Sie einen Benutzer zum Security-Equivalence-Supervisor machen, hat dieser Benutzer die gleichen Rechte wie der Supervisor.

**User Login
Script**

Nach Ausführung des Logins betrachtet NetWare den Benutzer als Anwender, der mit bestimmten Rechten ausgestattet ist. Diese Rechte sind durch die Statuskennzeichen und Sicherheitsmasken für den Benutzer in der Bindery festgelegt und können nur vom Supervisor oder dem Supervisor-Equivalence geändert werden. Für den Benutzer selbst ist jedoch noch keine vernünftige Arbeitsumgebung geschaffen, wie Vorgabe von Suchpfaden, Laufwerkszuordnungen und dergleichen. Deshalb ist es möglich, für jeden Benutzer ein sogenanntes Login Script zu erstellen, das automatisch nach einem erfolgreichen Login ausgeführt wird, wenn es existiert. Ein Login Script entspricht einer AUTOEXEC.BAT unter MS-DOS, allerdings auf die Netzwerkebene bezogen.

Nachdem ein Benutzer in der Regel Mitglied von verschiedenen Gruppen ist, kann die Verarbeitungsweise bestimmter Login-Script-Definitionen auch auf Gruppenzugehörigkeit abgestimmt werden. Beispielsweise wird, wenn der Benutzer nur Mitglied dieser Gruppe ist, eine entsprechende Definition innerhalb des Login Script ausgeführt.

Hierbei ist zwischen dem System Login Script, dem User Login Script und dem Default Login Script zu unterscheiden. Generell gilt: Existiert ein System Login Script, dann wird dies immer beim Login des Benutzers ausgeführt. Danach wird das User Login Script ausgeführt. Das User Login Script ist ein nur für diesen Benutzer eingerichtetes Login Script und gilt auch nur für diesen.

Ist kein User Login Script vorhanden, wird das Default Login Script ausgeführt. Im Default Login Script werden nur die wichtigsten Laufwerkszuordnungen und Suchpfaddefinitionen festgelegt. Die Ausführung des Default Login Scripts ist unabhängig von der Existenz des System Login Scripts. Das Default Login Script wird also nur dann ausgeführt, wenn kein User Login Script vorhanden ist.

NetWare verwendet die Bindery, um das Login-Verfahren und das Login Script zu integrieren. Ein Teil des Login-Verfahrens initialisiert die Sicherheitsberechtigungen des Benutzers, während das Login Script die Umgebung des Benutzers initialisiert. Das Resultat beider Verfahren wird als »Benutzerprofil« bezeichnet. Zusammengefaßt kann gesagt werden, daß das Benutzerprofil den Zugang eines Benutzers zum Netzwerk bildet.

15 Novell NetWare 3.2**Account-
Management**

Da der Supervisor für das Einrichten von Benutzern verantwortlich ist, kann er auch jederzeit das Account der Benutzer ändern. Der Benutzer selbst kann sein eigenes User Account nur einsehen, aber nicht ändern. Neben dem Supervisor hat der Workgroup-Manager die Berechtigung, das User Account der Benutzer zu ändern, die er selbst eingerichtet hat oder für die er als User-Account-Manager eingetragen ist.

Das Konto eines Benutzers kann vom Supervisor, Workgroup-Manager oder User-Account-Manager jederzeit gesperrt werden, ohne daß der Benutzer aus der Bindery gelöscht werden muß. Ist das Konto eines Benutzers gesperrt, kann dieser so lange nicht mehr am File-Server arbeiten bzw. den Login ausführen, bis sein Konto wieder freigegeben wird.

**Login-
Restriktionen**

Jedem Benutzer können sogenannte Login-Restriktionen auferlegt werden. Damit soll verhindert werden, daß nichtautorisierte Benutzer den Zugang zum Netz erhalten. Es handelt sich dabei um einen zusätzlichen Sicherheitsmechanismus, den NetWare 3.2 zur Verfügung stellt. Diese Login-Restriktionen können als Default-Werte eingestellt werden und gelten ab der Festlegung für alle neu eingerichteten Benutzer. Bereits existierende Benutzer werden von der Änderung der Default-Werte nicht berührt. Beim Benutzer selbst können diese Werte individuell angepaßt werden. Als Login-Restriktionen stehen die nachfolgenden Mechanismen zur Verfügung.

Account-Balance

Wenn Sie das Accounting-System zum Abrechnen von Ressourcen installiert haben, kann mit der Festlegung einer Account-Balance und der Vergabe eines Kreditlimits der Kontostand des Benutzers bestimmt werden. Sie überweisen dem Benutzer praktisch einen Geldbetrag (Account-Balance) auf sein Konto und legen fest, wie groß sein Dispositionskredit (Kreditlimit) ist.

Ist die Account-Balance aufgebraucht und der gewährte Kredit erschöpft, dann wird das User Account »disabled«. Das heißt, der Benutzer kann ab diesem Zeitpunkt so lange nicht mehr am File-Server arbeiten, bis er vom Supervisor, dem verantwortlichen Workgroup-Manager oder User-Account-Manager wieder freigegeben wird.

**Ablaufdatum des
User Account**

Für den Benutzer kann ein Ablaufdatum für das User Account festgelegt werden. Nach Ablauf dieses Datums kann sich der betroffene Benutzer nicht mehr am File-Server anmelden. Der Supervisor, Workgroup-Manager oder User-Account-Manager kann diese Sperrung wieder aufheben.

15.16 Die Login-Sicherheit**Beschränkung
der gleich-
zeitigen
Anmeldungen**

Es kommt immer wieder vor, daß ein Benutzer mit derselben Anmeldung an mehreren Workstations gleichzeitig arbeitet. Das kann unter NetWare auch eingeschränkt werden. Diese Angabe der Begrenzung gilt nur für die Verbindung zu einem File-Server, nicht jedoch für die Verbindungen im Internet. Ist ein Benutzer bereits mit der maximal möglichen Anzahl von Verbindungen am File-Server angemeldet, weist der Server jeden weiteren Versuch ab, bis eine der bestehenden Verbindungen aufgelöst worden ist. Wird die Anzahl der gleichzeitigen Logins vom Supervisor nicht begrenzt, kann sich ein Benutzer beliebig oft an einem File-Server anmelden, solange die maximale Anzahl von Benutzern noch nicht erreicht ist. Die Begrenzung der möglichen gleichzeitigen Verbindungen gilt auch für den Supervisor, wenn diese festgelegt worden ist.

**Beschränkungen
für die Paß-
wortvergabe**

Die Möglichkeiten für die Beschränkungen bei der Vergabe von Paßwörtern werden erst dann wirksam, wenn für den Benutzer ein Paßwort zwingend vorgeschrieben wird. Der Benutzer ist dann verpflichtet, sich an die Paßwortrestriktionen zu halten.

Die Möglichkeiten hierfür sind wie folgt:

■ *Minimale Länge des Paßworts*

Hiermit wird festgelegt, aus wie vielen Zeichen das Paßwort mindestens bestehen muß. Ein Paßwort, das kürzer als diese Vorgabe ist, wird nicht akzeptiert. Als Default-Wert gibt NetWare fünf vor. Es kann hier ein maximaler Wert von 20 festgelegt werden, das Paßwort muß dann mindestens 20 Zeichen lang sein. Das Paßwort darf insgesamt nicht länger als 127 Zeichen sein.

■ *Änderungsintervall des Paßworts*

Mit dieser Maßnahme wird festgelegt, in welchen Abständen der Benutzer das Paßwort ändern muß. Als Voreinstellung vergibt NetWare 40 Tage, d.h., das Paßwort muß spätestens alle 40 Tage geändert werden. Sie können Änderungsintervalle zwischen 1 (einem Tag) und 365 (365 Tage) definieren.

■ *Benutzer darf das Paßwort ändern*

Es kann festgelegt werden, ob der Benutzer die Berechtigung hat, sein Paßwort selbst zu ändern, oder ob dies dem Supervisor, Workgroup-Manager oder User-Account-Manager vorbehalten ist.

■ *Beschränkung der Grace Logins*

Hiermit kann bestimmt werden, wie oft der Benutzer den Login mit dem alten Paßwort durchführen kann, auch wenn es schon abgelaufen ist.

Als Default-Einstellung gestattet NetWare dem Benutzer, sich noch sechsmal mit einem bereits abgelaufenen Paßwort anzumelden. Wird in dieser Zeit das Paßwort nicht geändert, obwohl ihn das System beim Login dazu auffordert und die verbleibenden Grace

15 Novell NetWare 3.2

Logins auf 0 stehen, wird das User Account des Benutzers von NetWare gesperrt, und nur der Supervisor, Workgroup-Manager oder User-Account-Manager hat die Möglichkeit, dieses wieder freizusetzen.

Jedesmal, wenn der Benutzer nach dem Login und der Aufforderung, das Passwort zu ändern, mit No weitermacht, wird der Zähler der verbleibenden Grace Logins um eins reduziert.

■ *Eindeutigkeit des Passworts*

Der Benutzer kann damit gezwungen werden, beim Passwortwechsel zehn unterschiedliche Passwörter zu verwenden. Beim Versuch, ein Passwort zu verwenden, das unter die letzten zehn verwendeten Passwörter fällt, wird es vom System abgewiesen und nicht akzeptiert.

■ *Verschlüsselung des Passworts*

Bevor das Passwort eines Benutzers auf die Festplatte geschrieben wird, wird dieses mit Hilfe eines irreversiblen Algorithmus verschlüsselt. Personen mit direktem Zugriff auf den File-Server können somit die Passwörter nicht einsehen. Auch dem Supervisor ist es nicht möglich, das Passwort eines Benutzers einzusehen. Der Benutzer kann damit die gleichen Passwörter auf unterschiedlichen File-Servern verwenden, ohne daß der Supervisor des einen File-Servers sein Passwort für die anderen File-Server findet. Für den Fall, daß ein Benutzer sein Passwort vergessen hat, kann der Supervisor es jedoch neu definieren, ohne das alte Passwort des betreffenden Benutzers zu kennen. Außerdem ist das Passwort bei der Übertragung über die Leitung verschlüsselt, so daß auch mit Sniffen oder LAN-Analyser-Systemen nicht mehr eingesehen werden kann, welcher Benutzer mit welchem Passwort arbeitet.

Da es immer wieder vorkommt, daß ein Benutzer sein Passwort vergißt, haben der Supervisor oder entsprechend berechnigte Personen die Möglichkeit, das Passwort eines Benutzers zu ändern, ohne dessen altes Passwort zu kennen.

**Plattenplatz-
beschränkung
pro Volume**

Für jeden Benutzer kann individuell festgelegt werden, wieviel Plattenplatz ihm insgesamt auf jedem Volume zur Verfügung gestellt wird. Ist die freigegebene Volume-Kapazität des Benutzers aufgebraucht, kann er zwar noch am File-Server arbeiten, aber beim Versuch, Daten abzuspeichern, bekommt er eine Fehlermeldung, daß nicht genug Speicherplatz zur Verfügung steht. Der Supervisor, Workgroup-Manager oder User-Account-Manager kann die Plattenkapazität des Benutzers jederzeit erhöhen. Wie später noch zu sehen sein wird, kann unter NetWare 3.2 die Plattenplatzbeschränkung für einen Benutzer nicht nur pro Volume festgesetzt werden, vielmehr besteht auch die Möglichkeit, für jedes einzelne Directory eine Kapazitätsbeschränkung einzuführen.

15.16 Die Login-Sicherheit

- Zeitrestriktion** Einheitlich für alle Benutzer oder individuell für jeden einzelnen Benutzer kann bestimmt werden, wann sie sich am File-Server anmelden dürfen. Außerhalb der festgelegten Zeit wird ein Versuch des Logins abgewiesen. Ist ein Benutzer bereits angemeldet und die Zeit des erlaubten Logins abgelaufen, bekommt er von NetWare fünf Minuten vorher eine Mitteilung, daß er sich doch bitte abmelden sollte. Ignoriert er diesen Hinweis, dann bekommt er diese Meldung vier Minuten später noch einmal. Meldet er sich daraufhin immer noch nicht ab, dann tut dies eine Minute später NetWare für ihn.
- Stationenrestriktion** Unter Novell NetWare ist es auch möglich, festzulegen, daß ein bestimmter Benutzer sich nur an fest definierten Workstations ins Netz einloggen darf. Es kann sowohl die physikalische Netzwerknummer als auch die Knotenadresse von Workstations angegeben werden. Die Beschränkungen können für ganze Netzwerke von Workstations oder für einzelne Workstations gelten, wenn diese über ein Internet verteilt sind.
- Erkennung eines Eindringlings (Intruder) mit automatischem Sperren** Mit der sogenannten Intruder Detection können unter NetWare Hacker abgewehrt werden. Der Supervisor vergibt dabei einen Schwellenwert. Der Schwellenwert wird als eine Anzahl von falschen Login-Versuchen innerhalb einer bestimmten Zeitspanne definiert. Wird diese Zahl in der vorgegebenen Zeit erreicht, so wird eine entsprechende Protokollnachricht mit der Meldung erzeugt, daß ein »Intruder« entdeckt worden ist. Die Protokollnachricht enthält den Zeitpunkt des Eindringens, den Benutzernamen, mit dem die Versuche durchgeführt wurden, und die physikalische Stationsadresse (Node-Address) des Arbeitsplatzes, von wo aus der Intruder-Versuch ausgeführt wurde. Die Anzahl der falschen Login-Versuche wird auf Null gesetzt, wenn ein erfolgreicher Login ausgeführt wird oder wenn seit dem letzten Fehlversuch eine längere Zeit als die im Schwellenwert festgelegte vergangen ist.
- Neben der Festlegung, daß eine Protokollnachricht erzeugt werden soll, kann der Supervisor bestimmen, daß das betroffene Konto gesperrt wird, wenn ein Eindringling entdeckt worden ist. Mit dieser Festlegung muß der Supervisor auch die Dauer der Sperre bestimmen. Diese Sperre kann eine Minute bis maximal 40 Tage, 23 Stunden und 59 Minuten betragen. Durch diese Sperrfunktion, bei der ein Login innerhalb dieser Sperre nicht mehr möglich ist, auch wenn das Paßwort gleich beim ersten Versuch richtig eingegeben wird, kann die Zeit, die für einen Hacker über willkürlich ausgewählte Paßwörter nötig ist, so gewählt werden, daß ein Versuch des Eindringens unmöglich wird.

Der Supervisor kann die Sperrung des Kontos jederzeit außer Kraft setzen. Eine Aktivierung der Intruder Detection gilt für alle User, die sich am Server anmelden und dabei ihr Paßwort falsch eingeben, auch für den Supervisor.

15.17 Die Rechtesicherheit

Unter NetWare 3.2 sind die Konzepte der Sicherheitsfunktionen im Vergleich zu früher wesentlich geändert worden. Es wurde nicht nur die Rechtestruktur für NetWare 3.2 modifiziert, sondern auch die Möglichkeiten der Rechtevergabe und der zur Verfügung stehenden Rechte. Daneben ist es unter NetWare 3.2 auch möglich, die Rechte nicht nur auf Directory-Ebene zu vergeben, sondern Rechte bis auf Dateiebene festzulegen. Es ist möglich, daß Sie einem Benutzer für ein Directory Leserechte vergeben. Somit besitzt er die Berechtigung, alle Dateien in diesem Directory zu lesen. Für eine spezielle Datei in diesem Directory können Sie die Rechte für einen Benutzer jedoch erweitern oder einschränken. Sie können dem Benutzer für eine Datei die Berechtigung vergeben, diese zusätzlich auch noch zu ändern, d.h., Sie vergeben dem Benutzer das Schreibrecht. Sie können aber auch festlegen, daß der Benutzer für eine bestimmte Datei überhaupt keine Rechte mehr besitzt. Er kann dann mit dieser einen Datei nicht mehr arbeiten, aber mit allen anderen Dateien im Directory.

Zur Festlegung der Rechtestrukturen für die einzelnen Benutzer sind folgende Mechanismen zu unterscheiden:

- File-/Directory-Rechte
- Trustee-Rechte
- File-/Directory-Attribute
- Inherited Rights Mask

Auch für NetWare 3.2 gilt, daß bei der Vergabe von Rechten für den Benutzer die sogenannten effektiven Rechte bestimmt werden müssen, die Bestimmung der effektiven Rechte erfolgt jedoch auf eine andere Weise. Wenn Sie einen Benutzer einrichten, besitzt dieser am File-Server keinerlei Rechte, d.h., der Systemverwalter ist dafür verantwortlich, auf welche Directories und welche Dateien mit welchen Rechten er zugreifen darf. Der Benutzer muß somit zuerst die Berechtigung dafür erhalten, auf Directories und Dateien zuzugreifen. Solange dies nicht geschehen ist, besteht keinerlei Möglichkeit des Zugriffs.

15.17 Die Rechtesicherheit

Dieser Vorgang erfolgt durch die Vergabe sogenannter Trustee-Rechte für den Benutzer. Die Trustee-Rechte können für ein Directory, eine Datei oder beides vergeben werden. Ein Trustee für ein Directory oder eine Datei mit damit verbundenen Zugriffsrechten wird auch als »der Berechtigte« bezeichnet. Welches effektive Recht ein Benutzer für das Directory oder eine Datei besitzt, wird durch die Kombination der Trustee-Rechte mit der Inherited Rights Mask des Directory oder der Datei berechnet.

Eine Trustee-Recht-Definition ist somit immer für den Benutzer oder für die Gruppe maßgeblich. Die Inherited Rights Mask wird für ein Directory oder eine Datei vergeben und ist für alle Benutzer und Gruppen gültig. Daneben stehen Ihnen auch noch Directory- und Dateiattribute zur Verfügung, um nach Festlegung eines effektiven Rechts zusätzlich bestimmte Funktionen für das Arbeiten mit Directories und Dateien einzuschränken.

Besitzen Sie zum Beispiel als effektives Recht *Lesen und Schreiben*, bedeutet dies, daß Sie eine Datei auch ändern dürfen. Ist für diese Datei jedoch das Attribut *Read-Only* vergeben, können Sie keine Änderungen in dieser Datei durchführen. Die Anzahl und Bedeutung der Rechte zur Vergabe von Trustee-Rechten und zur Festlegung der Inherited Rights Mask auf Directory-Ebene sind gleichbedeutend und sollen nachfolgend aufgeführt werden.

Supervisory	Gewährt alle Rechte für das Directory, für die Dateien und Subdirectories. Das Supervisory-Recht überschreibt alle Beschränkungen, die für Subdirectories oder Dateien mit Hilfe einer Inherited Rights Mask beschränkt worden sind. Das heißt, das Supervisory-Recht kann in Subdirectory-Pfaden nicht mehr eingeschränkt werden. Benutzer mit diesem Recht können anderen Benutzern Rechte für dieses Directory bzw. für Subdirectories und Dateien vergeben.
Read	Gewährt das Lesen und Öffnen von Dateien in diesem Directory. Dateien können somit gelesen oder aufgerufen werden (Programm-Dateien).
Write	Gewährt das Schreiben und Öffnen von Dateien in diesem Directory. Der Inhalt einer Datei kann somit geändert werden.
Create	Gewährt das Recht, Dateien und Subdirectories in diesem Directory zu erstellen. Besitzt ein Benutzer für ein Directory das Create-Recht, kann er damit eine neue Datei erstellen, diese mit Daten füllen und danach schließen. Nach dem Schließen dieser Datei kann er darauf nicht mehr zugreifen.
Erase	Mit diesem Recht können ein Directory, dessen Dateien, Subdirectories und Subdirectory-Dateien gelöscht werden.

15 Novell NetWare 3.2

Modify	Mit diesem Recht können sowohl Directory- und Dateiattribute als auch der Directory- und der Dateiname geändert werden. Mit diesem Recht kann der Inhalt einer Datei nicht geändert werden.
File Scan	Mit diesem Recht wird Ihnen der Inhalt des Directory angezeigt (z. B. mit DIR).
Access Control	Mit diesem Recht können Directory- oder Datei-Zuweisungen geändert werden; dies beinhaltet auch die Änderung der Inherited Rights Mask. Benutzer mit diesem Recht können anderen Benutzern alle Rechte vergeben (Trustee-Recht-Zuweisung), außer dem Supervisory-Recht. Sie können Trustee-Rechte vergeben, die sie selbst nicht besitzen.
	Auf Dateiebene stehen Ihnen folgende Rechte zur Verfügung:
Supervisory	Mit diesem Recht besitzen Sie alle Rechte für diese Datei. Benutzer mit diesem Recht können anderen Benutzern Rechte für diese Datei vergeben und die Inherited Rights Mask für diese Datei ändern.
Read	Gewährt das Recht, die Datei zu öffnen und zu lesen.
Write	Gewährt das Recht, die Datei zu öffnen und zu beschreiben.
Create	Dieses Recht gestattet Ihnen nach Löschen einer Datei, sie mit Hilfe von SALVAGE wieder herzustellen. Das heißt, jeder Benutzer, der das Create-Recht für eine Datei besitzt, kann diese mit SALVAGE restaurieren.
Erase	Mit diesem Recht dürfen Sie die Datei löschen.
Modify	Mit diesem Recht können die Dateiattribute geändert werden, und Sie haben das Recht, der Datei einen anderen Namen zu geben. Sie haben nicht das Recht, den Inhalt einer Datei zu ändern.
File Scan	Mit diesem Recht wird Ihnen die Datei beim Auflisten des Directory-Inhalts angezeigt.
Access Control	Mit diesem Recht können Sie die Trustee-Zuweisungen und die Inherited Rights Mask ändern. Benutzer mit diesem Recht können anderen Benutzern alle Rechte für die Datei, außer dem Supervisory-Recht, gewähren.

In Abbildung 15.17 ist zusammengestellt, wie Sie die effektiven Rechte eines Benutzers für Directories berechnen müssen. Abbildung 15.18 hingegen stellt dar, wie Sie die effektiven Rechte für Dateien bestimmen müssen. Als Beispiel sehen Sie sich Abbildung 15.19 an und vergleichen dieses Beispiel mit den aufgezeigten Vorgehensweisen zur Bestimmung der effektiven Rechte.

15.17 Die Rechtesicherheit

Abbildung 15.17
Bestimmung der
effektiven Rechte
auf Directory-
Ebene

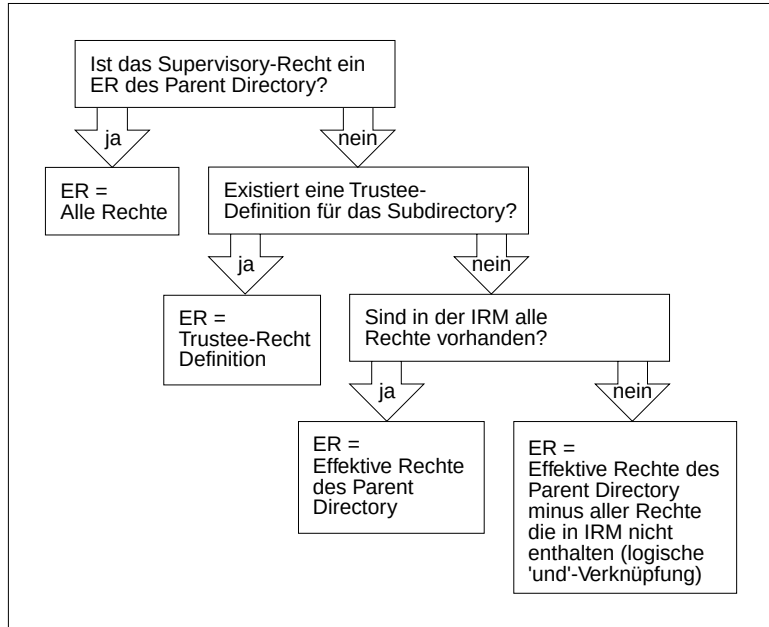
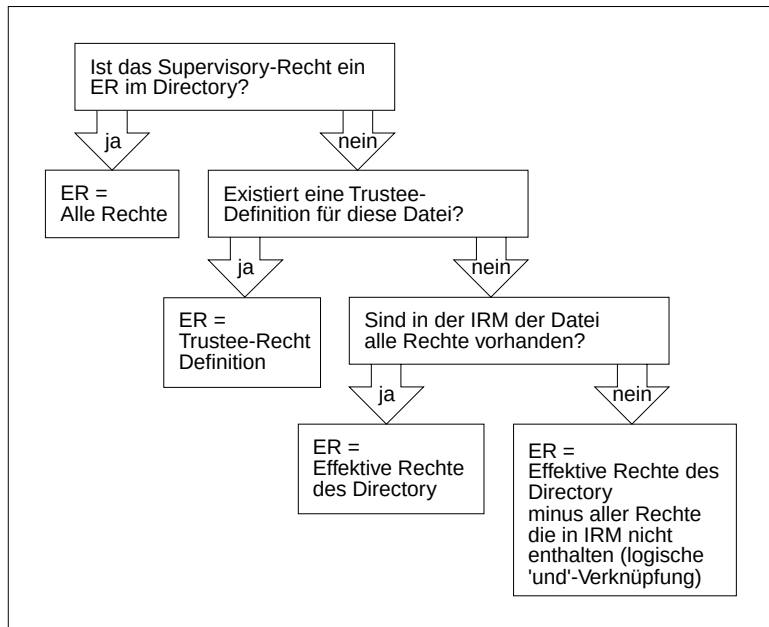
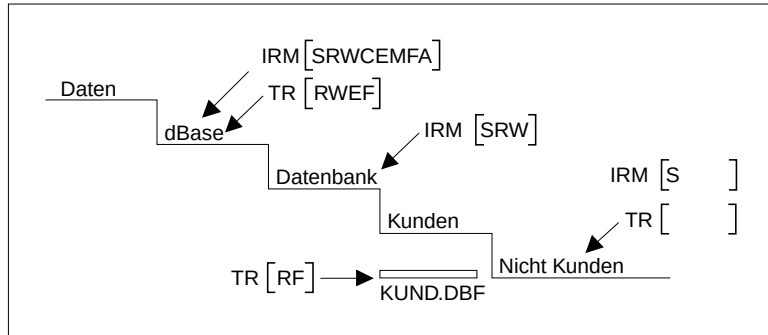


Abbildung 15.18
Bestimmung der
effektiven Rechte
für Dateien



15 Novell NetWare 3.2

Abbildung 15.19
Beispiel zur
Bestimmung der
effektiven Rechte



Als erstes müssen Sie bestimmen, für welches Directory in einem Directory-Pfad eine Trustee-Rechtzuweisung vergeben worden ist. Es gilt, daß diese Trustee-Rechtzuweisung gleich dem effektiven Recht ist, unabhängig davon, welche Rechte in der Inherited Rights Mask vergeben worden sind. Ist in der Trustee-Rechtzuweisung das Supervisory-Recht vergeben, besitzt der Benutzer für alle darunterliegenden Directories und Dateien alle Rechte. Das Supervisory-Recht kann auch nicht mehr eingeschränkt werden.

Als nächstes müssen die effektiven Rechte der darunterliegenden Subdirectories bestimmt werden. Hierbei gilt:

Ist im Subdirectory keine Änderung der Inherited Rights Mask durchgeführt worden, entspricht das effektive Recht des Subdirectory dem effektiven Recht des darüberliegenden Directory. Wurde die Inherited Rights Mask des Subdirectory eingeschränkt, berechnet sich das effektive Recht durch eine logische UND-Verknüpfung des effektiven Rechts des darüberliegenden Directory mit der Inherited Rights Mask des Directory.

Haben Sie auf Dateiebene keine Änderung der Inherited Rights Mask durchgeführt oder für eine bestimmte Datei keine expliziten Trustee-Rechte vergeben, dann entspricht das effektive Recht des Directory dem effektiven Recht der Datei in diesem Directory.

Ist für eine Datei ein Trustee-Recht vergeben, dann ist das effektive Recht der Datei gleich dem Trustee-Recht, das für die Datei vergeben worden ist. Haben Sie als effektives Recht das Supervisory-Recht, dann können Sie auch auf Dateiebene keine Einschränkungen mehr durchführen. Wurde für eine Datei keine Trustee-Rechtedefinition vorgenommen, dann ergibt sich das effektive Recht für die Datei aus der logischen UND-Verknüpfung der Inherited Rights Mask für diese Datei mit dem effektiven Recht des Directory.

15.17 Die Rechtesicherheit

Neben der Vergabe von Trustee-Rechten und Inherited Rights Masks für Directories und Dateien steht Ihnen auch noch die Vergabe von Directory- und Dateiattributen zur Verfügung. Hiermit können Sie zusätzlich den Zugriff auf Dateien regeln. Auf Dateiebene können folgende Attribute vergeben werden:

Archive Needed	Dieses Attribut wird von NetWare automatisch vergeben, wenn eine Datei seit dem letzten Backup geändert worden ist. Das Attribut wird beim nächsten Backup der Datei wieder zurückgenommen.
Copy Inhibit	Dieses Attribut hat nur Auswirkungen für Macintosh-Benutzer. Auch wenn der Benutzer Read- und File-Scan-Recht besitzt, kann eine Datei mit diesem Attribut nicht mehr kopiert werden.
Delete Inhibit	Auch wenn Benutzer das Erase-Recht besitzen, kann eine Datei mit diesem Attribut nicht mehr gelöscht werden.
Execute Only	Dieses Attribut kann, wenn es einmal vergeben worden ist, nicht mehr zurückgenommen werden. Damit legen Sie fest, daß eine Datei nur noch ausgeführt werden kann. Das Attribut kann nur für COM- und EXE-Dateien vergeben werden. Ein Kopieren, Umbenennen oder Überschreiben der Datei ist nicht mehr möglich.
Hidden	Eine Datei mit diesem Attribut wird beim Auflisten des Directory-Inhalts nicht mehr angezeigt.
Indexed	Wenn eine Datei mehr als 64 FAT-Einträge besitzt, wird dieses Attribut automatisch vergeben. Der Zugriff auf diese Datei wird durch das Anlegen einer Turbo FAT beschleunigt.
Purge	Eine Datei mit diesem Attribut kann nach dem Löschen durch SALVAGE nicht mehr wiederhergestellt werden.
Read Audit	Dieses Attribut wird derzeit noch nicht unterstützt. Sie können das Attribut zwar setzen, es hat aber keinerlei Wirkung.
Read-Only	Wenn Sie dieses Attribut vergeben, setzt NetWare automatisch die Attribute <i>Delete Inhibit</i> und <i>Rename Inhibit</i> . Die Datei kann dann nur noch gelesen werden, ein Überschreiben, Löschen oder Umbenennen der Datei ist nicht mehr möglich.
Rename Inhibit	Die Datei kann nicht umbenannt werden, auch wenn Sie das Modify-Recht besitzen. (Sie können mit dem Modify-Recht natürlich das <i>Rename Inhibit</i> ändern und dann umbenennen.)
Shareable	Die Datei kann von mehreren Benutzern gleichzeitig geöffnet werden. Wird hauptsächlich für netzwerkfähige Programme benötigt.
System	Die Datei wird beim Auflisten des Directory-Inhalts nicht angezeigt. Wird hauptsächlich von NetWare für NetWare-Dateien verwendet.

15 Novell NetWare 3.2

Transactional	Um Dateien mit Hilfe des TTS-Systems zu schützen, muß dieses Attribut vergeben worden sein.
Write Audit	Dieses Attribut wird derzeit noch nicht unterstützt. Sie können es zwar setzen, es hat aber noch keinerlei Auswirkung. Auf Directory-Ebene können folgende Attribute vergeben werden:
Delete Inhibit	Das Directory kann nicht mehr gelöscht werden, auch wenn Sie das Erase-Recht besitzen. Dateien des Directory können nach wie vor gelöscht werden, wenn Sie das Erase-Recht hierfür besitzen.
Hidden	Das Directory wird beim Auflisten nicht angezeigt. Wenn Sie die Berechtigung dazu besitzen und wissen, wie das Directory heißt, können Sie in dieses jedoch zum Beispiel mit CD wechseln.
Purge	Alle Dateien, die Sie in diesem Directory löschen, können mit SALVAGE nicht mehr restauriert werden. Die Dateien sind physikalisch auf der Platte nicht mehr vorhanden.
Rename Inhibit	Das Directory kann nicht mehr umbenannt werden, auch wenn Sie das Modify-Recht besitzen. Dateien in diesem Directory können nach wie vor umbenannt werden, wenn Sie das Modify-Recht hierfür besitzen und die Dateien nicht mit dem Attribut <i>Rename Inhibit</i> versehen worden sind.
System	Das Directory wird beim Auflisten der Directories nicht mehr angezeigt. Dieses Attribut verwendet NetWare für spezielle NetWare-Directories.

15.18 File-Server-Sicherheit

Unter NetWare 3.2 werden alle Module, die zum Server-Betrieb notwendig sind (LAN-Driver, Disk-Driver, Management-Utilities, zusätzliche Server-Module), als NetWare Loadable Modules (NLM) realisiert. Jedes NLM kann im laufenden Server-Betrieb geladen und auch wieder entladen werden. NLMs können dabei von Diskette, von der internen Platte des File-Servers oder von einem Server-Volume geladen werden. Damit nicht jeder Mitarbeiter, der physikalischen Zugriff zum File-Server hat, beliebig NLMs laden und wieder entladen kann, bietet NetWare 3.2 hierfür zwei Sicherheitsmechanismen an.

1. Das Keyboard der Server-Console kann über ein Modul, das am File-Server läuft, verriegelt werden. Nur der Supervisor oder die Person, die das Keyboard verriegelt hat, kann es wieder freigeben. Erst wenn die Console entriegelt ist, können wieder Console-Befehle eingegeben werden.

15.19 Das Open Data-Link Interface

2. An der Console kann der Befehl `SECURE CONSOLE` eingegeben werden. Damit wird der Server in einen sogenannten `SECURE`-Status versetzt. In diesem Status können NLMs nur noch aus einem Verzeichnis auf der Server-Platte geladen werden. Es handelt sich dabei um das Volume `SYS` und das Unterverzeichnis `SYSTEM`. Auf dieses Verzeichnis hat nur der Supervisor Zugriff. Das heißt, der Supervisor ist dafür verantwortlich, daß sich in diesem Verzeichnis nur NLMs befinden, die zum File-Server-Betrieb notwendig sind. Ein Laden von NLM über das Diskettenlaufwerk oder die interne Festplatte am File-Server ist dann nicht mehr möglich. Zugleich wird in diesem Status `DOS` aus dem Hauptspeicher des Servers entfernt.

NetWare 3.2 unterstützt SFT II als Sicherheitsstandard mit allen hierfür angebotenen Mechanismen. Eine SFT III gibt es für NetWare 3.2 nicht, da dieser Sicherheitsstandard nur von NetWare 4.11 angeboten wird. Wer jedoch unter NetWare 3.2 eine Art Serverspiegelung haben will, muß auf Dritthersteller zurückgreifen, die dann Produkte für die sogenannten Standby-Server-Mechanismen anbieten.

15.19 Das Open Data-Link Interface

Neben der erhöhten Leistungsfähigkeit und Funktionalität von NetWare 3.2 zeichnet sich NetWare 3.2 vor allem durch seine Transportprotokoll- und Communication-Protokollunabhängigkeit aus. Es handelt sich hierbei um neue Technologien, die maßgeblich den Erfolg von NetWare 3.2 begründen.

Wenn man die bisherigen Entwicklungen von LAN-Betriebssystemen genauer betrachtet, stellt man fest, daß File-Server bisher nur ganz bestimmte Transportprotokolle (Communication-Protokolle) und Service-Protokolle verstehen können. Für NetWare gilt zum Beispiel, daß der File-Server nur IPX als Communication-Protokoll und NCP als Service-Protokoll verstehen kann. Für die Einbindung von Workstations bedeutet dies, daß alle Workstations so angepaßt werden müssen, daß diese IPX und NCP einsetzen, um mit dem File-Server kommunizieren zu können.

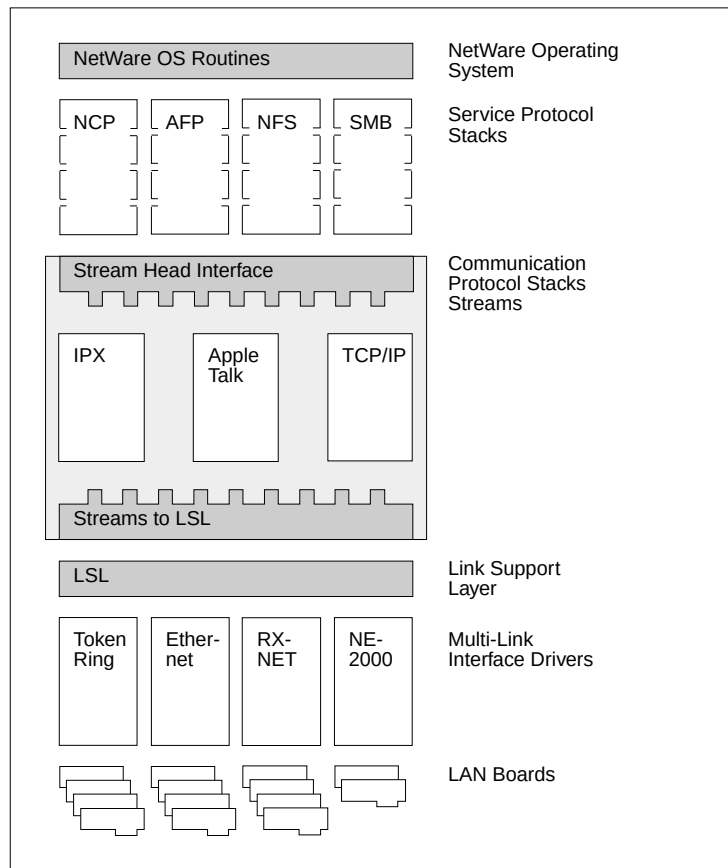
Das sieht unter NetWare 3.2 folgendermaßen aus: Der NetWare-3.2-File-Server wird auch als Multiprotokollmaschine bezeichnet. Das heißt, der File-Server ist in der Lage, mehrere Communication- und Service-Protokolle gleichzeitig zu verstehen. Dabei ist es vollkommen gleichgültig, über welche Netzwerkadapterkarte die unterschiedlichen Datenpakete eintreffen. Eine Token-Ring-Karte ist also in der Lage, neben IPX auch noch TCP/IP- oder Apple-Talk-Proto-

15 Novell NetWare 3.2

kolle zu akzeptieren. Das ist eine neue Funktion, die bisher noch nicht unterstützt wurde und NetWare 3.2 eine wesentlich höhere Flexibilität und Funktionalität verleiht.

In Abbildung 15.20 ist der funktionelle Aufbau von NetWare 3.2 dargestellt. Ich will Ihnen anschließend den Aufbau und die Funktion der einzelnen Ebenen näher erläutern.

Abbildung 15.20
NetWare-Streams-
Implementierung
unter 3.2



Maßgeblich für diesen Mechanismus ist das Open Data-Link Interface von Novell NetWare 3.2. Diese Schnittstelle bietet eine offene Kommunikationsplattform. Dadurch wird eine medien- und protokollunabhängige Kommunikation ermöglicht. Durch die offene Plattform kann NetWare 3.2 eine Vielzahl von Netzwerkkarten unterstützen und außerdem eine Vielzahl von Communication-Protokollen über dasselbe Kabelmedium gleichzeitig senden und empfangen (z.B. IPX/SPX, TCP/IP, AppleTalk).

15.19 Das Open Data-Link Interface

Die Implementierung des Open Data-Link Interface geschieht mit Hilfe mehrerer Schichten, die von einem Datenpaket durchlaufen werden müssen. Diese Schichten werden wie folgt aufgeteilt:

- Netzwerkadapterkarte und die Multi-Link-Interface-Driver-Ebene
- Link Support Layer
- Protocol Stack

15.19.1 Paketübertragung

Ohne Open Data-Link Interface schickt eine Netzwerkadapterkarte ein IPX-Paket zu einer anderen Workstation oder zu einem anderen Server, wo es vom Netzwerkadapter empfangen wird.

Der LAN-Driver der Netzwerkadapterkarte reicht das Paket zum IPX-Programm der Workstation weiter, von wo aus es entweder auf eine höhere Ebene transportiert oder an einen anderen Netzwerkadapter weitergegeben wird, um es in einen anderen Netzwerkstrang zu übertragen. Dieser Vorgang erlaubt zur gleichen Zeit nur ein Protokoll-Paket auf der Leitung, denn der LAN-Driver für die Netzwerkadapterkarte ist so konzipiert, daß nur ein spezieller Pakettyp identifiziert und akzeptiert wird, entweder ein IPX-, ein AppleTalk- oder ein TCP/IP-Paket etc.

Die NetWare-3.2-Implementierungen der Open-Data-Link-Interface-Spezifikationen unterstützen hingegen eine Vielzahl von Protokollen auf der Leitung oder der Netzwerkadapterkarte. In einem NetWare-3.2-Netzwerk kann ein Netzwerkadapter mit Hilfe der Open-Data-Link-Interface-Spezifikation jedes Paket (IPX, AppleTalk, TCP/IP etc.) zu einer anderen Workstation senden, wo dieses von der Netzwerkadapterkarte empfangen wird. Der LAN-Driver dieser Netzwerkadapterkarte kann, im Gegensatz zum LAN-Driver des NetWare-286-Netzwerks, jeden Pakettyp akzeptieren. Deshalb wird der LAN-Driver auch als Multiple Link Interface Driver (MLID) bezeichnet. Der MLID gibt das Paket zur nächsten Ebene im Open Data-Link Interface weiter, dem Link Support Layer (LSL).

Der Link Support Layer ist für die Identifizierung zuständig, d.h., er erkennt, welchen Pakettyp er erhalten hat, und gibt dieses Paket an den entsprechenden Protocol Stack in der nächsthöheren Ebene weiter. Der Protocol Stack Layer enthält eine Anzahl Protocol Stacks, wie zum Beispiel IPX, AppleTalk und TCP/IP. Trifft ein Datenpaket im entsprechenden Protocol Stack ein, wird es entweder zum nächsthöheren Layer transportiert oder über die LSL-Schnittstelle an eine MLID weitergegeben, um so über eine weitere Netzwerkadapterkarte in ein anderes Netzwerk übertragen zu werden (internes Routing von NetWare 3.2).

15.19.2 MLID Layer

Wie aus den vorherigen Beschreibungen ersichtlich ist, unterscheiden sich die NetWare-3.2-MLID-LAN-Driver wesentlich von den LAN-Drivern früherer Versionen. Ein MLID-LAN-Driver gestattet das Empfangen von mehreren unterschiedlichen Communication-Protokollen. Im Gegensatz dazu akzeptieren die NetWare-286-LAN-Driver nur das IPX Communication Protocol. Der MLID Layer führt keine Analyse des empfangenen Datenpakets durch, sondern kopiert die Information zur Identifizierung des Datenpakets in einen Receive ECB (Event Control Block) und reicht diesen ECB an den LSL-Layer weiter. Ebenso wird beim Versenden eines Datenpakets vom MLID Layer die Information zur Identifizierung des Datenpakets von einem Send ECB in ein Datenpaket kopiert und über das Netzwerk an den Empfänger verschickt.

15.19.3 Link Support Layer (LSL)

Der LSL ist eine Art Schalter, um Datenpakete zwischen dem LAN-Adapter und dem dazugehörigen MLID und den Protocol Stacks zu transportieren. Deshalb muß es Informationen über diese beiden Layer enthalten. Aus diesem Grund enthält der LSL Layer ein Daten-segment, das Informationen über den Netzwerkadapter, die Protocol-Stack-Informationen, Binding-Informationen und ECB-Informationen pflegt.

Der LSL vergibt für jeden LAN-Adapter eine logische Nummer und pflegt Informationen über jeden LAN-Adapter. Diese Information wird beim Laden festgehalten.

Obwohl der MLID Layer so konfiguriert werden kann, daß er Datenpakete für mehr als einen Protocol Stack senden und empfangen kann, sieht der LSL unter sich nur Netzwerkadapter und, verbunden mit jedem Netzwerkadapter, einen Datenblock, eine Senderoutine und eine Kontrollroutine. Obwohl Netzwerkadapter die gleiche Sende- und Empfangsroutine haben können (vom gleichen Driver gesteuert, wenn mehr als eine Netzwerkadapterkarte vom gleichen Typ eingesetzt wird), hat dies keine Auswirkung auf den LSL Layer, da jeder Netzwerkadapter immer seinen eigenen Datenblock hat.

Der LSL weist auch jedem Protocol Stack eine logische Protocol-Stack-Nummer zu und pflegt die entsprechenden Informationen über jeden Protocol Stack. Es werden bis zu 16 Protocol Stacks unterstützt.

15.19 Das Open Data-Link Interface

Zusätzlich zu den Informationen über den unter dem LSL liegenden Netzwerkadapter und den Protocol Stacks, die über dem LSL liegen, benötigt der LSL auch noch Informationen vom Event Control Block (ECB), die entweder als Receive-ECBs oder als Send-ECBs eintreffen. Der LSL benutzt die Paket-ID-Information in den ECBs und die andere Information über die Netzwerkadapter, die unterhalb des LSL liegen, und den Protocol Stacks, die oberhalb des LSL liegen, um Pakete von den Netzwerkadaptoren zu den Protocol Stacks und von den Protocol Stacks zu den Netzwerkadaptoren weiterzureichen.

Und schließlich muß der LSL auch noch eine Reihe von Routinen enthalten, um die Driver unterhalb des LSL zu unterstützen, sowie eine Reihe von Routinen zur Unterstützung der Protocol-Stacks, die über der LSL liegen. Durch den Einsatz dieser Informationen ist der LSL in der Lage, als Schalter zu dienen, um die Zusammenarbeit von Protocol-Stack/MLID und den Transport von Paketen innerhalb des Servers zu koordinieren.

15.19.4 Protocol-ID-Information

Jedes Paket auf der Netzwerkleitung besteht aus folgenden Komponenten:

- Kommunikationsprotokollpaket, z. B. IPX, TCP/IP oder Apple Talk
- Rahmen für das Medium
- Global verwalteter Wert (1 bis 6 Byte), der sich innerhalb der Medienkennung befindet. Dieser Wert wird als Protocol ID (PID) bezeichnet.

Die Protocol-ID wird in jedem Paket gesetzt und ist eine Art Label, die folgendes für das Paket kennzeichnet:

- Das Paket enthält einen bestimmten Communication Protocol Header.
- Das Paket enthält einen bestimmten Frame-Rahmen.

Wie in Abbildung 15.21 dargestellt, kennzeichnet die Protocol ID 8137h ein IPX-Paket mit einem Ethernet-II-Paketrahmen. Eine Protocol ID von FAh legt fest, daß es sich um einen AFP-Header in einem Ethernet-II-Rahmen handelt. Der LSL benutzt die Protocol ID, um das eingehende Paket an den entsprechenden Protocol-Stack weiterzugeben.

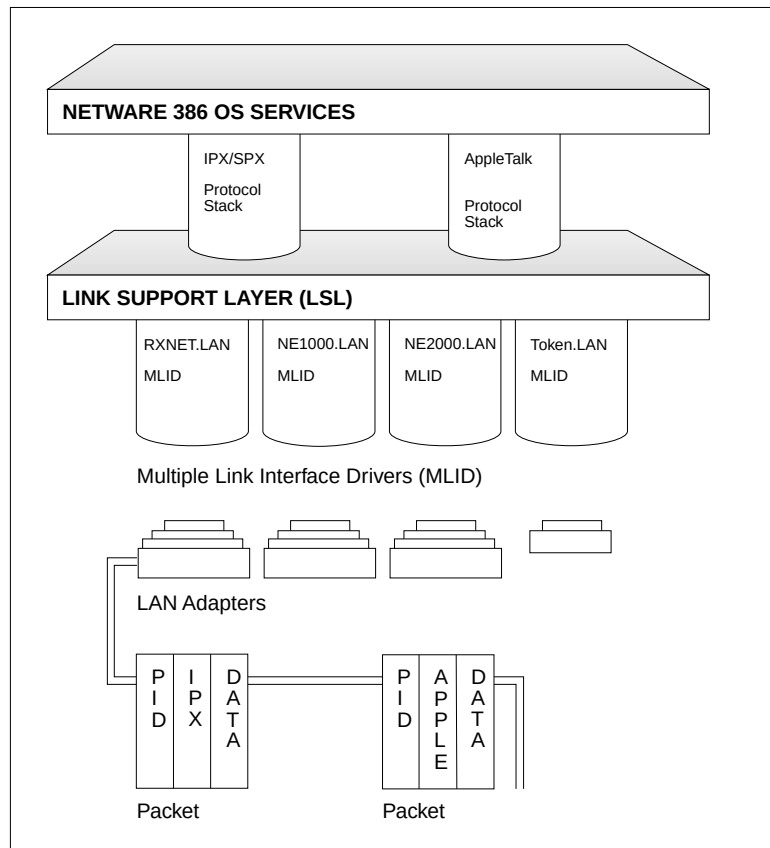
Obwohl die meisten Pakete einen PID-Eintrag besitzen, der es dem LSL erlaubt, das Paket zum richtigen Protocol-Stack zu transportieren, gibt es Pakete, die keine PID haben. Zum Beispiel enthalten Netzwerke, die Pakete mit einem 802.3-Header versenden, keine

15 Novell NetWare 3.2

PID, da diese Netzwerke nur ein Communication Protocol unterstützen. In diesen Fällen sollten die MLIDs so konzipiert sein, daß sie eingehende ECBs mit einem PID-Wert versehen.

IPX	AFP	TCP/IP
LocalTalk		
Ethernet II	8137	FA
Ethernet 802.2		
Token-Ring 802.2		
ARCNET		

Abbildung 15.21
Kennung der
Datenpakete mit
Hilfe der Protocol
ID (PID)



15.19.5 NetWare 3.2 Streams Interface

Bei den NetWare Streams handelt es sich um eine Reihe von Tools, die aus Systemaufrufen, Kernel-Ressourcen und Kernel-Utility-Routinen bestehen. Diese Tools werden benötigt, um einen Stream einzurichten, zu benutzen oder leer zu machen. Unter einem Stream versteht man einen voll duplex arbeitenden Datentransferpfad zwischen dem Driver am unteren Ende des NetWare-Betriebssystems und der Benutzeranwendung am oberen Ende.

AT&T haben die Streams entwickelt; sie sind für das Unix-V-System verfügbar. Die Streams-Implementierung für NetWare 3.2 baut auf dieser Entwicklung auf. Ein Stream legt die Schnittstelle für die Ein- und Ausgabe von Zeichen innerhalb des Kernels und zwischen dem Kernel und dem restlichen Betriebssystem fest. Ein Stream besteht aus drei wesentlichen Teilen:

- Der Stream Head, der mit Benutzeranwendungen zusammenarbeitet.
- Wahlweise eingesetzte Module, die genutzt werden, um den Datentransfer zwischen dem Stream Head und dem Stream End zu steuern.
- Stream End oder Driver, der eine Schnittstelle zur zeichenweisen Ein- und Ausgabe zur Verfügung stellt.

Die Unabhängigkeit von Medium und Protokoll ist auch einer der großen Vorteile, die in der Implementierung des Transport Level Interface (TLI) und Streams begründet sind. TLI ist eine Programmschnittstelle, die zwischen den Streams und den Benutzerapplikationen eingebettet ist und die Zusammenarbeit mit Transportprotokollen, wie zum Beispiel SPX, erlaubt.

NetWare 3.2 realisiert Streams durch eine Vielzahl von NetWare Loadable Modules (NLMs). Diese NLMs bilden die Anwendungsschnittstellen-Routinen, die Utility-Routinen für Stream-Module, die Log-Devices und Driver für das Open Data-Link Interface. Die Utility-Routinen im NLM enthalten alle gemeinsamen Funktionen, die von den Stream-Modulen benutzt werden. Andere NLMs, die getrennt geliefert werden und zur Verfügung stehen, enthalten eine große Anzahl Streams-Module, um Kommunikationsprotokolle wie IPX/SPX oder TCP/IP anbieten zu können.

Aufgrund der bisherigen Ausführungen zeichnet sich NetWare 3.2 nicht nur durch die Unabhängigkeit vom Medium aus, sondern auch durch die Transportprotokollunabhängigkeit. Als Novell die ersten Netzwerkbetriebssysteme entwickelte, gab es für LANs keine geeigneten Transportprotokolle. Die meisten Transportprotokolle wurden

15 Novell NetWare 3.2

fast ausschließlich zur Kommunikation von Hosts zu Arbeitsplatzrechnern eingesetzt und waren für eine Peer-to-Peer-Kommunikation zwischen intelligenten Endgeräten nicht geeignet. Für eine LAN-Topologie ist diese Peer-to-Peer-Kommunikation jedoch unabdingbar. Deshalb entwickelte Novell seinen eigenen Transportmechanismus. Dieser ist auf der Grundlage des Xerox Network System Protocol (XNS) aufgebaut und wird von Novell unter der Bezeichnung Internetwork Packet Exchange Protocol (IPX) vermarktet. IPX wird dazu verwendet, Anforderungen an NetWare Server zu übertragen und die Antworten des Servers zur anfordernden Station zurückzuschicken.

Der LAN-Markt hat sich jedoch weiterentwickelt. So gibt es heute nicht nur ein Transportprotokoll, das in Netzwerken eingesetzt wird. Neben IPX von Novell existieren NetBEUI/DLC von IBM, AppleTalk von Apple oder TCP/IP als universelles Transportprotokoll. Bei der Implementierung unternehmensweiter Netzwerke ist es sehr oft der Wunsch der Anwender, zentrale Netze auf Basis von Industriestandardprotokollen, wie z.B. TCP/IP oder den OSI-Protokollen, aufzubauen. In anderen Fällen reicht es aus, einen De-facto-Standard wie DECnet-Protokolle einzusetzen.

Damit alle unterschiedlichen Systeme mit dem File-Server arbeiten können, muß dieser transportprotokollunabhängig sein. Das heißt, NetWare darf nicht nur auf IPX fixiert sein, sondern muß die Möglichkeit bieten, parallel mehrere Protokolle zu unterstützen. Novell hat seit Beginn der Entwicklung den Benutzern die Freiheit gelassen, einen LAN-Adapter-Hersteller der eigenen Wahl einzusetzen. Mit NetWare 3.2 überläßt Novell den Netzwerkverwaltern auch die Wahlfreiheit, NetWare mit beliebigen Transportprotokollen einzusetzen.

Diese Transportprotokollunabhängigkeit wird für NetWare 3.2 durch zwei Komponenten erreicht: die Open-Data-Link-Interface-Schnittstelle (ODI) und die NetWare Streams. Wie bereits erwähnt, ist ODI eine Standardschnittstelle für Transportprotokolle, mit der über einen Netzwerkadapter problemlos mehrere Transportprotokolle eingesetzt werden können. Auf Hardware-Ebene stellt ODI eine konsistente Schnittstelle zu den LAN-Adapter-Treibern dar, und in ähnlicher Weise ist ODI eine konsistente Schnittstelle für die Transportprotokolle. Diese können somit unabhängig von der vorhandenen Netzwerkhardware betrieben werden.

Fremdhersteller können, wenn sie dazu bereit sind, für diese Schnittstelle Protokollstacks schreiben, damit ihre Protokolle mit jedem beliebigen Adapter, der einen ODI-Treiber verwendet, eingesetzt werden können. Ebenso ist jeder Adapter, der einen ODI-Treiber besitzt, mit jedem Protokollstack, der für diese Schnittstelle geschrieben ist, kompatibel.

15.19 Das Open Data-Link Interface

NetWare Streams bieten auf höherer Ebene eine ähnliche Sammlung von Schnittstellen. Zum einen sind die NetWare Streams eine gemeinsame Schnittstelle für die Transportprotokolle, die Daten und Anforderungen zur Bearbeitung an NetWare weiterleiten, zum anderen sind die NetWare Streams eine Schnittstelle zu NetWare selbst. Dadurch ist NetWare 3.2 in der Lage, mit jedem beliebigen Stream-unterstützten Protokoll zu kommunizieren. Da die NetWare Streams das Transportprotokoll für das Netzwerkbetriebssystem transparent machen, können die gleichen Dienste im gesamten Netzwerk zur Verfügung gestellt werden, unabhängig davon, welche Transportprotokolle eingesetzt werden. Deshalb können Netzwerkverwalter die Protokolle ihrer Wahl einsetzen und sogar die vorhandenen Protokolle ändern, ohne die Dienste, die dem Benutzer zur Verfügung gestellt werden, zu beeinträchtigen.

Neben der Unterstützung von IPX/SPX sieht Novell die Unterstützung von NetBEUI/DLC, SNA, TCP/IP und den OSI-Protokollen vor. Die unterschiedlichen Übertragungsmechanismen zwischen den Prozessen (IPC), die von Novell unterstützt werden, können durch den Einsatz der NetWare Streams die Server-Anwendungen protokollunabhängig unterstützen. NetBIOS, Named Pipes und das Transport Layer Interface (TLI) sind protokollabhängige Mechanismen, über die remote Prozesse verteilter Anwendungen miteinander kommunizieren können. Um zu garantieren, daß diese Anwendungen unabhängig vom eingesetzten Transportprotokoll auf einem NetWare-LAN eingesetzt werden können, unterstützt Novell diese IPC-Mechanismen innerhalb der NetWare-Stream-Umgebung. Auf diese Weise verlieren die IPC-Mechanismen ihre Protokollabhängigkeit, und die für sie geschriebenen Applikationen laufen in einer protokollunabhängigen Umgebung.

Für TCP/IP unterstützt NetWare unter anderem Telnet, FTP, SMTP, die R-Utilities und andere anerkannte TCP/IP-Anwendungen. Für die OSI-Umgebung unterstützt NetWare die bekanntesten OSI-Anwendungen, wie z.B. X.400.

Ich habe bereits darauf hingewiesen, daß bei der Entwicklung von NetWare keine leistungsfähigen Client-Server-Protokolle zur Verfügung standen. Um Benutzern die LAN-Funktionen verfügbar zu machen, wurde von Novell ein eigenes Client-Server-Protokoll, das NetWare Core Protocol (NCP), entwickelt. Dieses NCP wurde anfänglich speziell für DOS-Anwender entwickelt und wird inzwischen auch für OS/2-Anwender unterstützt.

Der LAN-Markt hat sich im Lauf der Zeit weiterentwickelt, und mit dieser Entwicklung wurden auch andere Client-Server-Protokolle zur Verfügung gestellt. Neben NCP sind heute als gängige Client-Server-

15 Novell NetWare 3.2

Protokolle das Server-Message-Block-Protokoll (SMB) für OS/2-Arbeitsplätze, das AppleTalk Filing Protocol (AFP) von Apple, das TOPS Filing Protocol (TOPS) von Sun Microsystems für Apple-Macintosh-Arbeitsplätze und das Network File System (NFS) von Sun Microsystems für Unix-Arbeitsplätze im Einsatz.

Anhand dieser Beispiele können Sie ersehen, daß Client-Server-Protokolle gewöhnlich für eine bestimmte Art Arbeitsplatzrechner entwickelt und eingesetzt werden. NCP zum Beispiel ist zwar für DOS und OS/2 sehr gut geeignet, kann aber die AFP-Funktionen unter normalen Umständen nicht unterstützen, um Macintosh-Systeme in ein Novell-Netzwerk einbinden zu können. Der entsprechende Vergleich kann für SMB, NFS oder jedes andere Client-Server-Protokoll angeführt werden.

Statt nun alle Arbeitsplatzrechner auf eine einheitliche Client-Server-Protokollebene zu drücken – damit wäre keinem so recht gedient –, entschied man sich bei Novell, auf dem Server unterschiedliche Client-Server-Protokolle zu unterstützen. Mit der Unterstützung der jeweils betriebssystemeigenen Server-Protokolle kann garantiert werden, daß das Workstation-Betriebssystem vollen Zugriff auf alle NetWare-Dienste hat, ohne den ursprünglichen Funktionsumfang zu verlieren. Man spricht auch davon, daß die Workstation im Native Mode eingebunden wird, d. h. in ihre ureigene Umgebung. Neben NCP wird von Novell auch AFP von Apple unterstützt. Durch die Implementierung von Unix Services ist man in der Lage, alle Komponenten zu installieren, um eine Unix-Workstation als Client unter NetWare betreiben zu können. In diesem Fall werden die NFS-Dienste auf dem NetWare Server installiert, um allen NFS-Clients die Möglichkeit zu geben, NetWare Volumes bzw. Directories so zu nutzen, als wären es herkömmliche Unix-Verzeichnisse. Durch die Integration der NFS-Dienste unter NetWare müssen auch alle sicherheitsrelevanten Einrichtungen durchgeführt werden, so daß nur die Anwender auf die Verzeichnisse zugreifen dürfen, an die Berechtigungen vergeben wurden. Es kann mit den Unix Services jedoch auch der umgekehrte Mechanismus aufgebaut werden. In diesem Fall »mountet« der NetWare Server ein Unix-Verzeichnis so, als wäre es ein NetWare Volume. Somit können alle berechtigten NetWare-User auf diese Verzeichnisse, sprich Volumes, zugreifen. Damit jedoch nicht genug. Durch die Installation der Print Services ist man in der Lage, Unix-Drucker unter NetWare zu nutzen und umgekehrt unter Unix ebenso transparent auf NetWare-Drucker die Druckaufträge auszugeben. Hierzu setzen die Unix Services auf dem LPD-Protokoll auf.

15.20 NetWare Loadable Modules (NLMs)

Mit NetWare 3.2 wurde im Vergleich zu den Vorgängerversionen 2.x ein komplett neues Konzept für die Multi-Tasking-Umgebung geschaffen. Dieses generelle Konzept hat auch bezüglich der NLM-Technik für NetWare 4.x und NetWare 5.x Gültigkeit.

Das Betriebssystem NetWare 3.2 weist diesbezüglich eine weit größere Flexibilität auf. Der Kernel von NetWare ist das einzige ausführbare Programm, das bei der Installation von NetWare 3.2 benötigt wird. Es handelt sich dabei um die SERVER.EXE. Zum Starten des File-Servers wird SERVER.EXE gestartet, und jedes andere Modul, z.B. LAN-Driver, Disk-Driver, Management-Programm etc., wird im laufenden Betrieb geladen und bei Bedarf wieder entladen. Man spricht auch davon, daß NetWare 3.2 aus dem Kernel-Betriebssystem und einer Sammlung von Run-Time-Loadable-Modules besteht. Das DOS-Betriebssystem ist deshalb notwendig, weil Novell keinen Bootstrap-Loader mehr entwickelt hat. DOS wird somit als Mittel zum Zweck benötigt. Es darf jedoch nicht der Fehler gemacht werden, jetzt den Schluß zu ziehen, NetWare würde unter DOS laufen. Nach dem Starten der SERVER.EXE schaltet das Ladeprogramm den Rechner in *Protected Mode* und stellt somit die volle Leistungsfähigkeit des Prozessors zur Verfügung. Ab diesem Zeitpunkt, wenn durch die SERVER.EXE auch die System Executive aktiv ist, kann mit der Erweiterung des Betriebssystem-Kernels durch Laden der NLMs begonnen werden.

Bei den NLMs handelt es sich um Programme, die zusammen mit dem Betriebssystem NetWare 3.2 im Hauptspeicher des Servers laufen. Sobald ein NLM geladen worden ist, wird es Bestandteil von NetWare 3.2. Das heißt, NLMs können über den Aufruf von internen Betriebssystem-Routinen auf NetWare-Dienste zugreifen, ohne auf Service-Protokolle zugreifen zu müssen.

Der Betriebssystem-Kernel wird durch das Starten von SERVER.EXE aktiviert. Alle weiteren Funktionen und Driver werden durch das Laden der entsprechenden NLMs aktiviert. Das Laden von NLMs erfolgt über den Befehl LOAD an der Server-Console. NLMs werden derzeit in vier Gruppen eingeteilt, wobei jede Gruppe durch eine spezielle NLM-Extension gekennzeichnet ist. Folgende Extensionen werden unterschieden:

- LAN-Driver besitzen die Extension .LAN.
- Disk-Driver besitzen die Extension .DSK.
- Utilities besitzen die Extension .NLM.
- Name-Space-Module besitzen die Extension .NAM.

15 Novell NetWare 3.2

Sobald ein NLM an der Server-Console über den Befehl LOAD geladen ist, wird das Modul durch den NetWare LOADER direkt an das Betriebssystem gebunden. Nach dem Laden verhält sich das Modul so, als wäre es direkt als Bestandteil von NetWare 3.2 programmiert worden.

NLMs können im laufenden Betrieb von der DOS-Partition einer Platte geladen werden, vom A- oder B-Diskettenlaufwerk, vom Volume SYS:SYSTEM oder jedem anderem Volume und Subdirectory-Pfad auf der Serverplatte. Nach dem erstmaligen Starten von NetWare 3.2 müssen Sie zum Beispiel das NLM INSTALL aktivieren, um alle notwendigen Installationsschritte durchzuführen, so daß Sie anschließend den Server in Betrieb nehmen können. Zum Laden des INSTALL NLM geben Sie zum Beispiel ein:

```
LOAD A:INSTALL
```

Wenn Sie mit der Installation fertig sind, können Sie das NLM wieder entfernen (dies gilt auch für jedes andere NLM). Durch das Entladen von NLMs werden alle belegten Ressourcen, die von diesem NLM beansprucht worden sind, wieder freigegeben (z.B. Speicher, Interrupt-Vektoren, I/O-Ports etc.). Zum Entladen des INSTALL NLM geben Sie an der Server-Console ein:

```
UNLOAD INSTALL
```

Es sei an dieser Stelle betont, daß durch das NLM-Konzept das Netzwerkbetriebssystem wesentlich flexibler und auch einfacher zu verwalten ist. Alle Module (Driver, Utilities etc.) müssen als NLM zur Verfügung stehen. Die von Novell angebotenen Module zum Einbinden von Macintosh-Rechnern, TCP/IP-Unterstützung, NFS-Unterstützung, OSI- und FTAM-Protokolle werden als NLM zur Verfügung stehen.

15.21 Neuerungen von NetWare 3.2

Die Änderungen von NetWare 3.2 im Vergleich zur Vorgängerversion 3.12 sind nicht so groß, daß sie vom normalen Anwender bemerkt würden. Eine Umstellung von 3.12 auf 3.2 wird der normale Anwender also gar nicht erkennen. Für den Netzwerkverwalter hingegen sind Zusätze eingebaut, die allgemein recht nützlich und hilfreich sein können. Generell sind in NetWare 3.2 alle Patches eingebaut, die bislang manuell in NetWare 3.12 eingespielt werden mußten. Der Kernel von NetWare 3.2 wurde drastisch verkleinert, da intern viele Optimierungen durchgeführt worden sind. Des weiteren hat man Sicherheitsfunktionen eingebaut, die ebenfalls für NetWare 3.1x manuell geladen werden mußten. Zur Optimierung der NetWare 3.2 sind

15.21 Neuerungen von NetWare 3.2

Funktionen wie Packet Burst Mode und Large Internet Packet Facility, ebenfalls integraler Bestandteil von NetWare 4.x, bereits in das Netzwerkbetriebssystem integriert worden. Lassen Sie uns die durchgeführten Änderungen näher betrachten.

NCP Packet Signature

Holländischen Studenten ist es unter NetWare 3.12 gelungen, durch geschickte Datenpaketmanipulation den unberechtigten Zugriff am Server als Supervisor zu erhalten. Nachdem dies bei Novell bekannt geworden war, wurde für NetWare 3.12 sofort ein Zusatz-NLM entwickelt (PBURST.NLM), um dies zu unterbinden (in Verbindung mit einer neuen Workstation-Shell). Diese bislang zusätzliche Funktion ist in NetWare 3.2 fest eingebaut und als NCP Packet Signature bekannt.

Dabei handelt es sich um einen erweiterten Sicherheitsmechanismus, der Server und Workstation vor unbefugten Manipulationen durch das NCP (NetWare Core Protocol) schützt. Jetzt sind Server und Workstation gezwungen, jedes Paket, das zwischen Server und Workstation transportiert wird, durch Hinzufügen einer Signature zu kennzeichnen. Die Signature ändert sich dadurch mit jedem Paket. Die Performance im Netzwerk wird dabei etwas reduziert, so daß sich jeder Netzwerkverwalter die Frage stellen wird, ob dieser Mechanismus auch wirklich nötig ist. Es steht im Entscheidungsbereich des Netzwerkverwalters, ob mit Packet Signature gearbeitet werden soll oder nicht. In einer sicheren Netzwerkumgebung kann also auf diesen Mechanismus verzichtet werden.

NetWare DOS Requester und VLMs

Bezüglich der Workstation-Umgebung hat Novell ebenfalls eine neue Strategie entwickelt. Nach über zehnjährigem Einsatz hat man sich von der altbekannten Shell-Umgebung verabschiedet und setzt auf die bessere und leistungsfähigere DOS-Requester-Umgebung. Diese neue Workstation-Software wurde zuerst mit NetWare 4.x eingeführt und steht jetzt auch standardmäßig für NetWare 3.2 und Personal NetWare zur Verfügung. Eine nähere Beschreibung dieser Umgebung finden Sie im Kapitel über NetWare 4. Die wichtigsten Funktionen sind:

- Unterstützung von Bindery-Servern, NDS-Servern und Personal NetWare (gleichzeitig).
- Modulare Architektur, die sich jederzeit um weitere Funktionalitäten erweitern läßt.

15 Novell NetWare 3.2

- Die Vorteile der automatischen Auslagerung in Extended oder Expanded Memory und die Nutzung der DOS-Redirection-Funktionen werden angeboten.
- Beinhaltet automatisch das Packet Burst Mode Protokoll und die Large Internet Packet Facilities.
- Beinhaltet ein Modul zur Unterstützung der bislang im Einsatz befindlichen NETX, so daß die Kompatibilität zu alten Shell-Versionen erhalten bleibt.

Auslieferung auf CD-ROM

NetWare 3.2 wird wie NetWare 4.x und NetWare 5 auf CD-ROM ausgeliefert. Dadurch wird die Installation einfacher und schneller. Wenn Sie NetWare 3.2 auf CD-ROM einsetzen, dann finden Sie auf der CD-ROM ebenfalls wie bei NetWare 4.x die gesamten Handbücher als elektronischen Text auf der CD. Sie können sich somit die gesamte Dokumentation unter Windows am Bildschirm betrachten und lesen. Bei Bedarf können Sie aber auch einen eigenen Satz Dokumentation bestellen. Im kleinen Paket der NetWare 3.2 auf CD-ROM findet man nur noch die Handbücher zur Installation: das Installations- und Upgrade-Handbuch und einen Satz Kurzübersichten der Installation der einzelnen NetWare-Umgebungen.

NetWare 3.2 gibt es aber auch auf Diskette. In diesem Fall erhalten Sie einen vollen Satz gedruckter Dokumentation, da die Anzahl Disketten zu groß sein würde, wenn man auch den Electronic Text auf Diskette ausliefern würde.

Neue Migration und In-Place Upgrade Utilities

Für die Umstellung von NetWare 2.x/3.12 oder LAN-Server stellt NetWare 3.2 ein neues Utility zur Verfügung. Für die Server-Umstellung muß in diesem Fall ein neuer Server mit NetWare 3.2 installiert sein. Das Migration Utility wird auf einer Workstation gestartet, wobei der Netzwerkverwalter an der Workstation an beiden Servern angemeldet sein muß. Mit diesem Utility müssen Sie dann den Source Server und den Destination Server auswählen. Nach Auswahl der Komponenten, die auf den neuen NetWare 3.2 Server übernommen werden sollen, erfolgt die Übertragung der Informationen auf den NetWare 3.2 Server. Innerhalb kürzester Zeit haben Sie einen neuen NetWare 3.2 Server. Auf dem NetWare 2.x/3.x Server oder LAN Server werden keine Änderungen durchgeführt. Für den Fall, daß während der Umstellung irgendwelche Fehler auftreten, kann dieser Vorgang beliebig oft wiederholt werden.

15.21 Neuerungen von NetWare 3.2

Wenn für die Umstellung auf NetWare 3.2 kein neuer Server benutzt werden soll, stellt NetWare 3.2 ein sogenanntes In-Place Utility zur Verfügung, das als NLM gestartet werden muß. Hierfür wird der alte NetWare 2.x/3.x Server umgestellt, indem auf der alten Hardware das In-Place Upgrade NLM gestartet wird. Es werden daraufhin alle notwendigen Umstellungen durchgeführt, um anschließend den neuen NetWare 3.2 Server verfügbar zu haben. Das heißt, Sie benötigen in diesem Fall keine neue Hardware. Da die Umstellung auf der gleichen Server-Hardware durchgeführt wird, wäre es sehr kritisch, wenn bei dieser Umstellung Fehler auftreten würden, die mit einem Datenverlust auf den Platten verbunden sind. Um diese Gefahr zu vermeiden, sollte auf alle Fälle vor der In-Place-Upgrade-Methode eine vollständige Datensicherung durchgeführt werden, so daß bei Bedarf der alte Server-Zustand wiederhergestellt werden kann.

CD-ROM-Unterstützung

Nicht nur, daß NetWare 3.2 auf CD-ROM ausgeliefert wird, es besteht auch die Möglichkeit, standardmäßig unter NetWare 3.2 CD-ROMs als Volume zu mounten. Wie bei NetWare 4.x werden mit NetWare 3.2 alle notwendigen NLMs ausgeliefert, um CD-ROMs anschließend als NetWare Volumes bereitstellen zu können. Es muß sich dabei um CD-ROM Laufwerke handeln, die an Controllern angeschlossen sind, für die auch Disk-Driver zur Verfügung stehen, z.B. Adaptec Controller. Für Mitsumi-Laufwerke stehen zum Beispiel noch keine NLMs zur Ansteuerung der Controller-Karte zur Verfügung stehen. Es kann dann zwar die Installation über CD-ROM darüber durchgeführt werden, da die Ansteuerung unter DOS erfolgt, anschließend kann das Mitsumi-Laufwerk jedoch nicht als Volume unter NetWare 3.2 eingebunden werden.

Nationale Tastaturunterstützung

Es wurde immer wieder bemängelt, daß nach dem Starten des NetWare-Servers die Server-Console nur eine amerikanische Bedienung anbietet. Da an den meisten Servern deutsche Tastaturen angeschlossen sind, tat man sich schwer, auf Anhieb spezielle Tasten zu finden, z.B. »=«, oder besondere Buchstaben (wie die deutschen Umlaute). Auch dies ist inzwischen mit Hilfe eines neuen NLM lösbar. Hierzu muß an der Server-Console nur das KEYB.NLM mit Angabe der Nationalität gestartet werden, und der Server unterstützt anschließend die richtige Tastatur. Will man zum Beispiel den deutschen Tastaturtreiber an der Server-Console aktivieren, muß nur `LOAD KEYB germany _i-` eingegeben werden.

15 Novell NetWare 3.2

Des weiteren stehen folgende Nationalitätsunterstützungen zur Verfügung: United States, France, Italy, Spain.

Not-Logged-In Clear

Unter NetWare 3.2 bedeutet das Laden der Workstation-Software, daß anschließend am Server eine User Connection belegt ist (Not-Logged-In), die für andere Benutzer dann nicht mehr zur Verfügung steht. Dies ist vor allem dann problematisch, wenn Sie mehr Workstations im Netzwerk haben, als Ihre NetWare-Lizenz unterstützen kann. Wenn in diesem Fall alle Anwender ihren Rechner einschalten, belegt jeder aktive Rechner eine Connection am Server, auch wenn der Benutzer noch kein Login durchgeführt hat. Um nicht genutzte Connections frei zu bekommen, die belegt sind, weil der Anwender gemeint hat, seinen Rechner einschalten zu müssen, ohne effektiv arbeiten zu wollen (also noch keinen Login durchgeführt hat), nutzt man das NLM NLICLEAR. NetWare 3.2 löscht in diesem Fall nach einer gewissen Zeit alle Not-Logged-In-Verbindungen.

Ethernet Frame

Schon seit längerer Zeit hat Novell Änderungen beim Einsatz neuer Ethernet-LAN-Driver durchgeführt. Diese Änderungen betreffen sowohl den LAN-Driver für den Server als auch für die Workstation. Bislang unterstützte Novell standardmäßig den Ethernet_802.3 Frame. Mit Einführung von NetWare 4.x wird beim Laden der LAN-Driver, wenn nicht explizit etwas anderes angegeben wird, der Frame Ethernet_802.2 aktiviert. Dies wäre alles nicht so tragisch, wenn es sich um eine komplette Neuinstallation handelte. Wenn Sie jedoch bereits Server und Workstations im Einsatz haben, werden diese mit dem Ethernet_802.3 Frame betrieben. Bei der Installation neuer Systeme werden diese mit Ethernet_802.2 Frames aktiviert, sofern Sie beim Einrichten der Umgebung nicht explizit den alten Frame-Typ spezifizieren. Es ist bei diesen Konfigurationen zu beachten, daß ein System, das auf Ethernet_802.3 eingestellt ist, keine Pakete verarbeiten kann, die mit einem Ethernet_802.2 Frame betrieben werden und umgekehrt. Sie sollten deshalb darauf achten, daß das IPX-Netzwerkprotokoll im Ethernet immer über den gleichen Frame-Typ transportiert wird. Es wäre zwar auch möglich, den Server mit beiden Frame-Typen zu konfigurieren, um das IPX-Protokoll auf beide Frames zu legen, dies verursacht jedoch einen zusätzlichen Protokoll-Overhead auf der Netzwerkleitung.

15.21 Neuerungen von NetWare 3.2

NetWare Patches

Alle bislang für NetWare 3.12 verfügbaren Patches sind bereits im Kernel von NetWare 3.2 eingearbeitet worden. Somit müssen die für NetWare 3.12 verfügbaren Patches nicht mehr explizit in NetWare 3.2 eingespielt werden.

Sie sehen, daß die Änderungen von NetWare 3.2 im Vergleich zu NetWare 3.12 nicht sehr groß sind. Funktionell sind im Prinzip keine Änderungen durchgeführt worden. Man hat nur an der einen oder anderen Stelle kleinere Modifikationen durchgeführt, um NetWare 3.2 noch optimieren zu können.

Entweder kann NetWare 3.2 als vollständiges Produkt gekauft oder ein bestehender NetWare 3.12 Server kann über das NetWare 3.2 Enhancement Pack auf NetWare 3.2 umgestellt werden. Wenn Sie eine vollständige NetWare 3.2 kaufen, dann erhalten Sie allerdings auch eine NetWare 3.12 (die zuerst installiert werden muß) und das NetWare 3.2 Enhancement Pack, das nach der Installation von NetWare 3.12 installiert werden muß. Das heißt, in beiden Fällen wird ein Update auf NetWare 3.2 mit Hilfe des NetWare 3.2 Enhancement Pack durchgeführt.

Erst nach der Installation dieses NetWare 3.2 Enhancement Pack sind alle Patches (inklusive Year-2000-Ready-Mechanismen) und die nachfolgend aufgeführten Funktionen vorhanden:

Vereinfachte Netzwerkadministration

Durch die Installation des NetWare 3.2 Enhancement Pack wird auch ein grafisches Administrationstool für das Einrichten und Verwalten der gesamten Benutzerumgebung installiert. Neben diesem Tool stehen weitere Verwaltungsprogramme zur Verfügung, die für das Arbeiten unter NetWare 3.2 sehr vorteilhaft sind. Hierzu zählen:

- *CRON.NLM*

Mit diesem NLM ist man in der Lage, am Server zeitgesteuert Module laden und entladen zu lassen. So kann man z.B. vor der Datensicherung eine Datenbank entladen lassen und nachdem die Datensicherung gelaufen ist, diese automatisch wieder laden. In einer Datei CRONTAB werden dazu alle notwendigen Angaben durchgeführt, welches Modul wann geladen bzw. entladen werden soll.

- *CONFIG.NLM*

Bislang war es nicht ganz einfach, mit einem Blick den Modulstand des Systems zu erfassen und zu erkennen, welche Module überhaupt geladen sind. Zur einfacheren und besseren Auswer-

15 Novell NetWare 3.2

tung stellt Novell hierfür das CONFIG.NLM zur Verfügung. Nachdem dieses Modul gestartet ist, werden alle relevanten Informationen in die Datei Config.txt geschrieben. Mit Hilfe des Config Reader können diese Informationen ausgewertet werden.

■ *Config Reader*

Der Config Reader CFGREADR.EXE für Windows 95 bzw. Windows NT ist in der Lage, den Inhalt der oben genannten Config.txt nicht nur zu lesen, sondern auch auszuwerten. Über eine Config-Datei, die über das Internet immer wieder aktualisiert werden muß, weiß der Config Reader auch über alle Patch-Level-Stände Bescheid und gibt zum Beispiel aus, welche Module auf dem Server älteren Datums sind und durch welchen Patch-Level sie aktualisiert werden müssen. Ebenso ist man in der Lage, Config.txt-Dateien von zwei unterschiedlichen Servern miteinander zu vergleichen, um zu erkennen, worin sich die Modulstände auf den jeweiligen Servern unterscheiden. Nicht zuletzt bekommt man auch eine Auswertung, ob die gewählten Interrupts für den Server korrekt gewählt sind.

■ *TBACKUP.EXE*

Man steht immer wieder vor dem Problem, daß die Trustee-Rechte und die Inherited Rights Mask der Verzeichnisse und Dateien nach versehentlichen Löschungen zum Beispiel mit Hilfe der Datensicherung restauriert werden müssen. Das Programm Tbackup.exe leistet hierbei sehr gute Dienste, indem man alle Informationen der Trustee-Zuweisungen und Inherited Rights Mask in die Datei Trestore.bat schreiben läßt. In dieser Batch-Datei stehen dann bereits die richtigen Befehle zum Setzen der ursprünglichen Rechte und Filter für Verzeichnisse und Dateien. Ist nur ein Teil dieser Zuweisungen durchzuführen, muß man nur die entsprechenden Passagen aus dieser Batch-Datei kopieren.

■ *TCOPY.EXE*

Mit diesem Programm ist man in der Lage, beim Kopieren von Verzeichnissen auch die Zugriffsberechtigungen kopieren zu lassen. Beim herkömmlichen Kopiervorgang werden diese Berechtigungen nicht kopiert, so daß man mit diesem Tool eine entsprechende Erleichterung erfährt.

Es sei an dieser Stelle darauf hingewiesen, daß die neuen strategischen Produkte von Novell NetWare 4 und NetWare 5 sind. Bestimmte Mechanismen und Eigenschaften, die NetWare 3.2 beinhaltet, sind ebenso in NetWare 4 enthalten. Andere Bereiche und interne Funktionen sind jedoch unter NetWare 4 grundlegend neu. Dies beginnt bei der NDS im Vergleich zu den Bindery-Diensten und endet bei den administrativen Funktionen. Man darf sich nur nicht

15.21 Neuerungen von NetWare 3.2

von diesen neuen Versionen abschrecken lassen und muß immer bedenken, daß sich auch NetWare 4 und NetWare 5 so einfach einrichten lassen, daß die Administration ähnlich »unkompliziert« wird, wie dies bei NetWare 3.2 der Fall ist. In einem Punkt sind sich NetWare 3.2/NetWare 4/NetWare 5 ähnlich: Alle drei Systeme haben eine grafische Administrationsoberfläche. Hierzu mehr in den nachfolgenden Kapiteln.

16

Novell NetWare, das fehlertolerante System

Ausfälle jeglicher Art verursachen unerwünschte Unterbrechungen in der Datenverwaltung. Wesentlich gravierender aber sind die dabei auftretenden Beschädigungen oder Datenverluste bei gemeinsam benutzten Datenbeständen. Im Single-User-Betrieb ist vom Ausfall des Rechners nur eine Person betroffen, im Netzwerk dagegen sind alle davon betroffen, die mit dem File-Server arbeiten. Dateien, Indexdateien, Baumstrukturen und periphere Geräte können durch unkontrollierte Ausfälle beschädigt werden. Der Ausfall kann dabei von einer Station ausgehen und das Übertragungsmedium, den File-Server oder gar die Platteneinheiten betreffen.

Im Bereich der Großrechner-DV wird dieses Problem seit langem erfolgreich bekämpft, allerdings sind die dazu nötigen Maßnahmen immer mit sehr hohen Hard- und Software-Kosten verbunden. Zudem werden die Lösungen von den Herstellern meist nur für den eigenen Computer angeboten.

Grundsätzlich muß dieser Schutz durch den vermehrten Einsatz von PCs, MDTs und Host-Systemen für all diese Systeme zur Verfügung stehen. Novell hat deshalb von vornherein eine Reihe von Sicherheitsmaßnahmen in das Netzwerkbetriebssystem integriert. Die Systemfehlertoleranz deckt folgende Bereiche ab:

- Duplizierung von Plattenverzeichnissen
- Duplizierung der File Allocation Table
- Read after Write Verification
- Fehlererkennung und Korrektur
- Directory-Überprüfung bei Power-up
- Bindery-Überprüfung bei Power-up
- UPS Monitoring

Außerdem gibt es zu diesen Mechanismen, die jede NetWare-Version abdecken, das Netzwerkbetriebssystem in drei unterschiedlichen Sicherheitsstufen: SFT I, SFT II und SFT III. Die Mechanismen SFT I und SFT II werden von NetWare 3.2 und NetWare 4 uneingeschränkt unterstützt. Der Mechanismus SFT III wird nur noch unter NetWare 4 angeboten.

16.1 SFT Level I

Ein fehlerhaftes Speichermedium führt in zahlreichen Fällen zu Anwendungs- und Netzwerkausfällen. Jedes Betriebssystem führt zwar bei der Formatierung einer Platte entsprechende Schritte durch, um defekte Sektoren erkennen und markieren zu können (Eintrag in eine Bad-Block-Table), es entstehen jedoch mit fortschreitender Alterung der Platte neue Defekte, die von den bisherigen Betriebssystemen nicht mehr behoben werden können. Von MS-DOS kennt jeder die Fehlermeldung: Fehler beim Lesen/Schreiben ABORT, RETRY, IGNORE. Ähnliche Reaktionen im Netzwerkbetrieb deckt Novell NetWare SFT I ab. Diese Version bedient sich mehrerer Techniken, um die Probleme, die sich durch nachträglich auftretende defekte Sektoren ergeben, zu lösen.

16.1.1 Das Kontrolllesen

Die SFT I führt nach jedem Schreiben von Datenbeständen ein Kontrolllesen durch. Dieses Verfahren stellt sicher, daß die geschriebenen Daten wenigstens einmal abgerufen werden können und zum Zeitpunkt des Abspeicherns korrekt auf der Platte stehen. Die Wahrscheinlichkeit von Fehlern bei künftigen Leseoperationen wird dadurch herabgesetzt.

16.1.2 Der Hot-Fix-Mechanismus

Ergänzt wird das Kontrolllesen durch einen Mechanismus, der Hot Fix genannt wird. Mit dieser Methode kann NetWare auftretende Plattenfehler während der Verarbeitung behandeln. Für den Hot-Fix-Mechanismus sollten ungefähr zwei Prozent jeder Platte als Reservebereich verwendet werden. Stellt NetWare beim Kontrolllesen fest, daß der Sektor, auf den gerade geschrieben worden ist, defekt ist, holt sich Novell aus dem Reservebereich einen neuen Sektor und schreibt darauf den Datenbestand. Somit ist gewährleistet, daß die Daten korrekt auf die Platte abgespeichert werden. Diese Maßnahme gilt jedoch nur für Schreiboperationen. Ein Sektor kann aber beim Abspeichern noch intakt gewesen sein und erst später zerstört werden, so daß im Lauf der Zeit beim Lesen Fehler auftreten. Diese Gefahrenquelle wird unter anderem durch SFT II von Novell abgedeckt.

16.1.3 Redundante Dateisystemkomponenten

Die Zuverlässigkeit und die Korrektheit von Systemen kann durch Redundanz verbessert werden. Deshalb arbeitet NetWare mit einem doppelten Dateiverzeichnis und einer doppelten File Allocation Table. Beide Komponenten werden bei Veränderungen ständig abgeglichen. Bei jedem Start des File-Servers werden die beiden Directory-Strukturen und die beiden FATs miteinander verglichen und geprüft. Erkennt NetWare während des Einschaltens oder während des laufenden Betriebs einen Defekt in einem der beiden Systeme (Directory oder FAT), wird mit dem Ersatz weitergearbeitet. Der File-Server schreibt eine entsprechende Meldung am Bildschirm bzw. macht eine Eintragung im Error-Log-File. Die Reparatur kann – so weit möglich – mit NetWare-Dienstprogrammen durchgeführt werden, oder das defekte Laufwerk wird ausgewechselt.

Alle Novell-NetWare-Systeme beinhalten die SFT-I-Sicherheitsvorkehrungen. Man kann auch sagen, daß es sich hierbei um Grundfunktionen handelt, die jede Grundinstallation von NetWare beinhaltet. Mit Hilfe der SFT-II- und SFT-III-Mechanismen stehen Ihnen Funktionen zur Verfügung, die Sie optional einsetzen und nutzen können. NetWare 3.2 und NetWare 4 unterstützen per Default auch die Mechanismen von SFT II. Eine NetWare für SFT-III-Unterstützung muß als spezielles Netzwerkbetriebssystem implementiert werden und steht nur noch unter NetWare 4 zur Verfügung.

Im Zuge der Einführung von NetWare 5 wird SFT III nicht mehr weiterentwickelt. Zur besseren Absicherung der Server und dem Schutz gegen Serverausfälle bietet Novell deshalb eine Vielzahl neuer Mechanismen an:

- Novell StandbyServer für NetWare
- Novell StandbyServer Many-to-One für NetWare
- Novell SnapShotServer für NetWare
- Novell Cluster (in unterschiedlichen Orion-Phasen)

16.1.4 UPS-Monitoring

An den File-Server wird aus Sicherheitsgründen eine UPS angeschlossen, die den Server mit Strom versorgt, falls dieser ausfällt. Zu diesem Zweck wird der Server mit der UPS über ein Signalkabel verbunden, so daß er über den Zustand der UPS informiert wird. Beim Laden des UPS-Moduls kann eine sogenannte Recharge Time angegeben werden. Sie legt für den Fall, daß die UPS den Server mit Strom versorgen mußte und der Strom vor der gesamten Ladung der UPS erneut ausfällt, fest, wie lange die UPS braucht, um wieder voll geladen zu sein. Bei NetWare 3.2 bzw. NetWare 4 ist die UPS-Moni-

16 Novell NetWare, das fehlertolerante System

toring-Funktion als NLM realisiert und kann bei Bedarf geladen werden, sofern eine von NetWare unterstützte USV-Anlage angeschlossen ist. Von NetWare unterstützte USV heißt, daß diese über ein Signalkabel mit dem Server verbunden wird, um die Funktionsfähigkeit der USV überprüfen bzw. bei einem Stromausfall entsprechende Aktionen durchführen zu können (Mitteilung der Benutzer, Shutdown des Servers, wenn die Batterie leer ist etc.). Die meisten UPS-Hersteller bieten für die Komponenten inzwischen eigene Module an, die für die Steuerung der UPS-Anlage verantwortlich sind. Nicht selten werden auch noch Add-on-Module oder Programme angeboten, um die Überwachung mit Hilfe eines grafischen Tools durchführen zu können. Wichtig dabei ist, daß man berücksichtigt, Komponenten einzusetzen, deren Software in ein Netzwerkmanagementsystem eingebunden werden kann.

16.2 SFT Level II

Eine weitere mögliche Fehlerursache wurde bei der Behandlung von Hot Fix unter SFT I bereits angesprochen. Sie kann aber nicht von SFT I, sondern nur von SFT II beseitigt werden. Die SFT II schützt den File-Server vor Datenverlust bei Ausfall von Plattenlaufwerken oder Platten-Controllern. Die SFT II bietet dazu zwei Möglichkeiten an:

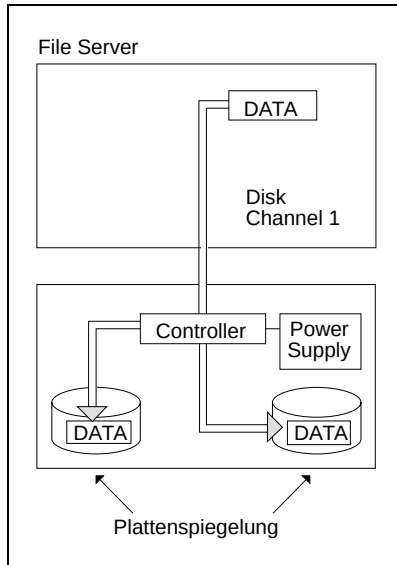
- Disk-Mirroring
- Disk-Duplexing

16.2.1 Disk-Mirroring

Abbildung 16.1 zeigt das Prinzip von Disk-Mirroring. Beim Disk-Mirroring werden identische Daten auf zwei getrennten Platten abgespeichert. Fällt eines der Laufwerke aus, arbeitet der File-Server mit der zweiten Platte weiter und schreibt eine Fehlermeldung auf den Bildschirm bzw. in das Error-Log-File. Wird die defekte Platte ausgetauscht, wird durch Eingabe eines Befehls ein automatischer Abgleich zwischen der intakten und der neuen Platte durchgeführt. In Zusammenarbeit mit Hot Fix schützt SFT II auch vor Lesefehlern. Tritt ein Lesefehler auf, holt sich der Plattenprozeß die Daten einfach von der gespiegelten Platte. Der defekte Bereich auf der anderen Platte wird gekennzeichnet und der richtige Datenbestand wieder auf die Platte übertragen. Diese Aktionen sind für den Benutzer im Netzwerk transparent. Durch Disk-Mirroring wird zudem der File-Server bei Leseoperationen leicht beschleunigt. Beim Lesen von Daten sucht sich der File-Server die Platte heraus, bei der der Schreib-/Lesekopf am günstigsten positioniert ist.

16.2 SFT Level II

Abbildung 16.1
Das Prinzip des
Disk-Mirroring



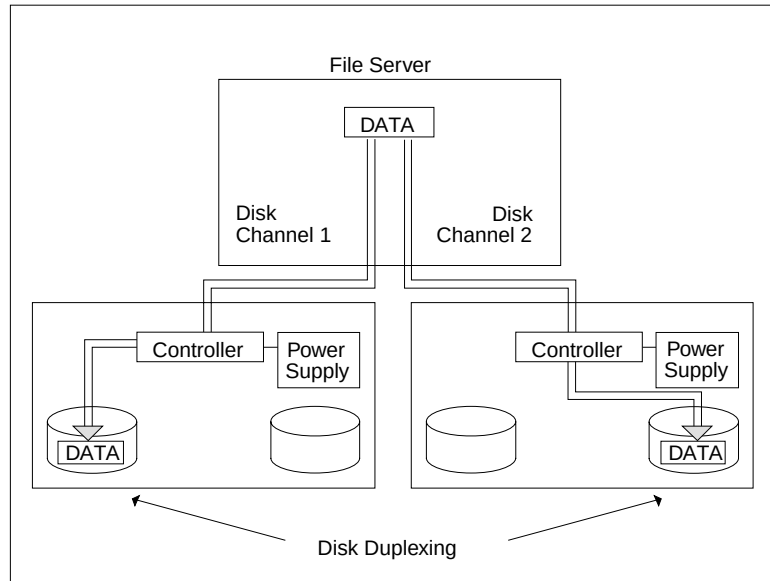
16.2.2 Disk-Duplexing

Disk-Duplexing schützt, genauso wie Disk-Mirroring, vor Ausfall des Plattenlaufwerks. Beim Disk-Duplexing wird jedoch zudem noch der Ausfall des Platten-Controllers abgesichert. Da beim Disk-Mirroring beide Platten, die gespiegelt werden, an einem Controller hängen, fallen bei Defekt des Controllers auch beide Platten aus. Anders bei der Verwendung von Disk-Duplexing. Das Disk-Duplexing wird so durchgeführt, daß identische Platten- und Dateispeicherkonfigurationen auf bis zu vier parallelen I/O-Kanälen angesprochen werden können. Novell NetWare und der Einsatz von Disk-Coprocessor-Boards ermöglichen die Kanalspiegelung durch die Verwaltung von vier separaten, unabhängigen Ein-/Ausgabe-Kanälen. Abbildung 16.2 zeigt das Prinzip des Disk-Duplexing.

Das Disk-Duplexing schützt zum einen vor Ausfällen des Controllers oder eines Plattenlaufwerks, zum anderen wird das Spiegeln von Platten optimiert. Ein zusätzlicher Vorteil besteht darin, daß der File-Server parallele Leseoperationen ausführen kann. Der File-Server kann das Lesen von Daten auf zwei Kanäle aufteilen, also halbieren. Das kann die Leistungsfähigkeit des Servers bei Spitzenbelastungen durch Leseoperationen verdoppeln. Mit SFT I und SFT II werden so ziemlich alle Risiken im Bereich der Hardware abgedeckt. Bis auf eines – nämlich den Schutz vor Ausfall des File-Servers selbst. Diese Sicherheitsmaßnahme wird durch die SFT-III-Version von Novell abgedeckt.

16 Novell NetWare, das fehlertolerante System

Abbildung 16.2
Das Prinzip des
Disk-Duplexing



Im Vergleich zu früheren SFT-II-Versionen wurde der Mechanismus von SFT II für NetWare 3.2 und NetWare 4 für das Spiegeln bzw. Duplexen von Platten erweitert. Konnte bislang unter NetWare nur die Primary-Platte auf eine Secondary-Platte gespiegelt werden, kann dies für NetWare 3 und NetWare 4 bei Bedarf erweitert werden. Mit NetWare 3.2 und NetWare 4 ist es jetzt möglich, eine Primary-Platte auf bis zu sieben Ersatzplatten zu spiegeln. Die Ausfallsicherheit wird dadurch nochmals um ein erhebliches Maß gesteigert.

16.2.3 Raid-Technologien

Raid wurde 1988 eingeführt und steht als Abkürzung für Redundant Arrays of Inexpensive Disks. Durch seinen Einsatz kann die Ausfallsicherheit von Plattensubsystemen erhöht werden. Im Prinzip unterscheidet man insgesamt fünf Raid-Level-Stufen, wobei jedoch in der Praxis Raid-2 und Raid-4 überhaupt nicht zum Einsatz kommen. Alle anderen Raid-Level-Stufen werden von einer Vielzahl von Herstellern unterstützt. Für NetWare kann die Raid-Technologie nur auf Basis passender Raid-Hardware eingesetzt werden (im Gegensatz zu Windows NT, bei der man die Raid-Technologie auf Softwarebasis einrichten kann). Man muß bei der Raid-Technologie folgende Raid-Stufen unterscheiden:

16.2 SFT Level II

■ *Raid-0*

Dieser Mechanismus bietet sehr hohe Geschwindigkeit mit sehr wenig Sicherheit beim Ausfall von Platten. Die Platten werden dabei in kleine Blöcke (Stripes) eingeteilt, auf denen die Speicherung erfolgt. Zudem liegen keine Paritätsinformationen vor; deshalb spricht man in diesem Falle auch von Striping ohne Parität. Da keine Parität und somit auch keine Ausfallsicherheit gegeben sind, bezeichnet man diesen Raid-Level gelegentlich auch als Pseudo-Raid. Da die Daten auf mehrere Platten (über die Stripes auf den jeweiligen Platten) verteilt werden, bedeutet der Ausfall einer Platte, daß auf keine Daten mehr im Array zugegriffen werden kann. Es ist keine zusätzliche Platte für Paritätsinformationen notwendig. Wenn jemand nicht nur »kostengünstig« ein Raid-System aufbauen will, sondern auch noch das Risiko liebt, für den sei Raid-0 empfohlen. Sollte man jedoch mehr Wert auf Sicherheit legen, auch wenn dies bekanntlich mehr kostet, dann sollte man einen der anderen Raid-Levels auswählen.

■ *Raid-1*

Bei dieser Raid-Stufe handelt es sich um die Implementierung von Disk-Mirroring. Hierzu notwendige Erläuterungen sind in Kapitel 16.2.1 zu erfahren. Wie man sieht, wird dieser Mechanismus von NetWare schon lange und von Haus aus unterstützt, ohne daß man hierfür einen speziellen Raid-Controller benötigt, wie dies für die Implementierung der einzelnen Raid-Levels der Fall ist.

■ *Raid-2*

Bei diese Stufe wird zur Absicherung Disk Striping auf Bit-Ebene verwendet. Man nutzt eine oder mehrere Platten, um die Paritätsinformationen zu speichern. Raid-2 wird aufgrund des Preises und der schlechten Performance wenig genutzt.

■ *Raid-3*

In diesem Fall wird Data Striping eingesetzt, und zwar immer auf Byte-Ebene, wobei eine Platte genutzt wird, um die Paritätsinformationen zu speichern. Striping verbessert den Durchsatz beim Lesen/Schreiben und nutzt in diesem Falle nur eine Platte pro Raid-3-Set, um die Paritätsinformationen zu speichern, wodurch sich die Kosten pro Megabyte Speicher reduzieren. Das Striping der Daten in kleinen Einheiten bietet sehr hohe Performance, wenn große Datenmengen übertragen werden, da alle Platten parallel arbeiten können. Innerhalb eines Raid-3-Systems müssen drei Platten ausfallen, bevor kein Zugriff mehr auf die Daten möglich ist.

■ *Raid-4*

Die Daten werden in größeren Einheiten verteilt, wodurch sich die Performance im Vergleich zu Raid-3 erhöht, wenn kleinere Datenmengen übertragen werden.

16 Novell NetWare, das fehlertolerante System

■ *Raid-5*

Es ist der Einsatz von Stripe-Sets mit Parität. Wie beim Striping ohne Parität werden die Volumes in »Streifen« aufgeteilt, und die Daten sozusagen »Quer« über die Volumes verteilt gespeichert. Zusätzlich werden aber Paritätsinformationen auf allen Platten geschrieben. Durch die Verteilung der Paritätsinformation über alle Platten verhindert Raid-5 den Flaschenhals, der ab und zu erzeugt wird, wenn nur eine Paritäts-Platte verwendet wird. Diese Technik wird inzwischen am meisten eingesetzt.

In den letzten Jahren bieten die einzelnen Raid-Controller-Hersteller auch noch das sogenannte Hot-Spare an. Mit Hot-Spare wird eine zusätzliche Ersatzplatte im Raid-System installiert. Sollte im Raid-Set eine Platte ausfallen, schaltet der Raid-Mechanismus die defekte Platte automatisch »ab« und hängt die Hot-Spare-Ersatzplatte automatisch in das Raid-System ein. Somit ist ein automatisches und vollständiges Weiterarbeiten möglich, und zwar mit vollständigem Plattensystem.

16.2.4 Hot Fix II

Hierbei handelt es sich um die Fähigkeit von NetWare, anhand der gespiegelten Platten einen nicht mehr lesbaren Datenbereich auf der Primary-Platte mit Hilfe der nochmals vorhandenen Daten auf der Secondary-Platte (bzw. den insgesamt möglichen sieben gespiegelten Platten) und der Redirection Area automatisch abzugleichen.

16.2.5 Split Seeks beim Lesen

Wenn in einem Server Festplatten-Controller und Festplatten doppelt vorhanden sind und der Mechanismus des Disk-Duplexing eingerichtet ist, dann sind auf den geduplexten Platten sämtliche Daten doppelt vorhanden und können über die separaten Platten-Controller getrennt voneinander angesteuert und gelesen werden. Deshalb können Leseanfragen vom Server auf beide Platten verteilt werden. Liegt eine Leseanfrage vor, ermittelt NetWare, welche Platte schneller auf die gewünschten Daten zugreifen kann. Ist eine Festplatte bereits mit der Bearbeitung von Daten beschäftigt, werden die Daten automatisch von der anderen Platte gelesen. Existieren mehrere Leseaufträge, werden diese auf die beiden Platten verteilt. Diese Arbeitsweise der verteilten Zugriffe wird Split Seeks genannt; sie trägt wesentlich zur Erhöhung der Zugriffsgeschwindigkeit bei Leseaufträgen bei. Wenn Sie sich jetzt noch vorstellen, daß NetWare auf bis zu acht Platten den Duplexing-Mechanismus ausdehnen kann, können Sie sich vorstellen, welche Effekte sich damit erzielen lassen.

16.2.6 Das TTS-System

Das TTS schützt gemeinsam benutzte Datenbestände vor Verlust oder Beschädigung durch unvollständige Transaktionen. Eine Transaktion wird dabei als ein Abschnitt innerhalb einer Applikation definiert, der entweder vollständig oder überhaupt nicht ausgeführt wird. Dieser Abschnitt besteht aus einer Reihe von Schreiboperationen und Dateiänderungen, die alle komplett ausgeführt werden müssen, damit die Konsistenz und die Integrität einer Datenbank oder einer Datei erhalten bleiben. Änderungen innerhalb einer Datei oder Datenbank betreffen aber nicht nur die Datensätze, sondern auch Index- und Schlüsselstrukturen, die für die Anwendung notwendig sind. Das TTS-System stellt sicher, daß alle Schreiboperationen in einer definierten Transaktion entweder vollständig oder überhaupt nicht auf der Festplatte gespeichert werden. Damit wird die Integrität und Konsistenz der Dateien gewährleistet, auch wenn Workstations, der File-Server oder die Übertragungsmedien ausfallen, bevor die Transaktion abgeschlossen ist.

Der Schutz vor Verlust oder Zerstörung der Daten oder Dateien wird dadurch gewährleistet, daß unvollständige Transaktionen zurückgesetzt werden. Die Dateien werden in den Zustand zurückversetzt, in dem sie sich befanden, bevor die Transaktion gestartet wurde. Dieser Mechanismus wird als Backward-Recovery bezeichnet. Es kann jedoch auch der Fall eintreten, daß Transaktionen vollständig abgearbeitet und beendet wurden, der File-Server die Aktualisierung jedoch noch nicht auf Platte hat und dann der File-Server abstürzt. Der Benutzer nimmt guten Glaubens an, daß er sich um nichts mehr kümmern muß, da seine Transaktionen vollständig abgearbeitet worden sind. Auch ein solcher Fall wird durch den Einsatz von TTS abgedeckt. Diese Art der Transaktionsfortschreibung wird als Forward-Recovery bezeichnet. Alle bereits als beendet definierten Transaktionen werden beim Wiederanlaufen des Systems nachgeholt.

Beide Mechanismen, Backward-Recovery und Forward-Recovery, sind altbekannte Funktionen aus dem Bereich der Großrechner-DV und stehen jetzt auch im PC-LAN unter Novell NetWare zur Verfügung. Die Sicherheitsstufen, die NetWare, beginnend mit SFT I bis hinauf zu SFT III, anbietet, sind einmalig für den LAN-Bereich, aber dennoch eine unabdingbare Forderung, wenn Wert auf Sicherheit gelegt wird.

Das TTS sollte immer aktiviert sein, auch wenn Sie keinen Einsatz von Multi-User-Datenbanken planen. TTS unter NetWare 3.2 schützt im Gegensatz zu früheren Versionen auch die NetWare Bindery und

16 Novell NetWare, das fehlertolerante System

Queue-Datenbankdateien vor Zerstörung. Auf Großrechner- und MDT-Rechnersystemen sind die TTS-Funktionen meist Bestandteil des Datenbanksystems und nicht Bestandteil des Netzwerkbetriebs-systems.

Wichtig ist an dieser Stelle, daß für die derzeitige Implementierung der NDS unter NetWare 4 das TTS-System eine wesentliche Rolle spielt. Da es sich bei der NDS um eine verteilte Datenbank handelt, wird auch diese NDS-Datenbank durch das TTS-System geschützt. Es ist somit unter NetWare 4 darauf zu achten, daß das TTS-System nicht abgeschaltet wurde. Sollte das TTS-System abgeschaltet sein, dann erfolgt mit diesem Server so lange keine Synchronisation der NDS-Datenbank, bis das TTS nicht reaktiviert worden ist.

Die Implementierung von TTS auf Betriebssystemebene auf dem File-Server bietet im Gegensatz zur Software-Implementierung auf Datenbanksystem-Ebene zwei wesentliche Vorteile:

- Die Performance wird drastisch erhöht, da Transaktionen auf dem Server, der die Schreiboperationen durchführt, überwacht werden. Aufgrund dieser Strategie wird der Transport von Daten über das Netzwerk reduziert, und alle Transaktionen können den Geschwindigkeitsvorteil des NetWare-Disk-Caching-Systems voll nutzen.
- Durch TTS wird Datenbankapplikationen, die nicht für einen Transaktions-Backout konzipiert sind, eine Backout-Fähigkeit verliehen. In diesem Fall wird eine sogenannte implizite Transaktionsdefinition eingesetzt. Das heißt, wenn eine Datenbankapplikation ohne Backout-Fähigkeit eine physikalische oder logische Satzsperrung für eine Datenbank durchführt, wird TTS darüber informiert, daß eine Transaktion beginnt. Ab diesem Zeitpunkt überwacht TTS die implizite Transaktion, so daß sie bei Auftreten eines Fehlers zurückgesetzt werden kann. Wenn die Applikation eine physikalische oder logische Satzsperrung freigibt, wird TTS darüber informiert, daß die Transaktion beendet ist. Ab diesem Zeitpunkt ist die Überwachung der Transaktion durch TTS beendet.

Es gibt drei Arten von Datenbankapplikationen, die TTS nutzen können:

- Applikationen, die nicht für einen Transaktions-Backout konzipiert sind. Diese nutzen die implizite Definitionsmethode für Transaktionsbeginn und -ende.
- Applikationen mit eingebauten Transaktions-Backout-Funktionen (z.B. Btrieve).
- Applikationen, die explizite NetWare-TTS-Aufrufe verwenden, um Transaktions-Backout-Funktionen zu nutzen. Beispiele für explizite Transaktionsaufrufe sind BEGIN, ABORT und END.

16.2 SFT Level II

Durch TTS soll garantiert werden, daß alle Dateiänderungen, die während einer Transaktion durchgeführt werden, entweder vollständig oder überhaupt nicht durchgeführt werden. Damit eine Transaktion für eine bestimmte Datei eingesetzt werden kann, muß die Datei durch das Dateiattribut Transactional gekennzeichnet werden.

Nachfolgend soll aufgezeigt werden, wie TTS den Schreibvorgang auf eine Datei durch eine Transaktion überwacht:

1. Eine Applikation schreibt neue Daten in eine Datei auf dem File-Server.
2. Der Server speichert die neuen Daten in einem Cache-Speicher. Die Zieldatei auf der Festplatte des File-Servers bleibt noch unverändert.
3. Der Server durchsucht die Zieldatei auf der Platte des File-Servers und stellt fest, daß Daten geändert worden sind; die alten Daten werden in einen Cache-Speicher kopiert. Der Server protokolliert auch den Namen und den Directory-Pfad der Zieldatei und die Länge und Position der alten Datensätze innerhalb der Datei. Die Zieldatei auf der Platte des File-Servers bleibt unverändert.
4. Der Server schreibt die alten Daten des Cache-Speichers in eine Transaktions-Work-Datei auf der Platte des File-Servers. Diese Transaktions-Work-Datei befindet sich im Root-Directory des Volumes auf dem File-Server. Die Zieldatei auf der Platte des File-Servers ist immer noch unverändert.
5. Der Server schreibt die neuen Daten des Cache-Speichers in die Zieldatei auf der Platte des File-Servers. Die Zieldatei ist jetzt geändert.

Der Server wiederholt diese Schritte für jeden Schreibvorgang innerhalb einer Transaktion. Dabei wird die Transaktions-Work-Datei immer größer, da die alten Daten eines jeden Schreibvorgangs gesammelt werden können. Wird die Transaktion unterbrochen, schreibt der Server den entsprechenden Inhalt der Transaktions-Work-Datei in die Zieldatei. Dabei wird die Datei in den Zustand zurückgesetzt, der vor Beginn der Transaktion bestand. Der Server setzt also die Transaktion zurück.

Wie bereits erwähnt, ist TTS ein integraler Bestandteil von NetWare 3.2 und NetWare 4 (da SFT-II-Unterstützung) und keine zusätzliche Option. Für NetWare 5 wird das TTS auch die gleiche Bedeutung für die NDS haben, wie dies auch unter NetWare 4 der Fall ist, so daß auf den Einsatz von TTS auch unter NetWare 5 noch nicht verzichtet werden kann. Das TTS wird immer dann aktiviert, wenn das Volume-SYS gemountet wird und noch genügend Platz auf der Platte und im Hauptspeicher des File-Servers vorhanden ist. Bei Bedarf kann das TTS an der Server-Console durch die Eingabe DISABLE TTS

16 Novell NetWare, das fehlertolerante System

abgeschaltet und durch die Eingabe `ENABLE TTS` wieder aktiviert werden. Wird TTS durch ein Problem am File-Server automatisch abgeschaltet, muß dieses Problem behoben werden, bevor Sie TTS wieder aktivieren können.

Ein automatisches Abschalten von TTS erfolgt dann, wenn das Volume-SYS voll ist oder der File-Server nicht mehr über genügend freien Hauptspeicher verfügt. Wenn TTS deaktiviert ist, kann auf einer Workstation trotzdem eine Transaktion ausgeführt werden; dann wird die Datenbank aber nicht mehr durch das TTS geschützt. Für NetWare 4 bedeutet eine Deaktivierung des TTS-Systems auch das Abschalten der NDS-Funktionen. Somit bedeutet ein abgeschaltetes TTS auf einem NetWare 4 Server, daß man nicht mehr auf diesem Server arbeiten kann, d.h., ein Einrichten von neuen NDS-Objekten und die Synchronisation mit den anderen Servern im Netzwerk ist nicht mehr möglich. Es muß somit sowohl für NetWare 3 als auch für NetWare 4 darauf geachtet werden, daß das TTS-System immer aktiv bleibt.

16.3 Das UPS-Monitoring

Mit Hilfe des UPS-Monitoring (Uninterruptable Power Supply) ist es möglich, den File-Server durch ein spezielles, von NetWare gesteuertes Notstrom-Versorgungssystem gegen Stromausfälle abzusichern. In Abbildung 16.3 ist ein möglicher Aufbau einer UPS an einem File-Server dargestellt. Dabei ist auf alle Fälle zu beachten, daß nur UPS-Anlagen eingesetzt werden, die Novell-tauglich sind. Für den Fall, daß das UPS die Stromversorgung des File-Servers übernehmen muß, wird der File-Server wie folgt reagieren. Alle noch aktiven Stationen, die vom Stromausfall nicht betroffen sind, erhalten unterschiedliche Meldungen am Bildschirm:

`You are on auxiliary power. Server will go down in xx minutes.`

Diese Meldung erscheint nach einem Stromausfall und der Übernahme der Stromversorgung des File-Servers durch UPS. `xx` gibt an, wie lange die UPS den File-Server mit Strom versorgen kann.

`Batteries are low. Server will go down in one minute.`

Diese Meldung erscheint eine Minute, bevor `xx` Minuten verstrichen sind.

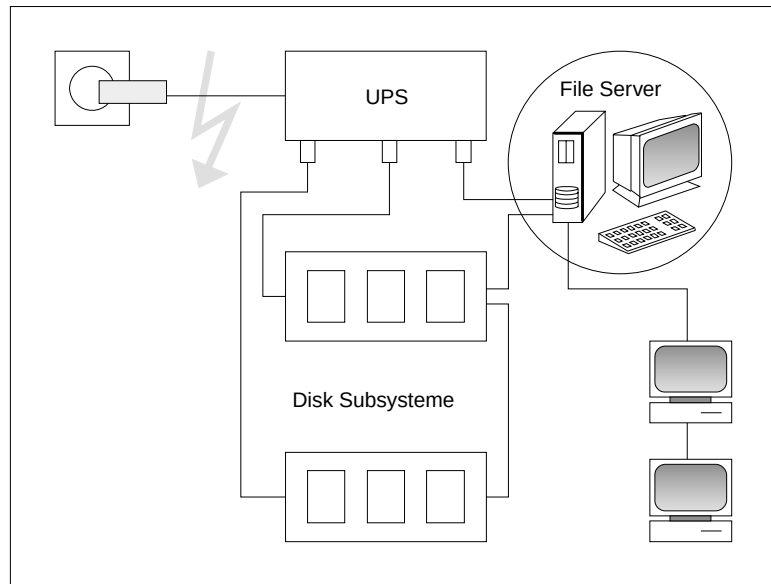
`Commercial power has been restored to server.`

Diese Meldung erscheint, wenn der Strom vor Ablauf der `xx` Minuten wieder zur Verfügung steht.

16.4 SFT Level III

Aus Sicherheitsgründen sollte auf alle Fälle jeder File-Server mit einer UPS, Novell-gesteuert, ausgestattet werden, um das System zusätzlich, neben allen anderen Sicherheitseinrichtungen, vor Ausfall zu schützen.

Abbildung 16.3
Die Funktionsweise einer UPS-Anlage, die von NetWare gesteuert wird



Da es in einem Netzwerkbetriebssystem und beim Einsatz von mehrplatzfähigen Programmen sehr unangenehme Folgen haben kann, wenn Programme unkontrolliert beendet werden, bietet Novell ab SFT II das gerade besprochene Transaction-Tracking-System an; es ist im Lieferumfang enthalten. Das UPS-Monitoring-System wird uneingeschränkt von allen NetWare-Versionen unterstützt.

16.4 SFT Level III

Die größte Ausfallsicherheit wurde bislang durch den Einsatz von SFT III erreicht. Mit NetWare 4.11 wird die letzte SFT-III-Version ausgeliefert, da sich Novell ab Auslieferung von NetWare 5 in eine neue strategische Richtung bewegt. Die damit verbundenen Möglichkeiten beginnen bei einer einfachen StandbyServer-Lösung und reichen bis zum ausfallsicheren Clustering-Konzept.

NetWare 4 wird standardmäßig auf der CD-ROM mit NetWare SFT III ausgeliefert. Zur Installation dieser SFT III benötigt man eine zusätzliche SFT-III-Lizenz-Diskette, die es in einer 100-User- und einer

16 Novell NetWare, das fehlertolerante System

Unlimited-Version gibt. Mit dieser Version ist eine ununterbrochene Arbeit, auch bei Ausfall des File-Servers möglich – ohne daß der Benutzer es merkt, wird mit dem zweiten Server weitergearbeitet, für den Fall, daß der Primary-File-Server ausfällt. Die Verbindung der beiden File-Server zum Abgleich der beiden Systeme wird mit ziemlicher Sicherheit mit Hilfe einer Glasfaserstrecke erfolgen. Die ist notwendig, da mit einer solchen Kopplung die notwendige Übertragungsgeschwindigkeit von ca. 100 Mbit/s erreicht werden kann. Weitere Informationen und Aspekte über NetWare SFT III, Standby-Server und Clustering erhalten Sie in den nächsten Kapiteln, nachdem ich Ihnen noch Grundsätzliches über die Benutzeroberfläche von NetWare 3.2 erzählt habe.

17

Benutzeroberfläche von NetWare 3.2

In diesem Kapitel will ich Ihnen zeigen, welche Möglichkeiten NetWare 3.2 bietet, als systemverantwortlicher Supervisor den File-Server zu bedienen und zu überwachen, und welche Utilities dafür auch dem Benutzer zur Verfügung stehen. Die Benutzeroberfläche kann in vier Bereiche unterteilt werden:

- Commandline-Utilities
- Supervisor-Utilities
- Menü-Utilities
- Consolen-Befehle

Diese Befehle und Menüsysteme sollen anschließend erläutert werden.

17.1 Commandline-Utilities

Unter Commandline-Utilities sind Programme zu verstehen, die jedem Anwender zur Verfügung stehen. Mit den verfügbaren Befehlen haben Anwender die Möglichkeit, sich zum einen spezielle Informationen über die Netzwerkumgebung ausgeben zu lassen, zum anderen aber neue Umgebungsbedingungen festzulegen. Die Commandline-Utilities werden auf DOS-Betriebssystemebene der Workstation eingegeben. Diese Befehle will ich Ihnen nun beschreiben.

LOGIN Anmelden am File-Server durch Angabe des File-Server-Namens (optional) und des User-Namens. Sie können an bis zu acht File-Servern gleichzeitig angemeldet sein. Nach einem erfolgreichen LOGIN wird jedes weitere Anmelden an einem File-Server mit dem Befehl ATTACH vollzogen.

ATTACH Anmelden an zusätzlichen File-Servern im Netzwerk, ohne sich von den bisherigen File-Servern abmelden zu müssen, d.h., alle bisherigen Anmeldungen bleiben bestehen.

LOGOUT Abmelden vom File-Server. Durch Eingabe eines File-Server-Namens melden Sie sich nur von einem bestimmten Server ab.

Wenn Sie auf mehreren Servern angemeldet sind und nur den Befehl LOGOUT ohne weiteren Parameter eingeben, melden Sie sich von allen File-Servern gleichzeitig ab.

17 Benutzeroberfläche von NetWare 3.2

SLIST	Anzeigen aller File-Server im Netzwerk.
SYSTIME	Das Datum und die Uhrzeit des File-Servers werden angezeigt. Zugleich erfolgt die Synchronisation der Workstation mit Datum und Uhrzeit auf dem File-Server. Es kann angegeben werden, mit welchem File-Server die Synchronisation erfolgen soll.
MAP	Dieser Befehl dient zum Einrichten von logischen Netzwerklaufwerken und Suchpfaden. Insgesamt stehen dem Anwender bis zu 26 Laufwerksbuchstaben zur Verfügung (A-Z). 16 Laufwerksbuchstaben können für Suchpfade verwendet werden (S1-S16).
USERLIST	Anzeigen aller momentan im Netzwerk angemeldeten Benutzer. Hierbei können zusätzliche Informationen über Datum und Uhrzeit des Logins, des Connection-Slots und des Objekt-Typs (User, Print-Server etc.) angezeigt werden.
SETPASS	Vergabe und Änderung des Paßworts. Es können damit auch die Paßwörter auf mehreren File-Servern synchronisiert werden.
SMODE	Mit diesem Befehl kann festgelegt werden, wie ein Programm Suchpfade verwenden soll, wenn Datendateien verwendet werden. Dieser Befehl ist mit dem APPEND-Befehl von MS-DOS vergleichbar, bietet aber eine wesentlich höhere Flexibilität.
WHOAMI	Anzeigen wichtiger Informationen über die eigenen Anmeldungen auf den jeweiligen File-Servern. Sie erhalten generelle Systeminformationen, Anzeige der effektiven Rechte, Anzeige der Gruppenzugehörigkeiten und die Security-Equivalences, die der Benutzer besitzt.
TLIST	Anzeige der Trustees (Benutzer oder Gruppen) eines Directory mit den dazugehörigen Rechten. Dabei kann unterschieden werden, ob nur Benutzer- oder nur Gruppeninformationen aufgelistet werden sollen.
SEND	Hiermit können kurze Nachrichten an andere Benutzer im Netzwerk verschickt werden. Die Nachricht erscheint auf dem Bildschirm des Empfängers in der 25. Statuszeile und muß durch eine explizite Tastenkombination entfernt werden.
CASTOFF	Der Empfang von Nachrichten kann mit diesem Befehl unterdrückt werden. Es kann unterschieden werden, ob nur der Empfang von Nachrichten anderer Workstations, des File-Servers oder beider Systeme abgeschaltet werden soll.
CASTON	Damit schalten Sie den Empfang von Nachrichten wieder ein.
CHKDIR	Da NetWare 3.2 die Möglichkeit bietet, den Plattenplatzbedarf eines Directory zu beschränken, können Sie mit diesem Befehl anzeigen lassen, wieviel Platz auf dem Volume insgesamt zur Verfügung steht,

17.1 Commandline-Utilities

wieviel belegt und wieviel noch frei ist, wieviel für das angegebene Directory definiert wurde und wieviel davon wieder belegt bzw. noch frei ist.

- CHKVOL** Zeigt die Volume-Größe, den belegten Platz auf der Platte, den belegten Platz gelöschter Dateien, den freiwerdenden Platz, wenn die wiederherstellbaren Dateien entfernt werden, die freie Kapazität auf dem Volume und die freie Kapazität auf dem Volume für den Benutzer, der CHKVOL aufruft.
- LISTDIR** Hiermit erhalten Sie die Auflistung der gesamten Directory-Struktur eines Volume. Sie können weitere Informationen über die Inherited Rights Mask, die effektiven Rechte sowie Erstellungsdatum und -uhrzeit angezeigt bekommen.
- NDIR** Mit diesem Befehl können Sie sich detaillierte Informationen über Dateien und Directories anzeigen lassen. Sie haben damit auch die Möglichkeit, nach bestimmten Dateien zu suchen, wenn Sie zwar noch wissen, wie die Datei heißt, sich aber nicht mehr daran erinnern können, in welchem Directory sich diese Datei befindet. Die Angabe von Parametern ermöglicht Ihnen eine gezielte Auswahl von Dateien und Directories und die Festlegung der Sortierung, wie die Informationen ausgewiesen werden sollen.
- RIGHTS** Hiermit werden dem Benutzer die effektiven Rechte für das angegebene Directory ausgewiesen, die er für dieses Directory besitzen muß.
- FLAG** Mit FLAG können Sie sich die Dateiattribute anzeigen lassen und neue Dateiattribute setzen.
- FLAGDIR** Hiermit können Sie sich die Directory-Attribute anzeigen lassen und neue setzen.
- NCOPY** Dieser Befehl ist ähnlich zu bedienen wie der DOS-COPY-Befehl. Die zu kopierende Datei bzw. Dateien werden dabei jedoch nicht über das Netzwerk in den Hauptspeicher der Workstation transportiert, sondern direkt zwischen Quelle und Ziel übertragen.
- Durch Parameter kann angegeben werden, daß auch Subdirectories kopiert und Dateiattribute beim Kopiervorgang übernommen werden sollen.
- PURGE** Alle restaurierbaren Dateien des Benutzers werden mit diesem Befehl unwiederbringlich gelöscht. Das heißt, diese Dateien können mit Hilfe des SALVAGE-Befehls nicht mehr wiederhergestellt werden.
- CAPTURE** Eine der wichtigsten Funktionen im Netz ist das Drucken. Um Druckaufträge von der lokalen Workstation auf einen Netzwerkdrucker umzuleiten, muß der CAPTURE-Befehl verwendet werden.

17 Benutzeroberfläche von NetWare 3.2

Durch Parametereinstellungen lassen sich sehr viele Einstellungen durchführen. Alle drei lokalen LPT-Schnittstellen lassen sich gleichzeitig umleiten.

ENDCAP	Das Umleiten von Druckaufträgen wird durch diesen Befehl aufgehoben. Jede LPT-Schnittstelle kann einzeln auf den lokalen Modus umgestellt werden.
NPRINT	Eine bereits vorhandene für den Druck aufbereitete Datei kann mit diesem Befehl auf einem Netzwerkdrucker ausgegeben werden. Ein vorheriges Umleiten der lokalen Schnittstelle ist bei diesem Befehl nicht notwendig.
GRANT	Mit dem Befehl GRANT können Benutzern oder Benutzergruppen Trustee-Rechte für Directories vergeben werden. Trustee-Rechte können hierbei sowohl für einzelne Benutzer als auch für Gruppen vergeben werden.
RENDIR	Mit diesem Befehl kann für ein Directory ein neuer Name vergeben werden, wenn Sie das Recht hierzu besitzen.
SETTTS	TTS nimmt an, daß eine Transaktion bei der physikalischen oder logischen Satzsperr beginnt (implizite Methode) und bei Aufhebung der Satzsperr endet. Von manchen Applikationen wird diese Satzsperr für interne Zwecke verwendet. Mit SETTTS kann man dem TTS eine spezifizierte Anzahl von physikalischen oder logischen Satzsperrn mitteilen. Diese werden dann von TTS ignoriert, bevor es den Beginn einer Transaktion festlegt.
NVER	Anzeigen der Netzwerkversion des File-Servers und der Versionen der Programme IPX/SPX, LAN-Driver, SHELL, DOS und NetBIOS auf der Workstation.
PSC	Ein Anwender kann damit sehr schnell – wenn er Print-Server-Operator ist – Print-Server und Netzwerkdrucker im Netzwerk überwachen und steuern. Man kann sich unter anderem den Status des Print-Servers bzw. der Netzwerkdrucker anzeigen lassen und andere notwendige Steuerungen durchführen.
ALLOW	Hiermit kann die Inherited Rights Mask für ein Directory oder eine Datei angezeigt, geändert oder neu definiert werden.
REMOVE	Dieser Befehl ermöglicht, daß ein Benutzer oder eine Gruppe aus der Trustee-Liste für eine Datei oder ein Directory gelöscht wird.
REVOKE	Damit können Sie einem Benutzer oder einer Gruppe die Trustee-Rechte für ein Directory oder eine Datei einschränken, Trustee-Rechte werden also entfernt.

17.2 Supervisor-Utilities

Supervisor-Utilities werden wie die Commandline-Utilities auf der Betriebssystemebene der Workstation ausgeführt. Aus Gründen der Sicherheit sollten diese Befehle nur vom Supervisor ausgeführt werden. Folgende Befehle, die im SYS:SYSTEM-Directory abgelegt sind, stehen Ihnen zur Verfügung.

- BINDFIX** Sollten irgendwann einmal Probleme mit der Bindery des Servers auftreten, kann mit diesem Befehl die Reparatur der Bindery durchgeführt werden. Die Bindery besteht unter NetWare 3.2 aus drei Dateien: NET\$OBJ.SYS, NET\$PROP.SYS und NET\$VAL.SYS. Bevor BINDFIX mit der Reparatur der Bindery beginnt, wird eine Kopie der drei bestehenden Bindery4-Dateien angelegt. Die Kopien werden mit der Extension .OLD im SYS:SYSTEM-Directory abgelegt.
- BINDREST** War die Durchführung von BINDFIX nicht erfolgreich, können Sie mit BINDREST den Zustand der alten Bindery wiederherstellen. Das geht nur, wenn alle drei Bindery-Dateien mit der Extension .OLD noch nicht gelöscht worden sind.
- PAUDIT** Mit diesem Befehl werden Ihnen alle Accounting-Transaktionen aufgelistet. Sie beinhalten, wann sich ein Benutzer am File-Server angemeldet hat (mit Angabe der Netzwerk- und Node-Adresse) und wie viele Ressourcen der einzelne Benutzer am File-Server belegt hat.
- SECURITY** Hiermit wird die gesamte Netzwerkeinrichtung mit Hilfe der Bindery auf sogenannte Sicherheitslöcher überprüft. Die Inhalte der Bindery werden u. a. auf folgende Komponenten durchsucht:
- Objekte ohne Paßwort
 - Objekte mit zu einfachen Paßwörtern
 - Objekte mit Security-Equivalence-Rechten
 - Objekte mit Rechten im Root-Directory
 - Objekte ohne Login-Script
 - Objekte, die kein Paßwort benötigen
- Sie erhalten damit eine gesamte Auflistung von Bindery-Definitionen, die aus Sicherheitsgründen geändert werden sollten.
- ATOTAL** Mit diesem Utility erhalten Sie eine Auswertung des Accounting-Systems von NetWare. Diese Auswertung bezieht sich auf folgende Angaben:
- alle gelesenen Blöcke
 - alle geschriebenen Blöcke
 - die gesamte »Verbindungszeit«
 - alle Service Requests
 - Festplatten-Speicherplatz in Blöcken/Tag

17 Benutzeroberfläche von NetWare 3.2

Die ausgegebenen Informationen werden in eine tägliche und eine wöchentliche Summierung aufgeteilt. Es besteht die Möglichkeit, durch Eigenprogrammierung wesentlich detailliertere Informationen auszuwerten (z.B. pro Benutzer).

Neben diesen Befehlen wird Ihnen auch noch eine Vielzahl von Menüsystemen zur Verfügung gestellt, die notwendig sind, um die Server-Umgebung einzurichten, d.h. Benutzer, Gruppen, Print-Server, Drucker etc. zu definieren und Berechtigungen für die einzelnen Objekte im Netzwerk zu vergeben. Das sind Menüsysteme, die benötigt werden, um das Netzwerk leicht verwalten zu können.

Daneben stehen dem Netzwerkverwalter noch eine Menge von Befehlen zur Verfügung, die an der File-Server-Console eingegeben werden können. Ich werde Ihnen nach Darstellung der zur Verfügung stehenden Menüsysteme und Consolen-Befehle ein Utility zeigen, mit dem es möglich ist, den File-Server von der Workstation aus nicht nur zu steuern, sondern auch zu installieren und zu konfigurieren. Es handelt sich dabei um die sogenannte Remote Management Facility. Dadurch wird die totale Steuerung des File-Servers vom Arbeitsplatz aus möglich, d.h., Sie benötigen keinen direkten, physikalischen Zugriff auf den File-Server. Sie müssen also nicht mehr in den File-Server-Raum gehen, um irgendwelche Server-Eingaben durchzuführen. Der weitere Vorteil liegt darin, daß Sie damit in der Lage sind, auch File-Server mit Hilfe von Remote-Verbindungen zu installieren und zu überwachen.

17.3 Menü-Utilities

Für die Verwaltung, Pflege und Überwachung des gesamten File-Server-Systems stellt NetWare 3.2 einige Menüsysteme zur Verfügung, die Ihnen das Arbeiten wesentlich erleichtern. Besonders hervorzuheben ist das grafische Syscon-Utility, auf das ich am Ende dieses Kapitel nochmals eingehen werde.

Jedes Menüsystem bietet Ihnen zu jedem beliebigen Zeitpunkt eine Online-Hilfe am Bildschirm, die immer mit der Taste F1 abgerufen werden kann. Es wird Ihnen damit am Bildschirm eine kurze Erläuterung der Menüoptionen (optionenabhängig) gegeben; im Lauf der Zeit können Sie so auch ohne Handbuch mit den Menüs arbeiten. Ich will Ihnen anschließend die grundlegenden Funktionen der NetWare-Menüs darstellen.

17.3 Menü-Utilities

17.3.1 Das Session-Menü

Mit diesem Menü kann jeder Benutzer im Netzwerk temporär logische Laufwerke definieren, ändern oder löschen. Das gleiche gilt für das Einrichten, Ändern und Löschen von Suchpfaden. Zudem besteht die Möglichkeit, sich an einem anderen File-Server anzumelden, auf diesen zu wechseln, sich von einem File-Server abzumelden oder sich unter einem anderen Namen anzumelden. Bei der Definition von logischen Laufwerken sind von Novell mit NetWare 3.2 durch den Einsatz einer neuen Shell und neuer Menü- und Commandline-Utilities für das Einrichten von logischen Laufwerken neue Möglichkeiten geschaffen worden. Diese Änderungen erlauben es jetzt, sogenannte fiktive Root-Laufwerke zu definieren.

Hiermit hat man die Möglichkeit, ein logisches Laufwerk, dem ein Directory-Pfad zugewiesen wird, so zu behandeln, als sei es ein Root-Directory. Dies ist unter anderem bei der Installation von speziellen Programmen notwendig, die ihr Programm-Directory direkt unter dem Root-Directory anlegen wollen bzw. dies verlangen. Die Möglichkeit der Definition dieser fiktiven Root-Laufwerke ist auch im Session-Menü enthalten.

Daneben können Sie sich im Session-Menü noch die vorhandenen Gruppen auflisten lassen und eine Meldung an eine bestimmte Gruppe versenden. Diese Meldung wird dann bei jedem Benutzer, der Mitglied dieser ausgewählten Gruppe und am File-Server angemeldet ist, in der 25. Statuszeile eingeblendet.

Eine weitere Option des Session-Menüs ist die Festlegung eines sogenannten Default-Drives. Wenn Sie mit dieser Option ein Laufwerk auswählen und das Session-Menü verlassen, befinden Sie sich sofort im ausgewählten Default-Drive.

Neben den Gruppen können Sie sich auch alle momentan angemeldeten Benutzer auflisten und sich über einen Benutzer Informationen anzeigen lassen oder nur diesem eine Meldung schicken. Diesem wird dann die Meldung in der 25. Statuszeile eingeblendet.

17.3.2 Das Filer-Menü

Dieses Menüsystem dient zum Überwachen der gesamten Directory-Struktur und der Dateien auf dem File-Server. Sie können sich damit über das Directory, das Sie momentan ausgewählt haben, die wichtigsten Informationen anzeigen lassen oder diese ändern. Es handelt sich dabei um den Owner, das Erstellungsdatum und die Erstellungszeit des Directory, um die Directory-Attribute, die effektiven

17 Benutzeroberfläche von NetWare 3.2

Rechte und die Inherited Rights Mask des Directory. Zudem verfügen Sie noch über die Möglichkeit, Benutzer oder Gruppen als Trustees für dieses Directory zu definieren.

Sie können sich auch den Inhalt des Directory (Dateien, Subdirectories) auflisten lassen und ändern. Sie können also Subdirectories oder Dateien löschen, Dateien kopieren oder verschieben, gesamte Subdirectory-Strukturen kopieren und sich über Subdirectories Informationen anzeigen lassen. Daneben besteht noch die Möglichkeit der Anzeige, wer auf ein Subdirectory oder eine Datei Rechte hat, oder Sie können sich den Inhalt einer Datei auflisten lassen.

Über das Filer-Menü ist es auch möglich, den aktuellen Directory-Pfad zu wechseln, um Informationen über ein anderes Directory zu erhalten. Die Option *Set Filer Options* erlaubt Ihnen die Einstellung bestimmter Parameter: ob zum Beispiel das Löschen von Dateien abgefragt werden soll oder welche Dateien oder Directories (Wildcards) aufgelistet werden sollen.

Man kann sich auch die momentane Auslastung eines Volume anzeigen lassen, um zum Beispiel zu überprüfen, zu wieviel Prozent das Volume bereits belegt ist.

17.3.3 Das Dspace-Menü

Sie haben mit diesem Menü wieder die Möglichkeit, den File-Server zu wechseln, sich an einem anderen File-Server anzumelden, Ihr Login zu ändern oder sich an einem bestimmten File-Server abzumelden. Diese Option werden Sie in mehreren Menüs finden, da hiermit die Möglichkeit besteht, mit einem Aufruf des entsprechenden Menüs die Option auch auf anderen File-Servern durchzuführen, ohne sie explizit von diesem File-Server starten zu müssen.

Zu den wichtigsten Funktionen, die mit *Dspace* zur Verfügung gestellt werden, gehört die Vergabe der Plattenplatzbeschränkung auf Volume-Ebene für einen Benutzer. Er hat dann nur den von Ihnen festgelegten Plattenplatz auf dem Volume zur Verfügung.

Zudem können Sie eine Plattenplatzbeschränkung auf Directory-Ebene durchführen. Sie gilt dann für alle Benutzer, die Zugriff auf dieses Directory haben. Ist die definierte Kapazität ausgeschöpft, kann im Directory nichts mehr abgespeichert werden. Der Supervisor muß dann entweder das Directory bereinigen oder die Kapazität erhöhen.

17.3 Menü-Utilities

17.3.4 Das Salvage-Menü

Für NetWare 3.2 hat man ein Menü entwickelt, da man unter NetWare 3.2 alle bisher gelöschten Dateien wieder zurückholen kann, es sei denn, die Platte ist voll und es wurde damit begonnen, die gelöschten Dateien (angefangen mit der zuerst gelöschten) auf der Platte zu überschreiben.

Sie haben jetzt die Möglichkeit, gelöschte Dateien in Directories und gelöschte Dateien, deren Directory ebenfalls gelöscht wurde, zu restaurieren. Wird beim Wiederherstellen der Datei festgestellt, daß inzwischen eine Datei unter diesem Namen im Directory existiert, werden Sie aufgefordert, die zu restaurierende Datei umzubenennen. Beim Wiederherstellen einer gelöschten Datei wird auch angezeigt, wann und von wem die Datei gelöscht worden ist.

Sie haben aber auch die Möglichkeit, auf eine gelöschte Datei einen PURGE durchzuführen, d.h., die Datei wird unwiederbringlich von der Platte entfernt, und der belegte Platz dieser Datei wird mit Hex 00 überschrieben.

17.3.5 Das Volinfo-Menü

Mit diesem Menü wird eine Aufstellung aller Volumes des File-Servers mit Angabe der Gesamtkapazität und der freien Kapazität gemacht. Es wird auch angegeben, wie viele Directory-Einträge angelegt wurden und wie viele davon noch frei sind. Beachten Sie, daß NetWare 3.2 die Directory-Einträge dynamisch einrichtet und Sie insgesamt 2.097.152 Directory-Einträge pro Volume zur Verfügung haben.

Auch in diesem Menü können Sie auf einen anderen File-Server wechseln, sich an einem anderen File-Server anmelden oder sich von einem File-Server abmelden.

17.3.6 Das Syscon-Menü

Es handelt sich hierbei um eines der wichtigsten Menüs für das gesamte Netzwerk. Mit diesem Menü wird die gesamte Netzwerkumgebung eingerichtet, also wer, wann, mit welchen Rechten am File-Server arbeiten darf, Accounting-Definitionen etc.

Mit der Option *Accounting* richten Sie beim erstmaligen Aufruf das Accounting-System ein. Anschließend können Sie für bestimmte Leistungen des Servers Gebührensätze festlegen, die vom Konto des Benutzers abgebucht werden, wenn dieser gebührenpflichtige Leistungen in Anspruch nimmt. Es sei an dieser Stelle nochmals betont,

17 Benutzeroberfläche von NetWare 3.2

daß es sich hierbei um eine optionale Funktion handelt. Welche Leistungen berechnet werden können, habe ich Ihnen bereits oben beschrieben.

Die Option *Change Current Server* bietet die Möglichkeit, auf einen anderen File-Server zu wechseln, um dort *Syscon* aufzurufen, sich an einem anderen File-Server anzumelden oder sich von einem File-Server abzumelden.

Mit der Option *File Server Information* werden Ihnen die wichtigsten Informationen über den ausgewählten File-Server gegeben. Dies sind unter anderem Server-Name, Netzwerkversion, Netzwerkadresse, Node-Adresse etc.

Mit der Option *Group Information* erhalten Sie die Auflistung aller momentan eingerichteten Gruppen. Sie können hiermit auch neue Gruppen anlegen oder bestehende löschen bzw. umbenennen. Ist eine Gruppe eingerichtet, kann für diese ein sprechender Name definiert werden, Sie können Manager für diese Gruppe festlegen oder löschen oder sich nur auflisten lassen, wer über diese Gruppe den Manager-Status besitzt. Zudem können bzw. müssen Sie festlegen, wer Mitglied dieser Gruppe ist. Sie können auch einem Benutzer die Mitgliedschaft wieder entziehen, indem Sie ihn aus der Tabelle löschen. Sie müssen definieren, welche Trustee-Rechte auf Directory- und Dateiebene die Gruppe besitzt. Jeder Benutzer, der Mitglied dieser Gruppe ist, besitzt automatisch diese Trustee-Rechte.

Mit der Option *Supervisor Option* werden dem Supervisor bzw. Supervisor-Äquivalent zusätzlich spezielle Möglichkeiten gegeben, die Netzwerkumgebung so optimal wie möglich einzurichten. Hierbei sind auch Optionen enthalten, die sogenannte Default-Einstellungen festlegen, um das spätere Einrichten von Benutzern zu erleichtern.

Es bestehen unter anderem die Möglichkeiten, Default Account Balance/Restrictions zu definieren. Das heißt, es wird eine Voreinstellung für das Konto des Benutzers festgelegt, und es werden die Login-Restrictions für einen Benutzer bestimmt. Nach Festlegung dieser Werte wird jeder neue Benutzer, den Sie einrichten, mit diesen Einstellungen definiert. Sie haben dann nachträglich die Möglichkeit, diese individuell zu ändern.

Das gleiche gilt für die Festlegung der Default Time Restrictions. Sie legen hiermit global fest, zu welchem Zeitpunkt sich Benutzer am File-Server anmelden dürfen. Jeder Benutzer, den Sie nachträglich einrichten, wird mit diesen Time Restrictions definiert, die individuell geändert werden können.

17.3 Menü-Utilities

Mit der Option *Supervisor Options* wird auch das System-Login-Script eingerichtet und definiert, wer den Workgroup-Manager-Status erhält. Da sich der Systemverantwortliche von Zeit zu Zeit über den Zustand des File-Servers informieren sollte, ist in dieser Option auch die Möglichkeit enthalten, sich über *View File Server Error Log* das Fehlerprotokoll des File-Servers anzeigen zu lassen. Daneben können Sie auch noch die *Intruder/Detection-Lockout*-Funktion aktivieren und festlegen, in welchen Intervallen diese gelten soll.

Mit der Option *User Information* werden Ihnen nicht nur alle im Netzwerk definierten Benutzer aufgelistet, sondern Sie haben hier auch die Möglichkeit, neue Benutzer einzurichten oder bestehende Benutzer zu löschen bzw. umzubenennen. Sie legen dann für jeden Benutzer das Accounting, die Login Restrictions, das Login Script, die Time Restrictions oder die Station Restrictions fest.

Zudem können Sie einen Benutzer über einen anderen Benutzer zum Manager definieren. Mit dieser Option können Sie auch für den Benutzer die Volume-Beschränkung festlegen, also wieviel Platz der Benutzer auf dem Volume zur Verfügung hat. Werden hier keine Angaben gemacht, steht ihm das gesamte Volume zur Verfügung.

Eine ganz wichtige Definition ist die Vergabe von Trustee-Rechten für Directories bzw. Dateien, die ein einzelner Benutzer erhalten soll.

17.3.7 Das Pconsole-Menü

Dieses Menü dient der gesamten Drucker- und Print-Server-Verwaltung im Netzwerk.

Mit den beiden Optionen *Print Queue Information* bzw. *Print Server Information* richten Sie die Druckerumgebung für Ihr Netzwerk ein bzw. überwachen diese. Mit der Option *Print Queue Information* können neue Print Queues eingerichtet oder bestehende Queues gelöscht bzw. umbenannt werden.

Für eine bestehende Queue können zudem folgende Funktionen durchgeführt werden:

- Auflisten der momentanen Druckaufträge in der Queue mit der Möglichkeit, die Priorität von Druckaufträgen zu ändern.
- Löschen eines oder mehrerer Druckaufträge.
- Ändern der Parameter eines Druckauftrags.
- Hinzufügen eines neuen Druckauftrags (vgl. mit NPRINT-Befehl).
- Anzeigen und Ändern des momentanen Queue-Status.
- Anzeigen der Print-Queue-ID.

17 Benutzeroberfläche von NetWare 3.2

- Festlegen, wer Print-Queue-Operator-Status erhält (können Benutzer oder Gruppen sein).
- Festlegen, welcher Print-Server diese Queue bedient.
- Festlegen, welcher Benutzer in diese Queue Druckaufträge ablegen darf.

Mit der Option *Print Server Information* stehen Ihnen folgende Möglichkeiten zur Verfügung:

- Vergabe und Änderung des Paßworts für den Print-Server. Jedemal, wenn der Print-Server gestartet wird, muß dieses Paßwort eingegeben werden.
- Vergabe eines sprechenden Namens für den Print-Server.
- Einrichten der Print-Server-Konfiguration: welche Drucker bedient der Print-Server, Festlegung der Notify-List (um Fehlermeldungen des Druckers an Benutzer und Gruppen zu schicken), Festlegung, welche Queue der Drucker bedient, etc.
- Anzeigen der Print-Server-ID.
- Festlegen, wer Print-Server-Operator ist (Benutzer oder Gruppen).
- Festlegen, welche Benutzer Print-Server-User sind; diese können sich dann Informationen über den Print-Server-Status anzeigen lassen, aber nichts ändern.

Unter NetWare 3.12 und beim Einsatz des Print-Servers können Sie im Netzwerk erst dann drucken, wenn Sie mindestens einen Print-Server ordnungsgemäß eingerichtet und gestartet haben.

17.3.8 Das Printcon-Menü

Das Printcon-Menü und das nachfolgende Printdef-Menü bieten weitere Möglichkeiten, mit denen es Ihnen erleichtert wird, das Drucken im Netzwerk zu steuern. Diese beiden Menüs müssen jedoch, im Gegensatz zum Pconsole-Menü, nicht eingesetzt werden. Mit dem Printcon-Menü kann sich jeder Benutzer eigene Druckkonfigurationen einrichten.

Wie bei der Behandlung der Commandline-Utilities angesprochen, können Sie mit dem Befehl CAPTURE Ihre Druckaufträge in eine Print-Queue umleiten, sofern dies nicht bereits von Ihrer netzwerkfähigen Software geregelt wird. Der CAPTURE-Befehl läßt sich mit einer Vielzahl von Parametern steuern, die in der Regel je nach Bedarf eingesetzt werden können. Es handelt sich dabei zum Beispiel um die Angabe der Queue, der Anzahl der Kopien, des Timeout, ob mit oder ohne Banner gedruckt wird, mit oder ohne Seitenvorschub nach Druckende etc. Um den Benutzern die Arbeit zu erleichtern, können sich diese mit Hilfe von Printcon-Druckjobkonfigurationen

17.3 Menü-Utilities

einrichten, in denen diese Parameterwerte bereits gesetzt sind. Beim Aufruf von CAPTURE wird dann nur noch die Druckjobkonfiguration angegeben, die verwendet werden soll. Zudem hat der Benutzer die Möglichkeit, eine Default-Druckjobkonfiguration zu definieren, die immer dann verwendet wird, wenn im CAPTURE-Befehl keine Druckjobkonfiguration angegeben ist.

Der Supervisor hat zudem die Möglichkeit, entweder von ihm eingerichtete Druckjobkonfigurationen oder die eines anderen Benutzers für einen Benutzer zu kopieren.

17.3.9 Das Printdef-Menü

Mit diesem Menü können sowohl Formulare als auch sogenannte Print-Devices festgelegt werden. Formulare werden immer dann eingesetzt, wenn Sie einen Drucker im Netzwerk verwenden, auf dem Druckaufträge ausgegeben werden, die auf unterschiedlichem Papier gedruckt werden müssen. Jedesmal wenn ein Druckauftrag ausgegeben wird, dessen Formularnummer nicht mit der übereinstimmt, die dem Drucker momentan bekannt ist, wird der Drucker angehalten und eine Meldung ausgegeben, daß das entsprechende Formular eingelegt werden soll. Ist dies geschehen, muß der Druckauftrag zum Ausdruck angestoßen werden. Mit der Option *Form* können Sie im Printdef-Menü neben den Formularnummern zusätzlich Namen definieren. An der Console wird dann zum Beispiel für das Formular mit der Nummer 7 und dem Namen *Geschäftspapier* der Hinweis gegeben, daß das Formular »Geschäftspapier« in den Drucker eingelegt werden muß. Bei der Behandlung des Print-Servers wird erklärt, wie sich die Druckausgabe über die Formulardefinitionen steuern läßt.

Print-Devices bieten die Möglichkeit, für einen Drucker Device-Functions zu definieren. Dabei handelt es sich um alle Steuersequenzen, die für den entsprechenden Drucker (Print-Device) zur Verfügung stehen (Schmaldruck, Fettschrift, Unterstreichen etc.). Mit Hilfe dieser *Device-Functions* können nun Device-Modes festgelegt werden. In ein Device-Mode werden alle notwendigen Device-Functions eingetragen, die notwendig sind, um den Drucker für eine bestimmte Arbeitsweise zu initialisieren. Wenn Sie nun einen Druckauftrag ausgeben und einen Device-Mode hierzu festlegen, wird der Drucker zuerst in die Arbeitsweise initialisiert, die mit dem Device-Mode festgelegt worden ist, und anschließend wird Ihr eigentlicher Druckauftrag ausgeführt. Am Ende des Druckauftrags wird der Drucker durch den Device-Mode *Re-Initialize* in Grundstellung gebracht.

17 Benutzeroberfläche von NetWare 3.2

Durch die *Import*-Funktion können bereits bestehende Print-Devices eingelesen werden (mit NetWare wird bereits eine Vielzahl solcher Print-Devices ausgeliefert). Mit der *Export*-Funktion können definierte Print-Devices auf Platte, Diskette oder auf einen anderen File-Server ausgelagert werden, um diese an einem anderen File-Server durch Import wieder einzulesen.

17.3.10 Das Fconsole-Menü

Das Fconsole-Menü bietet unter NetWare 3.2 nicht mehr all die Optionen, die man in der Vergangenheit hatte. Dies liegt daran, daß mit NetWare 3.2 sämtliche Informationen in das File-Server-Monitor-NLM verlagert worden sind. Die einzigen Optionen, die Ihnen unter NetWare 3.2 für das Fconsolen-Menü zur Verfügung stehen, sind das Versenden von Broadcast-Nachrichten, das Wechseln des File-Servers, die Connection-Information, die jedoch sehr eingeschränkt ist, da alle weiteren Informationen über das Monitor-File-Server-Menüsystem zur Verfügung stehen, das Runterfahren des File-Servers, die Status-Information, um Datum und Uhrzeit des Servers zu ändern, und den Login am File-Server zu aktivieren bzw. zu deaktivieren, das Ein- und Ausschalten des TTS-Systems und die Anzeige der Version des File-Server-Betriebssystems.

17.3.11 Das Colorpal-Menü

Mit dem Colorpal-Menü hat jeder Benutzer im Netzwerk die Möglichkeit, die Farbgestaltung der Novell-Menüsysteme an die eigenen Bedürfnisse anzupassen. Man kann dabei entweder die fünf bestehenden Farbpaletten ändern, dann ändern sich damit auch die Menüfarben der NetWare-Menüs (diese verwenden nur Palette 0 bis 4), oder neue Farbpaletten definieren, die dann speziell für selbst geschriebene Menüsysteme zur Verfügung stehen (siehe nachfolgende Beschreibung).

17.3.12 Das NetWare-Menüprogramm

In früheren NetWare-Versionen wurde bereits ein einfaches Menüsystem von Novell ausgeliefert. Das war jedoch wenig leistungsfähig im Vergleich zu anderen am Markt existierenden Menüsystemen (zu großer Speicherbedarf, wenig Möglichkeiten zur Gestaltung der Menüoptionen etc.). Dieses Manko wurde mit NetWare 3.2 und NetWare 4.x beseitigt. Das heißt, die beiden NetWare-Versionen werden mit einem neuen Menüsystem ausgeliefert. Novell bedient sich dabei einer Lizenzvereinbarung mit Saber Software und liefert NetWare mit einer eingeschränkten Software dieses Hersteller aus.

17.3 Menü-Utilities

Eine der bemerkenswerten Optionen dieses Systems besteht unter anderem darin, daß über zusätzliche Funktionen verhindert werden kann, daß der Benutzer das Menüsystem verläßt und dann auf der DOS-Betriebssystemebene landet. Wie beim alten Menüsystem auch werden die Menüsystemdateien mit einem herkömmlichen ASCII-Editor erstellt. Diese erstellte Datei (das Source File) muß mit einem Compiler übersetzt werden. Hierfür steht das Programm MENU-MAKE.EXE zur Verfügung. Durch die Eingabe MENU-MAKE source_file.SCR wird eine Datei source_file.DAT erzeugt, eine nicht mehr editierbare Datei zum Ausführen des Saber-Menüsystems. Das Menü selbst wird dann über den Befehl NMENU source_file aufgerufen. Für das Erstellen eines Menüsystems steht eine Vielzahl von Schlüsselwörtern (Syntax und Befehle) zur Verfügung. Die wichtigsten Funktionen dabei sind:

- Aufrufen von .COM-, .EXE-, .BAT-Dateien, das Verlassen des Menüsystems, das temporäre Verlassen, und zwar mit der Möglichkeit, wieder in das Menüsystem zurückzukehren oder einen regulären Logout auszuführen.
- Abrufen von Eingabeparametern, wenn Programme aufgerufen werden, die einen Eingabeparameter benötigen.
- Ausführen von Menüsubroutinen.

Ein großer Vorteil des Menüsystems ist darin zu sehen, daß es sehr wenig Hauptspeicher zur Ausführung belegt, ein Problem, das dem alten Menüsystem (in Abhängigkeit der Version) leider nachgesagt werden muß.

Wenn von NetWare 3.12 auf NetWare 3.2 oder NetWare 4.x umgestellt wird und bereits mit dem alten Menüsystem gearbeitet wurde, dann bietet das neue Menüsystem eine Konvertierungsroutine an, um alle bestehenden Menüsysteme in das neue System zu überführen.

Nachdem ich Ihnen alle Befehle und Menüsysteme, die auf der Workstation zur Verfügung stehen, kurz dargestellt habe, will ich anschließend alle Consolen-Befehle darstellen. Da man hierbei zwischen Befehlen und NLMs unterscheiden muß, werde ich in Klammern »Befehl« oder »NLM« dazuschreiben. Hierbei beachten Sie dann bitte, daß jedes NLM durch den Consolen-Befehl LOAD geladen werden muß. Zudem ist bei den NLMs zwischen Driver und Menüsystemen zu unterscheiden.

17.4 Consolen-Befehle

LOAD (Befehl) Er ist einer der wichtigsten Befehle. Hiermit werden alle NLMs am File-Server geladen. Als NLMs stehen derzeit unter anderem standardmäßig zur Verfügung (dies ist nur ein kleiner Auszug der unterstützten NLMs, andere werden von Drittherstellern bereitgestellt):

Disk-Driver	
AHA1520	Adaptec-SCSI-Plattencontroller
AHA1540	Adaptec-SCSI-Plattencontroller
AHA1640	Adaptec-SCSI-Plattencontroller
AHA1740	Adaptec-SCSI-Plattencontroller
AIC7770	Adaptec-SCSI-Plattencontroller
ISADISK	AT-Plattencontroller
IDE	AT-BUS-Plattencontroller
DCB	Novell Disk Coprocessor Board
PS2ESDI	IBM ESDI-Driver für PS/2 Modelle
PS2MFM	IBM MFM-Driver für PS/2 Modelle
PS2SCSI	IBM SCSI-Driver für PS/2 Modelle

LAN-Driver	
TRXNET	schneller RXNET-Driver für Novell-ARCNET-Karten, kann auch für alle RXNET-kompatiblen Boards eingesetzt werden
3C503	Ethernet-Karte von 3COM
3C505	Ethernet-Karte von 3COM
3C523	Ethernet-Karte von 3COM
MADGEODI3	Token-Ring-Karte von Madge
NE2	Ethernet-Karte von Novell PS/2 MCA
NE-32	Ethernet-Karte von Novell 32-Bit PS/2 MCA
NE1000	Ethernet-Karte von Novell ISA
NE2000	Ethernet-Karte von Novell ISA
NE3200	Ethernet-Karte von Novell EISA

17.4 Consolen-Befehle

LAN-Driver	
TOKEN	IBM-Token-Ring 4/16 Mbit/s, erkennt selbst, ob Karte mit 4 Mbit/s oder 16 Mbit/s eingesetzt wird
PCN2L	IBM PC-Network II & Baseband
TOKENDMA	IBM-Token-Ring-Bus Master
IPTUNNEL	IP Tunnel-Mechanismus für IPX-Transportprotokoll

DISKSET

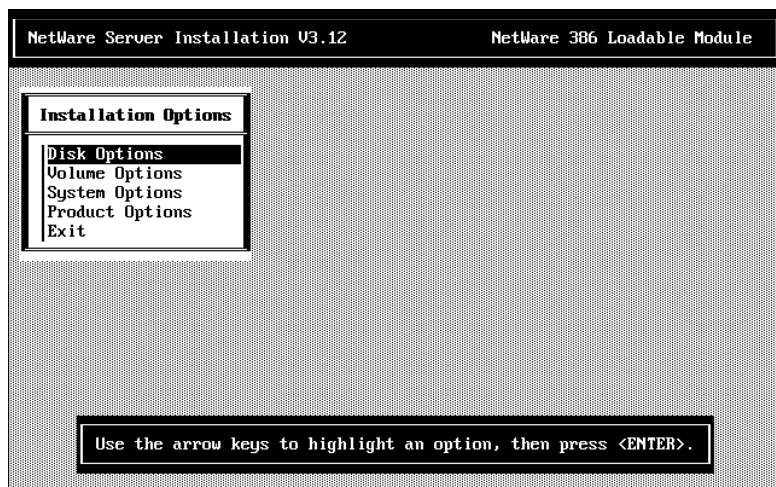
Spezielles Menüsystem zum Einrichten der DCBs, um diesen mitzuteilen, welche Platten am DCB angeschlossen sind. Nur beim Einsatz von Novell-DCBs notwendig.

Für Driver können mit dem Befehl *LOAD Driver* auch noch die benötigten Parameter (IRQ, DMA, PORT etc.) angegeben werden, ansonsten werden die benötigten Angaben interaktiv abgefragt.

INSTALL (NLM)

Dieses NLM-Menüsystem dient zum Installieren des File-Servers. Hiermit werden neue Platten hinzugefügt und eingerichtet, Platten formatiert, NetWare Partitions auf den Platten erstellt, Partitions gelöscht, der Hot-Fix-Bereich geändert, Platten gespiegelt oder geduplext (bis zu acht Stück), die Spiegelung wieder aufgehoben, die Platte getestet, Volumes eingerichtet, Volumes gelöscht, Volumes umbenannt, Volumes vergrößert, System- und Public-Dateien auf das Volume SYS übertragen und alle notwendigen Einstellungen durchgeführt, um den File-Server automatisch booten zu können. In Abbildung 17.1 ist dieses Menüsystem dargestellt.

Abbildung 17.1
Aufbau des
Install-NLMs für
NetWare 3.2



17 Benutzeroberfläche von NetWare 3.2

- REMOTE (NLM)** Modul, das zusammen mit RSPX auf dem Server geladen werden muß, um von der Workstation aus den File-Server mit dem Befehl RCONSOLE überwachen zu können.
- RSPX (NLM)** Muß zusammen mit REMOTE-NLM geladen sein.
- MAC (NLM)** Macintosh Name Space Module, damit auf dem Server die Dateien mit der Macintosh-Dateinamenskonvention abgelegt werden können.
- KEYB (NLM)** Einstellen der nationalen Tastaturtreiber für die Server-Console. Somit kann auch ein deutscher Tastaturtreiber geladen werden (ein Wunsch, der schon lange geäußert worden ist). Unterstützte Tastaturtreiber sind: United States, Germany, France, Italy, Spain.
- EDIT (NLM)** Dieses NLM dient dazu, an der Server-Console kleine Textdateien anzulegen und zu ändern. Damit lassen sich auch die beiden wichtigen Dateien auf der lokalen DOS-Partition am Server editieren (CONFIG.SYS, AUTOEXEC.BAT).
- PING (NLM)** Mit diesem Modul kann an der Server-Console überprüft werden, ob vom Server aus TCP/IP-Endgeräte erreicht werden können. Somit wird die korrekte Konfiguration der TCP/IP-Umgebung überprüft.
- TCP/IP (NLM)** Zum Laden des TCP/IP-Protokoll-Stacks muß dieses Modul aktiviert werden.
- TCPCON (NLM)** Zur Überwachung der TCP/IP-Netzwerkumgebung dient dieses Menüsystem, das an der Server-Console aktiviert und angewandt werden muß.
- SBACKUP (NLM)** Ein von Novell standardmäßig mitgeliefertes Backup-System. Es ist zwar nicht sehr günstig in seiner Bedienung, kann aber ganz gut, vor allem als Übergangslösung, eingesetzt werden, bis das richtige Backup-System gefunden ist.
- ADD NAME SPACE (Befehl)** Damit Dateien auf dem Volume anders als in der DOS-Format-Dateikonvention abgelegt werden können, muß dem Volume dies bekanntgegeben werden. Hierzu muß angegeben werden, welcher Name Space an welches Volume gebunden werden soll.
- BIND (Befehl)** Hiermit wird dem LAN-Treiber mitgeteilt, welche Transportprotokolle dieser unterstützen kann. Das Transportprotokoll wird an den LAN-Treiber gebunden.
- CONFIG (Befehl)** Anzeigen der wichtigsten File-Server-Informationen (Konfiguration des File-Servers), wie zum Beispiel File-Server-Name, geladene LAN-Treiber, unterstützte Transportprotokolle des LAN-Treibers oder auch die Node-Adresse der Netzwerkadapterkarte.
- DISPLAY NET-WORKS (Befehl)** Auflisten aller vorhandenen Netzwerkadressen im Internet.

17.4 Consolen-Befehle

DISPLAY SERVERS (Befehl)	Auflisten aller vorhandenen File-Server im Internet.
EXIT (Befehl)	Nachdem der Server runtergefahren ist, kann hiermit zu DOS gewechselt werden, wenn dieses nicht entfernt worden ist. Es kann auch ein Warmstart durchgeführt werden, sollte DOS nicht mehr vorhanden sein.
MODULES (Befehl)	Auflisten aller bereits geladenen NLMs am File-Server.
REMOVE DOS (Befehl)	DOS wird damit aus dem Hauptspeicher des File-Servers entfernt. NLMs können somit nicht mehr über das Diskettenlaufwerk oder die interne DOS-Platte (falls eingerichtet) geladen werden. Der freiwerdende Hauptspeicher wird dem File-Caching-Bereich zugewiesen.
RESET ROUTER (Befehl)	Die Router-Tabelle (wichtig für Internetwork) im File-Server wird neu aufgebaut.
SEARCH (Befehl)	Dieser Befehl wird verwendet, um für den File-Server Suchpfade zu definieren, also um diesem mitzuteilen, von welchen Directory-Pfaden NLMs geladen werden sollen. Es können zusätzliche Suchpfade definiert oder bestehende gelöscht werden. Insgesamt können 20 File-Server-Suchpfade eingerichtet werden.
UNBIND (Befehl)	Entfernen eines Transportprotokolls vom LAN-Driver.
UNLOAD (Befehl)	Entfernen eines NLMs aus dem Hauptspeicher des File-Servers. Der freiwerdende Speicher wird dem File-Caching-Bereich zugewiesen.
SET (Befehl)	Dieser Befehl dient zum Anzeigen und Ändern der Betriebssystemparameter von NetWare 3.2. Die Einstellungen werden normalerweise beim Starten und während des Betriebs von NetWare 3.2 selbst vorgenommen (Dynamic Ressource Configuration). Änderungen von Parametern sollten mit Sorgfalt durchgeführt werden, um die Leistungsfähigkeit des Servers nicht zu reduzieren. Sie haben folgende Möglichkeiten der Parameterbereiche zur Verfügung, die sich wiederum in Unterbereiche aufteilen: ■ Communications ■ Memory ■ File-Caching ■ Directory-Caching ■ File-System ■ Locks ■ Transaction-Tracking ■ Disk ■ Miscellaneous

17 Benutzeroberfläche von NetWare 3.2

BROADCAST (Befehl)	Versenden von Nachrichten an alle angemeldeten Benutzer oder nur an bestimmte Benutzer.
CLEAR STATION (Befehl)	Freigabe aller File-Server-Ressourcen, die von diesem Benutzer belegt worden sind. Schließen aller offenen Dateien, die dieser Benutzer im Zugriff hatte, und Löschen der Verbindung.
CLS (Befehl)	Löschen des File-Server-Bildschirms.
DISABLE LOGIN (Befehl)	Das Anmelden neuer Benutzer ist ab diesem Zeitpunkt nicht mehr möglich. Bereits angemeldete Benutzer sind davon nicht betroffen, außer sie melden sich ab und wollen sich an diesem File-Server erneut anmelden.
DISABLE TTS (Befehl)	Abschalten der TTS-Funktion am File-Server.
DISMOUNT (Befehl)	Ein bestimmtes Volume wird vom File-Server abgehängt. Auf dieses kann so lange nicht mehr zugegriffen werden, bis ein erneutes »Mounten« des Volumes erfolgt.
DOWN (Befehl)	Zurückschreiben aller Puffer des File-Server-Hauptspeichers, Schließen aller geöffneten Dateien und anschließendes Herunterfahren des File-Servers.
ENABLE LOGIN (Befehl)	Neue Logins am File-Server werden wieder zugelassen, nachdem diese mit DISABLE LOGIN unterbunden worden sind.
ENABLE TTS (Befehl)	Das TTS-System wird wieder eingeschaltet, nachdem dieses mit DISABLE TTS abgeschaltet worden ist.
MONITOR (NLM)	Das Monitor-System dient zur Überwachung des gesamten File-Servers. In Abbildung 17.2 ist das Hauptmenü dargestellt. Es werden Ihnen damit folgende Informationen gegeben: ■ Auslastung des File-Servers ■ Cache-Memory-Status ■ User-Connections und deren Status ■ Platten- und Volume-Information ■ Ressourcen-Auslastung ■ Sperren der File-Server-Tastatur ■ Auslastung der Volumes ■ LAN-Driver-Informationen ■ NLM-Kapazitäten ■ File-Lock-Status ■ Hauptspeicherauslastung
MOUNT (Befehl)	Einzelne oder alle bisher nicht »mounted« Volumes können mit diesem Befehl an den Server gebunden und somit für den Zugriff freigegeben werden.

17.4 Consolen-Befehle

Abbildung 17.2
Aufbau des Monitor-NLMs unter
NetWare 3.2

NetWare v3.12 (25 user) - 8/12/93		NetWare 386 Loadable Module	
Information For Server DRZENK			
File Server Up Time:	0 Days 5 Hours 43 Minutes 45 Seconds	Packet Receive Buffers:	100
Utilization:	0	Directory Cache Buffers:	189
Original Cache Buffers:	15,515	Service Processes:	3
Total Cache Buffers:	11,610	Connections In Use:	1
Dirty Cache Buffers:	0	Open Files:	43
Current Disk Requests:	0		

LAN Driver Information

3C5X9 [port=300 int=5 frame=ETHERNET_802.3]

MIRROR STATUS (NLM) Damit kann überprüft werden, ob die gespiegelten (geduplexten) Platten vollständig synchronisiert sind oder gerade synchronisiert werden.

NAME (Befehl) Anzeigen des File-Server-Namens.

OFF (Befehl) Löschen des File-Server-Bildschirms (vgl. CLS-Befehl).

SECURE CONSOLE (Befehl) Hiermit werden gewisse Sicherheitsmechanismen für das Arbeiten an der Server-Console implementiert. Dies bedeutet:

- NLMs können nur noch von SYS:SYSTEM geladen werden.
- Der Betriebssystem-Debugger ist abgeschaltet.
- Datum und Uhrzeit des File-Servers können nur noch vom Consolen-Operator geändert werden.
- DOS wird aus dem Hauptspeicher des File-Servers entfernt.
- Es lassen sich für das Laden von NLMs keine Suchpfade mehr einrichten, d.h., der SEARCH-Befehl ist abgeschaltet.

SET TIME (Befehl) Hiermit können Datum und Uhrzeit am File-Server geändert werden.

TIME (Befehl) Anzeigen von Datum und Uhrzeit des File-Servers.

VOLUMES (Befehl) Auflistung aller momentan »mounted« Volumes am File-Server.

CLIB (NLM) Dieses NLM wird von einigen NLMs benötigt (z.B. PSERVER, Btrieve). Normalerweise verwenden NLMs den Autoload-Mechanismus – das erste NLM, welches dieses CLIB NLM benötigt, lädt dieses von selbst.

17 Benutzeroberfläche von NetWare 3.2

IPXS (NLM)	Dieses Modul wird benötigt, wenn NLMs Stream-basierende IPX-Protokolldienste verwenden. Wird in der Regel bei Bedarf auch automatisch vom ersten NLM, das dieses benötigt, geladen.
MATHLIB (NLM)	Dieses Modul wird benötigt, um den Coprozessor im Server nutzen zu können. Beim Einsatz von 80486-Servern muß dieses Modul geladen werden, da hier der Coprozessor fest implementiert ist.
MATHLIBC (NLM)	Dieses Modul wird eingesetzt, wenn der Server keinen Coprozessor besitzt.
MEMORY (Befehl)	Anzeigen des gesamten installierten Hauptspeichers, den das System adressieren kann.
NMAGENT (NLM)	Überwachung und Übergabe von Netzwerkmanagement-Parametern. Dieses Modul wird in der Regel beim Laden des ersten LAN-Drivers automatisch geladen.
REGISTER MEMORY (Befehl)	Dieser Befehl wird benötigt, um den Speicher über 16 Mbyte adressieren zu können.
ROUTE (NLM)	Damit der File-Server auch Datenpakete über IBM-Bridges in einem Token-Ring-Netzwerk transportieren kann, benötigen Sie auf dem File-Server dieses NLM.
SPXS (NLM)	SPXS wird dann gebraucht, wenn NLMs Stream-basierende SPX-Protokolldienste einsetzen.
STREAMS (NLM)	Dieses Modul muß geladen werden, wenn NLMs das CLIB NLM oder Stream-basierende Protokolldienste verwenden.
TLI (NLM)	Verwenden NLMs TLI-Kommunikationsdienste, dann muß dieses Modul geladen werden.
TOKENRPL (NLM)	Beim Einsatz von Diskless Workstations mit einer Token-Ring-Karte muß dieses Modul am File-Server geladen werden, damit die benötigten Dateien zum Starten der Workstation von der Platte des File-Servers geladen werden können.
PSERVER (NLM)	Mit diesem Modul wird ein unter PCONSOLE eingerichteter Print-Server am File-Server gestartet. In Abbildung 17.3 ist das Menübild eines aktiven Print-Servers an der File-Server-Console dargestellt.
UPS (NLM)	Mit diesem NLM wird das UPS-Monitoring-System am File-Server geladen, damit dieser in der Lage ist, ein Novell-taugliches UPS-System am File-Server anzusteuern.
VREPAIR (NLM)	Mit diesem Modul kann versucht werden, auftretende Plattenprobleme zu beseitigen. In vielen Fällen sollte nach erfolgreicher Durchführung von VREPAIR ein Austausch der Platte erfolgen.

17.4 Consolen-Befehle

Ich habe Ihnen in dieser Aufstellung sämtliche Befehle und NLMs dargestellt, ohne auf die zusätzlichen Parameterangaben, die jeder Befehl und jedes NLM zur Verfügung stellt, näher einzugehen, da das den Rahmen dieses Buchs übersteigen würde.

Abbildung 17.3
Das PSERVER-NLM
für NetWare 3.2

Novell NetWare Print Server V3.76 Server PS_DRZENK Running	
0: Brother Not connected	4: HP500GLABA Not connected
1: HP4 Not connected	5: HP500MEIER Not connected
2: HP500MOEDL Not connected	6: HP500KROLL Not connected
3: HP500DRZENK Waiting for job	7: HP500WILLI Not connected

Es soll Ihnen mit dieser Auflistung auch nur ein Eindruck von der Leistungsfähigkeit und dem Potential vermittelt werden, die Ihnen der File-Server zur Verfügung stellt.

Für das Laden von TCP/IP-, NFS-, Macintosh-Protokollen etc. werden eigene zusätzliche NLMs und damit verbundene Konventionen angeboten.

Zwei weitere Aspekte der Bedienung der File-Server-Console erleichtern das Arbeiten, Installieren oder auch Überwachen des File-Servers erheblich.

Zum einen haben Sie die Möglichkeit, mit den Pfeiltasten nach oben und unten zwischen den letzten 20 eingegebenen Consolen-Befehlen vor- und zurückzublättern. Zum anderen können Sie zwischen den einzelnen aktivierten Menüsystemen (Tasks) hin- und herblättern. Dieses Blättern zwischen einzelnen Tasks geschieht mit der Tastenkombination Alt+Esc. Wenn Sie direkt in eine aktive Task gehen wollen, dann drücken Sie die Tastenkombination Ctrl+Esc, und es werden Ihnen alle aktiven Tasks, von 1 bis n durchnummeriert, angezeigt. Sie müssen nur noch die Nummer der Task eingeben, in die Sie wechseln wollen.

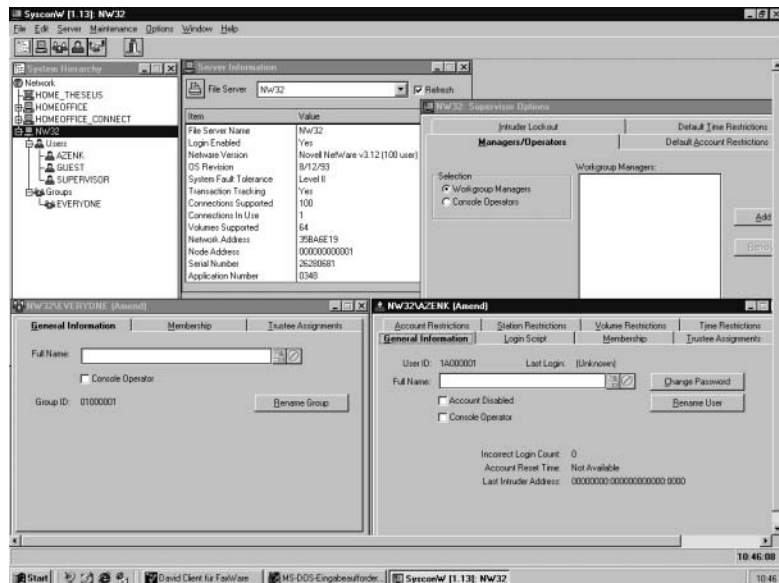
17 Benutzeroberfläche von NetWare 3.2

Die gesamten Consolen-Befehle müssen direkt am File-Server eingegeben werden. Ich habe eingangs bereits erwähnt, daß mit NetWare 3.2 ein Utility zur Verfügung steht, das es Ihnen erlaubt, den File-Server bequem von Ihrem Arbeitsplatz aus zu steuern. Es handelt sich dabei um die REMOTE CONSOLE. Dazu jedoch später mehr.

17.5 Das grafische SYSCON

Die gesamte Netzwerkverwaltung wird bei NetWare 4 bzw. NetWare 5 vollständig über ein grafisch orientiertes Administrations-Tool verwaltet. Um auch unter NetWare 3.2 die Administration etwas moderner zu gestalten, hat Novell das grafische SYSCON entwickelt. Es lassen sich damit zwar nicht alle administrativen Aufgaben erledigen, im Gegensatz zur grafischen Oberfläche von NetWare 4 bzw. NetWare 5 jedoch alles, was zum Einrichten der Benutzerumgebung notwendig ist. Um Ihnen einen ungefähren Eindruck zu vermitteln, sind in Abbildung 17.4 nahezu alle Möglichkeiten dargestellt. Aufgrund der bisherigen Beschreibungen und Möglichkeiten, die NetWare 3.2 bietet, erkennt man in dieser Abbildung sehr schnell, in welchem Menüfenster und den dazugehörigen Schaltflächen die einzelnen Einrichtungsmechanismen zur Verfügung gestellt werden und was sie im einzelnen bedeuten.

Abbildung 17.4
Das grafische SYSCON
unter
NetWare 3.2



17.5 Das grafische SYSCON

Durch die grafische Oberfläche werden wesentlich mehr flexible Optionen zur Verfügung gestellt, als man dies bislang von den C-Worthy-Menüs gewohnt ist. Dies beginnt beim bequemen Einrichten von Benutzern, Gruppen etc. und hört beim Ausdrucken von Benutzerkonfigurationen auf. Ebenso lassen sich die Server-Dateien Autoexec.ncf und Startup.ncf aus diesem Menüsystem heraus editieren und abspeichern. Nicht zu vergessen ist die Bearbeitung von Login-Scripts. Bei all diesen Eingaben kann man aufgrund der Windows-Umgebung mit Undo, Cut, Copy, Paste, Delete, Select All, Save File und Print einfach und schnell arbeiten. Ebenso gibt es ein Find-Icon und die Möglichkeit, den Editor Font zu ändern.

In der Vergangenheit war es nicht möglich, ohne Zusatz-Tools schnell und einfach für jeden Benutzer entsprechende Reports drucken zu lassen. Im grafischen Syscon ist die Möglichkeit standardmäßig vorhanden. Als Ergebnis erhält man in etwa die folgenden Informationen:

```
Novell Inc.                                     NW32:User Details
User Name:                                     [1A000001] AZENK

Full Name:                                     Andreas Zenk
Last Login:                                    Sat, 22 Aug 1998 at 15:13:07
Incorrect Login Count:                         0
Last Intruder Address:                        00000000:000000000000:0000
Account Disabled:                             No
Console Operator:                             Yes

Login Script:                                 map ins sl:=sys:public

Groups Belonged To:                           EVERYONE
                                                WINWORD

Security Equivalents:                         [Group]      EVERYONE
                                                [Group]      EVERYONE
                                                [User]       SUPERVISOR

Managed By:
Dir Trustee Assignments:                      [RWCEMFA]    SYS:AZENK
                                                [RWCEMF]     SYS:MAIL/1A000001

File Trustee Assignments:                     (None)

Account Expires:                              31 December 1998
Max. Connections:                             2
Days Between Password Changes:                30
Password Expires:                             24 August 1998
Grace Logins Allowed:                          6
```

17 Benutzeroberfläche von NetWare 3.2

Grace Logins Remaining:	6
Require Unique Password:	Yes
Require Password:	Yes
Minimum Password Length:	5
User Can Change Password:	Yes
Volume Restrictions:	SYS: Used: 0 Restriction: 10000
Station Restrictions:	00000100 (All Nodes) (None)
Login Times Allowed:	Sunday: 00:00-23:59 Monday: 00:00-23:59 Tuesday: 00:00-23:59 Wednesday: 00:00-23:59 Thursday: 00:00-23:59 Friday: 00:00-23:59 Saturday: 00:00-23:59

Man erkennt bereits an dieser kurzen Beschreibung, daß mit dem grafischen SYSCON sehr viele positive Effekte zur Verfügung gestellt werden, um das Einrichten und Verwalten von NetWare-3.2-Netzwerken zu vereinfachen. Es sei jedoch an dieser Stelle darauf hingewiesen, daß nach Möglichkeit statt NetWare 3.2 die Orientierung hin zu NetWare 4.11 bzw. NetWare 5 gehen sollte. Wem die neue NetWare-4.11-Umgebung zu komplex und kompliziert erscheint, für den bietet Novell die IntranetWare for Small Business. Diese Version läßt sich fast genauso einfach installieren und vereinfachen, wie dies mit NetWare 3.2 der Fall ist, allerdings mit allen Vorteilen, die die Novell Directory Services zur Verfügung stellen.

18

Novell NetWare SFT III

Die Sicherheitsmechanismen von NetWare sind so konzipiert, daß Sie einen Großteil der auftretenden Fehler im Netzwerkbetrieb gut in den Griff bekommen können. Sie werden sehen, daß ähnliche Mechanismen auch von anderen Netzwerkbetriebssystemen zur Verfügung gestellt werden. Das Vorgehen ist immer wieder das gleiche: Jeder Hersteller versucht Mechanismen anzubieten, die andere nicht oder noch nicht anbieten können.

Novell hat mit NetWare SFT III eine Netzwerkbetriebssystem-Version entwickelt, die einen noch größeren Sicherheitsaspekt darstellt und unterstützen kann: Das gespiegelte Server-Konzept. SFT III gibt es derzeit nur noch für NetWare 4, d.h., eine Version für NetWare 3.2 ist nicht verfügbar und wird es auch nicht mehr geben. Die erste SFT-III-Version wurde für NetWare 3.12 freigegeben, so daß es mit Sicherheit noch einige Implementierungen am Markt geben wird. Für diese Installationen ist es auf alle Fälle zu empfehlen, eine Umstellung auf NetWare 4 SFT III in naher Zukunft durchzuführen. Novell liefert auf der CD für NetWare 4 automatisch auch eine SFT-III-Version aus. Um diese SFT III installieren zu können, benötigt man lediglich die zusätzliche SFT-III-Lizenzdiskette. Die Konzepte für die SFT-III-Versionen-3.12 und -4.x entsprechen sich aber weitgehend. Deshalb gelten die hier getroffenen Aussagen im Prinzip auch für beide Versionen. Wenn ich an dieser Stelle von SFT III für NetWare 4 spreche, dann sind damit die Versionen NetWare 4.1, NetWare 4.11 und 4.2 gemeint.

Die nachfolgenden Ausführungen sollen helfen, das Konzept zu verstehen und zu sehen, welche Voraussetzungen erfüllt sein müssen, um die Mechanismen von SFT III nutzen zu können. Es sei nochmals erwähnt, daß SFT III in dieser Form zukünftig nicht mehr weiterentwickelt wird, da Novell die Cluster-Technologie und die StandbyServer-Mechanismen immer mehr forciert.

Es sei an dieser Stelle darauf hingewiesen, daß SFT III alle Mechanismen und Funktionen von SFT I und SFT II unterstützt. Da die Inhalte dieser Funktionen bereits ausführlich beschrieben worden sind, will ich mich nur noch auf die zusätzlichen Funktionen konzentrieren, die SFT III zur Verfügung stellt.

Es gibt Situationen, in denen es erforderlich wird, daß der Server im Netzwerk 24 Stunden am Tag, 7 Tage in der Woche, 12 Monate im Jahr betriebsbereit sein muß. Ein Ausfall des Servers von nur wenigen Sekunden darf nicht auftreten. Bislang konnte man nur Kon-

18 Novell NetWare SFT III

zepte anbieten, mit denen durch zusätzliche Ersatzhardware ein ausgefallener Server innerhalb von 30 Minuten wieder in Betrieb genommen werden konnte. Wenn das nicht schnell genug ist, muß auf NetWare SFT III umgestiegen werden.

Novell hat an dieser Version sehr lange gearbeitet, da es nicht ganz einfach ist, ein sicheres und stabiles System für ein gespiegeltes Server-Konzept zu entwickeln. Im Dezember 92 war es dann soweit: Die ersten Versionen von NetWare SFT III wurden ausgeliefert und installiert.

NetWare SFT III verbindet den Funktionsumfang von NetWare 4 mit zusätzlichen Fault-Tolerance-Funktionen. Es ist speziell für Unternehmen entwickelt worden, die den höchsten Grad der Zuverlässigkeit und Ausfallsicherheit benötigen. Wenn SFT-III-Funktionen nicht unbedingt benötigt werden, sollte man sich dieses System nicht bloß als Reserve zulegen, da SFT III im Vergleich zur normalen NetWare 4 teurer ist. SFT III unterstützt zwei Server im Netzwerk, auf denen ständig die gleichen Inhalte (Hauptspeicher, Platten etc.) vorhanden sind. Wenn ein Server ausfällt, übernimmt der »Ersatz-Server« ohne Verzögerung die Arbeit im Netzwerk, so daß der Anwender von diesem Ausfall nichts bemerkt, ähnlich wie ein Ausfall einer gespiegelten Platte für den Anwender nicht zu sehen ist.

Zu beachten ist dabei nur, daß es sich bei den eingesetzten gespiegelten Servern um die identischen Maschinen handelt. Novell beschreibt zwar Konfigurationen, bei denen auch unterschiedliche Server-Hardware-Komponenten eingesetzt werden, die Praxis zeigt aber, daß ein identisches Server-Paar stabil eingesetzt werden kann. Das heißt, man sollte nicht nur darauf achten, daß beide Rechner vom gleichen Rechnerhersteller sind, sondern auch das gleiche Modell repräsentieren, den gleichen Hauptspeicher und vor allem die gleiche Hauptspeicherausstattung aufweisen, die gleichen Netzwerkadapterkarten und auch die gleichen Videoadapter vorweisen können. Letztlich benötigt man für SFT III eineiige Rechner, um vor ungeahnten Folgen sicher zu sein. Alles andere kann dazu führen, daß es zu unerwünschten Nebeneffekten kommt, die aufgrund der ungleichen Rechnerausstattung verursacht werden. SFT III ist in diesem Punkt sehr eigen und empfindlich.

Zu den wesentlichen Features von SFT III zählen:

- Die Server können Online gepflegt und gewartet werden, da einer immer vollständig zur Verfügung steht und somit nacheinander zuerst der eine, dann der andere Server umgebaut und angepaßt werden kann.
- Es werden Tools zur Verfügung gestellt, die es erlauben, Fehler schnell zu isolieren und zu beheben.

- SFT III bietet die Möglichkeit zur Simulation eines Server-Ausfalls.
- Die Performance kann durch einen zweiten Prozessor erhöht werden (AMP).
- Unterstützung von TCP/IP-Protokoll-Umgebungen.
- Unterstützung von bis zu vier Mirrored Server Links (MSL-Verbindung), um auch diese Ausfälle absichern zu können.

Einsatzgebiete für SFT III

Wenn man die Frage stellt, wie lange man einen Ausfall des Servers akzeptieren könnte, erhält man nicht selten die Antwort: Der Server muß Tag und Nacht zur Verfügung stehen. Es gibt Unternehmen, die tatsächlich sehr kritische Anwendungen im Einsatz haben und bei denen der Server keine Sekunde ausfallen darf. Da bei SFT III die Server dupliziert sind, können kritische Anwendungen im Netzwerk eingesetzt werden, ohne Ausfallzeiten berücksichtigen zu müssen.

Vermeidung teurer Stillstandzeiten

Mit SFT III stehen Ihnen die Server-Funktionen immer noch zur Verfügung, auch wenn die Server-Hardware, Netzwerkadapterkarte, Netzkabel oder die High-Speed-Verbindung zwischen den Servern ausfällt oder der Netzwerkverwalter irgendwelche Maintenance-Aufgaben am Server direkt ausführen muß.

Der Platten- und Hauptspeichereinhalt des einen Servers wird auf den zweiten physikalischen Server dupliziert. Da die Informationen doppelt vorhanden sind, ist das Betriebssystem in der Lage, auf jeden Hardware-Ausfall zu reagieren, den ausgefallenen Server runterzufahren und den anderen Server die Netzwerkfunktionen übernehmen zu lassen.

Mit SFT III können Netzwerkverwalter einen Hardware-Upgrade am Server durchführen oder Routine Maintenance durchführen, ohne Stillstandzeiten im Netzwerk riskieren zu müssen. Der Hauptspeicher der Server kann erhöht werden, wenn man einen Server runterfährt, mehr Speicher einbaut, den Server wieder in Betrieb nimmt, synchronisieren läßt und dann den anderen Server runterfährt und dort den Hauptspeicher erweitert.

Sicherung der Investition

SFT III ist eine reine Software-Lösung mit einer geringen Hardware-Erweiterung. Das heißt, es können alle Server-Plattformen eingesetzt werden, die unter NetWare 4 betrieben werden. Man sollte jedoch darauf achten, daß man gerade beim Einsatz von SFT III Server-Hardware einsetzt, die speziell für diese NetWare-Version freigege-

18 Novell NetWare SFT III

ben ist, es sollte also eine Zertifizierung dafür existieren. NLMs, die nicht direkt mit der Hardware korrespondieren, können auch in der Regel unter NetWare SFT III eingesetzt werden. Zudem sind fast alle LAN- und Disk-Driver von NetWare mit SFT III kompatibel. Es wäre jedoch von Vorteil, sich vor dem Einsatz von bestimmten Modulen darüber zu informieren, ob sie auch unter SFT III lauffähig sind.

An dieser Stelle sei darauf hingewiesen, daß es derzeit in Deutschland nur einen Hersteller gibt, der eine Funkuhr zur Verfügung stellt, die auch mit SFT III eingesetzt werden kann.

Sicherheit und Recovery-Lösung

Um zu vermeiden, daß im Falle eines Falles nicht beide Server ausfallen, kann der sekundäre Server an einem anderen Ort des Unternehmens installiert werden, d.h. nicht in unmittelbarer Nähe des primären Servers. Wenn der primäre Server ausfällt, übernimmt der sekundäre Server an der Stelle die Aufgabe im Netzwerk, an der der primäre Server ausgefallen ist (so die offizielle Aussage von Novell). Das Umschalten vom ausgefallenen auf den gespiegelten Server vollzieht sich transparent, d.h., es müssen auf dem Server und auf der Workstation keinerlei manuelle Eingriffe durchgeführt werden. Für den Anwender ergibt sich bei einem Ausfall höchstens eine kurze Verzögerungszeit von drei Sekunden, bis der Requester auf der Workstation auf den neuen Server umgeschaltet hat.

Die zulässige Entfernung zwischen primärem und sekundärem Server hängt von der eingesetzten Verbindungsoption zwischen den beiden Servern ab. Der Mirrored Server Link (MSL) zwischen beiden Servern kann über Koaxialkabel oder Lichtleiterkabel durchgeführt werden. Die Koaxialverbindung ist nur für Testzwecke zu empfehlen. In der Praxis sollte die MSL-Verbindung ausschließlich über eine LWL-Verbindung erfolgen.

18.1 Produktübersicht

Durch SFT III wird das Netzwerk zuverlässiger, indem das Risiko eines Ausfalls der Server-Hardware reduziert bzw. minimiert wird. Durch die Unterstützung einer gespiegelten Server-Konfiguration ermöglicht die SFT-III-Architektur einem sekundären Server die Durchführung der Aktivitäten, die vorher vom primären Server durchgeführt wurden (Disk- und Hauptspeicheraktivitäten). Dadurch ist es möglich, daß der sekundäre Server beim Ausfall des primären Servers automatisch die Arbeit im Netzwerk übernimmt.

18.1 Produktübersicht

Architektonisch betrachtet, besteht SFT III aus zwei separaten Server-Maschinen, einem primären und einem sekundären Server, die das System in gespiegeltem Zustand hält. Den Netzwerkanwendern gegenüber erscheint nur der primäre Server – ähnlich wie Sie bei gespiegelten oder geduplexten Platten auch nur eine logische Platte zu sehen bekommen.

Auf dem sekundären Server sind jedoch Hauptspeicher und Platteninhalte identisch abgebildet. Wenn der primäre Server ausfällt oder angehalten wird, wird der sekundäre Server sofort zum aktiven primären Server.

Eine wichtige Eigenschaft sei in diesem Zusammenhang erwähnt. Der sekundäre Server läuft im Standby-Modus. Das heißt, die Aufgaben der Anwender werden nur vom primären Server übernommen, und Hauptspeicher sowie Platteninhalte werden sofort auf den sekundären Server abgebildet. Es ist also nicht so, daß der primäre und der sekundäre Server Aufgabenteilung im Netzwerk durchführen. Erst wenn der primäre Server ausfällt, kann der sekundäre Server seine ganze Leistung im Netzwerk unter Beweis stellen, vorher nicht.

Da SFT III eine Software-Lösung ist, werden keine zusätzlichen Anforderungen an die Workstation gestellt, außer dem Einsatz der aktuellen Workstation-Requester-Umgebung. Die einzige zusätzliche Voraussetzung für den effektiven Einsatz von SFT III ist die Installation eines Mirrored Server Link (MSL). MSL bietet eine bidirektionale Punkt-zu-Punkt-Verbindung zwischen primärem und sekundärem Server. Die MSL-Leitung wird benötigt, um primären und sekundären Server synchronisieren zu können.

Auch diese Verbindung kann aus Sicherheitsgründen redundant eingesetzt werden. NetWare SFT III erlaubt den Einsatz von bis zu vier MSL-Verbindungen, wobei zu einem Zeitpunkt nur ein MSL-Link aktiv ist. Sobald eine MSL-Verbindung ausfällt, schaltet NetWare SFT III automatisch auf eine Ersatzverbindung um.

Sowohl primärer Server als auch sekundärer Server sind im Netzwerk über das IPX-Protokoll ansprechbar. Das IPX-Netzwerk erfüllt dabei zwei Funktionen:

- Die Kommunikation der Workstations mit dem Server und umgekehrt.
- Die Überwachung beider Server untereinander, indem regelmäßig zwischen beiden Servern Pakete transportiert werden, um zu wissen, wie der Zustand beider Server ist.

Bei Bedarf kann SFT III auch mit TCP/IP ausgestattet werden. Hierzu müssen jedoch spezielle Installationsprozeduren beachtet werden.

18.1.1 Komponenten von SFT III

NetWare SFT III ist in zwei unterschiedliche Systeme unterteilt:

- Mirrored Server Engine (MSEngine)
- IOEngine

Der strukturelle Aufbau dieser beiden Engines ist in den Abbildungen 18.1 und 18.2 dargestellt.

Abbildung 18.1
Der Zusammen-
hang IOEngine
und MSEngine

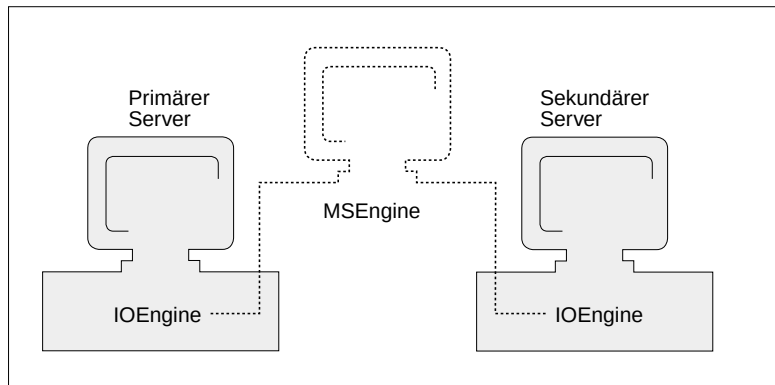
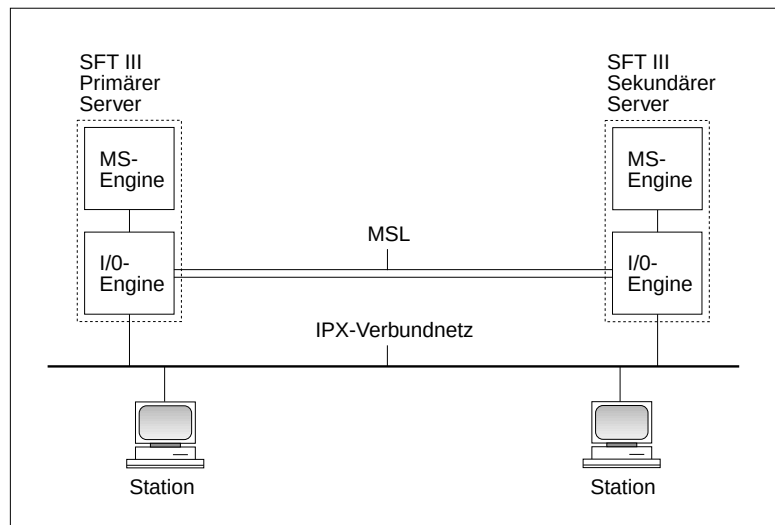


Abbildung 18.2
Funktionsweise
von SFT III



18.1 Produktübersicht

IOEngine (Input/Output Engine)

Es handelt sich dabei um den Teil von NetWare SFT III, der physikalische Prozesse durchführt, z. B. Hardware-Interrupts, Device-Drivers, Timing und Routing.

Die IOEngine transportiert Pakete zwischen dem Netzwerk und der MSEngine. Den Workstations gegenüber erscheint die IOEngine wie ein Standard-NetWare-Router. Primärer und sekundärer Server haben jeweils eine eigene IOEngine, sie benutzen aber die gleiche MSEngine.

Da die IOEngine nicht gespiegelt wird, werden auch NLMs und Anwendungen, die direkt über die Hardware am Server gekoppelt sind (z. B. Backup-Systeme), nicht gespiegelt. Hardware-abhängige Anwendungen und NLMs müssen somit auf der IOEngine auf beiden Servern installiert werden.

MSEngine (Mirrored Server Engine)

Es handelt sich hierbei um den Teil von SFT III, der keine physikalischen Prozesse durchführt, z. B. NetWare File System, Queue Management und die Bindery.

Dateisystem, Receive Buffers und Queue Management befinden sich alle in der MSEngine. Anwendungen und NLMs, die die Hardware nicht direkt adressieren können, werden gespiegelt, indem sie in der MSEngine geladen werden. Wenn ein Server ausfällt, laufen die NLMs und Anwendungen in der MSEngine weiter.

Die MSEngine kennt alle aktiven Netzwerkprozesse und bietet ununterbrochenen Netzwerkdienst, wenn der primäre Server ausfällt und der sekundäre Server die Aufgaben erledigen muß. Während des Umschaltens passiert folgendes:

- Geöffnete Dateien bleiben geöffnet.
- Workstation-Anforderungen, die im Receive Buffer eingetroffen sind, werden ohne Verzögerung verarbeitet. Anforderungen, die den Receive Buffer noch nicht erreicht haben, müssen nochmals verschickt werden.
- Druckaufträge, die bereits in der Print-Queue stehen, bleiben in der Queue erhalten, bis sie bedient werden. Druckaufträge, die noch nicht in der Queue stehen, müssen nochmals übertragen werden. Wenn die Queue nur von einem Drucker bedient wird, der am ausgefallenen Server angeschlossen ist, bleiben die Druckaufträge in der Queue, bis der ausgefallene Server wiederhergestellt ist.

18 Novell NetWare SFT III

Die IO- und MS-Engine haben folgende Eigenschaften:

- Jede Engine hat einen anderen Betriebssystem-Source-Code.
- Jede Engine besitzt einen eigenen Kernel, der einen eigenen Scheduler und Memory Allocator besitzt.
- Die beiden Engines adressieren den gleichen Hauptspeicher. Es wird jedoch festgelegt, ob das Segment im Hauptspeicher zur IO-Engine oder zur MSEngine gehört.
- NLMs die in der MSEngine geladen sind, werden automatisch immer dann gespiegelt, wenn der SFT III Server gespiegelt wird.
- NLMs in der IOEngine laufen unabhängig voneinander und werden nicht gespiegelt.

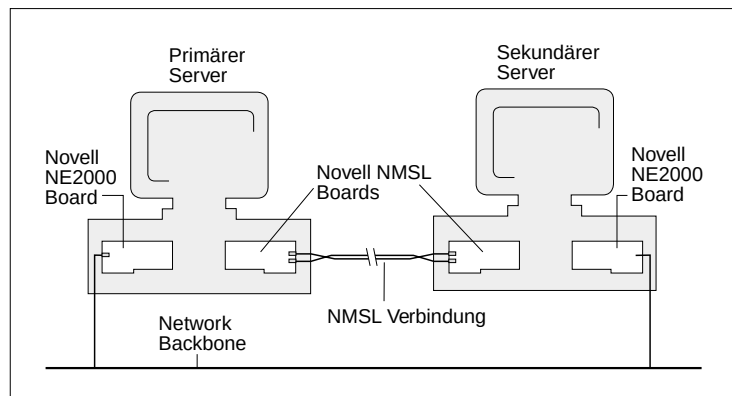
18.1.2 Server-Kommunikation

Jeder SFT-III-Server ist mit zwei Kommunikationsarten ausgestattet: IPX-Internet-Kommunikation und Mirrored-Server-Link-Kommunikation. Die IPX-Internet-Kommunikation wird zur Kommunikation mit den Workstations verwendet und zur Kommunikation von primärem und sekundärem Server, um den Status des Internet überwachen zu können.

Der MSL-Link wird zur Synchronisation beider Server benutzt. Informationen wie Client Requests und Acknowledgements werden darüber transportiert.

Die nachfolgende Abbildung zeigt, wie ein herkömmliches SFT-III-Konzept aussehen kann und welche Komponenten hierzu benötigt werden.

Abbildung 18.3
SFT-III-Implementierung



18.1 Produktübersicht

Fehlerbehandlung

Beim Einsatz von SFT III und aktivem primären und sekundären Server wird die Fehlerbehandlung sofort, automatisch und transparent für NetWare-Anwender durchgeführt. Workstations betrachten einen Serverausfall einfach als Routing-Änderung.

NetWare User können unter Umständen feststellen, daß eine kleine Pause auftritt, wenn zwischen primärem und sekundärem Server umgeschaltet wird. Die folgenden fünf Fehlersituationen und dazugehörigen Auflösungsmechanismen sind zu nennen:

■ *Fall 1: Hardware-Ausfall im primären Server*

Der sekundäre Server setzt eine Meldung an der Console mit etwa folgendem Inhalt ab:

```
Primary server failed ... this server is becoming the primary server.
```

Der sekundäre Server informiert alle aktiven Stationen, daß der sekundäre Server jetzt primärer Server ist. Workstation-Pakete werden nun zum neuen primären Server (vorher sekundären Server) weitergeleitet. SFT III behält alle Informationen, welche Änderungen auf der Platte nach dem Serverausfall durchgeführt worden sind.

Wenn das Problem des Serverausfalls behoben ist und dieser Server wieder in Betrieb genommen wird, stellt SFT III fest, daß beide Server nicht mehr synchronisiert sind. Der neue primäre Server überträgt die Änderungen über die MSL, um den wieder in-takten Server zu resynchronisieren.

■ *Fall 2: Hardware-Ausfall im sekundären Server*

Am primären Server wird an der Console etwa folgende Meldung ausgegeben:

```
Secondary Server failed... this server is remaining the primary server.
```

SFT III registriert, welche Änderungen auf der Platte seit dem Ausfall des sekundären Servers durchgeführt worden sind. Nachdem der sekundäre Server repariert worden ist und wieder in Betrieb genommen wird, erkennt SFT III, daß beide Server nicht mehr synchronisiert sind.

Der primäre Server überträgt alle Änderungen über die MSL zum sekundären Server, um beide Server zu resynchronisieren.

■ *Fall 3: Der Mirrored Server Link fällt aus*

Der sekundäre Server setzt den primären mit Hilfe der Internet-network Connection davon in Kenntnis, daß der Mirrored Server Link (MSL) ausgefallen ist. Erhält er vom primären Server daraufhin keine Antwort, wird dieser neuer primärer Server. Um nur den

18 Novell NetWare SFT III

Ausfall der MSL-Verbindung feststellen zu können, verschickt jeder Server zusätzlich 18mal pro Sekunde ein »I'm alive«-Paket.

Der sekundäre Server führt einen Neustart durch, wenn vom primären Server ein Antwortpaket kommt, und versucht, die MSL-Verbindung wieder herzustellen. Ist eine Ersatz-MSL-Verbindung vorhanden, dann schaltet der sekundäre Server auf diese um.

Ist keine MSL-Ersatzleitung vorhanden, dann muß SFT III registrieren, welche Diskänderungen seit dem Ausfall durchgeführt worden sind.

Nachdem der MSL repariert worden ist, wird der MSL Link Driver auf dem sekundären Server entladen und wieder geladen, und SFT III stellt fest, daß beide Server nicht synchronisiert sind. Der primäre Server überträgt seine Änderungen über den MSL, damit der sekundäre Server resynchronisiert werden kann.

■ *Fall 4: Ausfall des LAN-Adapters im primären Server*

Das Betriebssystem stellt die Störung des LAN-Adapters im primären Server fest. Es ermittelt den Zustand der Netzwerkkartenkarte im sekundären Server. Ist diese Karte noch funktionsfähig, übernimmt der sekundäre Server die Aufgaben im Netzwerk. Der Administrator erhält eine Nachricht über die Störung auf der Server-Console und in der Protokolldatei. SFT registriert die Plattenänderungen, die seit der Übernahme der Netzwerkaufgaben durch den sekundären Server durchgeführt worden sind.

Der ausgefallene Server wird zum sekundären Server, und der neue primäre Server überträgt seine Speicherinhalte und Plattenänderungen über die MSL an den neuen sekundären Server, um diesen zu aktualisieren und zu synchronisieren.

■ *Fall 5: Ausfall einer Festplatte*

Wenn eine Platte ausfällt, läuft das Netzwerk weiter, da alle Plattenanforderungen zur anderen Platte weitergegeben werden. Alle über einen SET-Parameter definierten Benutzer und Gruppen werden über den Ausfall der Platte informiert. Da SFT III in diesem Fall nicht mehr vollständig redundant ist, muß sobald wie möglich der Austausch der Platten erfolgen. Man kann sich natürlich auch Zeit lassen und hoffen, daß Murphy seine Hände nicht mit im Spiel hat.

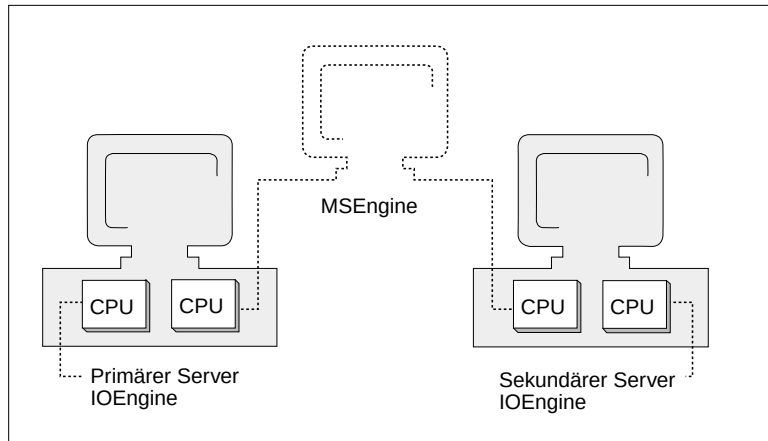
18.1.3**Dual-Prozessor-Unterstützung
(Asymmetrisches Multiprocessing)**

NetWare SFT III unterstützt die Möglichkeit, für den primären und sekundären Server eine Multiprocessing-Architektur zu verwenden, um die Performance zu erhöhen. In Abbildung 18.4 ist dargestellt, wie NetWare SFT III mit einem Multiprocessing-Konzept arbeitet.

18.2 System Management

Da SFT III in eine IOEngine und eine MEngine aufgeteilt ist, besteht die Möglichkeit, jede Engine auf einer eigenen CPU arbeiten zu lassen.

Abbildung 18.4
Dual-Processing-
Unterstützung



Zu beachten ist dabei, daß sich AMP und SMP gegenseitig ausschließen. Somit kann Symmetrisches Multiprocessing nicht in Verbindung mit Asymmetrischem Multiprocessing eingesetzt werden.

18.2 System Management

NetWare SFT III beinhaltet alle Server-Utilities, die auch in NetWare 4 enthalten sind. Einige davon mußten leicht geändert werden. Neue Utilities wurden speziell für SFT III entwickelt.

Diese neuen Utilities sollen kurz aufgeführt und erläutert werden.

Activate Server

Mit diesem Befehl wird die MEngine gestartet, der Hauptspeicher beider Server synchronisiert, und die Platteninhalte des einen Servers werden mit dem anderen Server synchronisiert. Bevor *Activate Server* ausgeführt werden kann, muß Mserver auf beiden Servern gestartet worden sein, d.h., beide IOEngines sind aktiv. Der Server, auf dem der Befehl *Activate Server* eingegeben wird, ist anschließend auch der primäre Server, und der andere Server wird automatisch zum sekundären Server. Es ist deshalb darauf zu achten, daß der Befehl *Activate Server* nur auf einer IOEngine wird und nicht in einer der vier Startdateien eingetragen wird. Wird auf beiden IOEngines *Activate Server* eingegeben, werden zwei unabhängige, nichtsynchronisierte primäre Server gestartet.

18 Novell NetWare SFT III

- Conlog** Der Befehl LOAD CONLOG wird verwendet, um alle anschließend eingegeben Befehle und Aktionen am Server in die Datei CONSOLE.LOG zu schreiben. In der Regel wird dieser Befehl ohne weiteren Parameter geladen (sofern es sich um eine NetWare-3.12- oder NetWare-4-Umgebung handelt). Da die SFT III eine IOEngine 1, IOEngine 2 und einen MServer besitzt, muß darauf geachtet werden, daß die Conlog-Datei auch in drei unterschiedliche Dateien geschrieben wird. Hierzu ist der Befehl LOAD CONLOG mit dem Parameter FILE=pfad\dateiname zu laden.
- Halt** Damit kann die IOEngine auf dem einen Server angehalten werden, während die IOEngine auf dem anderen Server weiterläuft. Der Befehl *Halt* ist nur dann gültig, wenn die SFT-III-Server gespiegelt sind oder auch die IOEngine gestartet worden ist. Dieser Befehl kann nur auf der IOEngine eingegeben werden. Wird der Befehl *Halt* auf dem primären Server eingegeben, dann wird der sekundäre Server automatisch der neue primäre Server. Die Eingabe dieses Befehls auf dem sekundären Server läßt den primären Server weiterlaufen. Man sollte darauf achten, daß man *Halt* auch nur dann eingibt, wenn die Platten der Server gespiegelt sind.
- Memory Map** Mit diesem Befehl erhalten Sie eine Aufstellung darüber, wieviel Speicher von DOS, IOEngine und MEngine benutzt wird. Der Befehl muß auf der IOEngine eingegeben werden. Wird dieser Befehl auf der MEngine eingegeben, wird der herkömmliche Memory-Befehl ausgeführt, und Sie sehen nur die Angabe des gesamten Speichers für den Server.
- Mirror Status** Hiermit erhalten Sie Informationen darüber, wie der Status der gespiegelten Platten aussieht. Wenn gerade ein RemIRRORing (Synchronisation) durchgeführt wird, bekommen Sie damit auch Informationen darüber, wieviel Prozent bereits durchgeführt sind. Dieser Befehl kann nur auf der MEngine ausgeführt werden.
- Mserver** Dieser Befehl lädt die IOEngine auf dem Server. Der Befehl *Mserver* wird unter DOS ausgeführt und ersetzt das SERVER.EXE-Programm von NetWare 4, mit dem der Server gestartet wird.
- NLMs, die unter der MEngine gestartet werden, werden auch automatisch auf dem anderen Server in der MEngine gestartet. NLMs, die in der IOEngine geladen werden, müssen auf beiden Servern separat geladen werden. Bei allen anderen Befehlen, die an der Server-Console abgesetzt werden können, ist zu unterscheiden, ob sie auf der IOEngine oder der MEngine gestartet bzw. eingegeben werden. In der Dokumentation von NetWare SFT III wird gezeigt, welche Befehle oder Module in welcher Engine zugelassen sind.

18.2 System Management

Restart

Mit diesem Befehl wird die IOEngine auf dem Server neu gestartet. Wird die primäre IOEngine neu geladen, dann wird der sekundäre Server automatisch zum primären Server. Auch hier sollte darauf geachtet werden, daß die Platten der Server voll synchronisiert sind.

Neben Befehlen wurden auch neue SET-Parameter eingeführt, die am NetWare-Server eingestellt werden können. Diese weiter auszuführen, würde dieses Buch noch dicker machen, so daß ich Sie auf die Dokumentation von NetWare SFT III verweisen möchte.

Es ist wichtig, zu verstehen, wie SFT III funktioniert und wo die Vorteile dieser NetWare-Version zu sehen sind. Für äußerst kritische Umgebungen mit großen Sicherheitsanforderungen und -bedürfnissen ist NetWare SFT III auf alle Fälle zu empfehlen. Die Installation, Bedienung und Handhabung ist nicht wesentlich schwieriger, als dies bei NetWare 4 der Fall ist. Für den Anwender selbst ändert sich gar nichts, nur der Netzwerkadministrator hat einige Zusätze, die er von NetWare 4 her noch nicht kennt.

Man sollte vor allem beim Einsatz neuer NLMs vorher prüfen, ob sie auch tatsächlich SFT-III-tauglich sind. Das sollte man jedoch nicht auf der produktiven Maschine austesten; vielmehr sollte man dazu, wie generell zu empfehlen, eine eigene Testumgebung im Einsatz haben.

Unternehmen mit weniger kritischen Datenbeständen, die in der Lage sind, bis zu 30 Minuten auf den Server zu verzichten, ist mit einem vernünftigen Ersatz-Server-Konzept gedient, da eine SFT-III-Installation doch sehr hohe Kosten verursacht. Schließlich kostet nicht nur NetWare SFT III etwas mehr als NetWare 4, auch die Hardwarekosten fallen noch ins Gewicht.

Sie benötigen für SFT III eine 1:1-Abbildung Ihrer Server-Umgebung, d.h., der Rechnertyp sollte der gleiche sein, pro Server sollten eine MSL-Karte und die gleichen Netzwerkadapterkarten vorhanden sein, es sollten gleiche Plattentypen auf beiden Servern und nach Möglichkeit auch ein gleicher Hauptspeicher existieren. Der gleich große Hauptspeicher muß zwar nicht sein, da Sie den größeren Hauptspeicher eines Servers an den kleineren Hauptspeicher durch Ausblenden von Speicher angleichen können, aber das ist nicht unbedingt zu empfehlen.

Mit SFT III ist es Novell gelungen, ein System zur Verfügung zu stellen, mit dem die notwendige Ausfallsicherheit implementiert werden kann. Im Vergleich zu den früheren Versionen ist inzwischen auch eine Vielzahl von weiteren Mechanismen verfügbar, die von wesentlicher Bedeutung sind. Dies betrifft unter anderem die Unterstützung von TCP/IP oder auch die Möglichkeit, Unix Services unter SFT III

18 Novell NetWare SFT III

einzusetzen. Andere Produkte können unter SFT III hingegen nicht eingesetzt werden. Dies betrifft unter anderem NetWare for SAA. Man muß sich deshalb mit dem Einsatz von SFT III auch damit abfinden, daß sich nicht mehr alle Add-on-Produkte auf dem SFT-III-Server einsetzen lassen. Es ist deshalb besonders wichtig, daß man sich vorher danach erkundigt, welche Zusatzanwendungen unter SFT III eingesetzt werden können.

Da SFT III nur noch für NetWare 4 ausgeliefert wird, muß zur Abrundung dieser Beschreibung von Netzwerkbetriebssystemen noch aufgezeigt werden, welche Möglichkeiten und Konzepte mit NetWare 4 verbunden sind. Einen umfassenden Überblick eines der Zugpferde von Novell soll deshalb im nächsten Abschnitt gegeben werden. Nach der Beschreibung von NetWare 4 werde ich Ihnen die ganz neuen Möglichkeiten und Konzepte von NetWare 5 näher erläutern.

19

Novell NetWare 4.2

In den vorherigen Abschnitten wurde eine Vielzahl von Funktionen und Mechanismen von NetWare 3 aufgezeigt. Als weitere leistungsfähige Betriebssystemplattform von Novell gilt die Version 4, deren Auslieferung vor ein paar Jahren begonnen hat. Seit dieser Zeit hat sie einige Neuerungen und Verbesserungen erfahren, ein Umstand, der sich bei keinem Netzwerkbetriebssystem vermeiden läßt. Novell will mit dieser Version Zeichen setzen in Richtung Realisierung kleiner, mittlerer und großer Netze. Das Konzept von NetWare 4 sieht dabei so aus, daß man sich bei der Umsetzung einer NetWare-Implementierung wahlfrei einfache und komplexe Systemumgebungen aufbauen kann. Das hängt stark von der Struktur des jeweiligen Unternehmens ab. Langfristig gesehen sollte NetWare 4 der vollständige Ersatz von NetWare 3 sein. Dies ist unter zwei Gesichtspunkten zu betrachten. Zum einen ist die Entwicklung von NetWare 3.2 mit seiner Auslieferung eingefroren worden (so zumindest die Aussagen bis zum heutigen Tag), d.h., für diese Version wird es keine Modifikationen bestehender Module direkt aus dem Hause Novell mehr geben. Nachdem NetWare 5 verfügbar ist, dürfte es auch für Novell einen zu großen Aufwand bedeuten, drei Netzwerkbetriebssysteme auf Dauer zu pflegen und zu vermarkten. Das bedeutet nun nicht, daß man sein NetWare 3.2 sofort aufgeben muß, aber man sollte sich Schritt für Schritt auf den Umstieg auf NetWare 4/5 vorbereiten. Sollten Sie vor der Entscheidung stehen, welches Netzwerkbetriebssystem Sie installieren wollen, werden Sie nach Lektüre dieses Kapitels wissen, welche Vorteile mit dem Einsatz von NetWare 4/5 gegeben sind. NetWare 4 soll als neue Plattform gedacht sein, deren Einsatz von den Anforderungen der jeweiligen Unternehmen abhängt. Schließlich wird nicht jeder die technischen Möglichkeiten von NetWare 4 vollständig ausschöpfen können und mit dem Leistungsangebot von NetWare 3 vollkommen zufrieden sein.

Es ist auch gewährleistet, NetWare 3 und NetWare 4 gemischt im Unternehmen betreiben zu können, wobei jedoch bereits jetzt darauf hingewiesen sei, daß dies langfristig nicht unbedingt zu empfehlen ist. Auf alle Fälle sollte zur Vereinfachung des Anmeldevorgangs in einer gemischten NetWare-3/4-Umgebung das Anmelden immer über den NetWare 4 Server erfolgen, da Sie ansonsten keinen vollständigen NetWare-4-Anmeldevorgang mit NDS-Unterstützung durchführen können.

19 Novell NetWare 4.2

Die nächsten Abschnitte sollen Ihnen die neuen Möglichkeiten der NetWare 4 aufzeigen. Mit NetWare 4 läutet Novell eine neue Generation einer Netzwerkbetriebssystem-Architektur ein. Die implementierten Funktionen sind eine logische und konsequente Weiterentwicklung von NetWare, die aufgrund der Anforderungen der bereits am Markt existierenden Benutzer von NetWare notwendig geworden sind. Mit NetWare 4 verabschiedet man sich vom serverorientierten Verwaltungsmechanismus und geht hin zum netzwerkweiten Verwaltungsmechanismus. Das heißt, der Server ist nicht mehr Mittelpunkt der Verwaltung, wie dies bisher mit der zentralen Bindery auf jedem einzelnen Server gewesen ist, sondern man betrachtet das Netzwerk als globale Einheit, ohne darauf Rücksicht zu nehmen, wo sich die einzelnen Server im Netzwerk befinden. Ab diesem Zeitpunkt ist es für den Benutzer wesentlich einfacher, Dienste im Netzwerk zu benutzen, da sie nicht mehr an einen Server gebunden sind. Dies bedeutet auf der anderen Seite, daß der Benutzer im gesamten Netz nur noch einmal einzurichten ist, egal wie viele Server im Netzwerk existieren. Dem Benutzer werden die Rechte auf die einzelnen Ressourcen im Netz (Drucker, Communication-Dienste, Dateien etc.) zur Verfügung gestellt. Mit NetWare 4 verwaltet man einen Pool von Ressourcen, der von allen Anwendern im Netzwerk genutzt werden kann, sofern sie die Rechte dafür haben. Dabei ist es unerheblich, von wo aus man sich im Netzwerk anmeldet. Das Ziel von NetWare 4 ist die Bereitstellung einer globalen Netzwerkinfrastruktur, um damit unabhängig von Zeit und Ort auf alle verfügbaren Ressourcen im Netzwerk Zugriff zu haben, sofern die Berechtigungen dafür existieren.

NetWare 4 besitzt nach wie vor die Eigenschaften der Vorgängerversion 3, allerdings verbessert, angepaßt und zusätzlich um eine Vielzahl wichtiger und notwendiger Funktionen ergänzt und erweitert. Nachfolgend werden die bereits bekannten Eigenschaften behandelt. Es sei darauf hingewiesen, daß man den internen Aufbau von NetWare 4 im Vergleich zu NetWare 3 vollständig geändert hat, ohne auf die wesentlichen und bewährten Funktionen, die bereits mit NetWare 3 eingeführt worden sind, aufgeben zu müssen. Aufgrund der vollständig neuen internen Aufbauten von NetWare 4 im Vergleich zu NetWare 3 hat sich Novell mit den ersten Versionen NetWare 4.0, 4.01 und 4.02 am Anfang einige »blutige Nasen« holen müssen, da gerade mit dem neuen Mechanismus NDS nicht immer alles so reibungslos lief, wie man sich das vorgestellt hat. Inzwischen hat man mit der NDS und damit verbunden mit NetWare 4 so viel Erfahrung, daß man ein sehr leistungsfähiges und stabil laufendes System vor sich hat. Das Produktspektrum von NetWare 4.2 umfaßt im wesentlichen:

- NetWare-4.2-Netzbetriebssystem
- NetWare/IP

19.1 Heterogener Workstation-Support

- DHCP Server
- FTP Server
- DNS Server
- Unix Print Services
- Web Server
- Multiprotokoll-Router (MPR)
- IPX/IP Gateway
- Netscape Navigator

Wie man sieht, enthält NetWare alle Produktkomponenten, um damit eine Systemumgebung aufbauen zu können, in der man alle Internet- und Intranet-Dienste anbieten kann. Dies beginnt beim Einsatz von IP als Protokoll und hört beim Einsatz der Unix-Druck-Dienste auf. Die nächste Generation von NetWare, NetWare 5, wird in seinen Mechanismen und im internen Aufbau nochmals gravierend geändert werden. Mit NetWare 5 kehrt Novell auch wieder zur alten Namengebung zurück. Ich werde deshalb in den nachfolgenden Ausführungen immer nur von NetWare 4 sprechen, auch wenn damit NetWare 4.2 gemeint ist.

19.1 Heterogener Workstation-Support

Nach wie vor ist es mit NetWare 4 möglich, über einen Arbeitsplatz-rechner die unterschiedlichsten Betriebssystemplattformen und Rechnersysteme zu nutzen. Es ist somit möglich, neben DOS auch Windows-, Macintosh-, OS/2-, Windows-NT-, Windows 95/98- und Unix-Systeme einzusetzen. Um den Einsatz dieser unterschiedlichen Systeme zu ermöglichen, müssen die bereits bekannten Add-ons für Macintosh, Unix etc. auf dem NetWare Server installiert werden. Dabei ist bei der Entwicklung von NetWare 4 darauf geachtet worden, daß die meisten NetWare-3-NLMs auch unter NetWare 4 eingesetzt werden können. Mit NetWare 4.2 stehen die Add-on-Module nahezu vollständig angepaßt zur Verfügung; nur der eine oder andere Hersteller wird die eigenen Produkte noch nicht vollständig für NetWare 4 angepaßt haben. Diese Produkte benötigen dann einen Mechanismus, der es erlaubt, daß sich NetWare 4 wie ein NetWare 3 Server verhält. Da diese Module auf dem Server eingesetzt werden können, benötigen sie eine Bindery. Damit NetWare 4 in der Lage ist, Bindery-basierende Produkte zu unterstützen, wird für den NetWare 4 Server eine Bindery-Emulation aktiviert bzw. unterstützt. In diesem Fall können bestimmte Bereiche der NetWare Directory Services in einer flachen Bindery abgebildet werden. Man sollte jedoch darauf achten, daß reine NDS-fähige Anwendungen zum Einsatz kommen, um auf die Bindery-Emulation vollständig verzichten zu können.

19.2 Performance und Kapazität

Performance und ausreichende erweiterbare Kapazitäten sind zentrale Kundenforderungen, wenn es um Downsizing und unternehmensweite Datenverarbeitung sowie um die Verwaltung zentraler Netzwerkressourcen geht. NetWare wird diesen Anforderungen durch ein stabiles 32-Bit-Multitasking-Betriebssystem gerecht, das die Möglichkeiten der heutigen PC-Hardware ab den 386-Prozessoren voll nutzen kann. Der Einsatz von 386-Prozessoren ist aber für einen produktiven Server-Einsatz nicht mehr geeignet. Wenn es darum geht, leistungsfähige Server zu implementieren, war man bis vor kurzem noch mit 486-Prozessoren 66 MHz sehr gut bedient. Aufgrund der immer größeren Anforderungen an das Netzwerkbetriebssystem benötigt man auch immer mehr Leistung für die Server-Maschine, so daß 486-Rechner fast nur noch in Testumgebungen eingesetzt werden, um den Restbestand solcher Rechnertypen nicht sofort ausrangieren zu müssen. Wirklich empfehlen kann man in einer produktiven Umgebung aber nur noch 586-Prozessoren und höhere. In Abhängigkeit davon, wann Sie dieses Buch lesen, könnte ich jetzt auch formulieren: Wenn Sie sich einen neuen Server kaufen, nehmen Sie immer das Beste, was Ihnen am Markt gerade angeboten wird.

Da unter Umständen ein Monoprozessorsystem nicht in der Lage sein wird, die gestellten Anforderungen zu erfüllen, kann man auch symmetrisches Multiprocessing für NetWare 4 implementieren. SMP-Unterstützung ist standardmäßig für vier Prozessoren im Produkt enthalten. Sollten Sie mehr als vier Prozessoren in Ihrem Server einsetzen wollen, dann müssen Sie sich mit Ihrem Rechnerhersteller in Verbindung setzen, damit Sie eine entsprechende NetWare-4-Version bekommen, die in der Lage ist, mehr als vier Prozessoren zu verwalten.

19.3 Zuverlässigkeit und Sicherheit

Beim Einsatz von LANs und Servern wird auch gefordert, daß diese Systeme »immer« verfügbar sein müssen. Um den Ausfall so gering wie möglich zu halten, bietet Novell seit langem unterschiedliche Sicherheitsstufen an (SFT I bis SFT III). Es liegt im Ermessen des Kunden, welche und wie viele dieser Sicherheitsanforderungen genutzt werden sollen.

Der Einsatz von Servern, auf denen in der Regel die Daten aller Anwender gespeichert werden, erfordert Mechanismen, die Daten und andere Ressourcen im Netzwerk gegenüber einem unbefugten Zu-

19.3 Zuverlässigkeit und Sicherheit

griff zu schützen. NetWare bietet dafür ein ausgereiftes und ausgefeiltes Sicherheitssystem, das zum Teil überlappend Zugriffsschutz bietet. Dieser beginnt auf Datei- und Directory-Ebene und erstreckt sich über Sicherheitsmechanismen auf User-Ebene, um Netzwerkressourcen jeglicher Art abzusichern. Mit NetWare 4 stehen Ihnen noch wesentlich mehr Möglichkeiten zur Verfügung, als dies für NetWare 3 der Fall ist. Die verbesserten Funktionen beruhen darauf, daß NetWare 4 die Ressourcen nicht mehr Bindery-basiert verwaltet, sondern in einem hierarchischen Baum einrichten und administrieren läßt. Dadurch lassen sich das Netzwerk und alle darin enthaltenen Ressourcen viel einfacher und flexibler darstellen und verwalten. Wie später noch zu sehen sein wird, hat man auch nicht mehr unbedingt einen Netzwerkverwalter, der auf alle Daten im Netzwerk unbeschränkte Berechtigung hat. Mit NetWare 4 lassen sich sogenannte Subadministratoren einrichten, die ausschließlich den eigenen streng abgesteckten Bereich verwalten dürfen. Dem Hauptadministrator können bei Bedarf Berechtigungen von bestimmten Bereichen, also auch von Volumes, entzogen werden. Auf diese Weise ist man in der Lage, ein globales Netzwerk ohne einen ausschließlichen alles kontrollierenden Hauptadministrator zu haben. Diese Einrichtung hat bei genauer Betrachtung sowohl Vor- als auch Nachteile. Es überwiegen aber in jedem Fall aufgrund der großen Netzwerkstrukturen, die sich mit NetWare 4 aufbauen lassen, die damit verbundenen Vorteile.

Um den Anforderungen der C2/E2-Sicherheit genügen zu können, sind in NetWare 4 alle notwendigen RSA-Public/Private-Key-Funktionen verankert, die es erlauben, die notwendige Sicherheit zu erhalten.

In einem Originaldokument von Novell ist bezüglich Sicherheit folgende Aussage zu lesen:

„IntraNetWare has the authentication, auditing, and other security features that make it the industry's most secure intranet solution. It is the only SOS (Anm. des Autors: Server Operating System) that meets the Class C2 certification standards of the National Computer Security Center (NCSC). Class C2 is a rating granted by the NCSC for products that have been evaluated against certain Department of Defense Standards. C2-Level security is required for many U.S. government computer installations, and it is recommended for any organization concerned about the security of its business data. With intraNetWare, your company can use the Internet as a secure, low-cost means of establishing a worldwide presence.“

19.4 Management

Der Einsatz kleinerer, mittlerer und großer Netzwerke erfordert Mechanismen, die es ermöglichen, das Netzwerk vollständig von einer zentralen Stelle aus zu überwachen und zu steuern. Hierzu gehören auch Methoden zur Fehlererkennung und -behebung. Mit NetWare werden integrierte und Add-on-Tools angeboten, die diese Anforderungen erfüllen und ein leichtes Überwachen des Netzes ermöglichen. So steht ein grafisches Administrations-Tool zur Verfügung – NWAdmin –, das es erlaubt, alle Einrichtungen, die für das Netzwerk zum Verwalten notwendig sind, durchzuführen. Dies beginnt beim Einrichten von Benutzern, der Vergabe von Berechtigungen und endet beim Aufteilen der NDS in entsprechende administrative Einheiten (Partitions und Replicas) bei alten NWAdmin-Versionen. Inzwischen wird für das Verwalten von Partitions und Replicas der NDS-Manager verwendet. Es ist somit nicht mehr notwendig, wie dies unter NetWare 3 der Fall war, von einem Menü in das andere zu wechseln, bis man alle Umgebungen eingerichtet und definiert hat. Am Server selbst stehen auch neue und erweiterte Mechanismen und Funktionen zur Verfügung, die das Arbeiten mit NetWare und vor allem die Verwaltung der NetWare Directory Services erleichtert. Durch den Einsatz von ManageWise zum Beispiel und der Implementierung der hierfür zur Verfügung gestellten NMS Agents wird der administrative Vorteil von NetWare 4 ebenfalls um ein vielfaches erhöht, da ManageWise Möglichkeiten zur Verfügung stellt, einen großen Teil der Administration über die ManageWise Console durchzuführen. Für NetWare 3 werden zwar die Agents, aber nicht die speziell für NetWare 4 installierten Administrationswerkzeuge unter ManageWise unterstützt.

19.5 Connectivity

Mit zunehmender Komplexität der Netzwerke steigt auch die Heterogenität dieser Netze, was bedeutet, daß neben NetWare auch noch andere Rechnersysteme, auf denen zentralisiert Daten abgelegt und verarbeitet werden, integriert sind. Dabei wird gefordert, daß eine kooperative Zusammenarbeit dieser Systeme ermöglicht werden soll. Mit NetWare werden die Möglichkeiten geschaffen, eine sogenannte Multi-Vendor-Client-Server-Umgebung aufzubauen und auf MDTs und Hosts zuzugreifen. Erreicht wird dies unter anderem durch Zusatzprodukte wie NetWare for SAA, Unix Services, Telephony Services, Web-Server etc. Novell bietet inzwischen eine so große Vielzahl von Zusatzprodukten an, um die Leistungsfähigkeit von NetWare 4 zu erhöhen, daß man allein mit deren Beschreibung

19.5 Connectivity

ganze Bücher füllen könnte. Deshalb soll auf die Zusatzprodukte an dieser Stelle nicht näher eingegangen werden. Wichtig ist nur, zu wissen, daß Sie die Funktionalitäten von NetWare durch passende und geeignete Add-on-Produkte erweitern und vergrößern können.

Welche zusätzlichen Möglichkeiten werden mit NetWare 4 zu den bisher bereits bekannten Mechanismen zur Verfügung gestellt, bzw. welche Funktionen von NetWare 4 wurden im Vergleich zu NetWare 3 verbessert oder geändert? Der nächste Abschnitt soll dies aufzeigen. Um einen ersten umfassenden Überblick zu erhalten, sind in der nachfolgenden Tabelle die wichtigsten Funktionen von NetWare 3 und NetWare 4 dargestellt.

*Tabelle 19.1
Die wichtigsten
Funktionen von
NetWare 3 und 4*

Dienst	Funktion oder Utility	NetWare 3	NetWare 4
Bindery / NetWare Directory Services	Datenbank für die Netzwerkressourcen	Server-basierende Bindery-Verwaltung	Globale und verteilte Datenbank
Betriebssystem	Sprachunterstützung NetWare Server für OS/2	Nur englische Sprache Nicht verfügbar	Multiple Language Support Standardmäßig enthalten, um die Non-dedicated-Funktion zu unterstützen
Installation	Installation über CD-ROM Simple- und Custom-Installation	Ab NetWare 3.12, jedoch wird eigene SERVER.EXE für Lizenzen benötigt Nicht verfügbar	Volle Unterstützung mit einer Diskette, auf der Lizenz (nicht SERVER.EXE) enthalten ist In Abhängigkeit der Netzwerkgröße kann zwischen diesen beiden Varianten gewählt werden
Dateidienste	Automatische File Compression	Nicht verfügbar	Enthalten
	Block Suballocation	Nicht verfügbar	Enthalten
	NetWare Peripheral Architecture	Ab 3.12 möglich	Enthalten
	High Capacity Storage System	Nicht verfügbar	Enthalten

19 Novell NetWare 4.2

Dienst	Funktion oder Utility	NetWare 3	NetWare 4
Storage Management System	SBACKUP Utility am Server	Basisfunktionen	Verbesserte Schnittstelle und Performance
	SBACKUP Utility	Schreibt Backup mit proprietärem Format auf das Band	Schreibt SIFD-konformes Backup-Format
	Target Services Agents	Beschränkte Unterstützung	Verbesserte Performance
Connectivity-Dienste	Protocol Mangement	Eingeschränkt	Verbesserter Support für Multiple Protocols und verbesserte Utilities zum Einrichten
	Large Internet Packets	Ab 3.12	Enthalten
	Packet Burst Protocol	Ab 3.12	Enthalten
	Laden und Konfigurieren mehrerer Protokolle während der Installation	Nicht so einfach möglich	AppleTalk, TCP/IP und IPX3
Druckdienste	Print Server, Print Queue und Printer Information	Bindery (kein Printer-Objekt verfügbar)	Directory-Service-Mechanismen
	Print Server	Bedient bis zu 16 Drucker	Bedient bis zu 256 Drucker
Sicherheitsdienste	RSA-Public/Private-Key-Verschlüsselung	Nicht verfügbar	Voll implementiert
	AUDITCON Utility	Nicht verfügbar	Bietet Auditing-Funktionen für Dateisystem und NDS

19.6 Memory Protection und Memory Management

Das Memory Management und die Memory-Allocation-Algorithmen von NetWare 4 sind vollkommen neu konzipiert. Damit wird eine erhöhte Performance, aber auch eine Sicherung von NetWare 4 und den darauf installierbaren Diensten erreicht. Wie bereits bekannt,

19.6 Memory Protection und Memory Management

wird der Kernel von NetWare 4 durch das Laden von NLMs und um bestimmte Funktionen erweitert. Alle zusätzlich geladenen Module laufen jedoch neben dem Kernel von NetWare im sogenannten Ring 0, so daß ein fehlerhaftes NLM bislang den Server zum Absturz bringen konnte. Mit NetWare 4.11 wurde ein wesentlich verbessertes Abend-Recovery-Verfahren implementiert. Dadurch wird NetWare 4 nicht nur sicherer, sondern auch stabiler.

Verbesserte Abend-Recovery-Optionen

Aufgrund der verbesserten Abend-Recovery-Optionen hat man in der neuen NetWare-Version auf den Einsatz von Protected-Ring-Mechanismen wieder verzichtet. Somit steht nicht mehr das DO-MAIN.NLM zur Verfügung, um das Netzwerkbetriebssystem um eine OS_Protected Domain zu erweitern. Die verbesserten Abend-Recovery-Techniken sollen nachfolgend näher erläutert werden:

- Am Bildschirm werden zusätzliche Informationen über den Verursacher des Abends ausgegeben. Diese Angaben identifizieren das NLM oder die Hardware-Ursache, aufgrund dessen der Abend verursacht worden ist. Der Administrator kann aufgrund dessen die notwendigen Maßnahmen gezielter einleiten.
- Wenn ein Abend auftritt, werden die Informationen darüber automatisch in die Datei ABEND.LOG geschrieben, die standardmäßig auf die lokale DOS-Partition des Servers geschrieben wird. Wenn der Server neu gestartet und dadurch auch das Volume-SYS gemountet wird, wird die ABEND.LOG-Datei an die ABEND.LOG-Datei im Verzeichnis SYS:SYSTEM geschrieben und die Datei ABEND.LOG auf der DOS-Partition gelöscht.
- *Auto Restart After Abend* ist ein neuer Parameter am Server, um den Server in die Lage zu versetzen, einen automatischen Wiederanlauf durchzuführen. Dieser Parameter ist automatisch aktiv.
- *Auto Restart After Abend Delay Time* ist ebenfalls ein neuer SET-Parameter, der am Server gesetzt werden kann. Über diesen Parameter können Sie festlegen, wie lange der Server nach einem Abend warten soll, bevor er den Server beendet und neu startet.

Die Performance von NetWare 4 wird auch dadurch gesteigert, daß ein neues Memory-Management-Schema eingeführt wurde, das im Vergleich zu NetWare 3 wesentlich effizienter ist. Kennt NetWare 3 noch fünf Memory Pools, jeder für ganz spezielle Systemressourcen auf dem Server, so nutzt man bei NetWare 4 nur noch einen Memory Pool. Auf diese Weise wird es für den Netzwerkverwalter auch einfacher, den Server zu optimieren, da nur noch ein Allocation Pool betrachtet werden muß. Zusammengefaßt hat das neue Memory Management folgende Vorteile:

19 Novell NetWare 4.2

- Vereinfachtes Memory Allocation Interface
- Gesteigerte Server-Performance
- Integriertes Paged Memory Management
- Integrierter Ring-Protection-Mechanismus

Durch dieses neue Memory Management kommt es auch zu keiner zu großen Speicherfragmentierung beim Laden und Entladen von NLMs mehr, wie dies bei NetWare 3 der Fall ist. Zudem führen die vereinfachten Memory-Management-Mechanismen dazu, daß die Entwicklung von NLMs wesentlich einfacher wird.

19.7 **Verbessertes Dateisystem**

Wesentliche Verbesserungen wurden auch für das Dateisystem von NetWare 4 eingeführt. Das Ziel ist es dabei, den Plattenplatz zu optimieren. Hierzu zählen folgende Eigenschaften:

File-by-File Compression

Die Funktion File-by-File Compression erhöht den Plattenplatz auf den NetWare Volumes unter NetWare 4, ohne dafür zusätzliche Hardware einsetzen zu müssen und ohne großen Performance-Verlust zu erleiden. Der Netzwerkverwalter kann dabei entscheiden, wann Dateien komprimiert werden und welche Dateien, Directories und Volumes mit dieser Funktionalität ausgestattet werden sollen. Sobald auf komprimierte Dateien zugegriffen wird, werden diese dekomprimiert. Das Komprimieren erfolgt im Hintergrund, d.h. als Hintergrundprozeß am NetWare Server, ohne daß der Anwender davon etwas bemerkt. Beim Einrichten eines Volume muß entschieden werden, ob dieses mit oder ohne File-Compression-Mechanismen genutzt werden soll. Standardmäßig führt NetWare zu einer vorgegebenen Zeit einen Compression-Lauf durch (täglich), um alle Dateien komprimiert abzulegen, wenn auf diese über eine vorgegebene Zeit nicht zugegriffen wurde. Die Plattenplatzersparnis beträgt im Schnitt zwischen 65 und 75 Prozent. Der gewonnene Komprimierungsfaktor hängt sehr stark davon ab, welche Dateien sich auf dem Volume befinden. So lassen sich herkömmliche Textdateien einfacher und effizienter komprimieren als Grafikdateien. Sind die Dateien aus einem bestimmten Grund bereits komprimiert, wird NetWare auch nicht mehr sehr viel herausholen können. Als Netzwerkverwalter haben Sie jedoch auch die Möglichkeit, festzulegen, wieviel Platz eine Komprimierung sparen soll, um die Entscheidung zu treffen, daß diese Datei dann komprimiert am Server abgelegt wird. Sie haben somit soviel Flexibilität, daß Sie selbst entscheiden können, welche Dateien komprimiert werden und wann die Komprimierungsläufe stattfinden sollen (standardmäßig zwischen 00:00 Uhr und 7:00 Uhr), wieviel Platz gewonnen werden soll und vieles mehr.

19.7 Verbessertes Dateisystem

Data Migration Mit dem Migration-Feature ist es möglich, Daten, die selten benötigt werden, von der teuren Platte auf billigere Medien, z.B. Streamer- oder magnetooptische Laufwerke, zu übertragen. Dem Anwender werden jedoch nach wie vor Directory-Einträge für alle Daten, die sich real auf einem ausgelagerten Medium befinden, angezeigt. Wird auf solche Daten zugegriffen, werden diese automatisch auf die Platte und das Volume zurückgespeichert, auf der sie ursprünglich abgespeichert waren.

Dem Netzwerkverwalter bleibt die Entscheidung überlassen, welche Dateien, Directories oder Volumes für die Migration der Daten ausgewählt werden sollen. Er kann auch die Entscheidung treffen, nach welchen Kriterien dies erfolgen soll (Aging-Mechanismus, Threshold). Novell führt diese Mechanismen unter der Bezeichnung HCSS (High Capacity Storage System). Nachteilig ist nur, daß das HCSS immer nur den jeweiligen Server bedienen kann. Es wäre von Vorteil, wenn HCSS von einem Server aus über das gesamte Netzwerk verteilt und angewendet werden könnte.

Suballocation Wie unter NetWare 3 kann die Disk-Allocation-Blockgröße für ein Volume beim Einrichten 4 Kbyte, 8 Kbyte, 16 Kbyte, 32 Kbyte oder 64 Kbyte betragen. Bislang war es so, daß eine gespeicherte Datei einen oder mehrere Blöcke in der jeweiligen Disk-Allocation-Block-Größe belegte.

Das heißt, daß eine Datei von 1 Kbyte auf einem Volume mit 8 Kbyte-Blockgröße einen ganzen Block von 8 Kbyte belegt, wobei 7 Kbyte ungenutzt bleiben, es sei denn, die Datei wird irgendwann einmal vergrößert.

Mit der Funktion der Suballocation werden der 1-Kbyte-Datei zwei 512-Byte-Suballocation-Blocks zugewiesen und die verbleibenden 7 Kbyte stehen für andere Dateien zur Verfügung. Da Suballocation-Blöcke in einer Größe von 512 Byte eingerichtet werden, bleiben bei einem Blockungsfaktor von 8 Kbyte 14 Suballocation-Blöcke übrig, die anderweitig genutzt werden können, also für Dateien, die ebenfalls in Suballocation-Blöcken abgelegt werden können, da diese keinen ganzen Block füllen. Legen Sie hingegen eine 9 Kbyte große Datei an, so belegt diese einen ganzen 8-Kbyte-Block und zwei 512-Byte-Suballocation-Blöcke. Sie sehen, daß entsprechend dem verwendeten Blockungsfaktor für das Volume Dateien immer einen oder mehrere ganze Blöcke belegen, wenn ein Block ganz gefüllt werden kann. Der verbleibende Überhang, der keinen ganzen Block füllen kann, wird in Form von Suballocation-Blöcken gespeichert. Für jedes Volume können andere Blockungsfaktoren eingerichtet werden. Im Vergleich zu NetWare 3 wird beim Einrichten eines Volumes nicht mehr standardmäßig ein Blockungsfaktor von 4 Kbyte

19 Novell NetWare 4.2

vorgegeben, vielmehr wird der Blockungsfaktor in Abhängigkeit von der gewählten Volume-Größe vorgeschlagen. Dieser kann bei Bedarf geändert werden. Die nachträgliche Änderung des Blockungsfaktors für ein Volume ist jedoch nicht möglich.

Mit Hilfe dieser drei Funktionen wird die Speicherkapazität eines jeden NetWare-4-Servers erhöht, und dies, ohne teure Zusatzhardware einsetzen zu müssen. Sie müssen somit seltener neue Plattensubsysteme kaufen und können Ihre bestehenden externen Speicherkapazitäten wesentlich besser nutzen.

**NetWare
Peripheral
Architecture**

Mit den NWPA-Mechanismen wird eine wesentlich breitere Treiberunterstützung für Host-Adapter und daran angeschlossene Endgeräte geboten. Die NWPA-Architektur trennt die Treiberunterstützung in die beiden Komponenten Host Adapter Module (HAM) und Custom Device Module (CDM). Das HAM-Modul steuert den physikalischen Adapter (SCSI- oder IDE-Controller), das CDM-Modul ist zur Steuerung der am Controller angeschlossenen Devices verantwortlich.

Der Hauptvorteil der Trennung von Controller- und Device-Treiber ist darin zu sehen, daß eine wesentlich höhere Flexibilität erreicht wird. Da das CDM-Modul auch noch in der Lage ist, die angeschlossenen Endgeräte selbst zu erkennen, wird die gesamte Verwaltung einfacher. Wenn ein neues Device am Controller angeschlossen wird, lädt man das entsprechende HAM-Modul, da anschließend das NWPA-Modul geladen wird (falls noch nicht geschehen) und der Controller nach angeschlossenen Devices untersucht wird, um das passende CDM-Modul zu laden. Auf diese Weise lassen sich auch neue CDM-Module laden, ohne den Treiber für den gesamten Controller entladen zu müssen. So bleiben zum Beispiel die Platten am SCSI-Controller aktiv, während man einen neuen CDM-Treiber für das angeschlossene CD-ROM-Laufwerk lädt.

**Verbesserte
Volume-
Verwaltung**

Mit der neuen NetWare sind auch die Funktionen zur Verwaltung der Volumes erweitert worden. Bislang konnte NetWare etwas mehr als 2.000.000 Directory-Einträge pro Volume verwalten. Die neue NetWare erlaubt pro Volume 8.000.000 Directory-Einträge, wenn mit mehreren Name Space Supports gearbeitet wird. Verwaltet man auf dem Volume nur DOS-Name-Space-Support, dann lassen sich 16.000.000 Directory-Einträge verwalten. Im Vergleich zu NetWare 4.1 wird man feststellen, daß das Mounten von Volumes noch schneller erfolgt als vorher.

**Unterstützung
für lange
Dateinamen**

Zur Unterstützung von langen Dateinamen verwendet die neue NetWare nur noch ein Modul: LONG.NAM. Beim Implementieren dieses Moduls können auf dem Volume anschließend die langen Dateina-

19.8 Verbessertes Sicherheitssystem und Auditing**Macintosh-
Unterstützung**

men sowohl für Windows 95/98, Windows NT als auch OS/2 Workstations genutzt werden. Somit wird auch das Arbeiten mit diesen Umgebungen einfacher und komfortabler.

Zur Unterstützung von Macintosh-Rechnern ist es nicht mehr notwendig, das AppleTalk-Protokoll zu verwenden. Optional kann man IPX und IP einsetzen. Zusätzlich muß beachtet werden, daß auf den Volumes das Macintosh-Name-Space-Modul aktiviert sein muß, sofern die Volumes von Macintosh-Rechnern im Zugriff sein sollen.

19.8 Verbessertes Sicherheitssystem und Auditing

**Login
Authentication**

Die Sicherheitsmechanismen von NetWare 4 umfassen nicht nur das Dateisystem und User Account Restrictions, sondern sie schließen auch folgendes ein:

Diese neueste Technologie, entwickelt von der RSA Corporation, bildet die Sicherheitsplattform für das gesamte Netzwerk. Wenn sich ein Benutzer unter NetWare 4 anmeldet, wird ein verschlüsselter Private Key über das Netzwerk vom Server zur Workstation übertragen.

Der Private Key wird vor der Übertragung mit dem Paßwort des Benutzers verschlüsselt, man spricht auch von einem symmetrischen Verschlüsselungsverfahren. Die weiteren Verschlüsselungsverfahren basieren auf einem asymmetrischen Verschlüsselungsmechanismus. Das Paßwort des Benutzers, das an der Workstation eingegeben wird, autorisiert den Benutzer und bildet aus dem Private Key einen Authenticator und Proof.

Immer wenn der Benutzer eine Ressource im Netzwerk anfordert, wird im Hintergrund mit Hilfe erzeugter Authentication-Daten ein Mechanismus aufgebaut und abgearbeitet, um zu überprüfen, ob diese Ressource auch genutzt werden darf. Eine Access-Control-Liste für die Ressource wird durchsucht, um zu gewährleisten, daß der Benutzer auch die vom Administrator zugewiesenen Rechte besitzt. Die Berechtigung für den Zugriff auf eine Ressource kann jedoch durch eine Vererbung der Rechte erhalten werden. Wichtig dabei ist, daß NetWare erkennt, daß die notwendigen effektiven Rechte für den Zugriff auf eine Ressource existieren, ansonsten wird der angeforderte Zugriff von NetWare verweigert.

Um diesen Sicherheitsmechanismus gewährleisten und durchführen zu können, mußte auch die NetWare-Umgebung auf der Workstation geändert werden. Hierzu sind nicht nur komplett neue Treiber nötig, sondern auch eine vollständig neue Arbeitsplatzumgebung. Novell

19 Novell NetWare 4.2

hat sich von der bislang eingesetzten Shell-Umgebung verabschiedet und verwendet jetzt den neuen NetWare-Requester-Mechanismus. Dabei handelt es sich um die gleiche Umgebung, die inzwischen auch für NetWare 3.12 eingesetzt wird. Sollen die neuen 32-Bit-Treiber verwendet werden, hat man keine VLM-Umgebung mehr, sondern die neue NIOS-Umgebung von Novell. Dazu jedoch später mehr.

**Directory
Services Security**

Die neuen Directory Services von NetWare 4 bieten neben den bereits bekannten Datei-Sicherheitssystemen zusätzliche Sicherheits-Level. Benutzer müssen Rechte haben, um Änderungen von Objekten innerhalb der NetWare Directory Services durchführen zu können. Sie werden noch sehen, daß hierbei eine wesentlich flexiblere Gestaltung der gesamten Netzwerkumgebung und Verwaltung der Objekte und Ressourcen ermöglicht werden kann. Dies hat in einer Multi-Server-Umgebung enorme Vorteile, da sich dadurch die Administration der gesamten Netzwerkumgebung im Vergleich zu NetWare 3 wesentlich einfacher gestalten und aufbauen läßt. Dies ist einer der wesentlichen Punkte, die das Arbeiten von NetWare 4 auszeichnet.

**File System
Security**

Das Dateisicherheitssystem von NetWare 4 wurde im Vergleich zu NetWare 3 nicht geändert. Das heißt, die Trustee-Rechte, Inherited Rights Filter (unter NetWare 3 als Inherited Rights Mask bekannt) und Datei- und Directory-Attribute sind die gleichen geblieben. Die Directory- und Dateiattribute wurden nur durch ein paar zusätzliche Attribute ergänzt, damit die neuen Mechanismen der Komprimierung und Data Migration unterstützt werden können.

**Management-
Aufgaben**

NetWare 4 unterstützt ein erweitertes Systemmanagement, indem unterschiedliche Levels der Supervisor Security unterstützt werden. Einem Benutzer können jetzt Rechte zugewiesen werden, die zum Beispiel erlauben, Benutzer einzurichten, allerdings ohne sie löschen zu können. Das Löschen für das Objekt Benutzer kann dann einem anderen Benutzer wiederum erlaubt werden, wobei dieser jedoch keine neuen Benutzer einrichten darf. Ebenso kann die Berechtigung existieren, Directory-Rechte im Dateisystem vergeben zu dürfen, aber nicht für Objekte des NetWare Directory Services Trustee. Dies sollen nur einige Beispiele dafür sein, wie sich mit Hilfe der NDS eine umfassende und flexible Netzwerkumgebung realisieren läßt. Im Vergleich zu NetWare 3 steht Ihnen eine Vielzahl von Mechanismen zur Verfügung, um die optimale Systemumgebung zu generieren.

Dies ist vergleichbar mit dem Workgroup-Manager-Konzept von NetWare 3, wobei die Möglichkeiten von NetWare 4 und den damit verbundenen NetWare Directory Services wesentlich umfangreicher gestaltet werden können.

19.8 Verbessertes Sicherheitssystem und Auditing

Mit NetWare 4 können Netzwerkadministratoren so eingerichtet werden, daß sie die Ressourcen zwar verwalten können, aber wichtige Daten nicht sehen dürfen. Damit wird ein weiterer Schritt in Richtung unternehmensweites Netzwerk gegangen, wobei man keine Angst mehr haben muß, daß ein »Supervisor« – wie früher – auf alle Daten zugreifen kann. Damit ist es auch wesentlich einfacher, Aufgaben der Administration im Netzwerk zu verteilen und dennoch den Überblick darüber zu behalten, was von wem durchgeführt worden ist. Es ist jetzt also auch möglich, eine größere Anzahl von Benutzern über einen Server verwalten zu lassen, d. h., die Ressourcen über einen Server verfügbar zu machen. Mit Hilfe der hierarchischen NDS-Struktur wird dann festgelegt, wer wie auf die einzeln definierten Ressourcen (inklusive Volumes und Printer) zugreifen darf. Da für die Ressourcen in der NDS separate Administratoren definiert werden können, besteht auch nicht mehr das Problem, daß ein einziger Supervisor, so wie dies unter NetWare 3 für einen Server der Fall gewesen ist, automatisch auf alle Ressourcen auf diesem Server zugreifen kann.

Der von früheren Versionen bekannte Supervisor heißt unter NetWare 4 *Admin* und wird während der Installation von NetWare 4 eingerichtet. Dieser Admin-User kann, im Gegensatz zum Supervisor bei NetWare 2.x und 3.x, gelöscht werden, wobei man vorher dafür sorgen muß, daß anderen Benutzern Admin-Rechte vergeben worden sind. Es ist damit unter NetWare 4 nicht mehr so einfach, herauszufinden, welcher Benutzer den Administratorstatus besitzt. Der Supervisor von früheren Versionen war inzwischen doch überall bekannt, und es gibt immer noch Installationen, bei denen mit der Vergabe von Paßwörtern sehr oberflächlich umgegangen wird.

Bei einer großen Unternehmensstruktur erfordern diese Mechanismen jedoch eine sorgfältige und ausgefeilte Planung, um das Optimum an Möglichkeiten und Sicherheitsfunktionen erreichen zu können. Eine »schnelle« Installation, wie dies unter NetWare 3 der Fall gewesen ist, kann mit NetWare 4 nicht mehr durchgeführt werden. Man muß sich dabei immer vor Augen halten, daß jeder NetWare 4 Server, aufgrund der NDS, einen Teil des Ganzen darstellt. Nähere Einzelheiten dazu erfahren Sie bei der Beschreibung der NetWare Directory Services.

Um den Sicherheitsanforderungen noch mehr gerecht zu werden, sind mit der NetWare 4 erweiterte Sicherheitsmechanismen eingeführt worden. Novell bezeichnet diese als NetWare-Enhanced-Security-Funktionen. Die NetWare Enhanced Security ist so konzipiert, um den Controlled-Access-Implementation-(Class 2)-Anforderungen der Trusted Network Interpretation (NCSC-TG-005) der Trusted

19 Novell NetWare 4.2

Computer System Evaluation Criteria (DoD5200.28-STD) gerecht zu werden. Hierfür werden die folgenden Funktionen zur Verfügung gestellt:

- Das Utility AUDITCON wurde dahingehend verbessert, das entsprechende C2 Auditing realisieren zu können.
- Audit-Log-Dateien werden jetzt als NDS-Objekte dargestellt und verwaltet. Auf diese Weise wird es möglich, den Zugriff auf Audit-Log-Dateien über NDS-Zugriffsmechanismen zu realisieren.
- Ein NetWare Server kann als Enhanced Security Server konfiguriert werden, indem neue zusätzliche SET-Parameter verwendet werden.
- Wird der Parameter Enable SECURE.NCF aktiviert, dann wird beim Starten von NetWare automatisch der Inhalt der NCF-Datei SECURE.NCF ausgeführt. Damit wird NetWare als Enhanced Security Server aktiviert.
- Ist die NCF-Datei SECURE.NCF nicht standardmäßig aktiviert, kann sie jederzeit im laufenden Betrieb geladen bzw. ausgeführt werden.

19.9 Erweiterte Client-Dienste

Mit NetWare 4 werden auch die Client-Dienste erweitert. Dies betrifft vor allem:

- Verbesserte DOS-Client-Software (VLM oder NIOS)
- Größere Unterstützung für Windows, Windows 95/98 und Windows NT
- Verbesserte Macintosh-Client-Unterstützung
- Erweiterte Utilities

19.9.1 Verbesserte DOS-Client-Software

Für DOS- und Windows-Workstations wird eine neue Client-Software angeboten, die in folgenden Punkten geändert worden ist:

- Open Data-Link Interface (ODI) zum Transportieren der Daten zum Zielgerät
- DOS-Requester (nicht mehr als Shell bezeichnet) – er interpretiert und bereitet die Daten zum Weitertransport auf

Die ODI-Treiber sind bereits von NetWare 3 her bekannt, mußten dort jedoch nicht unbedingt eingesetzt werden, außer man benötigte Multiprotokollunterstützung auf der Workstation (IPX und TCP/IP). Mit NetWare 4 können nur noch DOS-ODI-Treiber eingesetzt werden. Es ist zwar möglich, mit alten Treibern weiterzuarbeiten, dabei verzichtet man aber auf wichtige und grundlegende Sicherheitsfunk-

19.9 Erweiterte Client-Dienste

tionen, die dann nicht zur Verfügung stehen würden. Zum Beispiel ist das Administrieren der NDS mit einer herkömmlichen Shell-Umgebung nicht möglich. Mit einer alten Shell-Umgebung auf der Workstation können Sie sich nur als Bindery-User am NetWare Server anmelden.

In der neuen Client-Software wird automatisch das Burst Mode Protocol unterstützt, um den Datentransfer zwischen Server und Workstation zu beschleunigen. Für NetWare 3 (sofern es nicht NetWare 3.12 ist) mußte diese Funktion durch ein eigenes NLM und durch eine neue Shell implementiert werden. Mit dem Burst Mode stimmen sich Client und Server auf eine maximale Paketgröße ab, die mit einem Request übertragen werden kann. Bislang wurde das Laden von Dateien immer so vollzogen, daß die Workstation einen Request an den Server absetzte und daraufhin ein Paket erhielt; dann wurde das nächste Paket angefordert, das übernächste und so weiter. Jetzt fordert die Workstation bis zu 64 Kbyte Daten vom Server an und bekommt diese ohne zusätzlichen Request. Ist die Datei noch nicht vollständig geladen, werden die nächsten Datenblöcke angefordert. Dadurch wird die Geschwindigkeit im Netzwerk stark erhöht, und unnötiger Datenverkehr und ständige neue Requests werden vermieden.

Zudem ist automatisch der Large-Internet-Packet-Facility-Mechanismus aktiviert. NetWare 4 beinhaltet im Kernel bereits die Mechanismen Packet Burst Mode und Large Internet Packet Facility (dieser mußte unter NetWare 3.x explizit durch das PBURST.NLM geladen werden). Mit Large Internet Packet Facility tritt nicht mehr das Problem auf, daß bei einer Kommunikation zwischen Workstation und Server, wenn sich dazwischen ein Router befindet, die Paketgröße sich auf 576 Byte (brutto) reduziert. Dieser Vorgang ist gewissermaßen historisch bedingt, als nämlich NetWare beim Einsatz von Routern noch davon ausging, daß sich hinter dem Router ein ARCNET-Netzwerk befinden könnte, das in diesem Fall mit 576 Byte großen Paketen bedient werden mußte. Mit Large Internet Packet Facility sind Client und Server in der Lage, sich auf die mögliche Paketgröße abzustimmen, auch wenn ein oder mehrere Router zwischen diesen beiden Systemen implementiert sind.

Der DOS-Requester besteht aus einer Vielzahl sogenannter Virtual Loadable Modules (VLM). Diese werden vom VLM-Manager geladen (VLM.EXE). Der DOS-Requester ersetzt die frühere Shell, NETX.COM, und erlaubt jetzt die gleichzeitige Verbindung an bis zu 32 Server im Netzwerk. Um abwärtskompatibel mit NetWare 3.x zu bleiben, wird ein NETX.VLM angeboten, so daß auf NetWare 3.x Server zugegriffen werden kann bzw. Anwendungen genutzt werden können, die alte Shell-Aufrufe einsetzen.

19 Novell NetWare 4.2

Derzeit sind folgende VLMs, die vom VLM-Manager verwaltet werden können, wichtig:

- CONN.VLM: Connection Table Manager (Verwaltung gemeinsamer Tabellen, die gleichermaßen für alle VLMs erreichbar sind)
- IPXNCP.VLM: IPX Transport Module
- TRAN.VLM: Transportmultiplexer Module
- NDS.VLM: NetWare Directory Services Protocol Module
- BIND.VLM: NetWare Bindery Protocol Module (Kompatibilität mit früheren Versionen)
- NWP.VLM: NetWare Protocol Multiplexer Module
- FIO.VLM: File Input-Output Module
- GENERAL.VLM: General Purpose Function Module
- REDIR.VLM: DOS Redirector Module (führt den Attach zum Server durch)
- PRINT.VLM: Printer Redirection Module
- NETX.VLM: NetWare Workstation Shell Module (Kompatibilität zu früheren NetWare-Versionen)
- PNW.VLM: Personal-NetWare-Protokoll, um auch die Anbindung an Personal NetWare Server durchführen zu können

Mit der VLM-Umgebung und den neuen Bedienungsmechanismen unter Windows und DOS ist es auch problemlos möglich, auf allen drei NetWare-Server-Plattformen gleichzeitig zu arbeiten und angemeldet zu sein, d. h., Sie können unter NetWare 3.x, NetWare 4.x und Personal NetWare angebunden sein und auf jedem System die einzelnen Ressourcen nutzen. Man sieht auch hier wieder, daß eine nahtlose Integration all dieser Systeme möglich ist. Über eine Konfigurationsdatei NET.CFG kann für die Workstation-Umgebung unter anderem gesteuert werden, welches Server-System zuerst im Netzwerk gesucht werden soll, um daran die Anbindung der Workstation für den nachfolgenden Login durchzuführen. Die Reihenfolge NDS, BIND, PNW legt zum Beispiel fest, daß zuerst nach einem NetWare-4-System gesucht wird. Findet man dieses nicht, dann wird nach einem Bindery-Server gesucht, und wenn dieser auch nicht gefunden wird, dann sucht die Workstation nach einem Personal-NetWare-Server. Die Eingabe der Folge PNW, BIND, NDS bedeutet, welche Server der Reihe nach gesucht werden.

In diesem Zusammenhang wurden auch die Umgebungsbedingungen am NetWare Server geändert. Nicht nur, daß neue Befehle für die Ausführung der Login Scripts zur Verfügung stehen, es wurde auch eine zusätzliche Login-Script-Ebene eingeführt. Das heißt, beim Anmelden des Benutzers am NetWare Server existieren nicht mehr System- und

19.9 Erweiterte Client-Dienste

User-Login-Script, sondern System-Login-Script, Profile-Login-Script und User-Login-Script. Nach wie vor gilt, daß bei der Nichtexistenz von User-Login-Scripts ein Default-Login-Script ausgeführt wird. Da sich die LOGIN.EXE inzwischen stark vergrößert hat (über 300 Kbyte) und dies beim Ausführen von Login Scripts in Verbindung mit direkten Programmaufrufen innerhalb des Login Script zu Speicherproblemen führen kann, besteht nun die Möglichkeit, die LOGIN.EXE während dieser Zeit aus dem Speicher auszulagern.

Der Login-Ablauf eines Benutzers und der gesamten Netzwerkumgebung lassen sich somit wesentlich besser gestalten und strukturieren.

Hervorzuheben bei den neuen 32-Bit-Clients sind zuerst die Tools, um einen vereinfachten und automatischen Update auf neue Client-Umgebungen durchführen zu können. Novell stellt hierfür das Automatic-Client-Upgrade (ACU) zur Verfügung, um den notwendigen Umstellungsaufwand zu vereinfachen. Es können dabei die folgenden Umgebungen auftreten:

Umstellung von ...	Umstellung auf ...
Workstations mit 16-Bit-NetWare-DOS-Requester-Software	NetWare Client 32 für DOS- und Windows-Umgebung
Workstations mit einer älteren Version der NetWare-Client-32-für-Windows-95-Software	Aktuellste Version der NetWare-Client-32-für-Windows-95/98-Software
Workstations, die eine Microsoft-Client-Software für NetWare-Netzwerke nutzen	Aktuellste Version der NetWare-Client-32-für-Windows-95/98-Software

Da es inzwischen eine Vielzahl unterschiedlicher Clients gibt, die in einem Netzwerk zur Verfügung stehen, sollen nachfolgend die wichtigsten Neuerungen aufgeführt werden.

Auf die Funktion und den Aufbau des NetWare-DOS-Requester (VLM-Umgebung) ist bereits ausführlich eingegangen worden. Mit dem neuen NetWare-DOS-Requester für NetWare 4 sind dabei die nachfolgenden Verbesserungen verfügbar.

Diese Verbesserungen sind:

- Durch den Einsatz der Automatic-Client-Upgrade-Funktionen kann die Umstellung der VLM-Umgebung auf die zukünftige NetWare-Client-32-für-DOS- und Windows-Umgebung einfacher realisiert werden.

19 Novell NetWare 4.2

- Mit der 16-Bit-Version des NetWare-Application-Launcher-Utility können Workstations mit der VLM-Umgebung die NDS-Objekte nutzen, wenn diese Anwendungen repräsentieren.
- Die VLM-Umgebung wurde an die Anforderungen der Controlled Access Implementation (Class 2) angepaßt, um die Anforderungen der Trusted-Network Interpretation (NCSC-TG-005) der Trusted Computer System Evaluation Criteria (DoD5200.28-STD) erfüllen zu können.
- Mit der im Lieferumfang enthaltenen VLM-Umgebung werden auch die Anforderungen für 16-Bit-TCP/IP-Unterstützung, DHCP-Unterstützung und NetWare/IP-Unterstützung erfüllt.

19.9.2**NetWare Client 32**

Die neue 32-Bit-Client-Software basiert auf vollständig neuen Techniken, die nicht vergleichbar sind mit den Mechanismen, so wie sie für die VLM-Umgebung konzipiert worden sind. Die neue Client Software ist in der Lage, im Protected Mode betrieben zu werden. Zudem benötigt die Client-32-Software weniger als 5 Kbyte herkömmlichen Speicher, wobei jedoch mehr Cache zur Verfügung steht. Die Client-32-Architektur bietet die folgenden Vorteile:

- Die Installation der Client-32-Software kann über das Automatic-Client-Upgrade-Utility vereinfacht werden.
- Die Client-32-Software stellt Änderungen in der Workstation-Umgebung fest und Verbindungen im Netzwerk wieder her, sobald die verlorengegangenen Dienste wieder verfügbar sind. Auf der Workstation kann also weitergearbeitet werden, auch wenn Verbindungen zu Servern verlorengegangen sind. Damit ist die Client-32-Software robust und zuverlässig.
- Die Client-32-Software stellt häufig verwendete Benutzerdaten in den Cache (z.B. Dateiinhalte und Netzwerkinformationen). Dadurch reduziert sich der Netzwerkverkehr, und das Antwortzeitverhalten auf der Workstation wird verbessert.
- Mit der Client-32-Software kann man auf mehreren NDS-Bäumen gleichzeitig angemeldet sein und damit arbeiten.
- Die Client-32-Software kann mit 32-Bit- oder 16-Bit-LAN-Treibern ausgestattet werden. Folgende LAN-Treiber werden unterstützt:
 - 32-Bit-ODI-LAN-Treiber, die den neuesten NetWare-Treiber-Spezifikationen entsprechen.
 - 16-Bit-ODI-LAN-Treiber
 - 32-Bit- und 16-Bit-Network-Device-Interface-Specification-LAN-Treiber (NDIS), jedoch nur für NetWare Client 32 für Windows 95.

19.9 Erweiterte Client-Dienste

Diese aufgeführten Funktionen gelten im Prinzip für alle DOS/Windows- und Windows-95/98-Umgebungen. Da für DOS/Windows und Windows 95 zusätzliche Funktionen implementiert worden sind, sollen nachfolgend diese beiden Client-Betriebssysteme betrachtet werden.

NetWare Client 32 für DOS und Windows

Neben den bereits erwähnten Funktionen, stehen für DOS/Windows zusätzliche Optionen zur Verfügung:

- Das grafische User-Tool-Utility erleichtert dem Anwender die Verwaltung der Netzwerkumgebung, um Laufwerkszuordnungen und Druckerumleitungen durchführen zu können.
- Die Unterstützung für den 32-Bit-TCP/IP-Treiber ist enthalten.
- Die Unterstützung für die NetWare/IP-Software ist standardmäßig enthalten.
- Es steht ein grafisches Login-Utility zur Verfügung. Damit kann man sich unter Windows neu anmelden, und es werden auch die notwendigen Login Scripts ausgeführt, eine Funktion, die mit der VLM-Umgebung nicht zur Verfügung stand.

Im Vergleich zu Client 32 für Windows 95/98 unterscheidet sich der Client 32 für Windows in den folgenden Punkten:

- Das Kernstück der Client-32-Umgebung, das sogenannte NIOS (NetWare Input Output System), läuft als .EXE-Datei und nicht als virtueller Device Driver (VxD).
- Das NIOS nutzt die NET.CFG zur Konfiguration der Workstation und nicht die Registry.
- Es gibt keine grafische Oberfläche, um die Konfigurationsparameter zu ändern. Die NET.CFG muß in diesem Fall modifiziert und der Rechner neu gestartet werden.

NetWare Client 32 für Windows 95

Welche zusätzlichen Vorteile mit dem Client 32 für Windows 95 zur Verfügung stehen, soll in den folgenden Ausführungen erläutert werden:

- Das Kernstück des Client 32 für Windows – die NIOS-Umgebung – ist als virtueller Device-Treiber (VxD) implementiert und nicht als .EXE-Datei.
- Es gibt keine explizite Startup-Datei, da Windows 95 den Client bereits beim Starten aktiviert.
- Es gibt keine NET.CFG mehr, da die Konfigurationen für den Windows-95-Client in der Registry gespeichert werden. Aufgrund dessen kann der Windows-95-System-Policy-Editor eingesetzt werden, um die Client-32-Parameter zu überwachen.

19 Novell NetWare 4.2

- Der Client nutzt Microsofts Implementierung der Winsock, Named Pipes, NetBios und TCP/IP, so wie sie in Windows 95 standardmäßig verfügbar sind.
- Die Umstellung von Windows 3.1x auf Windows 95 in Verbindung mit der gleichzeitigen Installation von NetWare Client 32 für Windows 95 kann über einen Installationsprozeß durchgeführt werden.
- Der Client 32 für Windows 95 ist vollständig in den Explorer und die Network-Neighborhood-Utilities integriert. Zusätzlich kann über den grafischen Login-Prozeß zu jeder Zeit ein neuer Login im Netzwerk durchgeführt werden. Die Ausführung der Login Scripts ist gewährleistet, so daß anschließend die neue Netzumgebung zur Verfügung steht.
- Der Client 32 für Windows unterstützt die Verwendung von langen Dateinamen.
- Der Client 32 für Windows 95 unterstützt zudem die folgenden Standardprotokolle:
 - Windows-95-Implementierungen von TCP/IP, Winsock, Named Pipes und NetBIOS.
 - Der Client 32 IPX Protocol Stack unterstützt die Windows 95 WSOCK32.DLL.
 - Simple Network Management Protocol (SNMP)
- Der NetWare Client 32 für Windows 95 kann zusätzlich zum Microsoft Client für Microsoft-Netzwerke genutzt und parallel installiert werden.

19.9.3 Windows- und OS/2-Unterstützung

NetWare 4 bietet Ihnen eine grafische Oberfläche für Windows oder OS/2 (nur im Windows-Modus – Graphical User Interface), um die Verwaltung der Netzumgebung noch einfacher durchführen zu können. Für Windows NT wird bereits eine eigene 32-Bit-Version zur Verfügung gestellt. Die Bedienung mit der Maus ist somit eine Selbstverständlichkeit. Das bedeutet, daß nicht nur die Verwaltung des Netzwerks einfacher und bequemer ist, sondern auch das Durchsuchen des gesamten Netzwerks und aller darin verfügbaren Ressourcen.

NetWare Administrator und NETAdmin

Wie unter NetWare 4.1 bereits realisiert, wird auch in der Nachfolgeversion der größte Teil der Verwaltungsarbeit mit dem grafische Tool NWAdmin oder mit der DOS-Version-NETADMIN realisiert. Um das Arbeiten und die Verwaltung noch zusätzlich zu verbessern, wurden die folgenden Änderungen durchgeführt:

19.9 Erweiterte Client-Dienste

- Standardmäßig gibt es jetzt für den NWAdmin eine Windows-95-Version. Funktionell gibt es keinen Unterschied zur 16-Bit-Version unter Windows 3.1x. Für die Windows-95-Version gibt es jedoch im Verzeichnis SYS:PUBLIC ein eigenes Verzeichnis WIN95. Mit der Installation des Windows NT Client gibt es auch ein Verzeichnis SYS:PUBLIC\WINNT, in dem sich der 32-Bit-Client für Windows NT befindet.
- Die Oberfläche für den GUI NWAdmin kann an die Bedürfnisse des Benutzers angepaßt werden. So ist es möglich, die Menüleiste individuell anzupassen, um die sogenannten Shortcuts für die einzelnen Menüoptionen einzurichten. Die konfigurierbare Statusleiste und die Möglichkeit, einzelne Property Buttons ganz auszublenken oder die Sortierreihenfolge entsprechend den eigenen Vorstellungen zu modifizieren, zählt ebenfalls zu den vorteilhaften Änderungen in der grafischen Administration.
- Gemäß den Angaben neuer Mechanismen im NWAdmin ist es auch möglich, mehrere Bäume gleichzeitig zu administrieren – innerhalb der gleichen grafischen Oberfläche. Man kann mehrere Browse-Fenster für unterschiedliche Bäume gleichzeitig öffnen und zwischen den Browse-Fenster-Objekten hin- und herspringen.
- Bislang war es nicht möglich, mehrere Objekte im NDS-Baum zu markieren und bestimmte Property-Werte zu ändern. Mit der neuen Version von NetWare 4 kann man für mehrere markierte Objekte gleichzeitig bestimmte Properties ändern. Somit können die Properties für markierte Benutzer, Container, Templates oder auch Gruppen geändert werden.
- Das Umbenennen eines Containers erfolgt über die Option Rename Subtree, wohingegen das Verschieben eines Teilbaumes im NWAdmin über die Option Move Subtree erfolgt. Es ist also nicht mehr nötig, das Verschieben über den Partition Manager durchzuführen, allerdings muß zum Verschieben eines Teilbaumes, dieser Teilbaum als Partition definiert sein. Aus dem NWAdmin hat man die Option Partition Manager entfernt. Hierfür hat man ein eigenes Tools entwickelt, den sogenannten NDS Manager.

NDS Manager

Die gesamte Verwaltung der Partitions und Replicas ist aus dem NWAdmin entfernt worden. Hierfür gibt es das eigene GUI NDS Manager. Der NDS Manager besitzt eine grafische Oberfläche mit einem hierarchischen Browser und einer Vielzahl von Optionen und Mechanismen, die es bislang im Partition Manager nicht gegeben hat. Der NDS Manager enthält die folgenden Funktionen:

19 Novell NetWare 4.2

- Er kann als eigene Anwendung laufen oder als integrierter Part im NWAdmin installiert werden.
- Es werden damit die Partitions-Operationen und die Operationen mit den Replicas innerhalb der NDS durchgeführt.
- Es sind Funktionen enthalten, um von einer Client-Workstation aus die Reparatur der NDS durchzuführen. Bislang mußte man diese Arbeiten direkt an der Server-Konsole durchführen.
- Es ist eine Option enthalten, um einfach und schnell einzelne oder alle Server auf eine neue NDS-Version umstellen zu können. Daneben werden auch die einzelnen Versionen im GUI übersichtlich dargestellt.
- Im Hilfetext sind entsprechende Informationen hinterlegt, die Synchronisationsfehler erklären.

Gerade in einer großen Netzwerkumgebung bietet dieses Tool einen sehr großen Vorteil, da der gesamte Zustand der verteilten und globalen Datenbank sehr übersichtlich ist und daher schnell gesehen werden kann. Durch die wesentlichen Verbesserungen ist der Administrator damit in der Lage, gründlich und schnell über den Zustand der NDS zu informieren. Wer schon einmal große Netzwerke verwalten mußte, wird dieses Tool sehr zu schätzen wissen.

Für bestimmte Anwendungsbereiche steht die Möglichkeit zur Verfügung, NetWare 4 unter OS/2 zu betreiben; in diesem Fall spricht man von der Nondedicated Version NetWare for OS/2. Mit NetWare for OS/2 stehen im Prinzip die gleichen Mechanismen zur Verfügung wie auch mit Native NetWare 4. Diese Version zu verwenden, bietet sich vor allem dann an, wenn es darum geht, Anwendungen sowohl unter Netware als auch unter OS/2 zur Verfügung stellen zu müssen. Von außen sieht der NetWare for OS/2 Server aus, als würde es sich um einen herkömmlichen NetWare 4 Server handeln.

Zu beachten sind jedoch die Risiken, die mit einer Nondedicated-NetWare-Version verbunden sind. So bedeutet zum Beispiel der Absturz von OS/2 auch das Beenden der NetWare-4-Server-Umgebung, dann aber unkontrolliert.

19.9.4

Erweiterte Utilities

Viele von NetWare 3 bekannte Commandline-Utilities und Menüsysteme wurden angepaßt, um mit den neuen Directory Services arbeiten zu können. Ein großer Teil der Menüsysteme sind zusammengefaßt worden, so daß die Bedienung auf DOS-Ebene weniger Befehle zur Verfügung stellt, aber noch ebensoviel Unterstützung bietet wie bisher, da einfachere und kompaktere Menüsysteme bereitgestellt werden. Zum Beispiel sind die Menüsysteme *Salvage* und

19.10 Network Auditing

Volinfo im Menüsystem *Filer* integriert worden. Die Befehle *Allow*, *Grant*, *Remove*, *Revoke* und *Tlist* sind nun integraler Bestandteil des Befehls *Rights*.

- Im Befehl *Flag* sind die bisherigen Befehle *Flagdir* und *Smode* zusammengefaßt.
- Der Befehl *Map* beinhaltet den Befehl *Attach*.
- Im Befehl *Ndir* ist der bisherige Befehl *Listdir* integriert worden.
- *Nlist* (ein neuer Befehl) faßt die beiden alten Befehle *Slist* und *Userlist* zusammen.
- Der Befehl *Send* enthält jetzt zusätzlich die Befehle *Caston* und *Castoff*.
- Das *Syscon*-Menüsystem wird durch das Menüsystem *Netadmin* ersetzt, *Session* wird durch das Menü *Netuser* ersetzt.

Die einzelnen Befehl werden komplexer und aufwendiger, aber aufgrund der besseren Strukturierung sind bestimmte Zusammenhänge besser zu verstehen.

19.10 Network Auditing

In NetWare 4 sind Auditing-Funktionen integriert, um die Sicherheit und Integrität von Netzwerktransaktionen und -daten zu erweitern. Der Auditor ist ein herkömmlicher Benutzer, der diese Aufgaben unabhängig vom Netzwerkadministrator durchführt. Das Auditing hat nichts mit dem Accounting früherer NetWare-Versionen zu tun.

Wenn das Auditing installiert ist, werden entsprechende Logfiles eingerichtet. Diese Logfiles enthalten historische Daten über Logins und Logouts und Änderungen von Trustee-Rechten. Ein Auditor kann ebenfalls Datei- und Directory-Transaktionen wie Löschen, Schreiben oder Lesen beobachten und auswerten, Änderungen innerhalb der NDS einfügen, löschen, umbenennen; Rechteänderungen für NDS-Objekte können ebenfalls protokolliert werden. Auf diese Weise sind mögliche Fehlerquellen auf Datei- und Directory-Ebene wesentlich einfacher festzustellen. Es geht nicht darum, die Mitarbeiter zu überwachen, sondern darum, prüfen zu können, was in letzter Zeit auf Datei- oder Directory-Ebene durchgeführt worden ist, für den Fall, daß es wieder mal heißt: »Nichts geht mehr, aber wir haben gar nichts gemacht.«

Das Auditing-System steht sowohl für Volumes (Datei- und Directory-Ebene) als auch für die NDS zur Verfügung. Dabei ist das Auditing vollkommen losgelöst von den Netzwerkadministratoren zu sehen. Das heißt, Auditing kann von Benutzern ausgeführt werden (sofern diese die Berechtigung dazu haben), die selbst nicht mit der

Administration des Netzwerks konfrontiert sind. Für jedes Volume kann bei Bedarf ein eigener Auditor definiert werden. Ebenso flexibel läßt sich das Auditing für die NDS gestalten und aufbauen.

19.11 Verbesserte Druckdienste

Wesentliche Veränderungen haben die Druckdienste unter NetWare 4 erfahren. Hierzu zählen folgende Änderungen:

- Unterstützung von bis zu 256 Druckern über einen Print-Server.
- Ein Drucker kann jetzt über den Namen angesteuert werden (neuer Capture.Parameter) oder wie gewohnt über die Printer-Queue.
- Einfachere Installation.
- An der Workstation können bis zu neun LPT-Schnittstellen definiert werden (stehen bei entsprechender Konfiguration auch unter Windows zur Verfügung).
- Der Print-Server kann nur noch als NLM auf dem Server installiert werden, d. h., ein dedizierter Print-Server unter DOS ist nicht mehr verfügbar.
- An der Workstation können bis zu fünf Remote-Drucker gleichzeitig betrieben werden. Dies soll auch der Ersatz für den nicht mehr existierenden dedizierten Print-Server sein.
- Ein Print-Server-NLM ist jetzt auch in der Lage, einen Drucker an einem anderen Server anzusteuern, ohne daß auf diesem explizit ein Print-Server aktiviert werden muß. Der Drucker eines anderen Servers kann wie ein normaler Remote-Drucker behandelt werden.
- Der Durchsatz der Print-Server wurde wesentlich verbessert.

Da der Print-Server als NDS-Ressource definiert wird, ist es möglich, den Print-Server auf einem beliebigen Server zu starten. Damit kann man bei einem Server-Ausfall wesentlich schneller und flexibler reagieren, um Print-Ressourcen verfügbar zu machen.

Zu beachten ist auch, daß die gesamten externen Print-Server, wie sie zum Beispiel von Intel, HP, Extended Systems oder auch Axis zur Verfügung gestellt werden, auch in der Lage sind, NDS-Funktionen für das Drucken bereitzustellen. Wenn Sie bereits Komponenten unter NetWare 3 einsetzen, geschieht dies entweder durch einen Software-Upgrade der Firmware oder das Austauschen des jeweiligen Eproms, sofern ein Upgrade nicht möglich ist. Handelt es sich unter Umständen um ein besonders altes Modell, kann überhaupt kein Upgrade durchgeführt werden, in diesem Fall muß die gesamte Hardware ausgetauscht werden. Übergangsweise können diese Produkte über die Bindery-Emulation auch in einer NetWare-4-Umge-

19.12 National Language Support

bung eingesetzt werden, ohne ein Upgrade durchführen zu müssen. Dies sollte jedoch nur eine Übergangslösung sein. Zudem ist Novell dabei, den gesamten Mechanismus zum Drucken im Netzwerk auf neue »Beine« zu stellen.

Die bisher üblichen Druckdienste, so wie diese aus den früheren NetWare-Versionen und NetWare 4.1 bekannt sind, werden mit den neuen NetWare-Versionen verbessert. Novell hat hierfür die sogenannten NetWare Distributed Print Services (NDPS) konzipiert. Mit diesen neuen Diensten wird mehr Intelligenz in die Drucker verlagert, und die Vorteile für die Anwender steigen enorm. NDPS ist ein verteilter Dienst, der aus Client-, Server- und Connectivity-Komponenten besteht, um nahtlos Anwendungen mit Druckern verbinden und diese Drucker gemeinsam nutzen zu können. Es wird auch nicht mehr nötig sein, Print-Queue-, Printer- und Print-Server-Objekte einrichten zu müssen. Mit dem NWAdmin erfolgt die gesamte Verwaltung der NDPS-Umgebung. Die Vorteile von NDPS liegen unter anderem in folgenden Funktionen:

- Zentralisierte und vereinfachte Administration
- Bidirektionale Signalisierung und Steuerung
- Konfigurierbare Meldungs-Profiles
- Automatischer Download von Druckertreibern und -installation
- Vollständige Integration in die NDS
- Neue Job-Übertragungs-, Scheduling- und Notification-Optionen
- Kompatibel mit einer Vielzahl von Clients, Anwendungen und Betriebssystemen
- Unterstützung für bestehende Drucker und andere Ausgabegeräte

19.12 National Language Support

NetWare 4 erfüllt inzwischen eine lange geforderte Funktion: die Unterstützung unterschiedlicher Sprachen. Englisch ist dabei die Default-Sprache, die unterstützt wird. Das gilt für NLMs und Utilities. Andere Sprachen können bei der Installation oder bei der Ausführung von Utilities und Diensten gewählt werden. Dabei ist es möglich, daß jede Workstation bzw. jeder Benutzer eine andere Sprachunterstützung wählt. Die Arbeitsumgebung läßt sich also so gestalten, daß jeder Anwender mit seiner individuellen Sprachumgebung ausgestattet ist, egal von welchem Arbeitsplatz aus der Login im Netzwerk erfolgt.

Durch einen neuen Befehl KEYB x (x-Language-Nummer) an der Server-Console kann man jetzt auch die Bedienung der NetWare-Console in der gewünschten Sprache durchführen, d.h., es gibt eine deutsche Tastaturunterstützung am Server. Ein Netzwerkverwalter an

der Server-Console oder ein Benutzer an der Workstation kann Befehle und Utilities oder das Lesen der Dokumentation in der Sprache ausführen, die von NetWare unterstützt wird.

19.13 Dokumentation

NetWare 4 wird standardmäßig nur noch mit den wichtigsten Handbüchern und ein paar Schnellübersichten ausgeliefert. Die Dokumentation von NetWare 4 ist auf einer separaten CD-ROM enthalten. Die Auslieferung der Software auf CD-ROM inklusive der dazugehörigen Dokumentation ist ein regelrechter Trend geworden. Eine Vielzahl anderer Hersteller beschreitet inzwischen den gleichen Weg. Mit einem passenden Viewer ist das auch nicht das Problem. Man wird sich jedoch für wichtige Bereiche die Dokumentation ausdrucken, um schnell und einfach nachschlagen zu können. Mit der Dokumentation auf CD-ROM ist das nicht so einfach möglich.

Neben der elektronischen Dokumentation sind auch die Hilfetexte der einzelnen Befehle erweitert und verbessert worden. Dies betrifft sowohl die Workstation-Programme und Menüsysteme als auch die Consolen-Befehle. An der NetWare-Console gibt es jetzt den Befehl HELP, um eine Übersicht aller erlaubten Consolen-Befehle zu erhalten. Zu jedem Befehl kann man sich zudem weitere Informationen anzeigen lassen.

Die Hilfeunterstützung der Commandline-Utilities wurde endlich vereinheitlicht. Immer wenn Sie jetzt den Befehlsnamen und anschließend »/?« eingeben, wird Ihnen ein erklärender Text zum Befehl angezeigt. Neben der Befehlssyntax werden auch Befehlsbeispiele mit angegeben. Der Hilfebildschirm für jedes Menüsystem wird immer noch über die Funktionstaste **F1** angezeigt. Die Hilfetexte sind jedoch wesentlich ausführlicher als in früheren Versionen. Die GUI Utilities bieten diese Unterstützung durch Anklicken des Help-Buttons. Man erhält damit gute und ausführliche Informationen der ausgewählten Themen.

Eine gravierende Änderung hat das Einrichten und Verwalten der Netzwerkressourcen erfahren. Die altbekannte Bindery ist »tot« und wurde durch den Novell Directory Service ersetzt. Mit dieser neuen Technik wird es den Netzwerkverwaltern wesentlich einfacher gemacht, große und komplexe Netzwerke mit einer Vielzahl von Servern einzurichten. Die NDS (Novell Directory Services) sollen im folgenden Abschnitt näher erläutert werden.

19.14 Novell Directory Services

Bei den bisherigen NetWare-Versionen war es üblich, daß die Ressourcen im Netzwerk immer von dem Server verwaltet wurden, an dem sie angeschlossen waren. Die gleiche Situation ergab sich bei der Verwaltung der Benutzer. Jeder NetWare Server verwaltete seine eigene Bindery, in die eingetragen wurde, welche Benutzer und welche Gruppen am Server eingerichtet waren. Bei drei Servern im Netzwerk und insgesamt 100 Benutzern, die alle die Berechtigung haben sollen, an jedem Server zu arbeiten, bedeutet dies, insgesamt 300 Benutzer zu definieren. Bei großen Netzwerken ergibt sich ein enormer Verwaltungsaufwand und Overhead. Mit NetWare 4 muß man einen neuen Weg einschlagen.

NDS ist eine globale, replizierbare und verteilte Datenbank, die die Bindery ablöst. Während die Bindery dafür konzipiert war, einen einzelnen Server zu unterstützen, ist NDS dazu da, ein ganzes Netzwerk zu verwalten. Dadurch wird eine wesentlich höhere Flexibilität erreicht, und die Verwaltung des Netzwerks wird einfacher und bequemer.

Mit NDS wird die organisatorische Struktur eines Unternehmens auf eine logische Netzwerkstruktur umgelegt. Wenn sich der Benutzer im Netzwerk anmeldet, stehen ihm somit alle durch den Administrator bereitgestellten Ressourcen zur Verfügung, unabhängig davon, auf welchem Server sie installiert sind. Ein weiterer Login an anderen Servern wird dadurch hinfällig. Die Authentifizierung eines Benutzers an anderen Servern erfolgt für den Benutzer verdeckt im Hintergrund. Ein Anwender kann im Netzwerk gleichzeitig an bis zu 50 Servern angebunden sein.

NDS verwaltet Informationen über alle Ressourcen im Netzwerk – z. B. Benutzer, Gruppen, Drucker, Volumes, Print-Queues etc. – alles in einer einzigen, logischen und globalen Datenbank. Die Verbindungen im Netzwerk sind für den Anwender vollkommen transparent, da die Benutzer von der Komplexität des Netzwerks nichts wissen müssen.

Der Novell Directory Service ist, wie der Name schon sagt, ein »Directory«. Vergleichbar mit einem Telefonbuch oder Adreßbuch hilft Ihnen das Directory, Informationen über Ressourcen im Netzwerk schnell und einfach zu finden. Durch die Implementierung eines durchgängigen Namensschemas für Netzwerkressourcen kann es Organisationen erleichtert werden, Informationen im Directory zu finden und zu benutzen. Da es sich bei NDS um eine leistungsfähige

Datenbank handelt, können darin alle Informationen abgespeichert werden. Dies geht vom Namen der Ressource im Netzwerk bis hin zur Telefonnummer und Adresse der Benutzer im Netzwerk.

Objekte

Ein Novell-Directory-Services-Objekt (NDS) besteht aus einer Vielzahl von Informationen – Properties genannt – und den dazugehörigen Daten, die diese Properties haben können. All diese Informationen werden in der NDS gespeichert.

Einige Objekte können echte physikalische Einheiten darstellen. Zum Beispiel die Definition eines Benutzers – dieser existiert physikalisch – oder die Definition eines Druckers. Einige Objekte stellen jedoch nur logische Einheiten dar, zum Beispiel die Definition einer Print-Queue oder die Definition einer Gruppe. Andere Objekte dienen wiederum nur dazu, um den NDS-Directory-Baum besser zu strukturieren. Hierzu zählt zum Beispiel das Objekt *Organizational Unit*.

Es ist wichtig, zu verstehen, daß es sich bei einem NDS-Objekt um die Zusammenfassung gespeicherter Informationen handelt. Das Drucker-Objekt speichert Informationen über einen einzelnen Drucker, um dessen Verwaltung zu ermöglichen.

Objekt-Properties

Unter Properties versteht man die Informationskategorien, die in der NDS für ein Objekt gespeichert werden können. Jedes Objekt besitzt Properties, die Informationen über dieses Objekt enthalten, z. B. den Vor- und Nachnamen des Benutzers, den physikalischen Ort des Druckers und dergleichen mehr. Für jede Property können entsprechende Werte eingegeben werden, um das Objekt und die dazugehörigen Daten zu bestimmen. Ein Objekt-User kann folgende Properties enthalten: Login-Name, E-Mail-Adresse, Paßwort-Restriction, Gruppenmitgliedschaft, Telefonnummer, vollständige Adresse und vieles mehr.

In vielen Fällen kann für ein Property mehr als ein Wert eingegeben werden. Für das Property *Telefonnummer*, bezogen auf das Objekt *User*, können folgende Werte eingegeben werden: private Telefonnummer, Telefonnummer im Büro und dergleichen mehr.

19.14 Novell Directory Services

Novell Directory Services Rights

Unter NetWare 3 können Rechte auf Directory- und Dateiebene vergeben werden. Mit NetWare 4 können zusätzlich Rechte für Objekte und für die Properties von Objekten vergeben werden.

Es sei darauf hingewiesen, daß die Zugriffsberechtigungen auf Directory- und Dateiebene unter NetWare 4 im Vergleich zu NetWare 3 nicht geändert worden sind. Daher werde ich diese nicht noch einmal erläutern. Ich werde mich ausschließlich mit den Rechten für Objekte und Properties beschäftigen, die im Zusammenhang mit den NDS zu betrachten sind.

Unterscheiden Sie bei NetWare 4 deshalb bei der Rechtevergabe zwischen Rechten, die das NDS-System betreffen, und Rechten, die das Dateisystem (Directory und Files) betreffen.

Objekt-Rechte beziehen sich auf NDS-Objekte, haben aber keine Auswirkung auf die Properties der Objekte. Property-Rechte beziehen sich auf NDS-Objekt-Properties, aber nicht auf das Objekt selbst. Wenn zum Beispiel im User-Objekt eine private Telefonnummer als Wert des Property abgespeichert ist, kann das Einsehen dieser Telefonnummer für jedermann unterbunden werden, wohingegen die restlichen Property-Werte von allen gesehen werden könnten.

Durch das Aufsplitten dieser Rechtestruktur in Objekt- und Property-Rechte haben Sie eine optimale Umgebung, um exakt festlegen zu können, wer welche Informationen von Objekten oder die Objekte selbst in den NDS sehen, ändern oder auch löschen darf. So hat zum Beispiel jedes User-Objekt ein Property-Login-Script, mit dem das User-Login-Script des Benutzers definiert wird. Fehlt dem Benutzer selbst das Leserecht für dieses Property, wird er beim Login kein User-Login-Script ausführen. Damit das nicht geschieht, hat jeder Benutzer automatisch nach dem Einrichten per Definition das Leserecht für dieses Property. Auf andere Properties hat er in der Regel keine Rechte (außer zusätzlich auf das Property Print Job Configuration). Sie sehen, daß auch der Benutzer für sich selbst nicht alle Möglichkeiten besitzt, Manipulationen für sein eigenes Objekt durchzuführen, und das ist auch ganz gut so.

Access Control List

Jedes Objekt im NDS besitzt ein Property, als Access Control List (ACL) bezeichnet. Das ACL Property enthält Trustee-Assignments und die Inherited Rights Filter. Die ACL des Objekts unterstützt die Kontrolle, d.h., sie bestimmt, wer Zugriff auf dieses Objekt und seine Properties erhält, zum Beispiel ist ein Objekt, aufgeführt in der

ACL des Objekts Printer, Trustee für diesen Printer und hat für dieses Objekt die Rechte, die dafür definiert worden sind. Um den Trustee-Zugriff auf das Printer-Objekt zu ändern, muß die Trustee-Zuweisung in der ACL des Printer-Objekts geändert werden.

Jedes Objekt in der ACL eines anderen Objekts kann unterschiedliche Rechte für dieses Objekt-Property haben. Wenn zum Beispiel in der ACL des Printer-Objekts fünf User eingetragen sind, kann jeder dieser fünf User unterschiedliche Rechte für dieses Printer-Objekt und die Properties haben. Die ACL unterstützt somit nicht nur die Kontrolle eines einzelnen Property, sondern auch das Objekt als Einheit. Für ein Objekt User können Sie zum Beispiel verbieten, daß ein anderer Benutzer dessen eingetragene Telefonnummer sieht, wohingegen alle anderen Informationen zur Verfügung stehen.

Inherited Rights Filter

Während Trustee-Zuweisungen den Zugriff auf ein Objekt erlauben, erlaubt der Inherited Rights Filter (Inherited Rights Mask) das Filtern von Rechten von einem Objekt auf das andere. In einigen Fällen kann ein User-Objekt automatisch die Rechte von einem anderen Objekt vererbt (inherit) bekommen. Der Inherited Rights Filter kann das Vererben von Rechten unterbinden, so daß diese dem Objekt nicht mehr zur Verfügung stehen.

Effective Rights

Die Kombination der Inherited Rights, Trustee Assignment in einer ACL und andere Trustee-Assignments (Gruppen und Security-Equivalences), werden effektive Rechte genannt. Die effektiven Rechte eines Objekts legen fest, was der einzelne tatsächlich mit dem Objekt und den Properties machen darf.

Aufbau des NDS-Baums durch Objekte

Novell Directory Services bilden die logische Organisation. Sie wird als Directory-Baum bezeichnet, weil die Objekte in einer hierarchischen Baumstruktur gespeichert werden, die mit einer Wurzel beginnt und sich unten immer weiter verzweigt.

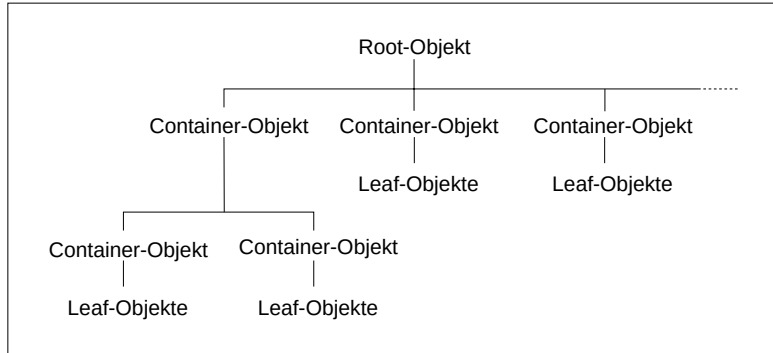
Es gibt zwei Objekt-Typen, die den Directory-Baum bilden: Container-Objekte und Leaf-Objekte (Leafs = Blätter).

Ein Zweig des Directory-Baums besteht aus einem Container-Objekt und all den Objekten, die darin enthalten sind, welche wiederum andere Container-Objekte enthalten können. Leaf-Objekte befinden sich nur am Ende eines Zweigs und enthalten kein anderes Objekt.

19.14 Novell Directory Services

In der nachfolgenden Abbildung ist der Aufbau eines Directory-Baums aufgezeigt.

Abbildung 19.1
Objekte in einem
Directory-Baum



Objekttypen: Container-Objekte und Leaf-Objekte

Container-Objekte enthalten weitere Objekte. Sie werden dazu verwendet, um alle anderen Objekte in einem Directory-Baum logisch zu strukturieren. Dies ist vergleichbar mit der Organisation (Directory-Struktur) von Festplatten. Hier speichern Sie auch nicht alles im Root-Directory, sondern bilden Directories und Subdirectories, um Daten und Programme besser zu strukturieren.

Ein Container-Objekt wird als Parent-Objekt bezeichnet, wenn es weitere Objekte enthält.

In Leaf-Objekten sind keine weiteren Objekte enthalten. Sie stellen Netzwerkressourcen dar, z. B. Benutzer, Computer, Drucker.

Zur logischen Strukturierung des Directory-Baums stehen folgende *Container-Objekte* zur Verfügung:

Root

Die Wurzel der NDS. Pro NDS bzw. NDS-Baum kann es nur ein Root-Objekt geben, das nicht gelöscht werden kann. Root wird bei der Installation von NDS erstellt und als [Root] dargestellt. Das Root-Objekt kann die Objekte Country, Organization und Alias-Objekte enthalten.

Beim Installieren des ersten NetWare 4 Servers werden Sie nach einem Baumnamen gefragt – dies ist der Name des Baums, in dem für den ersten Server das Root-Objekt eingerichtet wird. Wenn Sie weitere Server im Netzwerk hinzufügen, erhalten Sie während der Installation eine Auflistung aller gefundenen NDS-Bäume, wobei Sie festlegen müssen, in welchen Baum der Server integriert werden soll. An dieser Stelle können Sie dann auch einen neuen Baum kreieren, der dann mit einer eigenen Root ausgestattet wird.

19 Novell NetWare 4.2

Mit NetWare 4.1 wird es ein Utility geben, das es erlaubt, zwei NDS-Bäume zusammenzuführen, also einen Merge durchzuführen.

Das Root-Objekt kann nicht gelöscht oder umbenannt werden. Das Root-Objekt kann nur Country-Objekte, Organization-Objekte oder Alias-Objekte enthalten.

Country Das ist die Strukturierung des Directory-Baums, wenn sich das Unternehmen in unterschiedlichen Ländern befindet und NDS für das gesamte Unternehmen verwendet werden. Dieses Container-Objekt kann verwendet werden, muß aber nicht. Dargestellt wird es im NDS-Baum durch die Angabe »C=«. Es kann nur Organization-Objekte und Alias-Objekte enthalten.

Organization Angabe der Organisation des Unternehmens, um eine logische Strukturierung des NDS-Baums zu erhalten. Im NDS-Baum wird dies durch »O=« dargestellt. Das Container-Objekt Organization kann die Objekte Organizational Units und Leaf-Objekte enthalten.

Locality Dieses Container-Objekt kann nicht über die herkömmlichen Utilities eingerichtet werden. Die Angabe für das Container-Objekt Locality kann nur bei der Installation eines neuen Servers erfolgen. Mit diesem Objekt hat man also die Möglichkeit, in der NDS-Struktur die Lokation für das Unternehmen in der NDS-Struktur zu hinterlegen. Dieses Objekt kann in einem Country-, Organization- oder Organizational-Unit-Objekt eingesetzt werden. In der Regel kommt es nicht zum Einsatz dieses Objekts. Es befindet sich u.a. deshalb innerhalb der NDS, um NDS-X.500-Kompatibilität einzuhalten.

Organizational Unit Hierin wird die Organisation eines Unternehmens im NDS-Baum in Suborganisationen (Abteilungen in der Praxis) unterteilt. In den NDS wird das Objekt durch »OU=« dargestellt. Das Objekt Organizational Unit kann weitere Organizational Units oder Leaf-Objekte enthalten.

Als *Leaf-Objekte* stehen im NDS-Baum zur Verfügung:

AFP Server Ein Server, auf dem das AFP-Protokoll installiert ist. Dieses Objekt dient nur zur Dokumentation des Netzwerks, um aufzuzeigen, daß ein AFP-Server installiert ist.

Alias Ein Objekt, welches auf ein anderes existierendes Objekt verweist. Ein Alias-Objekt in einem Directory-Baum verweist auf ein anderes Objekt in einem anderen Directory-Baum, um den Zugriff zu vereinfachen. Wenn Sie mit dem Alias-Objekt arbeiten, dann führen Sie die Arbeit in Wirklichkeit mit dem Originalobjekt durch, ohne das zu bemerken. Somit können Sie in einem Container X ein Alias-Volume-Objekt installieren, das auf ein Original-Volume-Objekt im Container Y verweist. Immer wenn Sie mit dem Alias-Volume-Objekt arbeiten,

19.14 Novell Directory Services

greifen Sie in Wirklichkeit auf das Original-Volume-Objekt im Container X zu. Damit lassen sich gewisse Arbeiten und Beziehungen innerhalb der NDS wesentlich einfacher gestalten.

- Bindery Object** Werden Anwendungen unter NetWare 4 installiert, die Objekte einrichten, die es nicht unter NetWare 4, sondern nur unter NetWare 3 gibt, dann werden diese als Bindery-Objekte eingerichtet. Man sollte darauf achten, daß in den NDS langfristig gesehen so wenig Bindery-Objekte wie möglich eingerichtet sind.
- Bindery Queue** Wenn es um das Einrichten von Druckerumgebungen geht, werden in der Regel NDS Print Queues definiert und installiert. Bei speziellen Anwendungen werden keine NDS Print Queues, sondern Bindery Print Queues eingerichtet. Man sieht es dem Symbol nicht an, daß es sich um eine Bindery Print Queue handelt.
- CommExec** Beim Einrichten von speziellen Kommunikationsprogrammen, z. B. NetWare for SAA oder NetWare Connect, werden spezielle NDS-Objekte eingerichtet. Nach der Installation der Kommunikationsprogramme sollte das CommExec-Objekt nicht gelöscht werden.
- Computer** Damit können Informationen abgespeichert werden (Seriennummer, Verwalter etc.), um eine leichtere Inventarisierung durchführen zu können. Dieses Objekt wird auch nur zur Dokumentation genutzt und hat keinerlei funktionalen Charakter. Da man die Dokumentation der Hardware-Inventarisierung anderen Tools überlassen sollte, ist der Einsatz dieses Objekts in den NDS nicht unbedingt zu empfehlen.
- Directory Map** Dient der Durchführung einer einfachen Laufwerkszuweisung. Um sich in einem Login Script den direkten Zusammenhang von Volume/Directory zu ersparen, kann ein Directory-Objekt definiert werden, in dem hinterlegt wird, auf welches Volume und Directory dieses Objekt verweist. Sollte sich nun die Zuordnung ändern, weil zum Beispiel eine neue Programmversion installiert ist, dann muß nur die Zuordnung im Directory-Objekt durchgeführt werden. Die Laufwerkszuordnung im Login Script bleibt unverändert.
- Group** Vergleichen Sie dazu die entsprechenden Ausführungen zu NetWare 3. Mit Gruppendefinitionen wird die Vergabe von Rechtezuweisungen für Benutzer vereinfacht und besser strukturiert.
- NetWare Server** Ein NetWare 4 Server im Netzwerk. Dieses Objekt wird von vielen Objekten verwendet, wenn sie Dienste nutzen, die vom NetWare Server zur Verfügung gestellt werden. Ohne dieses Objekt geht nichts. Beim Installieren eines NetWare 4 Server in den NDS wird dieses Objekt automatisch eingerichtet.

19 Novell NetWare 4.2

Organizational Role	Diesem Objekt können bestimmte Rechte zugewiesen werden. Ein Benutzer, dem Sie dieses Objekt zuweisen, besitzt damit die dem Organizational-Role-Objekt zugewiesenen Rechte. Damit können einfach und bequem bestimmte Managementaufgaben vergeben werden, ohne einem Benutzer explizit die Rechte zuweisen zu müssen. Genauso schnell können die Rechte auch wieder entzogen werden, indem man die Organizational-Role-Zuweisung wieder wegnimmt.
Print-Server	Stellt einen Print-Server im Netzwerk dar. Dieser ist zuständig für das Abarbeiten von Druckaufträgen und das Verwalten der installierten und konfigurierten Netzwerkdrucker.
Printer	Stellt einen Drucker im Netzwerk dar, der von einem Print-Server verwaltet und angesteuert wird.
Print-Queue	Stellt eine Print-Queue im Netzwerk dar. Druckaufträge, die in die Print-Queue gestellt werden, werden von dem Drucker ausgegeben, der dieser Queue zugewiesen worden ist.
Profile	Repräsentiert ein Login Script. Es kann von Anwendern im Netzwerk gemeinsam genutzt werden, wobei sich die User-Objekte in unterschiedlichen Container-Objekten befinden können. Einem Benutzer kann zu einem Zeitpunkt immer nur ein Profile-Login Script zugewiesen werden.
Unknown	Beim Arbeiten mit NetWare 4 und den NDS kann es durchaus vorkommen, daß das eine oder andere Objekt beschädigt sein könnte. Tritt dieser Fall ein, können die NDS mit diesem Objekt nicht mehr arbeiten, und es wird als <i>Unknown</i> in den NDS gekennzeichnet. Da sich ein Unknown Object nicht mehr rekonstruieren läßt, kann man es nur noch löschen und neu einrichten.
User	Hiermit wird ein Benutzer im Netzwerk eingerichtet, wenn dieser die Berechtigung haben soll, im Netzwerk zu arbeiten.
Volume	Stellt ein Volume im Netzwerk dar, wenn dieses an einem NetWare 4 Server eingerichtet worden ist. Neben diesen standardmäßigen Objekten sind in NetWare 4.1 zusätzliche NDS-Objekte enthalten, die zur Installation der MHS-Mailing-Funktionen benötigt werden. Da das Mailing-Produkt unter MHS zum einen selten eingesetzt, zum anderen in der Nachfolgeverson durch GroupWise abgelöst wird, sollen diese Objekte nur der Vollständigkeit halber aufgeführt werden. Inwieweit eine Übernahme dieser NDS-Objekte für neue Mailing-Funktionen vollzogen wird, ist derzeit nicht bekannt.
External Entity	Mit diesem Objekt werden Informationen über Benutzer eingerichtet, die sich selbst nicht in den NDS befinden, wenn es sich zum Beispiel um ein fremdes Mailing-System handelt.

19.14 Novell Directory Services

List Sollen mehreren Benutzern Mailings geschickt werden, und dies in einer bestimmten Regelmäßigkeit, dann kann man sich ein Objekt einrichten, in dem diese Empfänger eingetragen sind. Beim Versenden von Mailings gibt man dann statt der einzelnen Benutzer nur noch den Namen des entsprechenden List-Objekts an.

Message Routing Group Speziell für MHS-Server werden alle Server in die Message Routing Group eingetragen, wenn zum einen darauf MHS installiert ist und zum anderen Mailings zwischen diesen Servern ausgetauscht werden sollen.

Messaging Server Wenn auf einem NetWare Server MHS installiert worden ist, wird dieser Server als Messaging Server in die NDS und das Objekt zugleich in die Message Routing Group eingetragen.

Mit jeder neuen Version der Directory Services wurden die damit verbundenen Dienste erweitert und verbessert. Mit der Einführung von NetWare 4.11 und 5 sind die folgenden zusätzlichen Optionen enthalten (NetWare 5 wird auch entsprechende Erweiterungen erfahren, weil auch hier wieder eine Vielzahl neuer Mechanismen direkt in die NDS integriert werden):

- Das User Template wird nicht mehr als Benutzer-Objekt angelegt, sondern als eigenes Objekt verwaltet. Man hat somit eine neue Objektklasse definiert. Mit Hilfe des User Template lassen sich die Benutzereinrichtungen in den NDS einfacher realisieren, da man eine Vielzahl von Standardwerten einrichten kann, die für jeden neu einzurichtenden Benutzer übernommen werden sollen. Es ist jetzt also möglich, neben den herkömmlichen Standardwerten auch Rechte für Dateien, Directories und die NDS zu definieren. Zudem kann ein Setup Script definiert werden, um damit festzulegen, welche Dateien in das Home Directory des Benutzers kopiert werden sollen. Mit dem User-Template-Objekt kann somit das Einrichten neuer Benutzer erleichtert und standardisiert werden, es kann aber nicht dazu verwendet werden, um bereits bestehende Benutzer damit zu ändern.
- Die Audit-Log-Dateien, die für das Verwalten des Auditing System über AUDITCON benötigt werden, werden jetzt als Directory-Services-Objekte verwaltet und dargestellt. Auf diese Weise kann der Zugriff auf Audit-Log-Dateien über NDS-Zugriffsrechte überwacht und gesteuert werden.
- Zudem hat man die Admin-Programme für die NDS wesentlich verbessert, wie nachfolgend beschrieben.

Application Services

Mit dem 32-Bit-Client für Windows 95 wurde bereits der NetWare Application Launcher zur Verfügung gestellt. Die wenigsten wissen jedoch, welche Vorteile damit verbunden sind. Mit der neuen NetWare-Version sind der NetWare Application Manager und der NetWare Application Launcher standardmäßig im Betriebssystem integriert, so daß es keine Umstände mehr macht, das Schema der NDS zu erweitern.

Über das NAM-Utility ist man in der Lage, Anwendungen als Objekte in den NDS anzubinden. Da es sich um herkömmliche NDS-Objekte handelt, können sie wie andere Objekte auch verwaltet werden. Über die Definition eines Objekts in den NDS kann für die Anwendung folgendes festgelegt werden:

- Festlegung des Verzeichnisses, in dem sich die Anwendung befindet, das Icon unter Windows, Parameter für den Aufruf der Anwendung und andere notwendige Attribute.
- Verwendung von Trustee-Zuweisungen, um den Zugriff auf die Anwendung zu regeln.
- Beim Einrichten der Anwendungsobjekte wird zudem über das NDS-Objekt festgelegt, ob es sich um eine DOS-, Windows-, Win95- oder Windows-NT-Anwendung handelt.
- Festlegung von Start-Scripts, um damit die notwendige Netzwerkumgebung zu definieren, sobald die Anwendung aufgerufen wird. Zu diesen Netzwerkumgebungen gehören Laufwerkszuordnungen und Druckerumleitungen. Ebenso werden sogenannte Cleanup-Scripts definiert, die vorher definierte Netzwerkumgebungen wieder zurücknehmen, um den ursprünglichen Zustand herstellen zu können.

Das NAL-Utility ist in einer 16-Bit- und in einer 32-Bit-Version verfügbar. Über dieses Utility können Anwender die Applikationen nutzen, die durch entsprechende Objekte in den NDS abgebildet worden sind und für die der Anwender entsprechende NDS-Rechte erhalten hat. Wenn der NetWare Application Launcher gestartet wird, zeigt er die entsprechenden Anwendungsobjekte an. Führt der Benutzer einen Mausklick auf das Objekt durch, wird die Workstation entsprechend vorbereitet und anschließend die Anwendung gestartet. Der Netzwerkverwalter legt fest, welcher Anwender auf welche Anwendungen Zugriff haben soll.

19.14 Novell Directory Services

Messaging Services

Mit der Auslieferung von NetWare 4.11 ist MHS und FirstMail als E-Mail-System nicht mehr integriert. In den weiteren NetWare-Versionen wird MHS und FirstMail durch das GroupWise-Produkt von Novell ersetzt. GroupWise bietet als E-Mail-System die folgenden Funktionen:

- GroupWise ist noch stärker in NetWare integriert, als dies in vorherigen Versionen der Fall war. So können GroupWise-Benutzer, Ressourcen oder auch Distribution Lists mit dem NetWare Administrator eingerichtet und verwaltet werden.
- Mit der sogenannten *Universal In Box* organisiert GroupWise E-Mail, persönliche Termine, Gruppenplanung und andere Aufgaben an einer Stelle.
- Ist man auf Reisen, kann man über den Remote-Client und ein Modem u.a. Mailings austauschen.
- Mit dem Async Gateway können Verbindungen zu anderen Abteilungen oder Firmen aufgebaut werden, wenn diese ebenfalls GroupWise benutzen.

Für GroupWise sind unter anderem die folgenden Gateways verfügbar:

- *SMTP MIME Gateway*
Über dieses Gateway können Nachrichten mit dem Internet ausgetauscht werden. Ebenso kann an elektronischen Diskussionsforen und Bulletin Boards teilgenommen werden. Nachrichten aus dem Internet werden in der *Universal In Box* abgelegt.
- *TAS Gateway*
Über jedes Touch-Tone-Telefon kann die *Universal In Box* abgefragt werden. Telefonische Nachrichten können über die *Universal In Box* empfangen werden.
- *Fax/Print Gateway*
Damit können über GroupWise Faxe verschickt und in der *Universal In Box* empfangen werden.
- *Pager Gateway*
Mit diesem Gateway können Nachrichten über GroupWise an einen alphanumerischen Pager verschickt werden.

Daneben gibt es für GroupWise noch eine Vielzahl von Gateways, so daß bei Bedarf eine weitere Prüfung der GroupWise Gateways notwendig ist. Erwähnt sei nur, daß es weitere Gateways für API, cc:Mail, Message Router, MHS, Microsoft Mail, Office Vision, SNADS, VMS Mail, X.25 und X.400 gibt.

19 Novell NetWare 4.2

Somit ist GroupWise ein weiterer Baustein von Novell, der sich vollständig in die NDS integrieren läßt und darüber hinaus auch eine vollständige Verwaltung ermöglicht. Man hat somit eine Umgebung, in der über die NDS auf alle eingerichteten Benutzerobjekte zurückgegriffen werden kann, um diese in einer anderen Anwendung nutzen zu können.

NetWare Licensing Services (NLS)

Der in der neuen NetWare enthaltene NetWare Licensing Service ist ein verteilter und unternehmensweiter Netzwerkdienst, der es den Netzwerkverwaltern erlaubt, im Netzwerk eingesetzte und lizenzierte Anwendungen zu überwachen und zu steuern. NLS ist eng mit den NDS verknüpft. Die NLS-Architektur besteht aus Client-Komponenten für unterschiedliche Plattformen und Systemkomponenten, die auf dem NetWare Server laufen.

NLS bietet zudem ein Metering-Tool zur Überwachung der Lizenznutzung. Zur Anpassung der Lizenzierungsmechanismen stehen auch für Entwickler entsprechende Libraries zur Verfügung.

Wenn Sie auf Ihrer Festplatte eine Datei bearbeiten oder ein Programm aufrufen wollen, muß Ihnen bekannt sein, wo sich diese befinden, oder es muß ein passender Suchpfad definiert worden sein. Ebenso verhält es sich, wenn Sie auf ein Objekt in den NDS zugreifen wollen. Deshalb soll Ihnen nachfolgend gezeigt werden, wie Sie innerhalb der NDS auf die einzelnen Objekte zugreifen können.

Context

Die Novell Directory Services ermöglichen es Ihnen, auf Objekte entsprechend der Lokation im Directory-Baum zuzugreifen. Wenn Sie ein Objekt im Netzwerk hinzufügen (Server, User, Print Server etc.), dann müssen Sie wissen, in welchem Container-Objekt sich dieses neue Leaf-Objekt befinden soll.

Die Position eines Objekts innerhalb der Container-Objekte wird als Context bezeichnet. In der nachfolgenden Abbildung ist der mögliche Aufbau eines NDS-Baums dargestellt.

Der Context für das Objekt A_Zenk ist:

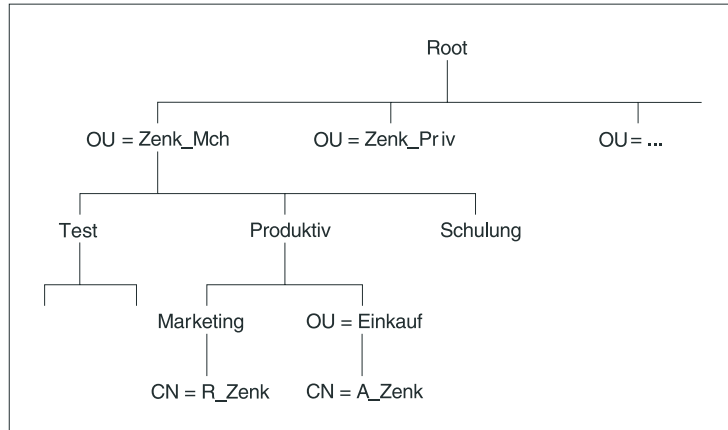
EINKAUF.PRODUKTIV.ZENK_MCH

Der Context für das Objekt R_Zenk ist:

MARKETING.PRODUKTIV.ZENK_MCH

19.14 Novell Directory Services

Abbildung 19.2
NDS-Directory-
Baum



Zu beachten ist dabei, daß die Angabe der NDS-Namen immer von unten nach oben erfolgt, d.h., zuerst geben Sie dem Leaf-Objekt Namen und dann allen darüberliegenden NDS-Container-Objekten.

Objekt-Namen

Der Context für ein Objekt bildet somit auch seinen kompletten Namen. Der Pfad vom Objekt bis zum ROOT des Directory-Baums ergibt den vollständigen Namen für das Objekt, der eindeutig sein muß und dadurch auch eindeutig bestimmt werden kann. Das heißt auch, daß zwei gleiche User-Namen für das Objekt User existieren dürfen, wenn deren Context-Name (vollständiger Pfad) unterschiedlich ist. Das ist zum Beispiel dann der Fall, wenn die beiden User in unterschiedlichen Organisationen eingerichtet sind.

Die meisten Leaf-Objekte haben einen sogenannten Common-Namen. Für User-Objekte ist der Common-Name der Login-Name, der im Directory-Baum ausgewiesen wird. Auch andere Leaf-Objekte haben Common-Namen, die im Directory-Baum angezeigt werden, z.B. Printer-Objekte oder der Objekt-Name für einen Server.

Container-Objekte besitzen keinen Common-Namen. Sie werden durch ihren Organizational-Unit-Namen, den Organization-Namen oder den Country-Namen bestimmt.

Bei der Angabe des vollständigen Namens für ein Objekt (Context des Objekts), wird der Common-Name – so vorhanden – zuerst angegeben, danach folgt ein Punkt (.), dann der Name des Container-Objekts, ebenfalls von einem Punkt (.) gefolgt. Beim Container-Objekt kann es sich dabei um eine Organizational Unit (OU), ein Organizational- (O) oder Country-Objekt (C) handeln.

19 Novell NetWare 4.2

Der vollständige Name für ein Objekt wird somit durch folgende Angaben bestimmt:

Common Name.Organizational Unit Name.Organization Name.Country Name

Wie zu ersehen ist, wird die Angabe des vollständigen Namens als Bottom-up-Angabe bestimmt: vom Blatt bis zur Wurzel. Beim Einsatz von Country-Objekten ist dabei zu beachten, daß bei der Angabe des Contexts oder des vollständigen Namens eines Objekts immer die Objekttypen angegeben werden müssen. Wenn wir davon ausgehen, daß für den NDS-Baum der Abbildung 19.2 das Country-Objekt C=DE eingefügt worden ist und sich darunter die Organization-Objekte befinden, dann wäre der Context für den Benutzer A_Zenk wie folgt anzugeben:

OU=Einkauf.OU=Produktiv.O=Zenk_k_Mch.C=DE

Wenn Sie bei der Abfrage der Directory-Informationen einen vollständigen Namen angeben, dann wird Ihnen genau dieses Objekt angezeigt. Oder Sie geben einen Property-Wert eines Objekts an und erhalten eine Liste aller Objekte, die diesen Wert haben.

19.15 Verwaltung der Novell-Directory-Services-Datenbank

Zur Verwaltung der NDS-Datenbank gehören die gleichen Aufgaben, die ein Netzwerkverwalter in den Vorgängerversionen von Netware auch hatte. Mit NetWare 4 sind die Möglichkeiten und die Flexibilität für dieses Aufgabengebiet jedoch viel größer geworden.

Es wurden auch sämtliche Utilities (DOS, OS/2 oder Windows-Programme) geändert und verbessert. Nicht nur, daß es weniger Menüsysteme und Befehle gibt, da man bisher bekannte Befehle und Menüsysteme zusammengefaßt hat, auch die gesamte Bedienung wurde wesentlich verbessert.

Es wird jetzt bei jedem Befehl einheitlich durch die Eingabe `befehl /?` ein Hilfstext am Bildschirm angezeigt mit Beispielen, wie der Befehl ausgeführt werden kann. Durch den National Language Support bekommt man die Menüsysteme und Fehlermeldungen in der selbst gewählten Sprache angezeigt. Jeder Anwender kann dabei mit einer eigenen Sprache konfiguriert werden.

19.15 Verwaltung der Novell-Directory-Services-Datenbank

User-Objekt Admin

Im Gegensatz zu NetWare 3 wird bei der Installation von NetWare 4 nicht mehr der Benutzer Supervisor, sondern der Benutzer Admin eingerichtet. Dieser ist zuständig und verantwortlich für die Verwaltung von NetWare 4 und sollte die gesamte Netzwerkumgebung so einrichten, daß einfaches und schnelles Arbeiten möglich ist.

Wenn bei der Installation von NetWare 4 der User Admin eingerichtet wird, erhält das User-Objekt Admin eine Default-Trustee-Zuweisung auf das Objekt ROOT. Durch diese Trustee-Zuweisung werden dem User-Objekt Admin alle Rechte für alle Objekte und Volumes (Directories und Dateien) im gesamten Directory-Baum gewährt. Diese Trustee-Zuweisung bedeutet für den User Admin, daß er über die Rechte verfügt, um alle anderen Objekte im Directory-Baum einzurichten und zu verwalten.

Das User-Objekt Admin hat keine so große Bedeutung mehr, wie dies für den User Supervisor unter NetWare 3 der Fall war bzw. immer noch ist. Admin ist nur das erste Benutzerobjekt, das bei der ersten Installation von NetWare 4 eingerichtet wird und deshalb die Rechte und Möglichkeiten haben muß, neue Objekte einzurichten.

Beim Einrichten neuer User-Objekte im Directory-Baum können Sie einige von ihnen mit Supervisor-(Admin-)Objekt-Rechten versehen, damit diese in der Lage sind, neue Container-Objekte oder Leaf-Objekte einzurichten und zu verwalten. Somit kann die Verwaltung des Netzwerks zentralisiert oder dezentralisiert eingerichtet werden. Je nachdem, auf welches Container-Objekt oder Leaf-Objekt Sie das Supervisor-Objekt-Recht vergeben, können Sie dieses und alles, was darunterliegt, managen.

Wenn Sie einem eingerichteten User-Objekt das Supervisor-Objekt-Recht auf das ROOT-Objekt vergeben, hat dieser all die Rechte, die der Benutzer Admin auch besitzt. Anschließend können Sie den User Admin löschen. Unter NetWare 3.x und den Vorgängerversionen konnte der User Supervisor hingegen nicht gelöscht werden. Bisher war es so, daß unter NetWare der User Supervisor alle Rechte hatte. Es war von daher schon immer interessant, als User Supervisor in das Netzwerk einzudringen. Mit NetWare 4 kann man NetWare so installieren, daß nicht mehr bekannt ist, welcher User mit Supervisor-Rechten arbeitet, wenn nach den notwendigen Anpassungen der User Admin gelöscht wurde. Zu beachten ist auch, daß bei der Installation des ersten NetWare 4 Servers der User Admin in der angegebenen Organization eingerichtet wird. Man kann das User-Objekt Admin unter NetWare 4 umbenennen oder auch in einen anderen Container verschieben.

19 Novell NetWare 4.2

Ein Teil der Flexibilität von NDS besteht darin, eine zentralisierte und/oder dezentralisierte Netzwerkverwaltung einzurichten. Deshalb ist es nicht mehr notwendig, daß ein einzelner Benutzer mit sämtlichen Rechten ausgestattet wird und somit Einblick in das gesamte Netzwerk hat. Gefordert ist jetzt jedoch eine vorsichtige und gut durchdachte Planung, um sich nicht selbst im Netzwerk auszusperrten, wenn es darum geht, wichtige Änderungen durchzuführen.

Partitions

Damit die NDS besser skalierbar und zuverlässiger sind, kann die NDS-Datenbank in kleinere Teile, Partitions genannt, unterteilt werden. Partitions müssen vom Netzwerkadministrator nachträglich, nachdem die NDS-Struktur als solche eingerichtet ist, definiert werden. Man benötigt hierfür allerdings einen Plan, um die Partitions entsprechend den Anforderungen zu definieren und – wie später noch zu sehen sein wird – die Replicas so zu verteilen, daß nicht nur Sicherheit, sondern auch Performance-Vorteile erzielt werden.

Jede Partition besteht aus einem Container-Objekt, allen Objekten in diesen Container-Objekten und den Daten für diese Objekte. Partitions enthalten keinerlei Informationen über das Dateisystem oder die Dateien und Directories in diesem Dateisystem. Man muß somit beim Einrichten von Partitions das jeweilige Container-Objekt auswählen und bestimmen, daß daraus eine neue Partition werden soll. Bei Bedarf können Partitions auch verschmolzen werden.

Wenn der erste NetWare 4 Server installiert wird, richtet das Installationsprogramm auf diesem Server die [Root]-Partition ein, da zugleich auch das [Root]-Objekt installiert wird.

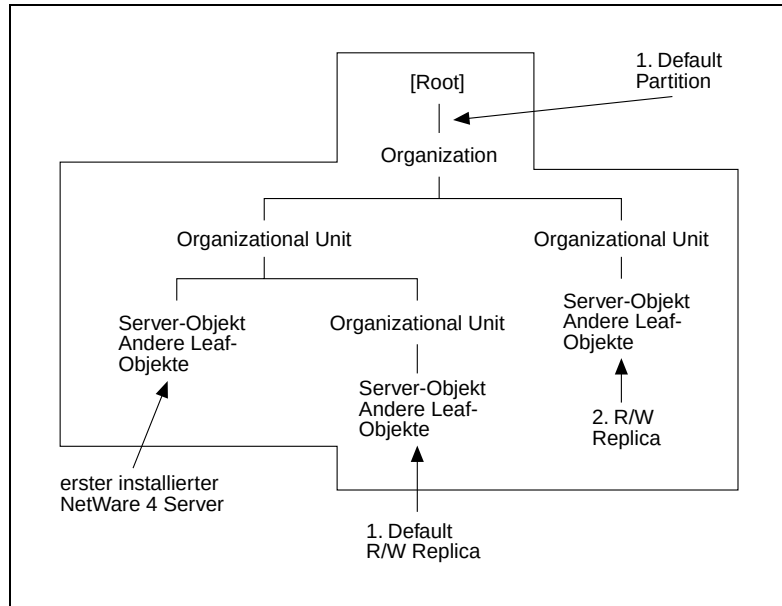
In der nachfolgenden Abbildung ist dargestellt, wie die Installation der Partition aussieht und wie sich die Situation für das Einbinden weiterer Server darstellt, sofern nicht manuell Änderungen in der Partitionierung der NDS durchgeführt worden sind.

Für Directory-Benutzer ist der Partition-Baum vollkommen transparent. Benutzer sehen nur den globalen Baum von Directory-Objekten. Um nun zusätzlich den Zugriff auf unterschiedliche Bereiche des NDS-Baums zu optimieren und die Sicherheit von NDS zu erhöhen, kann jede Partition repliziert und auf unterschiedlichen Lokationen gespeichert werden.

Mit NetWare 4 ist es jetzt auch möglich, Teilbäume zu verschieben. Hierzu muß jedoch zuerst aus dem zu verschiebenden Teilbaum eine Partition gemacht werden. Anschließend kann man die Partition unter einen anderen Container »hängen«.

19.15 Verwaltung der Novell-Directory-Services-Datenbank

Abbildung 19.3
Einrichten von
Default Partitions



Die Replizierung von Partitions verbessert den Zugriff und bietet für NDS zusätzliche Fault Tolerance. Da eine Partition auf unterschiedlichen Locations repliziert werden kann, bedeutet die Zerstörung einer Replica nicht, daß der Zugriff auf NDS-Informationen gestört ist. Zusätzlich können Sie bei der Installation der Replicas festlegen, ob sie als Read-Write oder Read-Only bestimmt werden sollen.

Damit durch die Verteilung der Replicas der Datenverkehr im Netzwerk nicht zu groß wird, muß beim Aufbau der NDS auch dieser Mechanismus sorgfältig geplant werden. Man halte sich dabei immer an den Spruch: Soviel wie nötig, so wenig wie möglich. Viel hilft viel – das gilt hier nicht, da jede Replica einen zusätzlichen Synchronisationsaufwand bedeutet.

Replicas

Um die NetWare Directory Services über das Netzwerk zu verteilen, muß die Datenbank auf unterschiedlichen Servern gespeichert werden. Statt eine Kopie der gesamten Datenbank auf allen Servern zu halten und zu verwalten, werden Replicas von Partitions auf unterschiedlichen Servern im Netzwerk verteilt.

Eine Replica ist die Kopie einer Partition. Sie können eine beliebige Anzahl von Replicas für jede Partition im gesamten Netzwerk verteilen. Mit dem Einsatz von Replicas werden folgende Ziele verfolgt:

19 Novell NetWare 4.2

■ *Kompensation des Ausfalls einer einzelnen Server-Komponente*

Wenn zum Beispiel eine Platte oder ein Server ausfällt, können mit Hilfe der Replica auf einem anderen Server in einer anderen Lokation nach wie vor die Benutzer und alle anderen Objekte identifiziert werden, die in der ausgefallenen Partition enthalten waren.

Weil die gleichen Informationen über mehrere Server verteilt sind, sind Sie nicht mehr von einem einzelnen Server abhängig, um Benutzer im Netzwerk zu identifizieren. Sie können eine Replica einer Partition mit der Replica einer anderen Partition auf demselben Server abspeichern. Die Replica des NDS-Baums bietet keine Fault Tolerance für Ihr Dateisystem. Es werden mit dem Replica-Service nur die NDS-Informationen im Netzwerk verteilt. Um Fault Tolerance für das Dateisystem (File- und Directory-Informationen) zu erhalten, müssen Sie die Mechanismen SFT II oder SFT III installieren (Disk-Mirroring, Disk-Duplexing, Server-Duplexing und Transaction-Tracking-System).

■ *Schnellerer Zugriff auf Informationen für Benutzer über WAN-Verbindungen*

Muß ein Benutzer häufig über WAN-Verbindungen bestimmte Directory-Informationen (NDS) abfragen und auf diese zugreifen, können Sie die Zugriffszeit und den Netzwerkverkehr reduzieren, indem Sie eine Replica, die die entsprechenden Informationen enthält, auf einem Server abspeichern, auf den diese Benutzer lokal zugreifen können.

Die Verteilung der Replica auf die Server im Netzwerk erlaubt Ihnen, auf Informationen der NDS schneller und zuverlässig zugreifen zu können, da die Informationen immer vom nächstgelegenen Server, der zur Verfügung steht, bereitgestellt werden.

Man unterscheidet vier Arten von Replicas:

- Master
- Read-Write
- Read-Only
- Subordinate (Subreference)

Obwohl eine Vielzahl von Replicas einer Partition in einem NDS-Directory existieren kann, ist nur eine davon die Master Replica. Nur diese Replica kann benutzt werden, um die Struktur der NDS in Relation zur entsprechenden Partition zu ändern. Sie können eine neue Partition in einer Directory-Datenbank nur in der Master Replica einrichten.

19.15 Verwaltung der Novell-Directory-Services-Datenbank

Die Master und Read-Write Replica wird benutzt, um Directory-Informationen zu lesen oder zu ändern, z. B. Hinzufügen oder Löschen eines Objekts. Die Read-Only Replica wird nur benutzt, um Directory-Informationen zu lesen, aber nicht um Informationen zu ändern. Die NetWare Utilities wählen automatisch die entsprechenden Partitions aus. Die Subordinate Partition wird automatisch eingerichtet, wenn die folgende Situation zutrifft: Auf dem Server befindet sich die Parent Partition, aber die dazugehörige Child Partition ist nicht auf diesem Server. Damit der Server weiß, wie die NDS nach »unten« weitergeht, richtet sich NetWare 4 deshalb diese Subordinate Partition ein. Man kann diesen Vorgang weder vermeiden noch die Subordinate Partition löschen.

Zum Verwalten der Partitions und Replicas wird ein eigenes Partition-Manager-Utility zur Verfügung gestellt.

Beim Einrichten der Partitions bzw. bei der Installation von Servern ist folgender Standardmechanismus zu beachten, der sich nicht beeinflussen läßt:

Wird der Server in einer Partition hinzugefügt, prüft NetWare folgendes nach: Existieren für diese Partition bereits eine Master Partition und zwei Read/Write Replicas, erhält der neue Server keine automatische Read/Write Replica. Stellt das Installationsprogramm fest, daß es für die Partition nur eine Master Partition gibt (sie muß auf alle Fälle vorhanden sein) und weniger als zwei Read/Write Replicas, dann erhält dieser neu zu installierende Server automatisch eine Read/Write Replica.

Bindery-Kompatibilität

Um die Kompatibilität mit Bindery-orientierten Utilities und Clients zu gewährleisten, die zusammen mit NetWare-4-NDS-Systemen im Netzwerk genutzt werden, bietet NetWare 4 eine Bindery-Emulation an.

Objekte der Bindery werden in einer »flachen« Datenbank verwaltet, statt wie NDS-Informationen in einer hierarchischen Datenbank (Directory-Baum). Bindery-Emulation tritt auf, wenn die NDS eine flache Struktur für Objekte innerhalb von Organizational- oder Organizational-Unit-Container-Objekten emulieren müssen.

Alle Objekte in einem Container-Objekt können dann sowohl von NDS-Objekten als auch von Bindery-basierenden Clients, Anwendungen und NLMS auf diesem Server und anderen Servern benutzt werden. Bindery-Emulation wird nur auf die Leaf-Objekte in einer Organizational Unit bzw. Organization angewandt. Dabei werden nur die Leaf-Objekte in der Bindery emuliert, die auch NetWare 3.x

19 Novell NetWare 4.2

in der Bindery abbilden konnte. Das heißt, die speziellen NDS-Objekte Alias, Computer oder Organizational Role können nicht in der Bindery-Emulation abgebildet werden. Wenn NetWare 4 installiert wird, ist die Bindery-Emulation standardmäßig eingeschaltet und verweist immer auf den Container, in dem der Server eingerichtet ist, womit in einer gemischten Netzwerkumgebung (NetWare 3.x und NetWare 4) Clients sofort mit existierenden Shells und Utilities auf NetWare-4.x-Server zugreifen können. Bei Bedarf kann die Bindery-Emulation auf einen anderen Container gesetzt werden. Damit gehen dann natürlich die vorherigen Informationen der Bindery-Emulation verloren. Dies ist wichtig, da beim Einsatz von Anwendungen, die Bindery-Emulation benötigen, immer sorgfältig geplant werden muß, damit sie die richtigen Objekte in der Bindery abbilden und benutzen können.

Zum derzeitigen Stand der Entwicklung wird NetWare 4.1 die Option unterstützen, pro Server nicht nur einen Container als Bindery zu emulieren, sondern bis zu 16 Container als Bindery abbilden zu können. Damit wird der Einsatz von Bindery-basierenden Anwendungen wesentlich vereinfacht. Die Bindery-Emulation ist nur so lange notwendig, wie noch Anwendungen zum Einsatz kommen, die keine NDS-Unterstützung bieten können. Es ist nur eine Frage der Zeit, bis auch die Dritthersteller in der Lage sind, ihre Anwendungen für die NDS anzupassen. Novell selbst will mit Auslieferung von NetWare 4.1 in der Lage sein, alle Add-on-Produkte NDS-fähig auszuliefern. Das ist auch einer der Gründe, warum für NetWare 3.x keine Entwicklungen mehr durchgeführt werden, da man sich voll auf die Entwicklung für die NetWare-4-Umgebung stützt.

Da es sich bei den NDS um eine verteilte und replizierte Datenbank handelt, müssen Einrichtungen innerhalb der NDS und Änderungen der NDS so synchronisiert werden, daß keine Überschneidungen auftreten. Das ist vor allem deshalb wichtig und notwendig, weil die Änderungen durchaus an unterschiedlichen Stellen in der NDS erfolgen können. Wichtigster Faktor ist deshalb für die NDS eine einheitliche Uhrzeit innerhalb der NDS und auf allen Servern. Zu diesem Zweck bietet NetWare 4 die sogenannte Time-Synchronization an.

Abschließend sei noch bemerkt, daß sich innerhalb der NDS alle Leaf-Objekte und Container-Objekte umbenennen lassen. Bei der Umbenennung eines Containers ist nur darauf zu achten, daß sich damit auch die Context-Bezüge ändern können. Dies betrifft sowohl den Name Context auf der Workstation als auch den Bindery Context am Server.

Time-Synchronization

NetWare 4 unterstützt einen Mechanismus, um die Uhrzeiten untereinander zu synchronisieren. Die Zeitsynchronisation ist wichtig für Operationen der NDS-Dienste, da diese eine Aufstellung der durchgeführten Operationen einrichten. Immer wenn ein Ereignis im NDS-Baum auftritt, z.B. wenn ein Paßwort geändert wird oder ein Objekt einen neuen Namen erhält, wird vom Directory Service eine Zeitänderung angefordert. Damit wird festgehalten, wann die Änderung durchgeführt worden ist. Dem Directory Services Event wird ein Zeitstempel zugewiesen, so daß die Reihenfolge, in der Replicas aktualisiert worden sind, korrekt ist.

Time-Server

Bei der Installation von NetWare 4 legen Sie fest, wie die Zeitsynchronisation der NetWare 4 Server erfolgen soll. Hierzu legen Sie fest, welche Art von Time-Server jeder einzelne NetWare 4 Server sein soll.

Jeder Time-Server führt dabei bestimmte Aufgaben zur Zeitsynchronisierung durch. Hierbei ist zwischen folgenden Möglichkeiten zu unterscheiden:

- *Single-Reference-Time-Server*

Dieser Server bestimmt die Uhrzeit für das gesamte Netzwerk und ist die einzige Quelle, von wo aus die Abstimmung der Uhrzeit erfolgt. Der Netzwerkverwalter stellt, wenn nötig, die richtige Uhrzeit am Single-Reference-Time-Server ein.

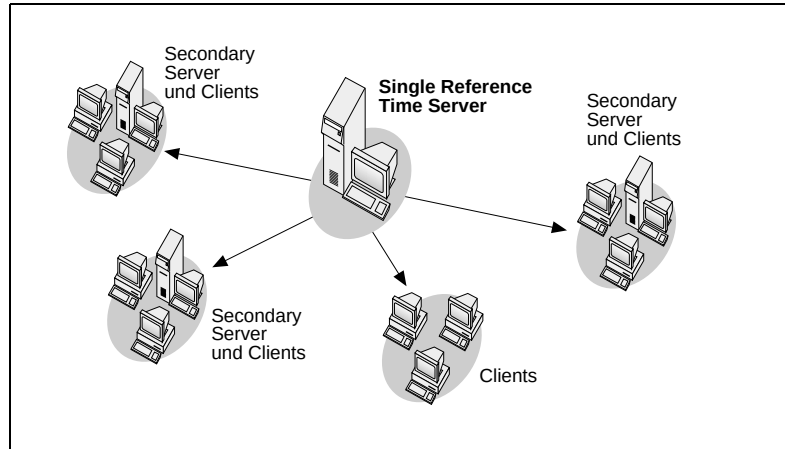
Die Default-Einstellung bei der Installation zur Zeitsynchronisierung legt einen Single-Reference-Time-Server fest, alle anderen Server werden als sekundäre Time-Server eingerichtet. Um am Single-Reference-Time-Server immer die einheitliche Uhrzeit zu haben, kann man ihn mit einer externen Zeitquelle ausstatten, z.B. einer Funkuhr, wie sie von Tobit angeboten wird.

- *Reference-Time-Server*

Reference-Time-Server werden mit Hilfe einer externen Funkuhr (so wie sie auch für Single-Reference-Time-Server eingesetzt werden können) synchronisiert. Reference-Time-Server stimmen sich nicht mit anderen primären oder Reference-Time-Servern ab, um festzulegen, welches die gemeinsame Uhrzeit im Netzwerk sein soll. Reference-Time-Server passen ihre internen Uhren nicht an, sondern geben generell die Uhrzeit im Netzwerk vor. An diese Vorgabe müssen sich die anderen Primary-Time-Server halten. Die internen Uhren der primären Server werden bei diesem Vorgang angepaßt, um mit der Uhrzeit des Reference-Time-Servers synchronisiert zu sein.

19 Novell NetWare 4.2

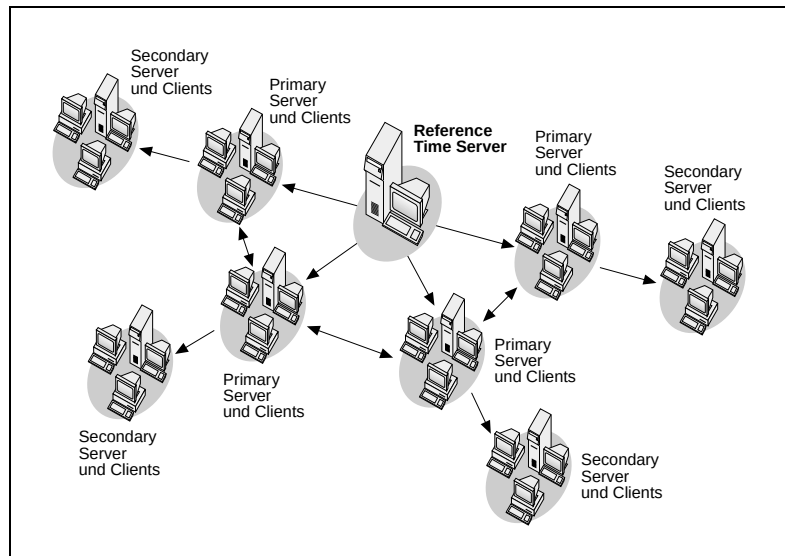
Abbildung 19.4
Zeitsynchronisation
bei einem Single-
Reference-Time-
Server



Ein Reference-Time-Server bestimmt zentral die Uhrzeit im Netzwerk. Notfalls müssen alle internen Uhren der primären Time-Server angepaßt werden, um mit der Uhrzeit des Reference-Time-Servers übereinzustimmen.

Der Reference-Time-Server muß mindestens einen Primary-Time-Server vorfinden, um Synchronizität zu erhalten. Erst wenn der Reference-Time-Server einen anderen Primary-Time-Server findet, stellt sich dieser so um, daß er vorgibt, mit dem Netzwerk synchron zu sein.

Abbildung 19.5
Zeitsynchronisation
bei einem
Reference-Time-
Server



19.16 Directory-Services-Sicherheit

■ *Primäre Time-Server*

Primäre Time-Server stimmen sich ebenfalls mit anderen primären Time-Servern oder Reference-Time-Servern ab, um festzulegen, welche die gemeinsame Uhrzeit sein soll. Primäre Time-Server passen aber ihre interne Uhr an, um mit der gemeinsamen Netzwerkzeit synchron zu laufen. Da alle primären Time-Server ihre Uhrzeit anpassen, kann die Uhrzeit im Netzwerk leicht differieren. Das wird jedoch mit Hilfe der Reference-Time-Server immer wieder ausgeglichen. Fällt der Reference-Time-Server aus, dann bleibt die Uhrzeit im Netzwerk synchron, da die Primary-Time-Server untereinander synchronisiert werden, und somit eine einheitliche Uhrzeit im Netzwerk erhalten wird.

■ *Sekundäre Time-Server*

Sekundäre Time-Server erhalten die Uhrzeit vom Single-Reference-Time-Server, primären Time-Server oder Reference-Time-Server und passen die interne Uhr an, um mit der Netzwerkzeit synchron zu sein. Sekundäre Time-Server bestimmen die Uhrzeit der Clients (Workstations). Sie sind nicht daran beteiligt, die korrekte Uhrzeit im Netzwerk zu bestimmen. In Abbildung 19.4 ist dargestellt, wie die Zeitsynchronisation im Netzwerk durchgeführt werden kann. Ich habe bereits darauf hingewiesen, daß unter NetWare 4 die Mechanismen zur Festlegung der Zugriffsberechtigungen auf Directory- und Dateiebene im Vergleich zu NetWare 3.x die gleichen geblieben sind. Mit NetWare 4 kommen in Verbindung mit NDS zusätzliche Sicherheitsvorkehrungen hinzu, um festzulegen, wer wie und mit welchen Rechten innerhalb der NDS arbeiten darf und kann. Dieser Mechanismus soll im folgenden Abschnitt näher erläutert werden.

19.16 Directory-Services-Sicherheit

Mit den Directory-Services-Sicherheitsmechanismen wird festgelegt, mit welchen Rechten auf Objekte und Properties in der NDS-Datenbank zugegriffen werden darf. Sie legen fest, wer auf die Informationen zugreifen darf. Auf diese Weise wird die Benutzung fast aller Ressourcen im Netzwerk überwacht und kontrolliert.

Zum Beispiel muß ein Benutzer Rechte für sein eigenes User-Objekt und die dazugehörigen Properties haben, um sich überhaupt im Netzwerk anmelden zu können. Ein Benutzer muß die entsprechenden Rechte für ein Objekt haben, um dieses Objekt innerhalb des Directory-Baums sehen zu können. Um die E-Mail-Adresse eines Benutzers sehen zu können, muß der Benutzer das Read-Recht für das Property E-Mail-Adresse haben.

19 Novell NetWare 4.2

Zur Realisierung der Zugriffsrechte auf das NDS-Directory werden verwendet:

- Objekt-Trustee-Rechte
- Objekt- und Property-Rechte
- Inheritance und Inherited Rights Filter (IRF)
- Security-Equivalence
- Effektive Rechte

Directory-Services-Sicherheitsmechanismen sind getrennt von File-System-Sicherheitsmechanismen zu betrachten. Zwischen NDS Security und File System Security bestehen folgende Unterschiede:

- NDS kennen zwei unterschiedliche Rechte: Objekt- und Property-Rechte.
- Rechte von NDS wirken nicht auf File-System.
- Das Supervisor-Objekt und das Property-Recht können in der NDS-Sicherheit unterbunden werden.

Objekt-Trustees

Unter einem Objekt-Trustee versteht man ein Objekt, das in der ACL-Property (Access Control List) in einem anderen Objekt eingetragen worden ist. Jedes Objekt besitzt ein ACL-Property. Diese ACL-Liste legt fest, von wem und auf welche Weise auf das Objekt zugegriffen werden kann. Benutzer und Gruppen werden die meisten Trustees sein, die verwendet werden.

Bevor ein Benutzer Rechte für ein Objekt und seine Properties haben kann, muß er als Trustee für dieses Objekt definiert worden sein. Das ist vergleichbar mit der Trustee-Rechte-Definition für das File-System. Damit Sie Rechte für ein Directory besitzen, müssen Sie als Trustee für das Directory definiert sein.

Mit Hilfe von Gruppendefinitionen können für Benutzergruppen Trustee-Rechte definiert werden. Wenn Sie als Benutzer Mitglied dieser Gruppe sind, dann haben Sie auch die Rechte für die darin aufgeführten Objekte. Die Definition von Gruppen erleichtert die Arbeit, wenn mehrere Benutzer die gleichen Trustee-Rechte auf dieselben Objekte benötigen. Um nicht jedem Benutzer diese Rechte explizit immer wieder vergeben zu müssen, verwendet man die Festlegung von Gruppen. Obwohl Gruppen- und User-Objekte die in einer ACL am häufigsten verwendeten Objekte sein werden, sind andere Objekte nicht davon ausgeschlossen, Objekt-Trustee zu sein.

19.16 Directory-Services-Sicherheit

Objekt- und Property-Rechte

NetWare 4 unterscheidet folgende Rechte für Objekte und Properties:

Objekt-Rechte	Property-Rechte
B Browse	R Read
C Create*)	C Compare
D Delete	W Write
R Rename	A Add or delete self
S Supervisor	S Supervisor

*) Gilt nur für Container-Objekte und nicht für Leaf-Objekte

Rechte legen fest, wie ein Trustee auf ein Objekt zugreifen darf. Ein Trustee kann auf einem Objekt nichts ausführen, wenn er keine Rechte hierfür besitzt. In den NDS existieren Objekt-Rechte und Property-Rechte.

Objekt-Rechte werden verwendet, um Objekte innerhalb von NDS zu verwalten, Property-Rechte legen fest, wie ein Trustee mit dem Objekt arbeiten darf.

Objekt-Rechte legen fest, was ein Trustee mit dem Objekt alles tun darf, d.h., wie das Objekt verwaltet werden kann. Diese Rechte kontrollieren das Objekt als einzelnes Item im Directory-Baum, erlauben aber nicht den Zugriff auf Informationen innerhalb des Objekts.

Die möglichen Rechte und deren Bedeutung sind wie folgt:

Browse	Sie erhalten die Berechtigung, die Objekte im Directory-Baum zu sehen. Damit haben Sie aber nicht die Rechte, die Property-Werte zu sehen.
Create	Sie erhalten die Berechtigung, ein neues Objekt unter diesem Objekt im Directory-Baum zu erstellen. Dieses Recht kann nur für Container-Objekte vergeben werden.
Delete	Sie erhalten die Berechtigung, das Objekt vom Directory-Baum zu löschen.
Rename	Sie erhalten die Berechtigung, den Namen des Objekts zu ändern. Leaf-Objekte können ab der Version 4.0 umbenannt werden. Container-Objekte können erst ab Version 4.1 umbenannt werden.
Supervisor	Sie erhalten alle Zugriffsprivilegien. Ein Trustee mit Supervisor-Objekt-Recht hat Zugriff auf alle Properties. Das Supervisor-Recht kann mit dem Inherited Rights Filter entfernt werden.

Da sich Objekt-Rechte auf die Verwaltung von Objekten beziehen, benötigen User nur das Browse-Recht für Objekte, die sie im Directory-Baum sehen sollen. Verwalter und Directory-Services-Manager haben eine Mischung der Rechte Browse, Create, Delete, Rename und Supervisor. Wenn ein User-Objekt eingerichtet ist, dann wird diesem das Browse-Objekt-Recht für sein eigenes Objekt zugewiesen

Mit den *Property-Rechten* wird festgelegt, ob und wie auf die Informationen der Property-Informationen eines Objekts zugegriffen werden kann und darf.

Folgende Property-Rechte stehen zur Verfügung:

Compare	Damit erhalten Sie das Recht, jeden Wert mit dem Wert, der für das Property definiert worden ist, zu vergleichen. Mit dem Compare-Recht ergibt eine Überprüfung des Property-Werts nur True oder False. Sie können nur mit diesem Recht den Wert nicht sehen.
Read	Erlaubt es Ihnen, den Wert eines Property zu lesen. Das Read-Recht beinhaltet auch das Compare-Recht.
Write	Gewährt das Recht, den Wert des Property beliebig zu ändern, also Werte hinzuzufügen, zu löschen oder zu ändern. Das Write-Recht beinhaltet das Add-Self-Recht.
Add Self	Man erhält mit diesem Recht die Berechtigung, sich selbst als Wert eines Property hinzuzufügen oder zu löschen. Dieses Recht ist nur für Properties bedeutungsvoll, die Objekt-Namen als Werte enthalten, z.B. Gruppenmitgliedschaften oder Mailing-Listen.
Supervisor	Hiermit haben Sie für das Property alle Rechte. Das Property-Supervisor-Recht kann mit einem Inherited Rights Filter für das Objekt ausgeblendet werden.

Inheritance

Rechte, die einem Trustee für ein Container-Objekt gewährt worden sind, vererben sich weiter auf Objekte, die darunterliegen, solange nicht explizite Trustee-Assignments weiter unten durchgeführt oder die Rechte durch einen Inherited Rights Filter (IRF) ausgeblendet werden.

Die Sicherheitsmechanismen für Novell Directory Services sind ein eigenes System und haben nichts mit dem Sicherheitssystem auf Datei- und Directory-Ebene zu tun.

19.16 Directory-Services-Sicherheit

Inherited Rights Filter

Ein Inherited Rights Filter verhindert, daß unnötige Rechte in den NDS auf darunterliegende Objekte vererbt werden. Mit dem IRF legen Sie fest, welche Rechte der Trustee-Recht-Zuweisungen vererbt werden können, die weiter oben durchgeführt worden sind. Wenn für ein darunterliegendes Objekt im NDS-Baum ein neues Trustee-Recht vergeben worden ist, hat dies keinen Einfluß durch einen gesetzten IRF. Das heißt, bei einem vergebenen Trustee-Recht gilt: Effektives Recht für das Objekt entspricht dem Trustee-Recht, und das effektive Recht der darunterliegenden Objekte ergibt sich aus der logischen UND-Verknüpfung von effektivem Recht des Parent und der IRF.

Jeder IRF kann die gleichen Rechte enthalten, die für Trustee-Recht-Zuweisungen zur Verfügung stehen. Das Objekt- und Property-Recht Supervisor kann im Gegensatz zum Supervisory-Recht auf Directory-Ebene im NDS-Baum weiter unten durch eine IRF wieder entfernt werden.

Security-Equivalence

Hiermit legt man fest, daß ein Benutzer A die gleichen Rechte erhält wie der Benutzer B, d.h., Benutzer A ist Security Equivalent Benutzer B.

Jedes User-Objekt hat ein Security Equivalent Property, in dem andere Benutzer und Gruppen eingetragen werden können, von denen der Benutzer die Rechte übernimmt, also Security Equivalent ist. Ein Benutzer mit Supervisor-Recht auf ein User-Objekt kann diesen Benutzer zum Equivalent für andere Benutzer oder Gruppen definieren. Das kann auch mit dem Write- oder Managed-Recht für das Security Equivalent Property eines Benutzers durchgeführt werden. Security-Equivalence ist nicht transitiv, d.h., wenn Benutzer A Security-Equivalent Benutzer B und Benutzer B Security-Equivalent Benutzer C ist, dann ist Benutzer A nicht Security-Equivalent Benutzer C. Das gleiche gilt übrigens auch für Gruppenzugehörigkeiten. Dies kann damit begründet werden, daß die Mitgliedschaft zu einer Gruppe nichts anderes bedeutet, als Security Equivalent zu dieser Gruppe zu sein.

Innerhalb der NDS kann man jeden Benutzer zu jedem anderen NDS-Objekt Security Equivalent machen. Auf diese Weise werden dem Benutzer die Rechte zugeteilt, die dem Objekt, zu dem der Benutzer Security Equivalent ist, explizit zugewiesen worden sind, d.h., wofür direkte Trustee-Rechte definiert wurden. Man sollte diese Möglichkeit jedoch nicht zu sehr ausreizen, da ansonsten die Über-

sichtigkeit zu stark leidet. So vorteilhaft all diese Möglichkeiten auch sein mögen, es bedarf immer und zu jeder Zeit einer gut durchdachten Planung und einer entsprechenden Dokumentation, um alle vergebenen und verwendeten Mechanismen auch Wochen, Monate und noch Jahre später nachvollziehen zu können.

Effektive Rechte

Unter effektiven Rechten versteht man die Rechte, die ein Benutzer auf ein Objekt tatsächlich besitzt. Sie legen fest, was er damit wirklich tun kann und darf. NetWare rechnet die effektiven Rechte für ein Objekt immer wieder neu aus, und zwar immer dann, wenn darauf zugegriffen wird. Das heißt, Änderungen der Rechte für ein Objekt werden für den Benutzer sofort gültig, sobald er erneut auf dieses Objekt zugreift.

Um die effektiven Rechte bestimmen zu können, muß bekannt sein, welche Rechte

- durch Trustee-Assignments für den Benutzer direkt vergeben worden sind,
- durch Security Equivalences vorliegen,
- durch Vererbungen vorliegen,
- durch Gruppen Trustee-Assignments vorliegen,
- durch die IRF entfernt werden.

Rechte für ein Objekt oder ein Property, die ein anderes Objekt für dieses direkt durch eine Trustee-Zuweisung erhält, entsprechen dem effektiven Recht für dieses Objekt oder Property. Das heißt, in diesem Fall ist eine gesetzte IRF vollkommen irrelevant. Die weitere Festlegung der effektiven Rechte für die darunterliegenden Objekte ergibt sich dann aus der logischen UND-Verknüpfung des effektiven Rechts für das Parent-Objekt und der IRF.

Auch bei der Planung der Rechte, sowohl für das Dateisystem als auch für die NDS, muß sorgfältig vorgegangen werden. Dies vor allem auch unter dem Aspekt, daß ein Container auch als Mechanismus verwendet werden kann, mit dem Rechte vergeben und vererbt werden können. Diese Zusammenhänge müssen genau verstanden werden, um nicht plötzlich mit unangenehmen Folgen konfrontiert zu sein. Vielleicht wird dadurch auch klarer, daß es sich bei NetWare 4 in Verbindung mit den NDS um eine sehr leistungsfähige und flexible Architektur handelt, aber eine Installation mal nebenbei eben nicht möglich ist.

19.17 Security Management

Wie bereits mehrfach angedeutet, bietet NetWare 4 neben einer zeichenorientierten Bedienung (Menüsysteme und Befehle) auch eine ausgefeilte und einfache, grafische Oberfläche zum Einrichten und Verwalten der Netzwerkkumgebung unter NetWare 4, damit die Aufgaben für den Netzwerkverwalter einfach gestaltet werden können.

Die GUI (Graphical User Interface) steht sowohl für Windows 3.x als auch für Windows NT in einer eigenen Version zur Verfügung. Die anderen Betriebssysteme – außer Macintosh-Rechner – müssen auf den NWAdmin unter Windows zurückgreifen. Für den Macintosh gibt es bislang keinen eigenen NWAdmin.

In den nachfolgenden Abschnitten sollen zusammengefaßt die wichtigsten zusätzlichen Merkmale von NetWare 4 aufgeführt werden.

19.17 Security Management

Diese Mechanismen können als »umfangreiche Konfiguration« und Zuweisung von Rechten bezeichnet werden. Damit werden die Kosten zur Administration von NetWare 4 reduziert und wesentlich erleichtert.

Der Zugriff auf Netzwerkressourcen kann individuell auf Dateiebene, Benutzergruppen, Properties und individuelle Benutzerobjekte (Telefonnummer eines Benutzers etc.) festgelegt und gesteuert werden. Auf diese Weise kann die Berechtigung, das Netzwerk zu verwalten, zentral für das gesamte Netzwerk durchgeführt werden, und die Verteilung der einzelnen Administrationsaufgaben kann je nach Bedarf festgelegt werden. Es ist zum Beispiel möglich, einen Administrator zur Verwaltung der Paßwörter in einer Abteilung einzurichten, um bei Bedarf Paßwortänderungen für eine bestimmte Gruppe von Benutzern durchführen zu können, wenn diese ihr Paßwort nicht mehr wissen. Somit könnten bestimmte Aufgaben vom Netzwerkverwalter delegiert werden, die ansonsten nur kostbare Zeit in Anspruch nehmen würden.

Das heißt, die Aufgaben in einem Netzwerk könnten je nach Bedarf und Anforderung verteilt werden, und jeder tut das, wovon er am meisten profitieren kann. Auf diese Weise lassen sich Subadministratoren oder auch Workgroup Manager definieren, denen genau die Aufgaben zugeteilt werden, die zur Bewältigung der einzelnen Verwaltungsaufgaben notwendig sind. Dabei kann die Rechtezuweisung über die gesamten NDS verteilt werden.

19.18 Connectivity

Neben dem Packet Burst Mode Protocol, das unter NetWare 3.x optional eingesetzt werden kann, unterstützt NetWare 4 auch standardmäßig den sogenannten LIPX-Modus (Large IPX), den NetWare 3.x ebenfalls optional unterstützen kann. Die Vorteile liegen in einer gesteigerten Performance beim Transportieren von Paketen.

Bislang besaß NetWare die Eigenschaft, zum Transport von Paketen über einen IPX-Router diese Pakete in 512 Byte große Einheiten zu unterteilen, ohne Rücksicht zu nehmen, ob die Station oder der Server auch größere Pakete aufnehmen können. Mit dem LIPX-Mechanismus stimmen sich beide Seiten darauf ab, wie groß die unterstützte Paketgröße sein darf, und verwenden daraufhin genau diese Paketgröße beim Austausch von Daten.

Das RIP (Routing Information Protocol) in NetWare 4 wurde neu geschrieben und gestaltet, um für den Router-Mechanismus (interner oder externer Router) eine höhere Performance zu erzielen. Da RIP in großen Netzwerken zu einer erhöhten Netzwerklast führt (Austausch der Informationen alle 60 Sekunden), soll NetWare 4.1 mit einem neuen Router-Mechanismus ausgestattet werden, der als NetWare Link State Protocol bezeichnet wird. Damit wird nicht mehr alle 60 Sekunden ein Broadcast auf das Netzwerk gegeben, sondern Informationen werden nur dann ausgetauscht, wenn sich der Aufbau des Netzwerks (z. B. neuer Router und neues Netzwerk hinzugefügt) geändert hat. Derzeit kann man die Belastung des Netzwerks durch RIP-Pakete durch Zeitparameter ändern. Man kann somit festlegen, in welchen Abständen RIP-Pakete erzeugt werden sollen. Ähnlich sieht die Situation für das wichtige SAP-Protokoll aus, mit dem jeder Netzwerkdienst in regelmäßigen Abständen bekanntgegeben wird (standardmäßig alle 60 Sekunden). Auch hier läßt sich das Zeitintervall entsprechend konfigurieren. Für die Router-Systeme stehen inzwischen auch Funktionen zur Verfügung, mit denen bestimmte SAP- und RIP-Vorgänge ausgefiltert werden. Informationen, die im anderen Netzwerk nicht benötigt werden, kann man auf diese Weise blockieren. Diese Vorgänge müssen jedoch bei einer großen und komplexen Netzwerkstruktur sorgfältig geplant und konfiguriert werden. Ansonsten kann es passieren, daß plötzlich Netzwerkdienste oder Netzwerke nicht mehr verfügbar sind, da deren Informationen im Router aus Versehen gefiltert worden sind. Zukünftig wird sich auch die SAP-Belastung von NetWare stark reduzieren, da in einer reinen NetWare-4-Umgebung langfristig nur noch das DS-Protokoll (Directory-Services-) notwendig ist.

19.18 Connectivity

Die oben aufgeführten Filter-Mechanismen dienen auch zur Performance-Steigerung bzw. in diesem Falle zur Reduzierung von Overhead auf den Leitungen. Auch diese Unterstützung ist unter NetWare 3.x optional verfügbar, bzw. der Multi Protocol Router (MPR) von Novell (und anderer Router-Hersteller) bietet auch diese Unterstützung. Mit dem SAP-Filter (Service Advertising Protocol) wird vermieden, daß zuviel und zu oft Kontrollinformationen zwischen Servern ausgetauscht werden. Jeder Server-Mechanismus (File-Server, Print-Server, Communication-Server etc.) verschickt in regelmäßigen Abständen SAP-Pakete, um allen anderen im Netzwerk bekanntzugeben, welche Dienste zur Verfügung gestellt werden. Wenn es zum Beispiel nicht notwendig ist, im Netzwerk München zu wissen, daß im Netzwerk Hamburg ein Print-Server zur Verfügung steht, muß über die remote Leitung keine SAP-Information vom Print-Server in Hamburg nach München transportiert werden. Das kann eben mit dem SAP-Filter kontrolliert werden.

Um das gesamte RIP/SAP-Problem unter NetWare noch besser in den Griff zu bekommen, stehen zusätzlich die Möglichkeiten zur Verfügung, auf das NetWare Link Services Protocol oder auf NetWare/IP umzustellen.

NLSP

Um die Internetwork-Kommunikation unter NetWare zu verbessern, hat Novell das NLSP-Protokoll entwickelt. Als Ersatz für das RIP/SAP-Verfahren, bei dem alle 60 Sekunden Informationen ausgetauscht werden, baut NLSP auf dem Link-State-Routing-Verfahren auf, ähnlich wie es für OSPF unter TCP/IP verwendet wird. NLSP tauscht zwischen den Routern Routing-Informationen aus, um aufgrund dieser Informationen die eigenen »Datenbanken« aufbauen zu können. Die Kommunikation zwischen dem Router und der Workstation erfolgt aber immer noch auf Basis von RIP/SAP-Mechanismen.

NLSP-Router tauschen Informationen über folgende Bereiche aus: Connectivity Status, Pfadkosten, Durchsatz, maximale Paketgröße (MTU-Größe) und Netzwerke, die durch RIP-Informationen gelernt werden (externe IPX-Netzwerke). In Netzwerken mit RIP/SAP-Endgeräten verwaltet der NLSP-Router Informationen über Dienste und externe Router-Verbindungen (RIP-basierend). Durch den Austausch all dieser Informationen mit den benachbarten NLSP-Routern bauen sich diese eine logische Abbildung des gesamten Netzwerks auf und verwalten die Informationen dynamisch. Entgegen dem 60-Sekunden-Intervall, so wie es bei RIP/SAP der Fall ist (sofern man keine Änderung für dieses Intervall durchführt), werden beim NLSP-Protokoll Informationsänderungen nur dann ausgetauscht, wenn sich eine Änderung ergeben hat, auf jeden Fall aber alle zwei Stunden.

19 Novell NetWare 4.2

Für den Einsatz von NLSP-Routing-Mechanismen muß eine sorgfältige Planung durchgeführt werden, weil die Link-State-Verfahren nicht einfach so implementiert werden können. Dies gilt vor allem dann, wenn auch noch WAN-Strecken zu berücksichtigen sind und wenn es sich um ein sehr vermaschtes Netzwerk handelt.

Bislang war es so, daß beim Einsatz von mehr als einer Netzwerkadapterkarte NetWare automatisch ein Routing zwischen diesen beiden Karten hergestellt hat. Mit NetWare kann man zum einen das IPX-Routing am Server abschalten und zum anderen durch NLSP auch noch Load Balancing einrichten. Load Balancing bedeutet hier, daß man zwei oder mehr Netzwerkkarten auf das gleiche Segment hängen kann, um somit eine noch bessere Performance zu erhalten. Zudem kann man dies auch als Ausfallsicherheit betrachten. Wenn also die eine Karte ausfällt, kann man den gesamten Netzwerkverkehr immer noch über die andere Karte abwickeln.

NetWare/IP

Mit NetWare/IP kann ein reiner IP-Transport für Netzwerke unter NetWare aufgebaut und installiert werden. Hierdurch wird das gesamte RIP/SAP-Verfahren, das von allen Servern und Routern derzeit in Abständen von 60 Sekunden initiiert wird, abgelöst. Da die RIP/SAP-Mechanismen einen relativ großen Overhead verursachen, der vor allem auf den WAN-Strecken eine hohe Grundlast erzeugt, können auch die Synchronisationsmechanismen von NetWare negativ beeinflusst werden. Dieses RIP/SAP-Verfahren wird durch den Einsatz von NetWare/IP sowohl auf den Servern als auch auf den Clients ersetzt.

Bis auf eine kleine Ausnahme ist laut Aussagen von Novell für die damit zugrunde gelegte Protokollstruktur vollkommene Kompatibilität für existierende IPX/SPX-Netzwerke gegeben. NetWare/IP steht zudem kostenlos für alle NetWare-4-Lizenzen zur Verfügung und ist momentan in der Version 2.2 zu haben. Neben den Vorteilen der Overhead-Reduzierung bedeutet der Einsatz von NetWare/IP auch, daß man eine geringere Protokollvielfalt, und somit auch Protokollpflege, auf den Clients (und den Servern) hat.

Die Netzwerkumstellung auf NetWare/IP ist für den Anwender vollkommen transparent, da nur die unteren Protokollschichten getauscht werden, sich an den Anwendungen selbst jedoch nichts ändert. Die Migration von IPX/SPX kann stufenweise erfolgen, sofern entsprechende IP/IPX-Gateways implementiert werden. Es können aber auch IP- und IPX-Netzwerke in einer Mischumgebung betrieben werden, wenn eine vollständige Umstellung nicht möglich sein sollte.

19.18 Connectivity

Bevor die weiteren Konzepte für eine NetWare/IP-Umgebung vorgestellt werden, sollten aufgrund der Wichtigkeit bereits vorweg wesentliche Bedingungen aufgeführt werden:

- NetWare/IP Clients können nur dann auf NetWare-Drucker (IPX) zugreifen, wenn ein Forwarding Gateway zwischen dem IPX-Segment (in dem sich der Drucker befindet) und dem IP-Segment (in dem die Workstation installiert ist) eingerichtet ist.
- Wird geplant, NetWare/IP tatsächlich in einer reinen IP-Umgebung einzusetzen, dann würde dies auch bedeuten, daß die Netzwerkdrucker alle das IP-Protokoll verwenden müssen. In diesem Fall müßte ein Gateway eingerichtet werden, das in der Lage ist, das Unix Print Protocol lpr zu implementieren, und es müßte ein NetWare-to-Unix-Printer-Mechanismus installiert sein.
- Für das Drucken müssen auf alle Fälle entsprechende Strategien überlegt werden, um eine ordnungsgemäße Implementierung zu erhalten.

Bei einer Integration von NetWare 4 und somit der NDS sind die nachfolgend aufgeführten Aspekte zu beachten.

In den vorherigen Ausführungen wurde bereits darauf hingewiesen, daß es sich bei den NDS um eine globale, verteilte und replizierte Datenbank handelt und somit vorausgesetzt ist, daß sich alle Server untereinander sehen und kennen. Da die NDS für das »Netzwerk« also eine gewisse Grenze darstellen, können »Daten« nicht zwischen zwei NDS-Bäumen ausgetauscht werden. In ähnlicher Weise fungiert eine NetWare/IP-Domain als »natürliche« Grenze zwischen NetWare/IP-Netzwerken. Für die Planung der NetWare/IP-Domain und der NDS muß die gegenseitige Koexistenz beachtet werden. Daraus folgt, daß die NetWare/IP-Domain alle Server des produktiven NDS-Netzwerks beinhalten muß. Es ist durchaus möglich, mehrere NDS-Bäume in einer NetWare/IP-Domain zu pflegen, jedoch sollte man nach Möglichkeit eine NetWare/IP-Domain für einen NDS-Baum einrichten.

Beim Aufbau von NetWare/IP werden die folgenden Komponenten benötigt:

- *Domain Name Service (DNS)*
Der DNS-Server kann entweder bereits existieren oder im Zuge der Installation von NetWare/IP auch auf einem NetWare Server eingerichtet werden. Der DNS-Server wird benötigt, damit NetWare/IP Server und Clients in der Lage sind, den nächsten DSS-Server zu finden. Beim Einrichten der DNS-Server müssen hierfür spezielle Einträge hinzugefügt werden.

19 Novell NetWare 4.2■ *Domain SAP/RIP Server (DSS)*

Auf diesem System werden die SAP-Informationen und die RIP-Informationen gepflegt, damit NetWare Server und Clients in der Lage sind, entsprechende Dienste im Netzwerk zu finden.

Für diese beiden Komponenten gilt es, eine durchdachte Planung im Netzwerk durchzuführen, damit der Datenverkehr für die Kommunikation dieser Systeme nicht plötzlich genauso groß und belastend wird, wie man es bereits von RIP/SAP-Mechanismen kennt. Hierfür sind nicht nur die Anzahl und die Position der DSS-Server ausschlaggebend, sondern auch die Synchronisationsintervalle der Systeme untereinander, die sich jedoch einstellen lassen. Neben diesen zu installierenden Systemkomponenten werden auch noch die NetWare/IP-Server-NLMs und die NetWare/IP-Client-Dateien benötigt.

■ *NetWare/IP-Server*

Hierbei handelt es sich um einen Server, auf dem TCP/IP und NetWare/IP installiert sind. Um die Koexistenz von IPX und IP im gleichen Netzwerk zu ermöglichen, kann der NetWare/IP-Server als Forwarding Gateway bzw. als Non-Forwarding Gateway installiert werden.

Das Zusammenspiel der NetWare/IP-Komponenten ist dabei wie folgt:

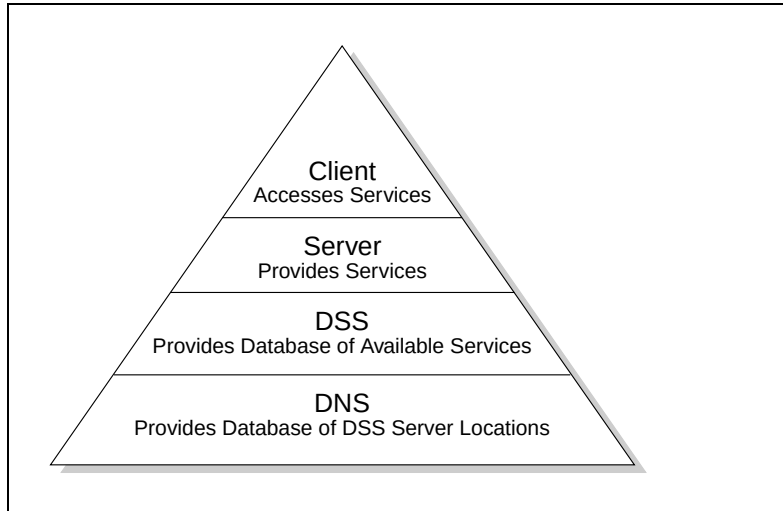
Der DNS-Server speichert Informationen über die Existenz bzw. die Lokation von DSS-Servern im Netzwerk. Solange dieser Dienst nicht läuft, können NetWare/IP-Server und -Clients, die als DNS-Clients oder Resolver definiert sind, keinen DSS-Server finden. Der DSS-Server speichert die Informationen über SAP- und RIP-Mechanismen. Ohne DSS sind die Server im Netzwerk nicht in der Lage, ihre Dienste registrieren zu lassen, und Clients somit nicht in der Lage, auf diese Dienste zuzugreifen. Die Abhängigkeit der einzelnen Komponenten ist in Bild 19.6 dargestellt.

Beim Einrichten der NetWare/IP-Umgebung sind die nachfolgend aufgeführten Schritte von Bedeutung:

1. Wo soll IP eingesetzt werden? Kommt auch noch IPX zum Einsatz? Werden IP und IPX im gleichen Segment parallel verwendet?
2. Werden alle Server auf NetWare/IP umgestellt?
3. Werden alle Clients auf NetWare/IP umgestellt?
4. Wird IPX aus Kompatibilitätsgründen benötigt (z.B. fürs Drucken)?
5. Einrichten einer IP-Infrastruktur, d.h. Vergabe von IP-Adressen für Server und Workstations ⇒ Planung IP-Konzept ⇒ Planung DHCP.

19.18 Connectivity

Abbildung 19.6
Abhängigkeit der
NetWare/IP-
Komponenten



6. DNS-Einrichtung planen (eigener DNS-Server oder auf NetWare Server installieren, Verteilung primärer und sekundärer DNS-Server); vorhandene DNS-Struktur berücksichtigen.
7. Die NetWare/IP Domain für NDS-Baum festlegen.
8. DSS-Server planen und verteilen. Wenn möglich sollte ein DSS-Server in der Nähe der NetWare/IP-Clients und der NetWare/IP-Server vorgefunden werden.
9. Für jeden NDS-Baum sollte eine eigene NetWare/IP-DNS-Domain eingerichtet werden, um die Verwaltung und Administration zu vereinfachen.
10. NetWare/IP-Server bringen mehr Last für den DSS-Server als NetWare/IP-Clients.
11. Die hierarchische DSS-Struktur sollte vorher geplant sein, d.h., nur Secondary-DSS-Server sollten mit Primary-DSS-Servern kommunizieren. NetWare/IP Server und Clients sollten nur mit sekundären DSS-Servern kommunizieren.

Aufgrund der Möglichkeiten, die Novell durch die Implementierung von NetWare/IP zur Verfügung stellt, läßt sich eine klassische IP-Netzwerkumgebung aufbauen, vorausgesetzt, die oben aufgeführten Punkte werden beachtet. Um ein endgültiges Konzept für NetWare/IP zu realisieren, bedarf es allerdings zusätzlicher Vorbereitungen und Planungsarbeit. Ein schnelles Umstellen auf IP ist vor allem in großen und komplexen Netzwerken so nicht möglich.

19 Novell NetWare 4.2

Vor allem drei Aspekte sind dabei von besonderer Bedeutung:

1. Drucken in einer NetWare/IP-Umgebung.
2. Planung von Außenstellen, d.h. Verteilung der DSS-Server, DHCP-Server und DNS-Komponenten – vor allem unter dem Aspekt der Ausfallsicherheit und der Reduzierung der Netzwerklast.
3. Nur eine DSS-Domain für einen NDS-Baum.

NetWare/IP stellt somit eine gute Alternative zum herkömmlichen IPX/SPX-Protokoll dar. Da die Bedeutung von IP in den letzten Jahren immer größer geworden ist – alles spricht von Intranet und Internet – ist der Schritt in Richtung NetWare/IP zur Vereinheitlichung der Protokollumgebung mit Sicherheit nicht verkehrt.

Es ist im Prinzip eine Übergangslösung, IP als Protokoll unter NetWare zu verwenden, solange es noch kein Native IP von Novell gibt. Man darf nicht vergessen, daß es sich bei NetWare/IP um ein proprietäres Protokoll von Novell handelt. Mit Einführung von NetWare 5 ist es Novell endlich gelungen, das NCP-Protokoll vollständig vom IPX-Protokoll zu lösen, so daß Native IP in der Lage ist, per NCP mit dem Server zu kommunizieren. Damit verbunden ist eine Vielzahl von Vorteilen und Neuerungen, die in einem eigenen Kapitel über NetWare 5 erläutert werden.

Es darf an dieser Stelle aber nicht vergessen werden, daß Windows NT 4.0 auch kein Native IP verwendet, sondern auch noch in der Situation ist, daß NetBios-Pakete im IP-Paket verpackt zwischen Server und Workstation transportiert werden. Erst mit Windows 2000 ist auch Microsoft in der Lage, Native IP zu sprechen.

19.19 Skalierbarkeit

NetWare 4 wird in unterschiedlichen Lizenzierungen angeboten. In der momentanen Planung werden folgende Lizenzen angeboten: 5-, 10-, 25-, 50-, 100-, 250-, 500- und 1000-User-Versionen. Bei Bedarf können diese Lizenzen in beliebiger Form aufgestockt werden. So kann man zu einer bestehenden 25-User-Version eine 5-User-Version addieren, um daraus eine 30-User-Version zu machen. Fügen Sie daraufhin noch eine 50-User-Version hinzu, dann erhalten Sie eine 80-User-NetWare-Version. Wenn die eine oder andere addierte Lizenz nicht mehr benötigt wird, dann kann man sie auch wieder entfernen, um sie auf einem anderen Server einzusetzen.

NetWare 4 bietet standardmäßig Utilities an, um von älteren NetWare-Versionen die Umstellung auf NetWare 4 durchführen zu können. Das erste Mal wird auch mit NetWare 4 ein Migrationsme-

chanismus zur Verfügung gestellt, um von einem anderen Betriebssystem auf NetWare 4 umzustellen. Nach der Migration ist aber immer noch die eine oder andere Nachbesserung notwendig.

19.20 Print-Services

Mit NetWare 4 sind die Druckdienste wesentlich verbessert, einfacher zu administrieren, einzurichten und zu benutzen. Nach wie vor benutzt NetWare 4 Print-Server und Print-Queues, um Netzwerkdrucker bedienen zu können. In einer Bindery werden der Print-Server und die Print-Queue als Bindery-Eintrag verwaltet, wohingegen Printer als Attribute des Print-Servers verwaltet werden.

Unter NDS werden der Print-Server, die Print-Queue und der Drucker als individuelles Objekt in der NDS erstellt, verwaltet und geändert. NetWare-4-Benutzer müssen nichts mehr über Print-Queues und Print-Server wissen, vielmehr schicken sie die Druckaufträge nur noch an den Drucker durch Angabe des Druckernamens, unter dem er in der NDS eingerichtet worden ist.

Netzwerkdrucker können direkt im Netzwerk, an jeden beliebigen Server oder an einer DOS-, Windows-, Windows-95- oder OS/2-Workstation installiert werden. Der NetWare-4-Print-Server kann jetzt bis zu 256 Drucker im Netzwerk unterstützen und verwalten (bisher 16). Zudem ist es möglich, festzulegen, in welchem Intervall der Print-Server in einer Queue nachsieht, ob neue Druckaufträge vorhanden sind (Default 15 Sekunden). Die neuen Print-Server für NetWare 3.x können diesen Mechanismus inzwischen ebenfalls über Parameterangabe beim Starten des Print-Servers unterstützen. Es sei nochmals daran erinnert, daß jede Workstation so konfiguriert werden kann, daß ihr bis zu neun LPT-Schnittstellen zur Verfügung stehen, um auf entsprechend vielen Druckern im Netzwerk gleichzeitig arbeiten zu können.

19.21 Sonstige Neuerungen für das Netzwerkbetriebssystem

Neben den oben aufgeführten Aspekten wartet NetWare 4.11 noch mit einer Vielzahl von Modifikationen und Mechanismen auf, die in diesem Kapitel aufgeführt werden. Es handelt sich dabei auch um Mechanismen, die bei einer Vielzahl von Anwendern noch gar nicht bekannt sind, da man häufig nur davon ausgeht, daß intraNetWare nur das NOS NetWare 4.11 ist. Es werden damit aber auch Module für die Integration in eine IP-Welt (z. B. Unix, Internet etc.) zur Verfügung gestellt, ohne daß man hierfür zusätzlich Geld bezahlen muß.

NetWare Web Server

Ursprünglich war NetWare 4.11 mit einem von Novell entwickelten Web Server ausgeliefert worden. Inzwischen hat Novell diese Entwicklung wieder eingestellt, da man eine Kooperation mit Netscape eingegangen ist. Aus dieser Kooperation stammt deshalb die freie Verfügbarkeit des Netscape FastTrack Server, das ist ein sehr leistungsfähiger Server, der auch in der Lage ist, die Informationen aus der NDS auszulesen. Hierzu ist dann aber die Installation der LDAP-Services auf dem NetWare Server notwendig. Mit dem Web Server können Dokumente im Intranet oder im Internet veröffentlicht werden. Im FastTrack Server von Netscape sind die folgenden Funktionen enthalten:

- Die Installation ist sehr einfach durchzuführen, auch wenn es um die Konfiguration des Web Server geht. Nach dem Einspielen der entsprechenden NLMs muß nur ein Befehl an der Console eingegeben werden, damit der Web Server startet.
- Der Web Server enthält BASIC- und PERL-Script-Interpreter. Ebenso wird der Einsatz von JavaScripts unterstützt.
- Durch die Verwendung der standardmäßigen Sicherheitsfunktionen von NetWare 4 können die Zugriffe am Server und der Zugriff auf das Dateisystem einfach und komfortabel eingerichtet und überwacht werden. Zusätzlich können die Zugriffe auf HTML-Dokumente über die IP-Adresse, Benutzername, Hostname, Directory-Struktur, Dateiname oder Gruppenzugehörigkeit gesteuert werden.
- Die Funktionen von SMP werden vom Web Server ebenfalls unterstützt.
- Um die Sicherheit zu erhöhen, nutzt der FastTrack Server nicht nur die NDS-Authentifizierung, sondern auch die Secure-Socket-Layer-3.0-Funktionen, ein im Internet anerkannter Sicherheitsstandard zur Verschlüsselung der Daten zwischen Server und Client. Der FastTrack Server unterstützt auch die Access Control Lists (ACLs), um damit festlegen zu können, wer mit welchen Rechten auf ein Dokument zugreifen darf.

FTP Server

Zum Lieferumfang von NetWare 4 zählt ein FTP Server von Novell, mit dem man in der Lage ist, jeden NetWare Server zum FTP Server zu machen. Über einen solchen installierten FTP Server ist man auch in der Lage, diesen FTP Server zu nutzen. Auf diesen kann per IP-Protokoll zugegriffen werden sowie von diesem aus mit dem IPX Protokoll auf andere NetWare Server. Es sind auch entsprechende Sicherheitsmechanismen vorhanden, um damit zu steuern, wer auf

19.21 Sonstige Neuerungen für das Netzwerkbetriebssystem

den FTP Server zugreifen darf und wer nicht. Die Installation dieses FTP Servers dauert im Prinzip nur Sekunden, und er kann in ebenso kurzer Zeit konfiguriert werden.

DHCP Server

Wenn man sich eine IP-Protokoll-Landschaft aufbaut, dann muß man auch die Entscheidung treffen, wie die Vergabe der IP-Adressen für die einzelnen Workstations im Netzwerk erfolgen soll. Entweder man vergibt die IP-Adresse pro Workstation »manuell«, indem man das IP-Protokoll auf jeder Workstation separat für sich konfiguriert, oder man setzt den standardmäßig im Lieferumfang enthaltenen DHCP Server ein. DHCP steht als Abkürzung für Dynamic Host Configuration Protocol und soll dazu dienen, einer Workstation beim Starten die IP-Adresse zuzuweisen. Dies kann dabei dynamisch oder statisch erfolgen. Dynamisch heißt, beim Starten der Workstation erhält die Workstation die nächste freie IP-Adresse zugewiesen. Damit nicht jede Workstation nach jedem Neustart eine neue IP-Adresse erhält und damit die Wartung und Pflege des Netzwerkes sehr unübersichtlich wird, hat man bei DHCP die Möglichkeit, eine sogenannte Lease Time zu definieren. Diese Lease Time legt fest, wie lange eine vergebene IP-Adresse der Workstation für diese reserviert bleibt. Wenn innerhalb dieser Lease Time die Workstation keine Verbindung zum DHCP Server aufgebaut hat, wird der Eintrag aus der DHCP-Tabelle gelöscht und steht als frei verfügbarer Eintrag zur Verfügung. Wird die Workstation innerhalb der Lease Time aktiviert, dann wird auch der Eintrag für die Workstation beibehalten. Man hat aber auch die Möglichkeit, statische IP-Adressen für die Workstations zu definieren. Hierzu trägt man in die DHCP-Tabelle einen statischen Eintrag ein, indem man eine MAC-Adresse (die der Workstation) und die hierfür zu vergebende IP-Adresse einträgt. Wird die IP-Adresse dynamisch vergeben, dann trägt der DHCP Server in die DHCP-Tabelle die MAC-Adresse der Workstation und die vom DHCP Server vergebene IP-Adresse ein.

Auf der Workstation muß in der TCP/IP-Konfiguration die Option aktiviert werden, daß die IP-Adresse vom DHCP Server bezogen wird; ist dieser Eintrag nicht aktiviert, dann erwartet die TCP/IP-Konfiguration eine manuelle Vergabe der IP-Adressen und alle hierzu notwendigen Angaben. Alle diese notwendigen Angaben, wie z.B. Default Gateway, Subnetz-Maske, DNS-Eintrag etc., können auch bereits für die DHCP-Server-Konfigurationen eingetragen werden.

Der DHCP Server von Novell ist auch in der Lage, Angaben für den sogenannten WINS-Dienst für Windows NT durchzuführen. Somit eignet sich der DHCP Server von Novell auch dafür, in einer gemischten NetWare/Windows-NT-Umgebung eingesetzt zu werden.

19 Novell NetWare 4.2

Es sei an dieser Stelle auch noch erwähnt, daß der DHCP Server von Novell auch noch Zusätze enthält, die es erlauben, für die Workstation Einträge durchzuführen, die für den Einsatz von NetWare/IP benötigt werden. Da es sich bei NetWare/IP um ein proprietäres Protokoll von Novell handelt, wird dieser NetWare/IP-Mechanismus nicht von anderen DHCP Servern unterstützt.

DNS Server

Wer sich mit einem Web-Browser im Internet bewegt, weiß, daß man hierfür eine Web-Adresse angeben muß. Wenn man z.B. eingibt `www.zenk.de`, dann wird man im Internet auf den Web-Server der Zenk GmbH geschleust. Wie wird dies durchgeführt? Der Web-Browser benötigt für das Auffinden des Web-Servers eine IP-Adresse, und die verbirgt sich hinter der sogenannten DNS-Adresse `www.zenk.de`. Hierzu werden sogenannte DNS-Server (Domain Name Server) aufgebaut und gepflegt. In einem solchen DNS-Server steht dann z.B. der Eintrag, daß `www.zenk.de` die IP-Adresse `a.b.c.d` zugeteilt bekommt. Ebenso benötigt man noch einen Domänen-Namen, den man in der Regel beim Internet Service Provider (ISP) beantragen kann. Im Internet ist man nicht in der Lage, und zwar aufgrund der Größe, alle DNS-Einträge über nur einen DNS-Server abzuwickeln. Deshalb gibt es eine Vielzahl von DNS-Servern, die eine geordnete Hierarchie bilden. Der DNS-Server von Novell kann problemlos in eine solche Hierarchie eingebunden werden. Ansonsten unterstützt der DNS-Server alle Mechanismen, die man zum Aufbau von DNS-Mechanismen benötigt. Auch der DNS-Server ist integraler Bestandteil von NetWare 4.

Unix Print Services

Es mag an der Beschriftung der CD liegen, aber es ist wenigen bekannt, daß auf der CD zur Installation des FTP-Servers auch die Unix Print Services vorzufinden sind. Mit den Unix Print Services ist man in der Lage, daß unter NetWare Drucker angesteuert werden können, die das LPR-Protokoll unterstützen. Die Unterstützung ist notwendig gewesen, um mit NetWare/IP eine vollständige IP-Welt zu schaffen. Hierzu gehört dann aber auch, daß das Drucken über IP abgewickelt wird. Hierzu dient das LPR-Protokoll, so wie dieses aus der Unix-Welt bekannt ist.

Neben diesen Funktionen beinhaltet intraNetWare auch noch NIAS 4, den sogenannten Novell Internet Access Server. Zum Inhalt von NIAS gehören der NetWare Multiprotocol Router 3.1, das IPX/IP Gateway, die WAN Extensions und Netscape Navigator.

Multiprotocol Router 3.1 (MPR)

Mußte man in der Vergangenheit den MPR noch als separates Produkt erwerben, so hat man jetzt einen vollwertigen Router zur Verfügung, der die Protokolle IPX, TCP/IP und AppleTalk unterstützt. Über die SNA Extensions ist man auch noch in der Lage, daß der MPR zusätzlich das SNA-Protokoll und Source Route Bridging für NetBIOS und LLS-Anwendungen unterstützt.

Zudem ermöglicht es der MPR, daß Hochgeschwindigkeits-WAN-Verbindungen aufgebaut werden, z.B. zu einem Internet Service Provider über ISDN, Mietleitungen, Frame Relay oder ATM. Diese erweiterte Unterstützung wird durch die WAN Extensions ermöglicht.

IPX/IP Gateway

Mit diesem Gateway ist man in der Lage, IP-basierende Anwendungen zu nutzen, ohne auf der Workstation das IP-Protokoll installieren zu müssen. Hierzu wird im Netzwerk ein IPX/IP Gateway installiert, das die entsprechenden IPX-Datenpakete der Workstation aufnimmt, in IP umwandelt und an das entsprechende IP-Zielsystem weitergibt. Am Anfang der Installation war man noch sehr euphorisch, was dieses Gateway anbelangte, da man nicht gezwungen war, jeden Arbeitsplatz mit IP auszustatten. Inzwischen ist die Ernüchterung gekommen, und man hat festgestellt, daß dieses IPX/IP Gateway zwar sehr schön ist, aber der Sinn immer mehr in den Hintergrund tritt, da ein flächendeckender Einsatz von IP als einziges oder zusätzliches Protokoll immer häufiger wird. Man will langfristig gesehen vom IPX-Protokoll weg und hin zu IP als dem Standardprotokoll. Dies ist auch der Grund, warum NetWare 5 das IP-Protokoll als Standardprotokoll einsetzt.

NetWare Symmetric Multiprocessing

Unter NetWare 4.1 mußte die SMP-Unterstützung noch vom jeweiligen Hersteller des Servers zur Verfügung gestellt werden. In der intraNetWare-Version ist diese Funktion standardmäßig im Produkt enthalten. Je nach Ausbaustufe stehen einem am Server mehr Verarbeitungskapazität und eine höhere Netzwerkperformance zur Verfügung. Abhängig von der Hardware des Servers könnte dieser unter NetWare 4 mit bis zu 32 Prozessoren ausgestattet werden.

UPS-Unterstützung an der seriellen Schnittstelle

Mit dem immer noch vorhandenen UPS.NLM kann NetWare die Steuerung und Überwachung der USV übernehmen, wenn diese am Maus-Port oder an der Karte eines Drittherstellers angeschlossen ist.

19 Novell NetWare 4.2

Mit dem neuen UPS_AIO.NLM wird in Verbindung mit dem AIO.NLM der Anschluß der USV an der seriellen Schnittstelle unterstützt. Zu beachten ist dabei nur, daß das serielle Kabel abgestimmt sein muß auf die eingesetzte USV-Anlage.

CLIB-Erweiterung

Bislang bestand die CLIB unter NetWare aus genau einem Modul. Um das Arbeiten unter NetWare und vor allem auch die Entwicklung und den Austausch einzelner Elemente zu erleichtern, hat man die CLIB in insgesamt sechs Module aufgeteilt. Der Vorteil dabei ist auch, daß diese neue Aufteilung der CLIB effizienter für das Arbeiten von und mit NetWare ist und etwa 80 Prozent weniger dynamischen Hauptspeicher benötigt als die alte CLIB.

Die CLIB ist wie folgt aufgeteilt:

- *CLIB.NLM*
Eine ANSI-kompatible Runtime-Schnittstelle für die alten CLIB-Funktionen. Zusätzlich wurden die Funktionen der bisherigen Module MATHLIB.NLM und MATHLIBC.NLM in das CLIB.NLM-Modul integriert. Somit sind die Module MATHLIB.NLM und MATHLIBC.NLM nicht mehr als einzelnes Modul vorhanden.
- *FPSM.NLM*
Dieses Modul wird für die Floating Point Support Library benötigt.
- *THREADS.NLM*
NetWare-Standard-NLM zur Unterstützung von Threads.
- *REQUESTR.NLM*
Das Standard-Requester-Modul.
- *NMLIB.NLM*
POSIX und andere grundlegende NLM-Runtime-Unterstützung.
- *NT.NLM*
Dieses Modul wird für alte Interface-Tools verwendet, die durch Schnittstellen im CALNLM32.NLM-Modul ersetzt worden sind.

Plattformabhängige Verbesserungen

Um den neuen Hardware-Techniken gerecht werden zu können, wurden im Kernel zusätzliche Verbesserungen eingebaut. Diese Modifikationen beziehen sich auf die folgenden grundlegenden Ergänzungen, die in NetWare 4.1 noch nicht verfügbar gewesen sind:

- Die Memory-Management-Routinen im Server wurden dahingehend verbessert, daß auch die Vorteile des Global-Page-Attributs genutzt werden können, so wie es für Intel-Pentium-Pro-Prozessoren zur Verfügung steht.

19.21 Sonstige Neuerungen für das Netzwerkbetriebssystem

- Die High-Resolution-Timer-Routinen wurden dahingehend verbessert, daß die Vorteile der internen Taktung genutzt werden können, so wie dies für Intel-Pentium- und Intel-Pentium-Pro-Prozessoren verfügbar ist. Dadurch werden die Performance und die Zuverlässigkeit der Packet-Burst-Funktionen verbessert.
- Die Unterstützung für die PCI-Architektur (Peripheral Component Interface) wurde noch weiter ausgebaut. Dies wirkt sich vor allem auf die Installation von NetWare 4.11 aus. In der Regel ist NetWare 4 sehr gut in der Lage, PCI-Karten im Server automatisch zu erkennen. Es funktioniert zwar nicht immer, aber immer öfter.

19.21.1 Installation

Die Installation wurde bislang in allen neuen NetWare-Versionen immer wieder verbessert und modifiziert. So auch jetzt wieder. Das Install-Utility versucht standardmäßig, die gesamte eingebaute Hardware im Server selbst zu erkennen. Hierzu zählen Platten-Controller, CD-ROM-Laufwerke, Netzwerkadapterkarten und was sonst noch alles eingebaut sein kann (z.B. mehrere Prozessoren). Daraufhin werden die notwendigen Devices-Treiber ausgewählt und zur Installation vorgeschlagen. Voraussetzung ist jedoch, daß es sich beim Server um eine Hardware handelt, die eine EISA-, PCI-, PNPIA-, PCMCIA- oder MCA-Architektur besitzt. Es ist jedoch immer von Vorteil, bei den vorgeschlagenen Komponenten zu prüfen, ob auch die ermittelten Hardware-Einstellungen für den zu ladenden Treiber die richtigen sind.

Um die Migration auf die neue NetWare zu erleichtern, ist es Novell inzwischen gelungen, ein sehr gutes Migrations-Tool zu integrieren. Es handelt sich dabei um das Produkt eines Drittherstellers, mit dem ich schon seit langem arbeite. Mit NetWare 4 besteht jetzt der Vorteil, daß ich mich um den Upgrade für dieses Tool nicht mehr kümmern muß. Das zur Verfügung gestellte Produkt unter NetWare DS Migrate stammt von Preferred Systems und wurde von dieser Firma als DS-Standard vertrieben.

DS Migrate

DS Migrate ist ein neues Utility zur Migration und Modellierung der NetWare-4-Umgebung. Über das DS Migrate Utility können Umstellungen von NetWare 2.x/3.x auf NetWare 4 durchgeführt werden. Das Utility erlaubt es Ihnen, Bindery-Informationen bestehender Server einzulesen, mit diesem Utility zu modellieren und anschließend als neue NDS in NetWare 4 zu übertragen. Mit diesem Utility können

19 Novell NetWare 4.2

aber nur Bindery-Informationen migriert werden; zum gleichzeitigen Migrieren der Daten steht das Tool NetWare File Migration unter Windows oder das Migrate Tool für DOS zur Verfügung.

Das DS Migrate Utility stellt auch Möglichkeiten zur Verfügung, eine vollständig neue NDS-Struktur aufzubauen, d.h., Sie können erst mit diesem Tool eine neue NDS modellieren und nach allen Regeln der Kunst anpassen. Wenn dieser Vorgang abgeschlossen ist, kann die neue NDS-Struktur in die NetWare-4-Umgebung übernommen werden. Auf diese Weise kann man zum Beispiel sehr schnell und einfach die produktive NDS auf ein Testsystem übertragen. Man braucht sich damit keine großen Gedanken mehr zu machen, wenn im Testsystem die NDS zerstört worden ist, da man sehr schnell eine neue produktive NDS einspielen kann.

NetWare File Migration

Nach der Übertragung der Bindery-Informationen mit Hilfe des Utility DS Migrate müssen die Daten vom NetWare 3 Server auf den NetWare 4 Server übertragen werden. Das grafische Tool bietet Ihnen einen sehr praktischen Weg zur Migration der Datenbestände.

Wer schon mit den früheren DOS-Programmen für die Migration gearbeitet hat, wird bei den neuen grafischen Tools feststellen, daß sie nicht nur sehr einfach zu bedienen sind, sondern auch eine Vielzahl weiterer Möglichkeiten zur Verfügung stellen, die es erlauben, genau festzulegen, was in welcher Form zu übertragen ist.

19.21.2 Graphical User Interface

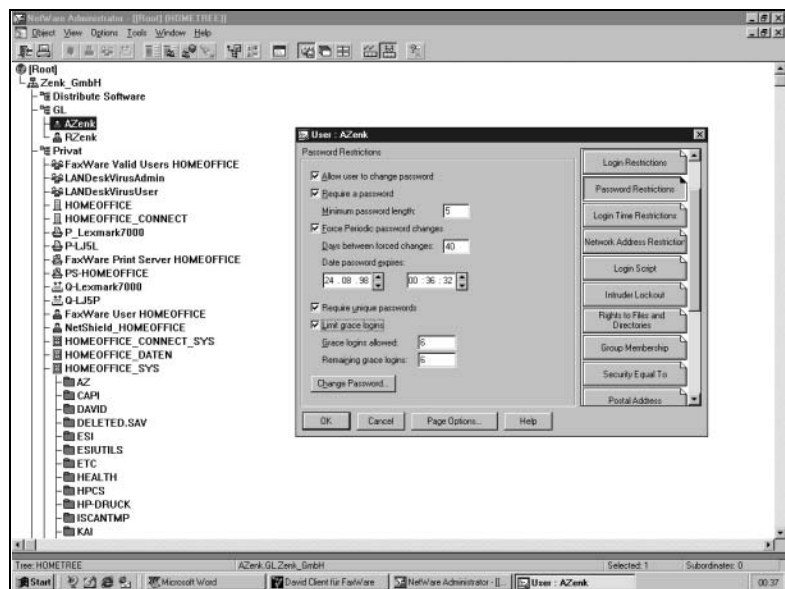
Nicht selten wird behauptet, daß NetWare 4 keine grafische Verwaltung vorweisen kann. Dies ist richtig, solange man sich administrativ am Server befindet. Alle Menüsysteme, die einem am Server zur Verfügung stehen, sind herkömmliche C-Worthy-Menüsysteme. Für die herkömmlichen Aufgaben, die man am Server durchführen muß, ist dies auch ausreichend; zudem leidet die Performance von NetWare 4 nicht darunter, daß grafische Oberflächen am Server eingesetzt werden. Der größte Teil der Netzwerkverwaltung wird jedoch von der Workstation aus durchgeführt. Der NetWare-Administrator erlaubt unter anderem die folgenden Einrichtungs- und Verwaltungsfunktionen:

- Einrichten, Ändern, Löschen, Verschieben oder Umbenennen von Benutzern
- Einrichten, Ändern, Löschen, Verschieben oder Umbenennen von Gruppen

19.21 Sonstige Neuerungen für das Netzwerkbetriebssystem

- Einrichten, Ändern, Löschen, Verschieben oder Umbenennen von Print-Queues
- Einrichten, Ändern, Löschen, Verschieben oder Umbenennen von Print-Servern
- Einrichten, Ändern, Löschen, Verschieben oder Umbenennen von Printern
- Einrichten, Ändern, Löschen, Verschieben oder Umbenennen von Volumes
- Modifikation der Server-Objekte
- Einrichten, Ändern, Löschen, Verschieben oder Umbenennen von Dateien und Verzeichnissen
- Einrichten, Ändern, Löschen, Verschieben oder Umbenennen aller weiteren Objekte, die über Snap-in-Module in den NWAdmin integriert werden können. In Abbildung 19.7 ist dargestellt, wie sich das neue GUI von NetWare 4 darstellt.

Abbildung 19.7
GUI-Oberfläche
NWAdmin



Man sieht, daß NetWare 4 bzw. intraNetWare mit einer sehr umfangreichen Produktpalette aufwarten kann, um damit leistungsfähige Intranets bzw. Intranets realisieren zu können.

19.22 Produktvoraussetzungen

Die Hardware des Servers muß bestimmte Voraussetzungen erfüllen, damit die NetWare-4-Software installiert werden kann.

Hardware-Voraussetzungen

- Ein PC mit einem 386-, 486- oder 586-Prozessor (besser ab 486-Prozessor wegen Performance).
- Mindestens 8 Mbyte Hauptspeicher. Damit können jedoch nur die Grundfunktionen abgedeckt werden. Ab 32 Mbyte Hauptspeicher hat das Ganze erst richtig Sinn.
- Eine Festplatte mit mindestens 55 Mbyte Speicherkapazität (5 Mbyte für DOS-Partition und 50 Mbyte für die Systemdateien). Das ist die minimale Anforderung an das Volume-SYS. Sehr viel Platz für andere Dateien bleibt Ihnen dann aber nicht mehr, wenn Sie alle NetWare-4-Optionen, die standardmäßig im Lieferumfang enthalten sind, einrichten und konfigurieren. Das sind nur Angaben für ein kleines Testsystem. Für einen produktiven Server wird man inzwischen nicht mehr unter 1 Gbyte Plattenkapazität anfangen.
- Eine zusätzliche Plattenkapazität von 25 Mbyte (nichtkomprimierter Datenbereich) auf einem Volume sollte zur Verfügung stehen, um die Electronic Online Documentation auf dem Server installieren zu können.
- Eine Netzwerkkartenkarte (oder mehr, wenn der Server als Router für mehrere Netzwerksegmente dienen soll).
- Die richtige Netzwerkverkabelung.
- Ein CD-ROM-Laufwerk, wenn Sie den Server von CD installieren. NetWare 4 wird standardmäßig auf einer CD ausgeliefert. Die meisten Hersteller von CD-ROM-Laufwerken bieten entsprechende Treiberprogramme an, um das CD-ROM unter DOS ansprechen zu können. Da NetWare mit Hilfe von DOS gestartet wird, ist auch zur Installation die Ansteuerung des CD-ROM-Laufwerks unter DOS notwendig. Befindet sich das CD-ROM-Laufwerk an einer Workstation oder einem anderen Server, kann die Installation von NetWare 4 dennoch durchgeführt werden. Das CD-ROM-Laufwerk muß also für die Installation nicht direkt am zu installierenden Server eingebaut sein.

Software-Voraussetzungen

- NetWare-4-CD-ROM (wenn von CD-ROM installiert wird).
- Wenn von Diskette installiert wird, werden folgende Disketten benötigt (ich kenne derzeit allerdings niemanden, der NetWare 4 auf Diskette besitzt):

19.23 Workstation-Befehle

- Install
- Alle Disketten, die mit »Language« bezeichnet sind (English, Deutsch etc. – je nach Nationalitätsversion)
- Alle Disketten, die mit NetWare bezeichnet sind
- Disketten eventueller Dritthersteller (LAN-, Disk-Driver etc.)

Die Installation von NetWare 4 ist im Vergleich zu NetWare 3.x nochmals verbessert und erleichtert worden. Alle notwendigen Angaben zur Konfiguration der Server-Umgebung und zum Laden der notwendigen Module werden interaktiv durchgeführt, so daß für die Grundkonfiguration nichts mehr vergessen werden kann, um einen lauffähigen Server zu installieren.

Zusammengefaßt kann gesagt werden, daß mit NetWare 4 ein Netzwerkbetriebssystem zur Verfügung steht, das es erlaubt, einfach und bequem kleine und große Netzwerk zu betreiben und zu administrieren. Die Möglichkeiten und die Leistungsfähigkeit sind bereits mit NetWare 3.x sehr groß und werden mit NetWare 4 noch um einiges übertroffen.

Einige wichtige und interessante Zusatzprodukte zu NetWare sollen später noch betrachtet werden. Dabei wird es vor allem um solche Produkte gehen, die von anderen Herstellern nicht oder zumindest nicht in dieser Form angeboten werden. Es ist inzwischen nicht mehr möglich, einen Überblick über die gesamte – nämlich riesige – Produktpalette zu geben.

Abschließend will ich Ihnen die in NetWare 4 zur Verfügung stehenden Menüsysteme und Befehle aufzeigen, sofern Sie nicht mit dem GUI die Netzwerkverwaltung durchführen wollen. Dabei ist zu unterscheiden zwischen Befehlen, die an der Workstation zur Verfügung stehen, und Befehlen, die direkt am Server eingegeben werden können.

19.23 Workstation-Befehle

Flag

In diesem Befehl sind die bisher bekannten Befehle *Flag*, *Flagdir* und *Smode* zusammengefaßt. Mit diesem Befehl werden im großen und ganzen die Datei- und Directory-Attribute geändert, und es wird der Search Mode für ausführbare Programme bestimmt. Der Befehl kann ebenfalls genutzt werden, um den Owner einer Datei oder eines Directory zu ändern.

Map

In diesem Befehl sind jetzt die Befehle *Map* und *Attach* zusammengefaßt worden. Zudem kann mit diesem Befehl aus einem herkömmlichen Netzwerklaufwerk ein Suchlaufwerk gemacht werden und umgekehrt. Dies vereinfacht das Arbeiten mit Laufwerksbuchstaben und Suchpfaden.

19 Novell NetWare 4.2

Ndir	Dieser Befehl umfaßt die bisher bekannten Befehle <i>Listdir</i> und <i>Ndir</i> . Außer einer kleinen Änderung im Format der Anzeige am Bildschirm haben sich keine weiteren Modifikationen ergeben. Dies ist einer der leistungsfähigsten Befehle, um alle Informationen über Dateien und Directories zu erhalten.
Nlist	Der bisher bekannte Befehl <i>Slist</i> heißt jetzt <i>Nlist</i> und beinhaltet auch den Befehl <i>Userlist</i> . Zudem lassen sich mit diesem Befehl alle Informationen über die NDS und die einzelnen NDS-Objekte gezielt auswerten. Hiermit können auch Abfragen nach dem Yellow-Page-Prinzip erfolgen.
Rights	In diesem Befehl sind die meisten Befehle der bisherigen NetWare zusammengefaßt. <i>Rights</i> umfaßt jetzt die Befehle: <i>Allow</i> , <i>Grant</i> , <i>Remove</i> , <i>Revoke</i> , <i>Rights</i> und <i>Tlist</i> . Dieser Befehl arbeitet zur Regelung der Sicherheitsmechanismen auf Datei- und Directory-Ebene.
Send	In diesem Befehl sind <i>Caston</i> , <i>Castoff</i> und <i>Send</i> zusammengefaßt.
Capture	Dieser Befehl zum Umleiten von Druckaufträgen zu einem Netzwerkdrucker steuert jetzt auch über Parameter die Aufhebung der Druckerumleitung, d.h., der Befehl <i>Endcap</i> wurde in <i>Capture</i> integriert.
Cx	Dieser Befehl ändert den Kontext der Workstation, also den Pfad, unter dem ein Objekt gesucht wird, wenn dieser nicht explizit angegeben wird. Daneben besteht auch die Möglichkeit, den derzeit aktuellen Kontext abzurufen und sich den gesamten NDS-Baum auflisten zu lassen.
Nprint	Dient wie bisher zum Ausdrucken von druckfertigen Dateien auf einem Netzwerkdrucker. Dabei kann es sich entweder um eine Textdatei handeln oder um eine Datei, die von einer Applikation erstellt worden ist. Bisher bekannte Befehle von NetWare 3.x existieren als solche entweder gar nicht mehr oder wurden umgestaltet. Folgende Änderungen haben sich dabei ergeben.
Auditcon	Die Befehle <i>Atotal</i> und <i>Paudit</i> wurden in das Menüsystem <i>Auditcon</i> integriert. Hiermit werden die gesamten Mechanismen für das Auditing unter NetWare 4 eingerichtet, verwaltet und ausgewertet.
Dsrepair	Der Konsolen-Befehl <i>Dsrepair</i> beinhaltet die Mechanismen zur Korrektur von Sicherheitseinrichtungen, die bisher in der Bindery vorhanden waren und mit <i>Bindfix</i> und <i>Bindrest</i> behandelt worden sind. Die Befehle <i>Bindfix</i> und <i>Bindrest</i> gibt es nicht mehr, da es auch keine Bindery mehr gibt. Sie wurden durch den Befehl <i>Dsrepair</i> ersetzt (nur an der Server-Console möglich).

19.23 Workstation-Befehle

Netadmin	Die bislang benutzten Befehle und Menüsysteme <i>Dspace</i> , <i>Security</i> , <i>Syscon</i> und <i>Userdef</i> wurden in das Menüsystem <i>Netadmin</i> aufgenommen.
Login	In den <i>Login</i> -Befehl wurden die beiden Befehle <i>Login</i> und <i>Attach</i> vereint. Als Neuerung von NetWare 4 ist es jetzt möglich, nicht nur an acht Servern, sondern an bis zu 50 Servern im Netzwerk zu arbeiten.
Logout	Dient zum Abmelden von allen File-Servern oder einem speziellen File-Server.
Ncopy	Kopieren von Dateien im Netzwerk. Die Leistungsfähigkeit dieses Befehls ist wesentlich größer als die von DOS bekannten COPY- und XCOPY-Befehle. Beim Kopieren von Dateien innerhalb des gleichen Servers wird zudem an Performance gewonnen, da die Daten innerhalb des Servers transportiert werden.
Uimport	Das <i>Makeuser</i> -Menüsystem ist ersetzt worden, aber <i>Uimport</i> bietet ähnliche Funktionen. Für diesen Befehl kann eine eigene Datendatei und Steuerdatei erzeugt werden, um die NDS einrichten zu können.
Monitor	Das Konsolen-Menüsystem <i>Monitor</i> ersetzt jetzt das <i>Fconsole</i> -Menüsystem auf der Workstation vollständig.
Netuser	Das bisherige <i>Session</i> -Menüsystem wurde durch <i>Netuser</i> ersetzt. Die Funktionalitäten sind ähnlich geblieben.
Rconsole	Die Programme <i>Aconsole</i> und <i>Rconsole</i> , die die Remote-Administration des Servers von einem beliebigen Arbeitsplatz ermöglichen (im Netzwerk oder remote), wurden in das <i>Rconsole</i> -Programm integriert.
Nprinter	Zum Aktivieren eines Remote-Netzwerkdruckers an der Workstation hat man bislang den Befehl <i>Rprinter</i> ausgeführt. Dieser wurde geändert in den Befehl <i>Nprinter</i> und muß an der entsprechenden Station ausgeführt werden, deren Drucker als Netzwerkdrucker installiert werden soll.
Nver	Dient wie bisher der Abfrage der wichtigsten NetWare-Versionsinformationen und der Server, an denen Sie derzeit arbeiten.
Psc	Dient wie bisher der Abfrage und Steuerung der Netzwerkdrucker im LAN.
Rendir	Man hätte vielleicht auch diesen Befehl konsolidieren können, aber er ist als einzelner Befehl beibehalten worden. Er bietet die Möglichkeit, Directories am Server umzubenennen.
Setpass	Zum Ändern des Paßworts wird nach wie vor dieser Befehl verwendet.

19 Novell NetWare 4.2

Settts	Zum Setzen der Parameter für die TTS-Funktion kann dieser Befehl verwendet werden (hat sich auch nicht geändert).
Systime	Um die Workstation-Uhrzeit mit der Server-Uhrzeit zu synchronisieren, wird dieser Befehl eingesetzt.
Whoami	Damit Sie Informationen darüber erhalten, an welchen Servern Sie derzeit arbeiten und wie Ihre Netzwerkumgebung aussieht, verwenden Sie diesen Befehl.
Wsupdate	Um aktuelle Dateien von der Server-Platte auf die lokale Platte der Workstation zu übertragen, wird dieser Befehl verwendet. Führt man diesen Befehl im Login Script aus, wird gewährleistet, daß beim Login-Vorgang neue aktuelle Dateien von der Server-Platte abgeholt werden. Die Steuerung der notwendigen Schritte erfolgt über Parameter.

19.24 Neue und geänderte Menüsystem-Befehle

Colorpal	Zur Festlegung, wie die Farben der NetWare-Menüsysteme aussehen sollen (Vorder-, Hintergrundfarbe und die Farbe der einzelnen Optionstexte), verwenden Sie dieses Menüsystem.
Filer	Zur Verwaltung der gesamten Dateisysteme auf dem NetWare 4 Server steht Ihnen dieses Menüsystem zur Verfügung.
Netadmin	Zum Einrichten der NDS-Objekte und Informationen (Benutzer, Gruppen, Rechte etc.) steht dieses Menüsystem zur Verfügung. Vergleichbar mit <i>Syscon</i> , jedoch mit wesentlich mehr Möglichkeiten.
Netuser	Diese Möglichkeiten, vergleichbar mit <i>Session</i> , sind erweitert worden. Zum Beispiel kann jetzt auch mit diesem Menü die Umleitung der lokalen Druckerschnittstellen durchgeführt werden.
Nwadmin	Das Windows-basierende Administrations-Tool, um die NDS und alle darin enthaltenen Objekte verwalten zu können. Unter Windows lassen sich damit alle Aufgaben durchführen, ohne Nwadmin verlassen zu müssen, wofür unter DOS eine Vielzahl von Menüsystemen benötigt wird (z.B. Pconsole, Printdef, Printcon, Filer etc.). Darin enthalten sind auch Mechanismen wie die Abfrage nach dem Yellow-Page-Prinzip, Partition-Manager, Rconsole und mehr. Wer viel unter Windows arbeitet, wird für die Verwaltung von NetWare 4 selten auf DOS-Ebene wechseln müssen.
Wsupgrd	Mit diesem Befehl kann eine Shell-basierende Workstation-Umgebung auf DOS-ODI-Umgebung umgestellt werden.
Partmgr	Dieses Menüsystem ist notwendig, um die NDS-Partitions und -Replicas im Netzwerk zu verwalten und zu steuern.

19.25 Workstation-Unterstützung

Pconsole	Zum Einrichten und Verwalten der Netzwerkdrucker dient dieses Menü. Es ist zwar vergleichbar mit den Optionen, die unter NetWare 3.x zur Verfügung stehen, es ist jedoch um sämtliche Funktionen und Möglichkeiten der NDS-Dienste erweitert worden.
Printcon	An der Definition von Druck-Job-Konfigurationen hat sich unter NetWare 4 nichts geändert. Nähere Informationen sind in der Beschreibung für NetWare 3.x zu finden.
Printdef	Auch hier hat sich nichts geändert, es sei also auf die Beschreibung unter NetWare 3.x verwiesen.

19.25 Workstation-Unterstützung

Neben der standardmäßigen Unterstützung von DOS-Workstations ist unter NetWare 4 auch die notwendige Software enthalten, um OS/2-Workstations im Netzwerk zu betreiben.

Die GUI-Programme für Windows sind der NetWare Administrator und der Partition Manager. Für den OS/2 Presentation Manager stehen keine eigenen GUI-Systeme mehr zur Verfügung. Für OS/2 müssen die Windows-Anwendungen eingesetzt werden, um NetWare 4 unter OS/2 zu administrieren. Für Windows und OS/2 steht zudem ein neues NetWare-User-Tool zur Verfügung, das sich über Hot Key an beliebiger Stelle aktivieren lässt und dazu dient, zusätzliche Netzwerkverbindungen zu anderen Servern aufzubauen, Laufwerke zu definieren oder auch Druckerumleitungen festzulegen. Auch das Versenden von Nachrichten lässt sich mit diesem Tool problemlos ausführen.

Die Anzahl der OS/2-Command-Line-Utilities ist etwas geringer, deren Bedeutung und Handhabung aber vergleichbar mit den bereits beschriebenen Befehlen.

Folgende OS/2-Befehle werden unterstützt:

- Capture, Cx, Flag, Login, Logout, Map, Ncopy, Ndir, Nlist, Nprint, Nver, Psc, Rights, Send, Setpass, Settts, Systime, Whoami.

Eine 32-Bit Version des NWAdmin für Windows 95 und Windows NT ist inzwischen eine Selbstverständlichkeit. Der Einsatz von OS/2 hingegen nimmt immer mehr ab und ist auch der Grund für die immer geringer werdende Unterstützung – und dies nicht nur bei Novell.

19.26 Neue Konsolen-Befehle

Für den Netzwerkadministrator bietet NetWare 4 auch neue Konsolen-Befehle. Die für NetWare 3.x beschriebenen Befehle stehen nach wie vor zur Verfügung. Einige wurden jedoch ergänzt und erweitert. Es sollen an dieser Stelle nur die neuen Befehle besprochen werden.

Help	Auflistung aller zur Verfügung stehenden Befehle am Bildschirm. Sie müssen deshalb nicht unbedingt mehr in der Dokumentation nachsehen, welche Befehle zur Verfügung stehen, da sie direkt am Bildschirm angezeigt werden können.
Abort Remirror	Ein Abgleich gespiegelter oder geduplexer Platten kann mit diesem Befehl abgebrochen werden. Das sollte nur im äußersten Notfall erfolgen, da der Datenbestand beider Platten so lange inkonsistent bleibt, wie ein Remirroring nicht komplett und erfolgreich durchgeführt werden konnte.
Keyb Ländercode	Dieser Befehl ist vergleichbar mit dem DOS-KEYB-Befehl und dient dazu, die gewünschte nationale Tastatur auszuwählen, mit der am NetWare Server gearbeitet werden soll. Durch den NLS (National Language Support) kann jetzt mit der gewohnten Tastatur am Server gearbeitet werden.
Language	Hiermit wird festgelegt, in welcher Sprache NLM-Meldungen ausgegeben werden sollen. Es ist jedoch notwendig, daß die entsprechende Sprache am Server installiert und eingerichtet worden ist.
List Devices	Auflistung aller am Server bekannten Devices (Platten, CD-ROMs, WORMs etc.).
Magazine	Mit diesem Befehl wird dem Server mitgeteilt, ob eine Konsolen-Meldung zum Einlegen oder Entfernen eines Magazins durchgeführt worden ist oder nicht.
Media	Hiermit wird eine Aufforderung des Servers, das Medium zu wechseln, beantwortet.
Mirror Status	Hiermit erhalten Sie Angaben darüber, wie der Status der gespiegelten bzw. geduplexten Platten aussieht. Insgesamt gibt es fünf Zustände, die auftreten können (Not Mirrored, Orphaned State, Fully Synchronized, Out of Synchronization, Being Remirrored).
Remirror Partition	Hiermit wird das Remirroring von NetWare Partitions angestoßen. Normalerweise wird ein Remirroring von NetWare automatisch durchgeführt, sofern notwendig. Wenn ein Remirroring jedoch aus irgendwelchen Gründen abgebrochen wurde, kann der Prozeß mit diesem Befehl erneut durchgeführt werden.

19.27 Neue NLMs

Scan For New Devices

Der Server überprüft alle Devices, wenn er gestartet wird. Mit diesem Befehl sucht der Server nach Devices, die nach dem Starten neu hinzugefügt wurden.

19.27 Neue NLMs

Neben neuen Befehlen, die an der Server-Console ausgeführt werden können, sind auch neue NLMs entwickelt worden, die jedoch zusätzlich für die Neuerungen von NetWare 4 benötigt werden. Es wurden jedoch auch neue NLM-Menüsysteme entwickelt, durch die eine Administration des Servers wesentlich verbessert wird, da zusätzlich nützliche und wichtige Informationen abgefragt werden können.

Das bereits bekannte Monitor-NLM wurde um eine zusätzliche Funktion erweitert, um weitere Informationen über die Server-Konfigurationen und deren Status zu erhalten.

Ebenfalls überarbeitet und verbessert wurden das Install-NLM, um neue Systemkomponenten am Server zu konfigurieren. Vor allem die Bedienung ist übersichtlicher und einfacher geworden.

Ein ganz neues Menüsystem am Server bildet das NLM SERVMAN. Mit diesem Menüprogramm lassen sich

- System-Parameter anzeigen und ändern,
- die STARTUP.NCF und AUTOEXEC.NCF anzeigen und ändern,
- IPX/SPX-Konfigurationseinstellungen anzeigen und ändern,
- Adapter-, Device- und Disk-Partition-Informationen anzeigen,
- Volume-Informationen und
- Netzwerkinformationen anzeigen.

Am Bildschirm selbst werden generelle Informationen über die Prozessorauslastung, Server Up Time, Prozessorgeschwindigkeit, Anzahl der Server-Prozesse, Anzahl geladener NLMs, gemountete Volumes, aktive Print-Queues, Anzahl angemeldeter Benutzer und Anzahl gemeldeter Name Spaces angezeigt.

Somit erhält man auf Anhieb einen umfangreichen Überblick über alle notwendigen Einstellungen und Konfigurationen am Server.

19.28 Änderungen im Rechtesystem

In den bisherigen Ausführungen wurde bereits darauf hingewiesen, daß NetWare 4 keine Modifikationen aufweist, um Benutzern Trustee-Rechte auf Datei- und Directory-Ebene zu vergeben. Das heißt, alle Ausführungen in der entsprechenden Beschreibung von NetWare 3.x bleiben gültig. Änderungen ergeben sich jedoch bezüglich

19 Novell NetWare 4.2

der Dateiattribute, da NetWare 4 neue Mechanismen besitzt, die mit Hilfe der Attribute gesteuert werden können. Die nachfolgende Aufstellung soll einen Überblick darüber geben. Die in Klammern gesetzten Ausdrücke verwendet NetWare bei der Anzeige der gesetzten Attribute am Bildschirm.

Directory-Attribute

- *Normal (N)*
Das Directory besitzt anschließend keine Attribute mehr.
- *Delete Inhibit (DI)*
Verhindert, daß irgendein Benutzer das Directory löscht.
- *Hidden (H)*
Das Directory bleibt beim DIR-Befehl unsichtbar.
- *Purge (P)*
Weist NetWare an, das Directory und die Dateien in diesen Directories unwiederbringlich zu entfernen, wenn Löschungen durchgeführt werden. Ein Zurückholen gelöschter Dateien kann mit dem *Salvage*-Befehl nicht durchgeführt werden.
- *Rename Inhibit (Ri)*
Das Directory kann nicht umbenannt werden.
- *Immediate Compress (Ic)*
Alle Dateien im Directory werden von NetWare komprimiert gespeichert.
- *Don't Compress (Dc)*
Dateien im Directory werden nie komprimiert abgespeichert.
- *Don't Migrate (Dm)*
Die Dateien im Directory werden nie auf ein anderes Medium (Tape, Optical Disk) ausgelagert.
- *System (Sy)*
Kennzeichnet, daß dieses Directory nur vom Betriebssystem verwendet wird. Der DOS-DIR-Befehl zeigt solche Verzeichnisse nicht an.

Dateiattribute

- *Archive Needed (A)*
Die Datei wurde seit der letzten Datensicherung geändert. Dieses Attribut ist notwendig, um einen Incremental Backup durchführen zu können.
- *Can't Compress (Cc)*
Ein Statusattribut von NetWare. Hiermit zeigt NetWare an, daß eine Datei nicht komprimiert werden kann. Dieses Attribut kann nicht von Benutzern gesetzt werden, sondern nur von NetWare.

19.28 Änderungen im Rechesystem

- *Compressed (Co)*
Ein Statusattribut von NetWare. Hiermit wird angezeigt, daß die Datei komprimiert abgespeichert ist. Das Attribut wird in der Attributliste angezeigt, kann aber von Benutzern nicht geändert werden.
- *Copy Inhibit (Ci)*
Dieses Attribut hat nur für Macintosh-Rechner Gültigkeit. Eine Datei mit diesem Attribut kann nicht mehr kopiert werden.
- *Delete Inhibit (Di)*
Die Datei kann nicht gelöscht werden, auch wenn das Erase-Recht vorhanden ist.
- *Don't Migrate (Dm)*
Die Datei wird auf kein anderes Medium ausgelagert (Tape oder Optical Disk).
- *Execute Only (X)*
Das Attribut kann nicht mehr rückgängig gemacht werden. Die Datei kann nicht mehr kopiert oder umbenannt werden. Backup-Programme sichern Dateien mit gesetztem Execute-Only-Attribut nicht mehr.
- *Hidden (H)*
Die Datei ist beim DOS-DIR-Befehl nicht aufgeführt. Die Dateien können nicht gelöscht oder kopiert werden.
- *Immediate Compress (Ic)*
Sobald das Netzwerkbetriebssystem in der Lage ist, wird die Datei komprimiert auf der Platte abgespeichert.
- *Indexed (I)*
Hiermit wird angezeigt, daß die Datei mehr als 63 FAT-Blocks à 4 Kbyte belegt, so daß NetWare für diese Datei eine Turbo FAT einrichtet, sobald auf die Datei zugegriffen wird. Statusanzeige von NetWare, da dieses Attribut vom Anwender nicht gesetzt werden kann.
- *Migrate (M)*
Ein Statusattribut von NetWare, mit dem angezeigt wird, daß die Datei ausgelagert wurde. Das heißt, der Directory-Eintrag existiert noch, aber der Inhalt der Datei wurde auf Tape oder Optical Disk ausgelagert. Das Attribut kann nicht durch den Anwender gesetzt werden.
- *Purge (P)*
Eine Datei mit diesem gesetzten Attribut wird beim Löschen unwiederbringlich von der Platte entfernt. Ein Restaurieren der Datei mit der *Salvage*-Option im *Filer*-Menü ist nicht mehr möglich.

19 Novell NetWare 4.2

- *Read Only (Ro)*
Dieses Attribut legt fest, daß die Datei nicht mehr geändert werden kann. Gleichzeitig werden die Attribute Rename Inhibit und Delete Inhibit vergeben, so daß der Name der Datei nicht mehr geändert werden kann und ein Löschen der Datei untersagt wird.
- *Rename Inhibit (Ri)*
Eine Datei mit diesem Attribut kann nicht mehr umbenannt werden.
- *Shareable (S)*
Die Datei kann von mehr als einem Anwender gleichzeitig geöffnet werden. Dieses Attribut ist vor allem für netzwerkfähige Programme wichtig oder für solche, auf die von mehreren Anwendern gleichzeitig zugegriffen wird.
- *System (Sy)*
Diese Datei wird vom Betriebssystem genutzt. Mit dem DIR-Befehl unter DOS bleibt diese Datei unsichtbar.
- *Transactional (T)*
Die Datei wird vom TTS abgesichert. Die Aufgabe des TTS-Systems wurde an anderer Stelle bereits ausführlich erläutert.

Wenn man sich die gesamten Funktionalitäten von NetWare 4 betrachtet, könnte der Eindruck entstehen, daß das Einrichten und Verwalten, speziell in Hinblick auf die NDS, nicht ganz unproblematisch ist. Dieser Eindruck täuscht, sofern es sich nicht um große Netze, mit einer großen NDS und vielen Servern, verteilt über mehrer Standorte handelt. Dennoch ist der Eindruck, vor allem bei kleineren Kunden, geblieben, daß NetWare 4 aufgrund der NDS-Implementierung eine Nummer zu groß sein könnte. Um diesen Eindruck zu entkräften, hat Novell einen »kleinen Bruder« von NetWare 4 auf den Markt gebracht, intraNetWare for Small Business, d.h. eine NetWare 4 Version für kleinere Unternehmen. Funktionell und technisch ist es im Prinzip nichts anderes als eine NetWare 4.11, nur mit dem Unterschied, daß die Installation, die Administration und der Produktumfang geändert wurden. Die wesentlichen Details sollen deshalb anschließend kurz näher besprochen werden.

19.29 intraNetWare for Small Business 4.11

Diese Version ist wie bereits erwähnt aufgrund der Einfachheit in der Administration und Installation für kleinere Unternehmen mit nicht mehr als 25 Benutzer gedacht und konzipiert. Dieses System eignet sich deshalb besonders gut, wenn folgende Bedingungen erfüllt sind:

19.29 intraNetWare for Small Business 4.11

- Ein Unternehmen an einem Standort mit nicht mehr als 25 Benutzer.
- Es wird ein System benötigt, das sich sehr einfach installieren und verwalten läßt, aber dennoch die Möglichkeit besteht, auf die NetWare 4.11 umzustellen, wenn der Betrieb wächst und mehr als 25 Benutzer am System arbeiten oder das Unternehmen plötzlich auf mehrere Standorte verteilt werden muß.
- Sie benötigen ein System, dessen Verwaltung leicht erlernt werden kann, ohne daß man hierfür zu große Anforderungen an den Netzwerkverwalter stellen muß.
- Es wird ein System benötigt, das gleichzeitig auch die Möglichkeit integriert hat, über remote Access-Mechanismen darauf zuzugreifen.
- Es wird ein System benötigt, das auch gleichzeitig ein leistungsfähiges Electronic Mail System besitzt.

Die intranetWare for Small Business arbeitet wie NetWare 4.11 ebenfalls mit der NDS, nur werden die Möglichkeiten durch die vereinfachte Installation und das spezielle Administrations-Tool NEAT (NetWare Easy Administration Tool) so stark vom Netzwerkverwalter abgeschottet, daß dieser bei der Installation und beim Verwalten der Benutzer, Gruppen, Drucker etc. nur ganz wenige Informationen benötigt, um damit zurechtzukommen. Diese Einfachheit wird somit durch zwei wesentliche Faktoren erreicht:

- Simple Installation mit wenigen Benutzereingaben
- Simple Administration durch NEAT

Standardmäßig wird intraNetWare for Small Business mit GroupWise 5.x ausgeliefert, einem sehr leistungsfähigen Electronic Mail System, das alle nur erdenklichen Möglichkeiten bietet, internen und externen Mailverkehr damit abzudecken. Für den eventuell benötigten Internet-Zugang beinhaltet intraNetWare for Small Business den MPR, um damit Dial-up-Verbindungen zum Internet aufbauen zu können. Ebenso sind enthalten der Netscape Web Browser und der FastTrack Web Server, um damit auch alle weiteren Internet-Aktivitäten realisieren zu können.

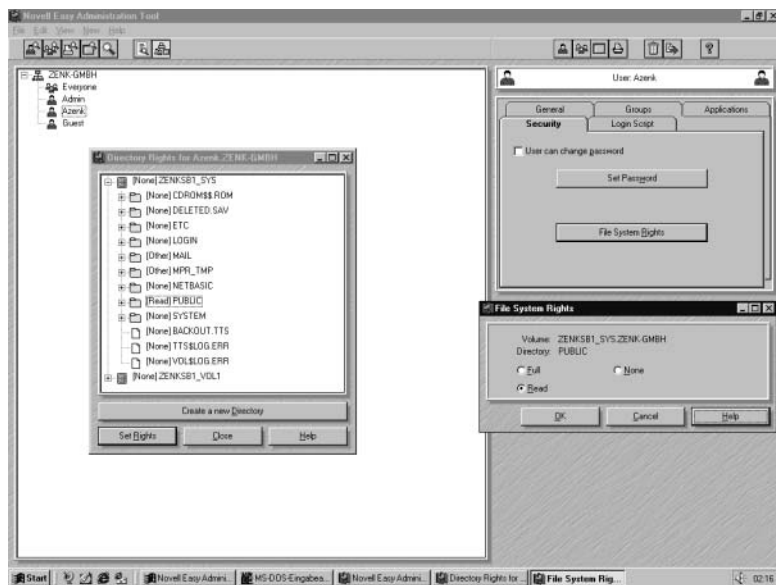
Gerade bei kleinen Betrieben wird nicht selten die Forderung gestellt, von zu Hause auf das System zugreifen zu können. Um dies durchführen zu können, bietet intraNetWare for Small Business standardmäßig einen NetWare Connect Server (8 Port), der Dial-in-Funktionen zur Verfügung stellen kann. Ebenso können darüber Dial-out-Mechanismen realisiert werden. Nicht vergessen werden darf, daß in der intraNetWare for Small Business auch die Funktionen des NetWare Application Launcher verankert sind, um damit eine zentrale Verwaltung und Bereitstellung der Netzwerkanwendungen durchführen zu können. Daß von intraNetWare for Small Business auch

19 Novell NetWare 4.2

alle sonstigen Funktionen wie Unterstützung der unterschiedlichsten Hard- und Software-Umgebungen, Unterstützung der unterschiedlichsten Clients etc. zur Verfügung gestellt werden, so wie man das auch von NetWare 4 gewohnt ist, sei nur am Rande erwähnt.

Die Bedienung am Server oder auch die zur Verfügung gestellten Command Line Utilities unterscheiden sich nicht von einer NetWare 4.11, so daß auf weitere Ausführungen diesbezüglich verzichtet werden kann. Damit Sie einen Eindruck bekommen, wie sich die Administration von intraNetWare for Small Business darstellt, sind in den Abbildungen 19.8 und 19.9 einige Administrationsfenster dargestellt.

Abbildung 19.8
Die Vergabe von
Trustee-Rechten
auf das Datei-
system

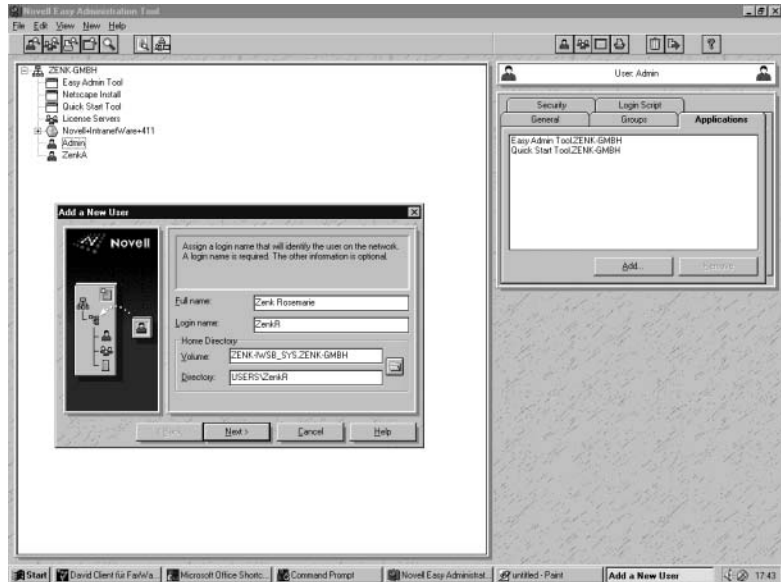


Wer es gerne möchte, kann jedoch auch mit dem »großen« NWAdmin die Verwaltung durchführen; auch dieser steht nach der Installation zur Verfügung.

Hervorzuheben ist zum Beispiel noch, daß intraNetWare for Small Business auch SMP-fähig ist und zum Beispiel beim Einrichten der Druckmechanismen nach dem Hinzufügen von neuen Druckern an den Print-Server dieser von intraNetWare for Small Business automatisch am Server entladen und neu geladen wird, sobald die Änderungen über das NEAT Tool aktiviert werden. Man hat somit alles versucht, um das Arbeiten und das Administrieren so einfach wie möglich zu gestalten.

19.29 intraNetWare for Small Business 4.11

Abbildung 19.9
Das Einrichten
eines neuen
Benutzers



Zusammengefaßt kann gesagt werden, daß mit der gesamten NetWare-4-Produktfamilie ein starkes und leistungsfähiges Netzwerkbetriebssystem zur Verfügung steht, das sich durch die flexible Gestaltung der logischen Netzwerkebene auszeichnet.

Dem Anwender bleibt dabei verborgen, wo die Ressourcen im einzelnen eingerichtet und vorhanden sind. Die Verwaltung auch großer Netzwerke ist dadurch, im Vergleich zu NetWare 3.x, wesentlich einfacher durchzuführen. Auch Microsoft arbeitet im Zuge der Windows-NT-5.0-Entwicklung an einer Directory-Services-Implementierung. Hierzu nähere Informationen bei der Behandlung von Windows 2000 und aller weiteren dazu gehörenden Mechanismen.

Die technologische Weiterentwicklung von Novell ist NetWare 5. Ich will Ihnen deshalb im nächsten Kapitel aufzeigen, was sich ändert und vor allem, mit welchen neuen Mechanismen NetWare 5 aufwarten kann und welche Vorteile damit verbunden sind.

20

NetWare 5

NetWare 5 ist seit geraumer Zeit verfügbar, so daß man genau weiß, mit welchen neuen Mechanismen Novell sein Betriebssystem NetWare 5 ausgestattet hat. NetWare 5 ist das neue Flaggschiff der Netzwerkbetriebssysteme von Novell und weist Komponenten und Mechanismen auf, die sich zum Teil gravierend von den Vorgängerversionen, vor allem NetWare 4.x, unterscheiden. Eine der gravierenden Änderungen ist, daß NetWare 5 vollständig auf Native IP setzt, d.h., die bisherige Protokollstruktur IPX/SPX wird zukünftig nicht mehr das Kommunikationsprotokoll zwischen Client und Server sein. Man kann jedoch, wie später noch zu sehen sein wird, IPX/SPX als Protokoll auswählen bzw. einen Kompatibilitätsmechanismus installieren, wenn man NetWare 5 vollständig auf IP-Basis installiert hat. Ebenso ist auffallend, daß Novell wieder zur alten Namensgebung übergegangen ist, d.h., NetWare ist wieder NetWare, so wie man dies gewohnt ist.

Die nächsten Ausführungen sollen zeigen, mit welchen neuen Funktionen Sie bei NetWare 5 rechnen können und welche Vorteile für Sie dadurch entstehen. Ich will Ihnen dabei in der folgenden Reihenfolge die Neuerungen aufzeigen und näher beschreiben:

- Betriebssystem
- Novell Directory Services (NDS)
- Network Services
- Installation und Upgrade
- Erweiterungen für Entwickler
- Third-Party Add-Ons.

Sofern nicht explizit erwähnt, gelten für NetWare 5 immer noch die grundsätzlichen Mechanismen, die Performance und Sicherheit bieten. Dies gilt unter anderem für den Caching-Mechanismus, die Zugriffsberechtigungen, Disk Mirroring bzw. Disk Duplexing und eine Vielzahl bereits näher beschriebener Funktionen.

20.1 Betriebssystem

NetWare 5 weist eine Vielzahl von Änderungen im Betriebssystem-Kernel auf, die das System nicht nur sicherer machen, sondern auch die Performance enorm steigern werden. Diese gesamten Änderungen weisen auch darauf hin, daß NetWare 5 immer mehr in Richtung Applikations-Server forciert wird, damit es nicht nur als reiner File-

und Print-Server eingesetzt werden kann. Dies spiegelt sich vor allem auch darin wider, daß NetWare 5 eine vollständige Java-Plattform bietet, um auf diesen neuen Mechanismen Anwendungen entwickeln und einsetzen zu können. Die ersten Tests mit NetWare 5 haben auch gezeigt, daß man sich eine beliebige Java-Anwendung aus dem Internet holen, und diese dann ohne jegliche Modifikation auf einem NetWare 5 Server laufen lassen kann.

20.1.1 NetWare 5 Kernel

Der Kernel eines Betriebssystems bildet die Basis für alle Aufgaben, die von einem Betriebssystem erfüllt werden können, und legt auch fest, in welcher Art und Weise die Aufgaben erledigt werden können. Der Kernel von NetWare 5 bietet nicht nur neue Funktionen, sondern auch noch eine Vielzahl neuer Dienste, und, was ganz wichtig ist, er bietet die Unterstützung für Java-Anwendungen. Eine der wesentlichen Änderungen, die der NetWare 5 Kernel erfahren hat, ist die MPK-Fähigkeit, d.h., NetWare 5 weist (im Gegensatz zu NetWare 4) einen Multiprocessing-Kernel (MPK) auf. Das heißt, neben der allgemeinen Multiprocessing-Fähigkeit ist der NetWare-Kernel auch in der Lage, die Verfügbarkeit von mehr als einem Prozessor voll zu nutzen. Ohne zusätzliche Modifikation ist es möglich, den Kernel sowohl auf Monoprozessor- als auch auf Multiprozessor-Systemen einzusetzen. Hat man NetWare 5 bei der ersten Installation auf einer Monoprozessor-Maschine installiert und baut im nachhinein einen weiteren Prozessor ein, dann erkennt NetWare beim Starten dies von selbst und lädt die entsprechenden MPK-Module selbstständig nach, ohne daß der Netzwerkverwalter hierzu zusätzlich etwas tun müßte. Der NetWare-MPK ist in der Lage, bis zu 32 Prozessoren zu unterstützen. Zusätzlich unterstützt der MPK das sogenannte Load Balancing, wodurch gewährleistet ist, daß die Abarbeitung von Anwendungen optimal auf die vorhandenen und verfügbaren Prozessoren verteilt wird.

Bei der Entwicklung von Anwendungen spricht man auch immer wieder von Threads. Ohne weitere Erläuterung kann man einen Thread einfach als eine ausführbare Einheit bezeichnen, wobei eine Anwendung aus mehreren Threads bestehen kann, die unabhängig voneinander ausgeführt werden können. Der MPK hat deshalb die Aufgabe, Threads und Prozessor-Ressourcen zu verwalten, Interrupts und Ausnahmefälle zu handhaben und den Zugriff auf den Hauptspeicher und die I/O-Systeme zu steuern.

Zur Abarbeitung von Threads pflegt der Kernel Datenstrukturen zu gebrauchen, die man als Run Queue bezeichnet. In dieser Run Queue befinden sich Threads, die zur Abarbeitung im sogenannten Ready-

20.1 Betriebssystem

Status bereitstehen. In einem Monoprozessor-System gibt es nur eine Run Queue, aus der dem Prozessor die ausführbaren Threads zugewiesen werden bzw. aus der sich der Prozessor die ausführbaren Threads zur Abarbeitung holt. Für die Multiprozessor-Umgebung gibt es mehrere Ansätze, um die Aufteilung der Threads auf die jeweiligen Prozessoren zu realisieren. Die Verteilung der Threads auf mehrere Prozessoren kann mit Hilfe einer Global Queue (alle Prozessoren bedienen eine Run Queue) oder mit Hilfe einer Per-Prozessor Run Queue (auch als lokale Run Queue oder Distributed Run Queue bezeichnet) oder einer Kombination davon erfolgen. Die Vor- und Nachteile dieser beiden Ansätze sollen kurz erläutert werden:

■ *Global Run Queue*

Greifen alle Prozessoren auf eine einzige Run Queue zu, dann hat dies den Vorteil, daß ein automatisches Load Balancing erfolgt, da kein Prozessor im Idle-Zustand verweilt, solange sich noch Threads in der Run Queue befinden. Dies kann jedoch dazu führen, daß mit zunehmender Prozessoranzahl ein Engpaß entsteht, obwohl für bestimmte Scheduling-Mechanismen (z.B. Real-Time-Anwendungen) der Einsatz von Global Run Queues notwendig ist.

■ *Per-Processor Run Queue*

Dieser Ansatz hat den Vorteil, daß die Verteilung der Threads dergestalt erfolgt, daß Threads den Prozessor nutzen, auf dem sie auch zuvor bereits gelaufen sind. Zudem kann der Nachteil, wie er bei einer Global Run Queue entstehen kann, nicht auftreten. Man muß jedoch bei diesem Verfahren darauf achten, daß die Anzahl der Threads in einer Queue nicht zu einem Ungleichgewicht führt. Deshalb ist ein Load-Balancing-Mechanismus notwendig, der dafür sorgt, daß nicht die ganze Last von einem Prozessor getragen werden muß und die anderen Prozessoren im Idle-Zustand verweilen.

Der Kernel von NetWare 5 nutzt den Mechanismus der Per-Processor Run Queue, so daß ein Prozessor nur Threads seiner eigenen Run Queue abarbeiten kann. Dadurch wird der Scheduler von NetWare 5 im Vergleich zu anderen Verfahren skalierbarer und einfacher. Um jedoch das Problem der Load-Balancing-Mechanismen lösen zu können, nutzt NetWare 5 einen sehr ausgefeilten Load-Balancing-Algorithmus.

Der NetWare 5 Scheduler errechnet periodisch die systemweite Last und dann die durchschnittliche Last. Die berechnete durchschnittliche Last wird verwendet, um einen Vergleich durchführen zu können. Das heißt, es wird dadurch bestimmt, ob ein Prozessor überlastet oder nicht ausgelastet ist. Der Threshold für Load Balancing und

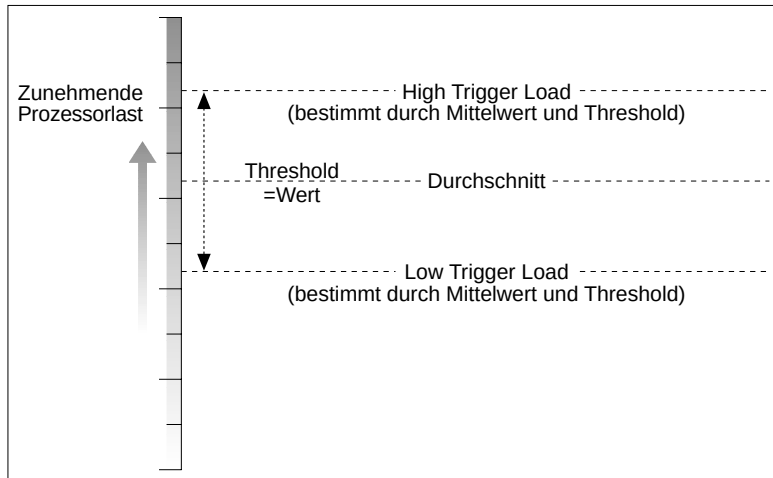
20 NetWare 5

der berechnete Durchschnittswert werden verwendet, um damit die High- und Low-Trigger-Last bestimmen zu können. Dabei wird folgendes festgelegt:

- Ein Prozessor ist überlastet, wenn die Last über der High-Trigger-Last liegt.
- Ein Prozessor ist nicht ausgelastet, wenn die Last unter der Low-Trigger-Last liegt.

In diesem Falle verlagert der Scheduler Threads vom überlasteten Prozessor zum unterlasteten Prozessor, um eine »ausgeglichene« Verteilung der Thread-Bearbeitung zu erzielen. In Abbildung 20.1 ist die Beziehung zwischen durchschnittlicher Last, Load Balancing Threshold und der High- bzw. Low-Trigger-Last aufgezeigt.

Abbildung 20.1
Berechnung der
Lastverteilung



Der Threshold kann bei Bedarf über einen Server-Parameter modifiziert werden.

Bislang arbeitete NetWare nur nach dem »nonpreemptive« Mechanismus, d. h. nach dem sogenannten Round-Robin Verfahren – First in First out (FIFO). Die Threads wurden in der Reihenfolge des Eintreffens in der Run Queue abgearbeitet. Dieses Verfahren gilt auch weiterhin für ältere Module, die unter NetWare 5 betrieben werden. Neue Module für NetWare 5 können für den preemptive Mechanismus geschrieben werden. Hierzu müssen im »Programmcode« Kennzeichen gesetzt sein, damit dieser im preemptive Modus ausgeführt wird. Im Laufe der Zeit werden dann auch Module auf dem Markt zur Verfügung stehen, die im preemptive Modus laufen können.

20.1 Betriebssystem

Die Multiprozessor-Unterstützung für NetWare 5 wird durch ein Plattform Support Module (PSM) erreicht, indem man dieses Modul zusätzlich lädt bzw. es beim Starten automatisch geladen wird. Während der Installation von NetWare 5 wird die Multiprozessor-Fähigkeit des Systems automatisch erkannt, indem die MP-Konfiguration im BIOS ausgelesen und daraufhin bestimmt wird, welches PSM für die entsprechende Plattform geladen werden muß. Neben der Skalierbarkeit bietet die Multiprozessor-Unterstützung von NetWare 5 die folgenden Vorteile:

- Abwärts-Kompatibilität für Anwendungen, die für NetWare 4.11 SMP geschrieben worden sind.
- Integrierter MPK, der auch Monoprozessor-Unterstützung bietet, wodurch man nur einen Binärcode benötigt, der sowohl auf Mono- als auch auf Multiprozessor-Plattformen läuft.
- Kernel-Unterstützung für preemptives Scheduling, sobald die entsprechenden Module entwickelt sind.
- Plattform-Unterstützung für MPK in einem einzigen Plattform Support Module.

20.1.2 Speicherschutz

NetWare 5 benötigt mindestens 64 Mbyte Hauptspeicher und kann bis zu 4 Gbyte Hauptspeicher adressieren. Nachdem der Kernel (SERVER.EXE) und alle dazugehörigen Module geladen sind, wird der gesamte verfügbare Rest des Hauptspeichers für das Caching verwendet. Dieser Cache-Bereich wird für weitere NLMs verwendet und für Daten, die von der Platte des Server gelesen bzw. auf die Platte des Servers geschrieben werden müssen. Die Vorteile in Verbindung mit Caching wurden bereits ausführlich erläutert. Der Cache-Speicher wird kleiner, wenn am Server die folgenden Aktionen durchgeführt werden:

- Speichern von FAT-Tabellen und Suballocation-Tabellen beim Mounten von Volumes
- Speichern der Directory Entry Tabellen (DET)
- Speichern von Daten (zum Schreiben, zum Lesen)
- Laden von zusätzlichen NLMs
- Aufbau von Hash-Tabellen für den Zugriff auf DETs
- Einrichten von geschützten Speicherbereichen

Speicher, der nicht mehr benötigt wird, geht zurück an den Cache und steht somit wieder zur Verfügung. Bei NetWare 5 sind die sogenannten Directory Cache Buffer und File Cache Buffer zu unterscheiden. Directory Cache Buffer werden nur noch benötigt, wenn mit dem traditionellen Dateisystem von NetWare gearbeitet wird, um darin die DET speichern zu können. Sobald mit dem neuen NSS (No-

vell Storage Services) System gearbeitet wird, benötigt NetWare für Volumes auf Basis von NSS keine Directory Cache Buffer mehr. File Cache Buffers werden sowohl für das alte als auch für das neue Dateisystem benötigt. Der File Cache wird in Blöcken von 4 Kbyte verwaltet und dient zum Speichern von Daten, die von einem Volume gelesen worden sind oder auf das Volume zurückgeschrieben werden müssen. Ebenso werden im File-Cache-Bereich Informationen der NDS gespeichert, um den Zugriff zu beschleunigen. Der File Cache wird somit dynamisch verwaltet, und die Performance des File Server hängt unter anderem auch davon ab, wieviel File Cache insgesamt zur Verfügung steht. In einem gut konzipierten Server ist so viel Hauptspeicher eingebaut, daß der größte Teil der Zugriffe auf Daten aus dem Cache bedient werden kann. Um jedoch nicht unnötig viel Speicher einzubauen, bietet NetWare einen überwachbaren Parameter, die sogenannte LRU Sitting Time. Dieser Wert besagt, wie lange sich ein gelesener Block im File Cache befindet, bevor er überschrieben werden muß, weil kein freier Cache-Block mehr zur Verfügung steht, aber neue Daten von der Platte des Servers in den Cache gelesen werden müssen. Eine LRU Sitting Time von 20 Minuten ist dabei schon recht ordentlich, d.h., die gelesenen Daten bleiben 20 Minuten im Cache, bevor sie aufgrund von »Eigenbedarf« überschrieben werden müssen.

Bei Bedarf kann nun ein Teil des Cache Speichers »abgespaltet« werden, um diesen als geschützten Speicherbereich nutzbar machen zu können. Man bezeichnet diesen geschützten Speicherbereich auch als Benutzer-Adreßbereich oder Ring 3. Ein geschützter Adreßbereich ist somit ein Teil des Cache-Speichers, über den eine »sorgfältig« überwachte Kommunikation mit dem Netzwerkbetriebssystem durchgeführt wird. Alle geschützten Speicherbereiche nutzen zudem virtuellen Speicher (hierzu später mehr). Der Einsatz von geschützten Speicherbereichen dient vor allem dazu, unausgetestete Software oder »unsichere« Software auf dem Server einsetzen zu können, ohne den gesamten Serverbetrieb in Gefahr zu bringen. Dies liegt darin begründet, daß Module, die im geschützten Speicherbereich laufen, das Netzwerkbetriebssystem nicht zerstören oder keine Server-Abends verursachen können. Somit bietet der geschützte Speicherbereich einen sicheren Platz, um Anwendungen laufen zu lassen. Zu beachten ist jedoch, daß das Betriebssystem selbst nur im Ring 0 laufen kann, auch als OS-Adreßbereich oder Kernel-Adreßbereich bezeichnet. Das Modul `syscalls.nlm` in Verbindung mit dem Speicherschutz-Subsystem hindert Module im geschützten Speicherbereich daran, auf andere Adreßbereiche außerhalb des geschützten Speicherbereichs zuzugreifen. Dies bedeutet auch, daß das `syscalls.nlm` und das Speicherschutz-Subsystem als Schnittstelle

20.1 Betriebssystem

zwischen dem geschützten Speicherbereich und dem Netzwerkbetriebssystem dient. Sie hindern NLM-Programme im geschützten Speicherbereich daran, Aufrufe an das Netzwerkbetriebssystem abzusetzen, die das Betriebssystem zerstören oder zu Ausfällen des Netzwerkbetriebssystem führen würden. In den geschützten Speicherbereich können Module geladen und daraus entladen werden, der Speicherbereich kann gelöscht oder, wenn notwendig, auch »zerstört« werden.

Jeder geschützte Speicherbereich verwendet seine eigene Page Translation Table, um die logische Speicheradressierung durchführen zu können. Das Speichermanagement-Modul gewährleistet, daß die Page Translation Table eines jeden geschützten Speicherbereichs auf unterschiedliche physikalische Speicheradressen verweist. Zu einem gegebenen Zeitpunkt kann nur eine Translation Table in das Speichermanagement-Subsystem geladen werden. Wenn es mehr als einen geschützten Speicherbereich gibt, dann lädt das Speichermanagement-Subsystem für eine bestimmte Zeit eine Translation Table und ersetzt sie danach durch eine andere. Das Ersetzen von Translation Tables bezeichnet man in diesem Zusammenhang auch als Context-Wechsel. Da ein Context-Wechsel relativ zeitintensiv ist, sollten nur so viele geschützte Speicherbereiche wie nötig eingerichtet werden. Zu beachten ist auch, daß unter anderem die folgenden Module nicht im geschützten Speicherbereich laufen können:

SERVER.EXE

Das Netzwerkbetriebssystem kann nicht im geschützten Speicherbereich laufen, da jedes Modul im geschützten Speicher bei Bedarf temporär gestoppt und auf die Platte ausgelagert werden kann (Verwendung von virtueller Speichertechnik).

LAN- und Disk-Treiber

Disk- und LAN-Treiber müssen im Ring 0 (OS-Adreßbereich) laufen, da sie nur physikalische Speicheradressen verwenden und der geschützte Speicherbereich eine logische Speicheradressierung verwendet.

MONITOR

Ein wichtiges Überwachungs- und Informations-Tool von NetWare ist das Monitor-NLM, also Monitor-Programm, um damit alle wichtigen und notwendigen Informationen über den Server, seinen Zustand, seine Auslastung, seine geladenen Module etc. erfahren zu können. Da das Monitor-Programm Betriebssystem-Aufrufe durchführt, die im geschützten Speicherbereich nicht erlaubt sind, kann dieses Modul nur im Ring 0 laufen.

NSS

Das neue, flexible und schnelle Dateisystem NSS kann ebenfalls nicht im geschützten Speicherbereich laufen.

20 NetWare 5

- Module, die im geschützten Speicherbereich laufen sollen, müssen hierfür auch konzipiert und geschrieben sein. Alle Module, die dies nicht erfüllen, müssen im Ring 0 laufen.
- Module werden in der Regel nur dann in den geschützten Speicherbereich geladen, wenn man sich über die Stabilität des Moduls nicht ganz sicher ist oder ein Modul bereits auf einem produktiven Server starten will, ohne genau zu wissen, ob dies reibungslos funktioniert.
- Der Speicherschutz wird unter NetWare 5 auch für Java-Anwendungen unterstützt.

Geschützte Speicherbereiche können durch das Laden von Modulen eingerichtet werden. Hierzu müssen nur die richtigen Ladebefehle verwendet werden, die ich nachfolgend kurz aufzeigen will. An dieser Stelle sei auf eine sehr große Vereinfachung für das Laden von Modulen am Server hingewiesen:

Bis jetzt mußte man für das Laden von Modulen den Befehl `LOAD modulname` eingeben.

Mit NetWare 5 kann man auf die Eingabe des Befehls `LOAD` verzichten. Um z.B. das Monitor-Programm am Server zu starten, gibt man nicht mehr `LOAD monitor` ein, sondern nur noch `MONITOR`. Deshalb verzichte ich bei allen weiteren Befehlen auf das explizite `LOAD`-Kürzel.

Laden von geschützten Speicherbereichen

- *PROTECTED modulname*
Laden eines Moduls in den geschützten Speicherbereich, der den Namen `ADDRESS_SPACEn` zugewiesen bekommt.
- *RESTART modulname*
Lädt ein Modul in den geschützten Speicherbereich, das aber zusätzlich mit Restart-Funktionalität ausgestattet ist. Der geschützte Speicherbereich erhält den Namen `ADDRESS_SPACEn`. Restart-Funktionalität bedeutet in diesem Zusammenhang, daß im Falle eines Abends des geschützten Speicherbereichs dieser bereinigt und das Modul anschließend neu geladen wird.
- *ADDRESS_SPACE=spacename modulname*
Lädt ein Modul in den geschützten Speicherbereich; der Anwender hat einen eigenen Namen für den geschützten Speicherbereich definiert.
- *PROTECT dateiname*
Dieser Befehl wird verwendet, um mehrere Module in den geschützten Speicherbereich zu laden. Als Dateiname wird eine `.NCF`-Datei verwendet. Der Name des geschützten Speicherbereichs ist der Name der `.NCF`-Datei.

20.1 Betriebssystem

- *PROTECTION NO RESTART spacename*
Von einem bereits existierenden geschützten Adreßbereich wird die Restart-Funktionalität entfernt.

Entladen von geschützten Speicherbereichen

- *UNLOAD ADDRESS SPACE=spacename modulname*
Entlädt das angegebene Modul vom angegebenen Adreßbereich.
- *UNLOAD ADDRESS SPACE=spacename*
Entlädt alle Module vom angegebenen Adreßbereich und entfernt auch noch gleichzeitig den Adreßbereich.
- *UNLOAD KILL ADDRESS SPACE=spacename*
Der Adreßbereich wird entfernt, ohne jedoch zuvor die Module zu entladen. Dies ist die »harte« Methode, um den Adreßbereich zu bereinigen und zu entfernen.

20.1.3

Virtueller Speicher

Durch den Einsatz der virtuellen Speichertechnik bietet NetWare 5 einen effizienten Weg der Speicherausnutzung und verringert die Gefahr, daß der Server einen Abend verursacht, nur weil der Speicherausbau im Server zu gering ist.

Der verfügbare Speicher wird »bewertet«, um feststellen zu können, welche Daten zuletzt genutzt worden sind. Wann Daten zuletzt genutzt worden sind, wird durch ein Bit in jedem Feld der Translation Table festgelegt, über die wiederum festgelegt wird, ob die Address Translation seit der letzten Überprüfung eingesetzt worden ist. Daten, die über einen bestimmten Zeitraum nicht genutzt worden sind, können vom Hauptspeicher auf die Festplatte transferiert werden. Auf diese Art und Weise wird Hauptspeicher für andere Anwendungen frei. Wenn die Daten, die sich ausgelagert auf der Platte befinden, wieder benötigt werden, werden sie in den Hauptspeicher zurückgeholt. Da die Daten auf Platte ein- und ausgelagert werden, kann der verfügbare Hauptspeicher für wesentlich höhere Datenmengen genutzt werden, als der physikalische Hauptspeicher tatsächlich abdeckt.

Die Java Virtual Machine und jedes Modul, das in den geschützten Speicherbereich geladen ist, nutzen die virtuelle Speichertechnik. Sowohl die Module als auch die Daten, auf die von den Modulen zugegriffen wird, können auf die Platte ausgelagert werden. Betriebssystem-Module nutzen keinen virtuellen Speicher, da diese nicht auf die Platte ausgelagert werden können. Das Speichermanagement-Subsystem legt den Speicherbedarf für alle Server- und NLM-Prozesse fest und bestimmt, wo der freigewordene Speicher genutzt

werden soll. Das Subsystem speichert den freigewordenen Speicher im sogenannten Disk Cache. Wenn Daten vom Hauptspeicher auf die Platte ausgelagert werden, werden sie in einer Swap-Datei gespeichert. Für jedes NetWare Volume kann eine eigene Swap-Datei eingerichtet werden, wobei für das Volume SYS per default eine Swap-Datei eingerichtet wird.

Mit dem Befehl SWAP kann eine Swap-Datei erstellt oder gelöscht werden. Ebenso können notwendige Swap-File-Parameter geändert und angezeigt werden. Über das Monitor-Programm können notwendige Informationen ebenfalls angezeigt werden. Das Swapping von Daten zwischen Speicher und Platte erfordert zwar zusätzliche System-Ressourcen, da jedoch der verfügbare Hauptspeicher für das gesamte System vergrößert wird, kompensieren sich diese Aspekte.

20.1.4 Logische Speicheradressierung

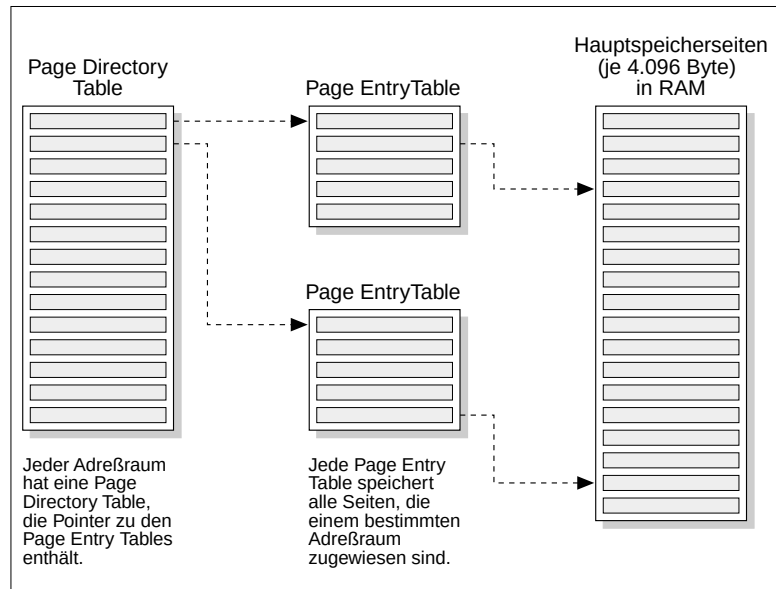
Der physikalische Speicher des Servers wird in Blöcke von 4 Kbyte Größe aufgeteilt, so wie dies von Intel definiert worden ist. Wenn ein Prozeß Daten im Speicher ablegen will, werden zusammenhängende Speicherseiten angefordert, so daß alle Informationen in einer sequentiellen Abfolge von Seiten gespeichert werden kann. Da im Laufe der Zeit Speicher auch wieder freigegeben und neu angefordert wird, entsteht nach einiger Zeit die Situation, daß Speicher »überig« bleibt, der zu klein ist, um noch sinnvoll genutzt zu werden. Diese Situation bezeichnet man als Speicherfragmentierung, d.h., der Hauptspeicher ist zerklüftet. Aufgrund der Speicherfragmentierung kann der Server häufig keine Speicheranforderungen mehr erfüllen.

Das logische Speicheradressierungsschema von Novell hilft dabei, diese Speicherfragmentierung zu vermeiden. Hierzu bietet das Speichermanagement-Subsystem eine Page Directory Table, die logische Speicheradressen von 0 bis 4 Gbyte vorweisen kann. Die Tabelle weist auch dann Adressen von bis zu 4 Gbyte aus, wenn der Server nur den minimalen Speicher von 64 Mbyte eingebaut hat. Wenn ein Prozeß einen zusammenhängenden Speicherblock benötigt, dann findet das Betriebssystem alle notwendigen und zusammenhängenden Adressen in der Page Directory Table. Da in der Tabelle so viele Adressen vorhanden sind (4 Gbyte), kann das Betriebssystem fast immer den vom Prozeß angeforderten zusammenhängenden Speicherbereich finden. Andere Tabellen hingegen, Page Entry Table genannt, haben die Aufgabe, die logischen Adressen in physikalische Adressen umzusetzen, was nicht unbedingt zu einem zusammenhängenden physikalischen Speicherbereich führt, sondern die physikalischen Adressen im Hauptspeicher verstreut. Solange die logi-

20.1 Betriebssystem

schen Adressen zusammenhängend sind, macht es überhaupt nichts aus, wenn der physikalische Speicher nicht zusammenhängend ist. Die Page Directory Table und die Page Entry Table zusammen bilden die Page Translation Table. In Abbildung 20.2 ist der Zusammenhang zwischen diesen Tabellen aufgezeigt.

Abbildung 20.2
Page Translation
Table



20.1.5

ConsoleOne

Mit Einführung von NetWare 5 ist man jetzt auch in der Lage, am Server ein grafisches Administrations-Tool zu starten und zu nutzen. Ermöglicht wird dies, weil ConsoleOne eine Java-basierende Anwendung ist und NetWare 5 eine vollständige Java-Unterstützung bietet. Die Java-Anwendung ConsoleOne kann aber nicht nur auf dem Server gestartet werden, sondern auch auf einer Windows 95/98 bzw. Windows NT Station, sofern die Java-Unterstützung hierfür installiert ist. Mit dem neuen Z.E.N.works-Client von NetWare ist dies zum Beispiel problemlos installierbar und ab diesem Zeitpunkt auch einsetzbar. Das Erscheinungsbild und die Bedienung von ConsoleOne ist einer X-Windows-Umgebung sehr ähnlich, so wie man dies von einer Unix-Plattform gewohnt ist. Über ConsoleOne ist man somit in der Lage, die Administration einer NetWare-Umgebung vollständig vom Server aus durchzuführen. Dies hat unter anderem den Vorteil, daß man im Serverraum zum Administrieren der NetWare-Umgebung keine Workstation mehr suchen muß, um z.B. Änderungen in der

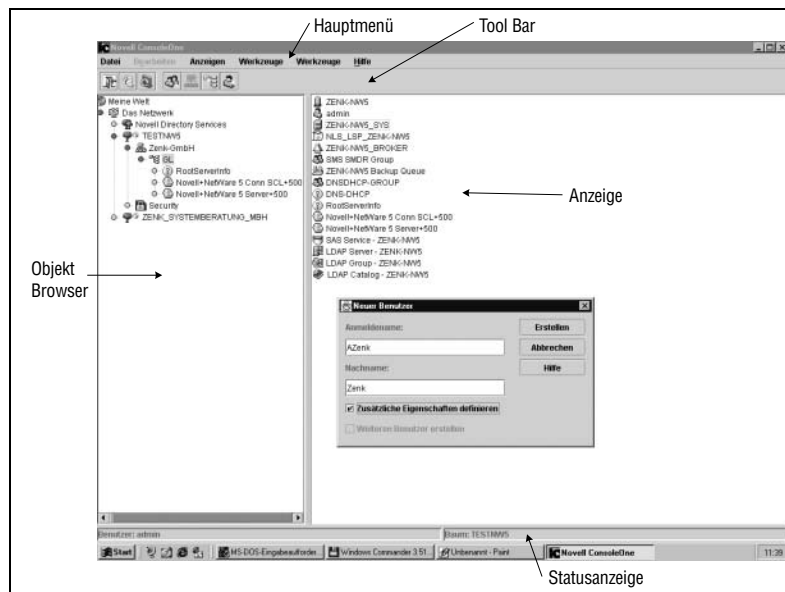
20 NetWare 5

NDS durchführen oder Informationen auslesen zu können, sondern man kann dies direkt am Server ausführen. ConsoleOne kann auch mit Hilfe zusätzlicher Snap-in-Module um weitere Funktionen ergänzt werden, die z. B. für andere Anwendungsbereiche benötigt werden. Ziel von Novell ist es, ConsoleOne als die neue einheitliche Administrationsoberfläche zu implementieren. Im Laufe der Zeit werden auch entsprechende Anpassungen für ManageWise und andere Produkte rund um NetWare zur Verfügung stehen. Mit Einführung von ConsoleOne ist man auch gezwungen, den Server mit einer Maus auszustatten, damit man die grafische Oberfläche überhaupt vernünftig bedienen kann.

Es sei jedoch erwähnt, daß man nicht gezwungen ist, mit dieser Oberfläche am Server zu arbeiten; es steht dem Netzwerkverwalter vollkommen frei, dieses Add-on zu nutzen oder auf die herkömmliche Art und Weise zu agieren.

Aus Abbildung 20.3 ist zu ersehen, wie sich ConsoleOne dem Netzwerkverwalter gegenüber darstellt. Dabei ist das Erscheinungsbild immer identisch, ganz gleich ob ConsoleOne von einer Workstation aus oder auf dem Server gestartet wird.

Abbildung 20.3
ConsoleOne



Es ist zu erkennen, daß ConsoleOne aus einem Hauptmenü besteht, in dem unter File, Edit, View, Tools und Help die unterschiedlichsten Aktionen durchgeführt werden können. Daneben existiert die

20.1 Betriebssystem

sogenannte Tool Bar, um bestimmte Aktionen nur über Anklicken des entsprechenden Symbols ausführen zu können. Im unteren Bereich ist die Statuszeile zu sehen, aus der man bestimmte Informationen über das aktuell angewählte Objekt ersehen kann, und das Hauptfenster selbst unterteilt sich in den linken Teil, das Objekt-Browser-Fenster, und den rechten Teil, das sogenannte Anzeigefenster. Im linken Teil wandert man durch die einzelnen Objektebenen und erhält für jeden ausgewählten Objektteil im rechten Fenster den Inhalt angezeigt. Es kann sich dabei zum Beispiel um den Inhalt eines NDS-Containers oder auch um den Inhalt eines Volume oder eines Verzeichnisses handeln. Wenn man ein Objekt ausgewählt hat, kann man über die rechte Maustaste, in Abhängigkeit vom ausgewählten Objekt, zusätzliche Optionen erhalten.

Markiert man zum Beispiel eine Datei und drückt die rechte Maustaste, kann man die Datei löschen, umbenennen, kopieren etc. ConsoleOne bietet somit eine Vielzahl von Möglichkeiten, um einfaches und effizientes Verwalten der Netzwerkumgebung zu ermöglichen. ConsoleOne ist somit auch die erste große Anwendung, die von Novell für NetWare 5 ausgeliefert wird, die sowohl auf einem Server als auch auf einer Workstation ausgeführt werden kann.

20.1.6 Jahr-2000-Fähigkeit

Für NetWare 5 ist die Jahr-2000-Fähigkeit von Haus aus gegeben. NetWare 4 ist erst ab der Version 4.11 und NetWare 3 erst ab der Version 3.2 Jahr-2000-fähig. Was bezüglich der Jahr-2000-Problematik noch zu beachten ist, wird in einem eigenen Kapitel besprochen.

20.1.7 Merced-Prozessor-Unterstützung

NetWare 5 unterstützt die 32-Bit-Architektur von Intel und wird bei Auslieferung des 64-Bit-Prozessors »Merced« auch in der Lage sein, diese neue Architektur zu unterstützen.

20.1.8 Hot Plug PCI

NetWare 5 unterstützt einen Mechanismus, der es erlaubt, Netzwerkkarten und/oder Platten-Controller im laufenden Betrieb zu tauschen, ohne den Server hierfür herunterfahren zu müssen, etwa für den Fall, daß defekte Karten ausgetauscht werden müssen oder neue Karten hinzugefügt werden sollen. Die Server Uptime wird dadurch wesentlich erhöht. Damit dies funktioniert, müssen die Device-Treiber für diese Karten modifiziert werden, um Hot-Plug-fähig zu sein. Zur Zeit haben sich unter anderem die Hersteller Adaptec, BusLogic,

Mylex und SysKonnect dazu bereit erklärt, passende Treiber zu entwickeln. Zusätzlich hat z.B. Compaq für die eigenen PCI-Systeme wie Compaq NetFlex Controller, Compaq Netelligent Controller, Smart-2 Array Controller und Compaq SCSI Adapter passende Treiber entwickelt.

20.1.9 I₂O

Intelligent I/O (I₂O) ist eine von der Industrie ins Leben gerufene Spezifikation, die darauf abzielt, Standard-basierende Lösungen zu bieten, um die CPU beim I/O-Transfer zu entlasten. Zudem soll den Entwicklern dadurch ermöglicht werden, einen einzigen Treiber zu entwickeln, der mit allen Netzwerkplattformen arbeitet. NetWare 5 bietet die Unterstützung von Intelligent I/O für Ethernet- und SCSI-basierende Endgeräte. Dadurch wird die Leistung des Servers zusätzlich gesteigert, da die CPU von unnötigen I/O-Belastungen befreit ist.

20.2 Novell Directory Services (NDS)

Der Aufbau der NDS und die damit verbundenen Vorteile wurden bereits ausführlich im Kapitel über NetWare 4 beschrieben. Hierbei wurde ausführlich erklärt, auf welche Art und Weise die NDS den Single Point of Administration, den Single Sign-On oder auch zusätzliche Sicherheitsmechanismen unterstützen. Alle diese bisher getroffenen Aussagen gelten auch für NetWare 5. Zusätzlich wurde jedoch NetWare 5 mit NDS-Erweiterungen ausgestattet, die weitere positive Funktionen zur Verfügung stellen.

20.2.1 Transitive Synchronisation

Mit NetWare 5 erfolgt die Synchronisation der Replicas nicht mehr innerhalb eines Replica-Rings. Das heißt, wenn auf dem Server A in der Replica eine Änderung durchgeführt wird, dann hat der Server bislang im Replica-Ring für diese Partition nachgesehen, auf welchen anderen Servern ebenfalls von dieser Partition Replicas liegen, und daraufhin die Änderungen nacheinander an diese betroffenen Server geschickt. Die Transitive Synchronisation arbeitet über einen Migration Agent Server, der den Replica-Ring und für jeden Ziel-Server den ReplicaUpto Vector prüft. Wenn der ReplicaUpto Vector des Quell-Servers nicht aktueller ist als der ReplicaUpto Vector des Ziel-Servers, dann muß der Quell-Server nicht mit diesem Ziel-Server synchronisiert werden. Dieser Vorgang verringert den Synchronisationsverkehr, belegt dadurch weniger Bandbreite und funktioniert sowohl für das IPX- als auch für das IP-Protokoll.

20.2 Novell Directory Services (NDS)

20.2.2 Management gezielt verteilen

Bereits in den früheren NetWare-4-Versionen war es möglich, über eine gezielte NDS-Rechtevergabe festzulegen, wer welche administrativen Aufgaben erledigen darf. Bislang war es jedoch zum Beispiel nicht möglich, ohne zusätzliche Add-on-Tools einem Subadministrator das Recht zu erteilen, die Paßwörter von Benutzern zu ändern. Mit NetWare 5 ist dies anders geworden. Fehlte bislang ein eigenes Property »Paßwort« für das Benutzer-Objekt, so ist dieses inzwischen vorhanden und kann mit entsprechenden Rechten versehen werden, so daß man jedem »beliebigen« Benutzer das Recht auf dieses Property geben kann, das Paßwort zu ändern. Für die Berechtigung, das Paßwort zu ändern und für alle anderen NDS-Berechtigungen gilt, daß alle diese administrativen Aufgaben sorgfältig geplant und eingesetzt werden müssen. Ohne korrekte Planung kann dies ansonsten sehr schnell im »Kein Durchblick mehr« enden.

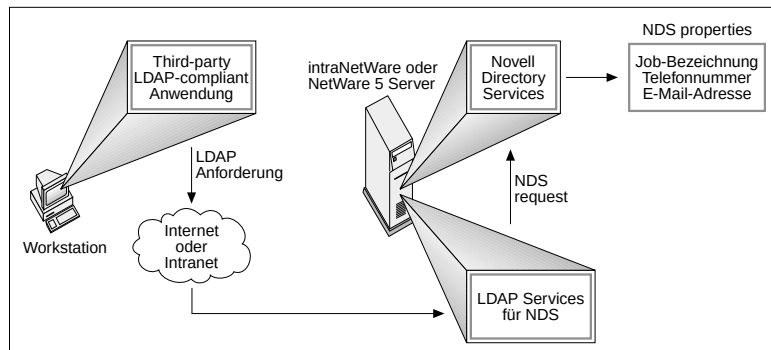
20.2.3 Catalog Services

Bereits mit Einführung der NDS wurde immer wieder beklagt, daß es dem Anwender nicht zugemutet werden kann, sich den sogenannten Context zu merken, indem das Benutzerobjekt existiert, um einen reibungslosen Login durchführen zu können. Solange auf dem Rechner, über den man den Login durchführen will, der gleiche Context eingestellt ist, der für den Benutzer in Frage kommt, ist dies noch kein Problem. Sobald jedoch ein Rechner verwendet wird, auf dem ein anderer Context eingestellt ist, fängt das Problem für den Anwender an. Mit den Catalog Services soll unter anderem dieses Problem behoben werden. Mit den Catalog Services werden der Anmeldevorgang und das Erstellen von NDS-fähigen Anwendungen einfacher. Zudem werden der Zugriff und die Performance beim Zugriff auf die NDS beschleunigt. Durch den sogenannten Context-loosen Login ist der Benutzer in der Lage, sich von jeder beliebigen Workstation im Netz anzumelden, ohne nähere Kenntnisse über die NDS haben zu müssen. Wenn die Directory-Informationen in einem Catalog bzw. Index abgespeichert sind, dann werden dadurch Suchvorgänge, die Sortierung und die Auswertung erleichtert. Die Verteilung und Replizierung dieser Index-Informationen (Catalog-Informationen) erlauben einen schnellen Zugriff auf einen »Schnappschuß« der NDS. Zur Verwaltung der Catalog Services gibt es ein GUI-Programm, den sogenannte Catalog Services Manager, der als Snap-in-Modul für den NWAdmin zur Verfügung gestellt wird. Der Catalog Services Manager dient unter anderem dazu, den Bereich der NDS festzulegen, der im Catalog verwaltet werden soll. Zudem können die Bedingungen für die Erstellung des Catalog definiert werden.

20.2.4 LDAP

Das Lightweight Directory Access Protocol (LDAP) wurde entwickelt, um Anwendern mit LDAP-fähiger Software einen einfachen Zugriff auf X.500-basierende Directories zu ermöglichen, so wie dies bei den NDS der Fall ist. Da LDAP ein relativ einfaches Protokoll ist, benötigt es weniger Computerleistung als dies beim Directory Access Protocol (DAP), der Vorgängerversion, der Fall gewesen ist. LDAP ist inzwischen zu einem De-facto-Standard geworden, und die Internet Engineering Task Force (IETF) richtet LDAP als offiziellen Internet-Standard ein. Die LDAP-Dienste für die NDS sind eine serverbasierende Schnittstelle zwischen den NDS und LDAP-fähigen Anwendungen, die auch noch optional Secure Socket Layer (SSL) nutzen können. NetWare 5 unterstützt den derzeit gültigen Standard LDAP Version 3. LDAP wird als NLM aktiviert, in die NDS integriert und über ein Snap-in-Modul im NWAdmin verwaltet, um damit die Rechte festlegen zu können, wer Daten aus der NDS über LDAP lesen und schreiben darf. Nicht zu vergessen ist, daß LDAP als Kommunikationsprotokoll TCP/IP einsetzt. In Abbildung 20.4 ist aufgezeigt, wie die Integration von LDAP in einer NDS-Umgebung erfolgt.

Abbildung 20.4
Zugriffe auf die
NDS über LDAP



20.2.5 NDS Manager

NetWare 5 stellt den NDS Manager als Stand-Alone-Programm und als Snap-in-Modul für den NWAdmin zur Verfügung. Die Arbeitsweise und Funktionen für den NDS Manager sind im Vergleich zu NetWare 4.11 nicht anders, mit zwei Ausnahmen:

- Es wird ein 32-Bit-Code verwendet statt des bisherigen 16-Bit-Code. Dadurch wird auch die Arbeitsweise für den NDS Manager wesentlich schneller

20.2 Novell Directory Services (NDS)

- Der Schema-Manager, bislang als Zusatz für den NWAdmin unter NetWare 4.11 verfügbar, ist unter NetWare 5 standardmäßig im NDS Manager integriert. Hiermit ist es ziemlich einfach, die NDS zu erweitern oder sich Informationen über den NDS-Aufbau anzeigen zu lassen. Man sollte jedoch mit dem Schema-Manager sehr vorsichtig umgehen.

20.2.6 WAN Traffic Manager (WTM)

Die NDS ist eine verteilte, replizierbare und globale Datenbank. Beim Aufbau eines Netzwerks ist generell darauf zu achten, daß die Synchronisationsvorgänge zwischen den Servern aufgrund der Replica-Verteilung nicht überhandnehmen. Dies gilt im besonderen beim Einsatz von WAN-Strecken, vor allem wenn die Bandbreite der WAN-Strecke nicht sehr groß ist. Dies ist aber noch nicht das größte Problem. Wenn die WAN-Strecke als Wählverbindung realisiert ist, tritt das zusätzliche Problem auf, daß die WAN-Strecke sehr oft geöffnet wird, um die Synchronisation zwischen Replicas durchführen zu können. Auch mit den standardmäßig verfügbaren Parametern für die NDS ist es nicht möglich, dieses Problem in den Griff zu bekommen, ohne daß die Telefonkosten für die Wählverbindung monatlich höher werden. Aus diesem Grund hat Novell den WAN Traffic Manager entwickelt, der für Netware 5 standardmäßig zur Verfügung steht und für die NetWare-4.11-Umgebung als zusätzliches Modul erworben werden kann.

Der WAN Traffic Manager ist ein Policy-basierendes Programm, das der WAN-Verkehr-Steuerung dient. Der NDS-Client (zuständig für die Kommunikation der NDS auf den Servern untereinander) fordert eine Policy-Entscheidung an, bevor eine WAN-Kommunikation angestoßen wird. Der WAN Traffic Manager prüft die vom Netzwerkverwalter eingerichteten Policies und versucht, eine Übereinstimmung mit den Kriterien zu erreichen. Wird eine solche Übereinstimmung festgestellt, dann wird die Policy ausgeführt, um feststellen zu können, ob der NDS-Abgleich über das WAN zu diesem Zeitpunkt erlaubt ist oder auf einen späteren Zeitpunkt verschoben werden muß. Policies werden als Text in einem hierfür eingerichteten Server-Attribut und LAN-Area-Attribut gespeichert. Der Policy Manager wird als Snap-in-Modul für den NWAdmin ausgeführt.

20.2.7 DSDIAG (DS Diagnostics)

NetWare 5 wird standardmäßig mit dem DSDIAG NLM ausgeliefert. Damit können ausführliche Tests mit den NDS durchgeführt und so in Erfahrung gebracht werden, ob es irgendwo in den NDS zu Feh-

lernen gekommen ist. Alle diese Informationen dienen auch dazu, um rechtzeitig Gegenmaßnahmen ergreifen zu können. Man ist dabei nicht auf nur einen NDS-Baum festgelegt, sondern kann über das gestartete Modul am Server gleichzeitig andere NDS-Bäume im Netzwerk analysieren und auswerten.

20.3 Netzwerkdienste

Nach außen hin sieht der Anwender kaum Unterschiede zu NetWare 4, jedoch wird der Netzwerkverwalter feststellen, daß NetWare 5 sehr viele neue Netzwerkdienste vorweisen kann, die man in dieser Form bislang noch nicht gekannt hat. In diesem Abschnitt will ich Ihnen deshalb aufzeigen, welche neuen Netzwerkdienste zur Verfügung gestellt werden und was Sie damit erreichen können.

20.3.1 Native IP

NetWare hat bisher traditionell IPX und die dazugehörigen Protokolle (RIP, SAP) für die Kommunikation im Netzwerk verwendet. Die ersten Ansätze für den Einsatz von TCP/IP als Kommunikationsmechanismus wurden bereits mit NetWare/IP etabliert. Da es sich jedoch bei NetWare/IP um ein proprietäres Protokoll handelt, wurde der Einsatz von NetWare/IP nur sehr zögerlich durchgeführt. Mit NetWare 5 hat man die Wahl, für die Kommunikation im Netzwerk IPX, IP oder nur IP einzusetzen. Da NetWare 5 zudem eine Vielzahl von Internet-Mechanismen und das Internet-Protokoll einsetzt, ist Native-IP-Unterstützung eine zwingende Voraussetzung. Man hätte dies mit der proprietären IPX-Protokollwelt nie erreichen können. Um IP unter NetWare lauffähig zu machen, müßte das Standardprotokoll IP vollständig in NetWare integriert und IPX als Protokoll ersetzt werden. Wie später noch zu sehen sein wird, nutzt man die NDS auch dazu, um alle Verwaltungsaufgaben und Informationen für IP in die NDS zu integrieren. Auf diese Art und Weise kann die gesamte IP-Umgebung über das GUI NWAdmin verwaltet werden.

Um die Kompatibilität zu IPX aufrechterhalten zu können, unterstützt NetWare 5 den sogenannten Compatibility Mode. Es gibt die folgenden drei Möglichkeiten zur Installation des Server bzw. des Clients:

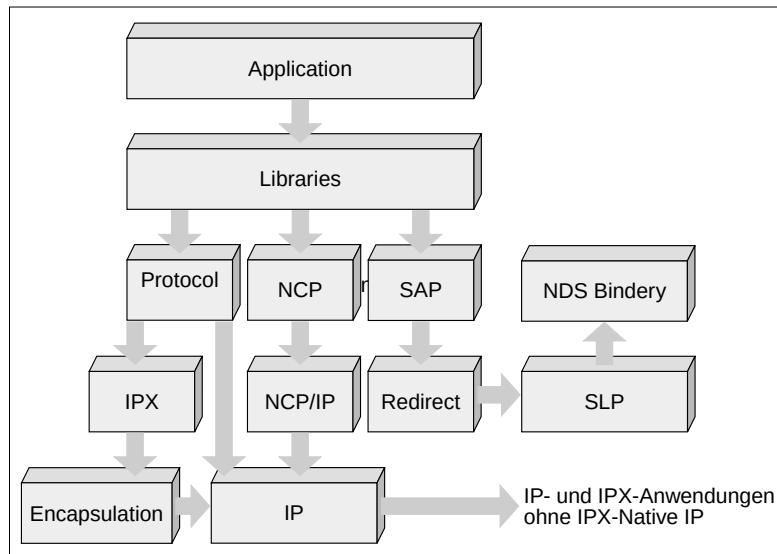
- IP (mit Compatibility Mode)
- IPX
- IP und IPX

Der Compatibility Mode besteht aus drei unterschiedlichen Technologien, die gewährleisten, daß IPX-basierende Anwendungen in ei-

20.3 Netzwerkdienste

ner reinen IP-Welt arbeiten und eingesetzt werden können. Als erstes ist zu bedenken, daß die gesamte NCP-Kommunikation unter NetWare 5 über IP realisiert wird. Wenn eine IPX-Anwendung Zugriff auf den NetWare 5 Server über NCP benötigt, erfolgt dies über den Compatibility-Mode-Treiber. Der Transport der Informationen erfolgt dennoch über IP und nicht über IPX. In Abbildung 20.5 ist dargestellt, wie die Arbeitsweise des Compatibility-Mode-Treibers aussieht.

Abbildung 20.5
Compatibility-
Mode-Mechanismus



Zum zweiten besteht der Compatibility Mode aus einer Technologie, die man als Migration Gateway bezeichnet. Die dritte und letzte Technologie für den Compatibility Mode ist das Bindery Gateway, um kompatibel zu NetWare 3 zu bleiben.

Die Compatibility-Mode-Treiber bestehen aus einem Server-Compatibility-Mode-Treiber und einem Workstation-Compatibility-Mode-Treiber. Die entsprechenden Technologien werden standardmäßig geladen, aber nur dann genutzt, wenn eine IPX-Anwendung oder ein IPX-Dienst in der IP-Umgebung eingesetzt wird. In allen anderen Fällen ist der Compatibility-Mode-Treiber »schlafen« gelegt.

Für die IPX-Kompatibilität-Funktionen sind die folgenden Abhängigkeiten zu beachten:

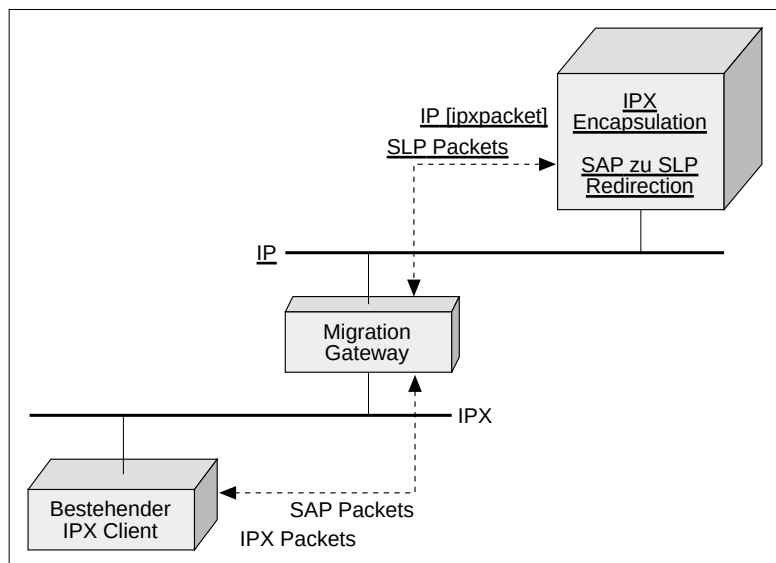
Wenn IPX-Anwendungen/-Dienste in der NetWare-5-IP-Umgebung eingesetzt oder IP-Systeme mit IPX-Systemen verbunden werden sollen, muß gewährleistet sein, daß das Service Location Protocol

20 NetWare 5

(SLP) im Netzwerk aktiviert ist. Dies liegt darin begründet, daß die IPX-Compatibility-Mode-Treiber vom Vorhandensein der SLP-Mechanismen abhängig sind. Zudem muß für die Verbindung von IPX- und IP-Netzwerken mindestens ein Migration Agent vorhanden sein.

In Abbildung 20.6 ist dargestellt, wie der Migration Agent arbeitet. Der Migration Agent ist verantwortlich für die Verbindung von IPX- und IP-Netzwerken. Ebenso ist es mit dem Migration Agent möglich, einen IP Backbone zu bilden, um damit IPX-Netzwerke zu koppeln. Der vorrangige Einsatz findet in der Regel statt, wenn man während der Umstellungsphase die Migration von IPX auf IP Schritt für Schritt durchführen will.

Abbildung 20.6
Arbeitsweise
des Migration
Gateway



Wenn sowohl der Compatibility Mode als auch der Migration Agent eingesetzt wird, können beide Protokollwelten, Paketinformationen und Adressierungsmechanismen auf jedem Segment eingesetzt werden (Client-Client-, Server-Server-Kommunikation oder eine Kombination davon). Da der Migration Agent ein NetWare Loadable Module ist, benötigt man keine zusätzliche Konfiguration. Der Migration Agent besitzt eine herkömmliche IPX-Router-Funktionalität und ist deshalb in der Lage, Routing zwischen IPX- und IP-Segmenten durchzuführen.

Die dritte Funktionalität des Compatibility Mode liegt in der NetWare-3-Bindery-Kompatibilität. Dieser Dienst ist in einer NetWare-5-IP-Umgebung nur dann notwendig, wenn man IPX-basierende An-

20.3 Netzwerkdienste

wendungen und Dienste auf einem NetWare 3 Server einsetzen will. Mit dem Compatibility Mode Bindery NLM, das auf dem Server gestartet werden muß, werden dynamische Objekte in statische Objekte umgewandelt und in die NDS eingefügt. Auf diese Art und Weise können Anwendungen, die von der Bindery abhängig sind, die notwendigen Objektinformationen in den NDS finden und so laufen, als hätte sich nichts geändert.

In diesen Ausführungen wurde bereits erwähnt, daß SLP für den Compatibility Mode notwendig ist. Es stellt sich jetzt die Frage, was unter SLP zu verstehen ist.

In NetWare 5 ist das IETF Service Location Protocol (RFC 2165) eingebunden, um einen Naming-Dienst und Discovery-Mechanismus in einer TCP/IP-Umgebung einbinden zu können. SLP ersetzt die Service-Discovery-Funktion, die bislang vom SAP-Dienst unter NetWare erbracht worden ist. Mit SLP ist man in der Lage, im Netzwerk abzufragen, welche Dienste insgesamt zur Verfügung stehen. Gleichzeitig wird das Netzwerk weniger belastet als bei bisherigen SAP-Mechanismen der früheren NetWare-Versionen – vor allem auch dann, wenn das Netzwerk sehr groß ist.

Das SLP ist nicht notwendig, wenn man sich in einer reinen IP-Umgebung befindet. Der einzige Grund, der es notwendig macht, SLP einzusetzen, ist die Erhaltung der Kompatibilität zu Diensten und Anwendungen, die SAP-Mechanismen benötigen, um Dienste im Netzwerk zu finden. Wenn der Compatibility Mode installiert ist, kann SLP für IPX-Clients genutzt werden, um die IP-Adresse des Servers ausfindig zu machen – es ist jedoch nur eine von mehreren Möglichkeiten für den Client, die IP-Adresse eines NDS-Servers zu finden (SLP, DHCP, DNS, lokale Hosts-Datei).

Die NetWare-5-TCP/IP-Implementierung unterstützt sowohl die sogenannten Open-Standards als auch die De-facto-Standards. Hierzu gehören:

- Dynamic Host Configuration Protocol (DHCP)
- Novell Directory Services (NDS)
- Domain Name Service (DNS)
- Service Location Protocol (SLP)
- TCP/IP
- WinSock 2
- Secure Socket Layer (SSL)
- Network Time Protocol (NTP)

20.3.2 DNS/DHCP

DNS- und DHCP-Dienste werden beim Einsatz von TCP/IP benötigt, um die Handhabung und Verwaltung von IP-Adressen zu vereinfachen. So hat ein DNS-Server (Domain Name Service) die Aufgabe, Domänen-Namen, die einem Endgerät zugewiesen werden (z.B. www.zenk.de), in IP-Adressen umzuwandeln (z.B. 120.10.12.143). In NetWare 5 ist der DNS-Mechanismus in die NDS integriert, wodurch sich eine Vielzahl von Vorteilen ergibt.

Das Dynamic Host Configuration Protocol (DHCP) hingegen hat die Aufgabe, einem Endgerät nach einem DHCP Request eine IP-Adresse zuzuweisen. Die Adressenzuweisung kann dabei statisch oder dynamisch erfolgen. Bei einer statischen Definition wird dem DHCP-Server mitgeteilt, welcher MAC-Adresse welche IP-Adresse zugewiesen wird. Erfolgt die Zuweisung hingegen dynamisch, dann wird einem Endgerät nach einem DHCP Request die nächste freie IP-Adresse zugewiesen, sofern nicht bereits eine Zuweisung durchgeführt wurde und die eingestellte Lease Time noch nicht abgelaufen ist. Die Verwaltung der DHCP-Mechanismen ist ebenfalls vollständig in die NDS integriert.

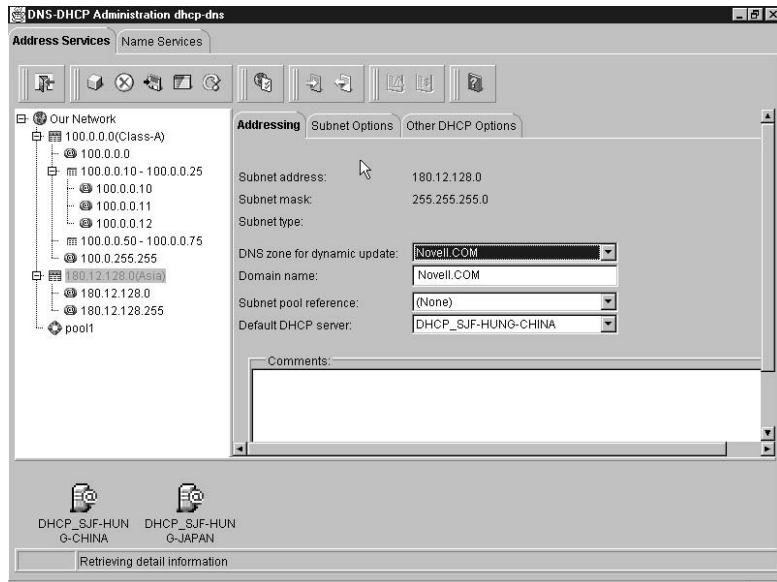
Neben DNS und DHCP unterstützt NetWare 5 zudem auch noch DDNS, den Dynamic-DNS-Mechanismus. DHCP weist einem Endgerät eine IP-Adresse zu; dies kann dynamisch erfolgen, so daß sich von Zeit zu Zeit die IP-Adressen von Endgeräten ändern könnten. DNS hingegen vergibt dem Endgerät einen bestimmten Namen. Das heißt, in beiden Fällen wird von den Systemen eine Tabelle gepflegt, indem der DHCP-Server die Zuordnung von MAC-Adresse und IP-Adresse durchführt, wohingegen der DNS-Server die Zuordnung der IP-Adresse zu DNS-Namen durchführt.

Wenn sich nun die IP-Adresse eines Endgeräts ändert, müßte in der DNS eine entsprechende Anpassung des Eintrags durchgeführt werden, da zwar noch der DNS-Name stimmt, aber nicht mehr die IP-Adresse. Um diese Verwaltung zu vereinfachen, erfolgt die Aktualisierung der DNS-Einträge dynamisch, sobald eine Änderung im DHCP-Server erfolgt. Die DNS-Einträge werden somit dynamisch gepflegt.

Durch die Integration von DHCP und DNS in die NDS werden alle diese Vorgänge wesentlich vereinfacht. In Abbildung 20.7 ist gezeigt, wie man sich die Verwaltung der DNS/DHCP-Komponenten vorstellen muß. Eingesetzt wird hierfür ein Java-basierendes grafisches Administrations-Tool.

20.3 Netzwerkdienste

Abbildung 20.7
DNS/DHCP-
Verwaltung



Die Vorteile der DNS/DHCP-Dienste liegen vor allem in den folgenden Bereichen:

- Es wird die IP-Namensvergabe und die IP-Adressenverwaltung durch die NDS vereinfacht.
- Die Kosten für das Management werden reduziert.
- Die Ausfallsicherheit wird erhöht, da die DNS- und DHCP-Daten in den NDS verwaltet werden, die NDS über Replikationen auf unterschiedliche Lokationen verteilt werden können und somit definiert werden kann, wo diese Informationen zur Verfügung gestellt werden sollen, um nicht nur den Zugriff zu beschleunigen, sondern auch die Ausfallsicherheit zu erhöhen.
- Durch die Integration in die NDS werden auch die Sicherheitsmechanismen verbessert, da die bereits bekannten Zugriffsberechtigungen der NDS genutzt werden können.
- Es besteht nicht mehr die Notwendigkeit, einen sogenannten Zone-Transfer durchzuführen, da die DNS-Daten auf einem beliebigen NDS-Server geändert werden können und durch die Replikation der NDS die Informationen für jeden NDS-basierenden DNS-Server automatisch zur Verfügung stehen.
- Der DNS-Server kann als Primary oder Secondary Server fungieren, und zwar in Verbindung mit anderen traditionellen Berkeley Internet Name Domain (BIND) DNS Servern.
- Die IP-Adressenzuweisung und der Update der Host-Namen wird automatisiert.

- Die DNS-Software in Novell DNS/DHCP basiert auf BIND 4.9.6, wohingegen sich die DHCP-Software an die RFCs 2131 und 2132 hält.
- Die DNS- und DHCP-Daten können importiert und exportiert werden.
- Die Adressenzuweisungen können benutzerindividuell vergeben und eingerichtet werden, bezogen auf bestimmte Subnetze oder Benutzerlevels mit Hilfe der NDS-Rechtemechanismen.

20.3.3 Novell Storage Services (NSS)

Die Einführung von NetWare 5 bringt auch ein neues Dateisystem mit sich: NSS (Novell Storage Services). Daneben kann jedoch auch noch das traditionelle NetWare-Dateisystem eingesetzt werden. Für beide Dateisysteme gilt, daß zum Einrichten und Verwalten von Verzeichnissen und Dateien Volumes notwendig sind und daß für beide Dateisysteme die gleichen Zugriffsberechtigungen und Rechtevergaben zur Verfügung stehen. Die bisher übliche Art und Weise zur Berechtigungsvergabe auf Dateien und Verzeichnisse bleibt ebenfalls erhalten, indem man einem Benutzer, einer Gruppe oder zum Beispiel einem Container entsprechende Rechte für Dateien und Verzeichnisse zuweist.

NSS sind ein neues, leistungsfähiges und modulares Dateisystem, das nur für NetWare 5 zur Verfügung steht, jedoch zum alten Dateisystem kompatibel bleibt. Beim Einrichten eines NSS Volume sind zwei Methoden zu unterscheiden:

- Es existiert nichtpartitionierter freier Platz auf der Platte.
- Es wird freier Platz bereits bestehender Volumes verwendet.

Wird freier nichtpartitionierter Plattenplatz genommen, dann richtet man für NSS eine neue Partition ein und teilt diese in entsprechende Volumes ein. Dabei ist es möglich, daß auf ein und derselben Platte eine traditionelle NetWare-Partition und eine NSS-Partition eingerichtet wird.

Hat man keine nichtpartitionierte Plattenkapazität mehr frei und will dennoch NSS nutzen können, ohne bestehende Volumes (Partitions) löschen und neu einrichten zu müssen, dann besteht die Möglichkeit, über das NSS-Installationsprogramm freie Volume-Kapazitäten suchen zu lassen, um diese dann für NSS Volumes zu verwenden. Hierbei können 100 % der freien Volume-Kapazität für NSS genutzt werden. Wird das NSS Volume eingerichtet, dann registriert das traditionelle NetWare Volume die NSS-Volume-Einrichtung als Datei. Die freien Speicherkapazitäten innerhalb des traditionellen NetWare Volume werden dabei in Größen von 2-Gbyte-Einheiten zur Verfü-

20.3 Netzwerkdienste

gung gestellt. Damit mit dem NSS Volume (innerhalb des traditionellen NetWare Volume) gearbeitet werden kann, müssen beide Volumes gelöscht werden. Wird ein solches angepaßtes traditionelles NetWare Volume gelöscht, dann ist auch das NSS Volume damit gelöscht.

Mit NSS kann auch die lokale DOS-Partition des Servers als Volume verfügbar gemacht werden. Hierzu muß nur das zusätzliche Modul DOSFAT.NSS geladen werden, und die lokale DOS-Platte wird als NetWare Volume sichtbar. Der Name des Volume ist zusammengesetzt aus dem Label der DOS-Platte, ergänzt um _C (für die erste DOS-Partition). Ab diesem Zeitpunkt kann man mit der DOS-Platte so arbeiten, als wäre es ein »echtes« NetWare Volume.

Zu beachten ist noch, daß außer einem Volume alle anderen Volumes unter NSS eingerichtet werden können. Das einzige Volume, das noch im traditionellen Dateiformat genutzt wird, ist das Volume SYS. Die Ursache hierfür liegt darin begründet, daß NSS noch nicht in der Lage ist, das Transaction Tracking System zu unterstützen. Das TTS ist jedoch zwingende Voraussetzung dafür, daß die NDS funktionieren. Dies ist aber nicht so tragisch, da man das Volume SYS noch auf die herkömmliche Art und Weise einrichten kann, und für alle anderen Volumes nutzt man NSS.

Die nachfolgende Aufstellung soll Ihnen zeigen, mit welchen Vorteilen man bei NSS rechnen kann:

Anzahl Dateien pro Server	8 Trillionen
Maximale Dateigröße	8 Terabyte
Anzahl gleichzeitig geöffneter Dateien	Pro Server 1 Million
Zeit, die Datei zu öffnen	Unabhängig von der Dateigröße – alle Dateien werden sofort geöffnet
Maximale Volume-Größe	8 Terabyte
Maximale Volumes pro Server	Unlimited – sichtbar für den Anwender derzeit nur 255
Anzahl Volume-Segmente	Beliebig viele
Verzeichnistiefe	Beschränkung, vom Client-Betriebssystem vorgegeben
Zeit, um Volume zu mounten	Auf keinen Fall länger als 60 Sekunden, egal wie groß das Volume ist

Hauptspeicheranforderung	Minimum 4 Mbyte, Maximum in der Regel 32 Mbyte ganz gleich, wie groß die gesamte Volume-Kapazität pro Server ist
Name-Space-Unterstützung	Standardmäßig integriert, keine Name-Space-Module mehr notwendig

Wesentlich und auffallend bei dieser Aufstellung ist die Tatsache, daß der NetWare Server mit sehr viel weniger Hauptspeicher für die Verwaltung der gesamten Volumes auskommt; es reichen 32 Mbyte Hauptspeicher für eine beliebig große Volume-Kapazität aus. Bislang mußte man den Hauptspeicherbedarf immer unter Berücksichtigung der Volume-Kapazitäten kalkulieren, wobei man davon ausgegangen ist, daß man pro 1 Gbyte Volume-Größe ca. 1,5 Mbyte Hauptspeicher kalkulieren muß. Wenn viel Hauptspeicher im Server eingebaut ist, dann kann NetWare den größten Teil des Hauptspeichers zum reinen File Caching bzw. Disk Caching nutzen. Die Verwaltung und der Zugriff auf CD-ROM-Laufwerke, DVDs und andere Storage Devices wird vollständig in die NSS-Mechanismen integriert, so daß man auch hier mit wesentlichen Performance-Vorteilen rechnen kann.

20.3.4

Novell Distributed Print Services (NDPS)

Mit NDPS bietet NetWare 5 neue Wege und Möglichkeiten, um das Drucken im Netzwerk einzurichten und zu verwalten. NDPS sind das bevorzugte Drucksystem unter NetWare 5 und unterstützen sowohl IP-basierendes als auch IPX-basierendes Drucken. Ebenso wird das bisher eingesetzte Queue-basierende Drucken nach wie vor unterstützt und eingesetzt werden können. Die gesamte Verwaltung der NDPS-Druckerumgebung wird durch folgende unterstützte Dienste vereinfacht:

- Sehr starke NDS-Integration.
- Vereinfachte und zentralisierte Verwaltung aller Druck-Ressourcen über NWAdmin.
- Automatischer Download und automatische Installation der Druckertreiber auf der Workstation. Hierzu wird von NDPS eine Printer-Driver-Datenbank gepflegt, die jederzeit erweitert werden kann.
- Bidirektionale Kommunikation mit dem Drucker, um Informationen über Job- und Printer-Status, Druckerfunktionen und Druckereinstellungen zu erhalten.
- Konfigurierbare Fehlerbenachrichtigung, um festzulegen, wer eine Nachricht erhalten soll, um aktuell den Druckerstatus und ähnliches mehr zu erfahren.

20.3 Netzwerkdienste

- Es werden bestehende Drucker und Drucker-Technologien unterstützt, so daß die Rückwärtskompatibilität erhalten bleibt.
- Neue Optionen für die Drucker- und Job-Konfiguration spezieller Drucker.
- Neue Optionen für die Print-Job-Steuerung (Job-Steuerung nach Tageszeit oder Jobgröße).

20.3.5

Z.E.N.works Starter Pack

In einem Netzwerk mit mehr als zehn Stationen kann die Verwaltung der Workstations, der Software und die Steuerung für benutzerspezifische Einstellungen bereits sehr aufwendig und zeitintensiv werden. Aus diesem Grund hat Novell Z.E.N.works entwickelt, um damit das Erreichen zu können, was sich hinter der Abkürzung verbirgt: Zero Effort Networking. Z.E.N.works besteht dabei aus einer Reihe von Modulen, die zum Teil standardmäßig zum Lieferumfang gehören und andererseits zusätzlich gekauft werden dürfen. Zu den Komponenten, die im Z.E.N.works Starter Pack enthalten sind, gehören:

- Workstation Manager
- Novell Application Launcher (NAL)

Die Komponenten von Z.E.N.works ermöglichen es dem Netzwerkverwalter, Workstation-Probleme des Anwenders zu lösen, ohne direkt vor Ort zum Arbeitsplatz des Benutzers gehen zu müssen. Dadurch, daß Workstation-Objekte und Workstation-Gruppen-Objekte in die NDS hinzugefügt werden, ist der Netzwerkverwalter in der Lage, die Arbeitsplatzkonfiguration zu verwalten, Software zu verteilen und Workstation-Pflege über die NDS durchzuführen. Wenn Z.E.N.works installiert ist, dann werden Workstations jedesmal in den NDS registriert, wenn ein Anmeldevorgang des Benutzers erfolgt. Diese Registrierung ermöglicht es dem Netzwerkverwalter, sich ein Workstation-Objekt näher anzusehen, um weitere Informationen zur Verwaltung herausfinden zu können. Bei der Software-Distribution ist zu erwähnen, daß sich die Verteilung der Software individuell auf die Belange des Anwenders oder auf die Belange des Netzwerkadministrators abstimmen lassen (zeitgesteuerte Verteilung, zwangsweise beim nächsten Login etc.). Die Software-Verteilung erfolgt mit Hilfe von Distribution-Paketen, die erzeugt und eingerichtet werden müssen. Dahinter verbergen sich Einträge in den NDS und Informationen auf entsprechenden Volumes. Die Erzeugung eines solchen Pakets ist relativ einfach: Zuerst wird mit Hilfe eines Snapshot-Programms der Ist-Zustand der Workstation ermittelt, anschließend wird die neue Software installiert, und danach wird ein neuer Snapshot der Workstation erzeugt. Die Differenz dieser beiden Snapshots, das

sogenannte Delta, bildet das Distribution-Paket. In den NDS müssen dann noch entsprechende NAL-Objekte eingerichtet werden, die notwendige Anpassungen müssen durchgeführt werden, und die Einstellungen für den Benutzer sind noch zu definieren.

Der Workstation Manager bietet vor allem für Windows NT Workstations und dessen Benutzer wesentliche Vorteile. Damit man auf einer Windows NT Workstation arbeiten kann, muß man erfolgreich angemeldet sein, und zwar unter Windows NT. Entweder man richtet auf jeder Windows NT Workstation einen entsprechenden Benutzer-Account ein, oder man hat im Hintergrund einen Windows NT Server, über den die Verwaltung der Benutzer-Accounts für den Anmeldevorgang realisiert wird, installiert. Beide Vorgehensweisen sind nicht optimal. Im ersten Fall gibt es eine große Anzahl Benutzer, die pro Workstation verwaltet werden muß, sofern man verlangt, daß jeder Anwender auf jeder Workstation arbeiten kann. Im zweiten Fall ist eine doppelte Benutzerverwaltung vorhanden.

Der NT Workstation Manager von Z.E.N.works nimmt einem diese Probleme ab, indem das Benutzerobjekt der NDS verwendet wird, um den Anwender auf der NT Workstation zu authentifizieren. Damit das funktioniert, wird auf der NT Workstation beim Anmelden ein temporärer Benutzer-Account (der gleiche Account wie der NDS-Name) eingerichtet und mit diesem Namen der Anmeldevorgang durchgeführt. Über das User-Policy-Package-Objekt in den NDS werden alle hierfür notwendigen Einrichtungen festgelegt. So wird zum Beispiel auch festgelegt, daß die Benutzerprofile auf dem NetWare Server liegen sollen und Policy-Einstellungen aus der NDS ausgelesen werden. Zudem besteht die Möglichkeit, dem Benutzer oder auch der Workstation Drucker zuzuweisen. Alle diese Einrichtungen haben den Vorteil, daß der Benutzer auf jedem NT-Rechner im Unternehmen immer seine gleiche Einstellung erhält.

Neben diesen Funktionen werden auch noch kostenpflichtige Optionen angeboten, die man separat erwerben muß. Hierzu gehören:

■ *Help Requester*

Mit dieser Anwendung gibt man den Anwendern im Netzwerk die Möglichkeit, dem Administrator oder den Help Desks im Unternehmen eine Nachricht zu übermitteln, daß mit der eigenen Workstation Probleme auftreten. In dieser Nachricht sind automatisch die Detailinformationen aus dem Workstation-Objekt enthalten, so wie dieses in der NDS gespeichert ist. Man kann anschließend aufgrund der Nachricht und den Workstation-Informationen aus den NDS versuchen, das Problem zu lösen.

20.4 Erweiterte Sicherheit

■ *Workstation Inventory*

Der Inventory Manager von Z.E.N.works ermöglicht auf einfache Art und Weise, alle Hardware-Informationen der Workstations in den NDS zu speichern, um später bei Bedarf entsprechende Auswertungen durchführen zu können, z.B. wie viele und welche Rechner nur 16 Mbyte Hauptspeicher eingebaut haben.

■ *Remote Control*

Wenn man telefonischen Support geben muß, ist es immer schwierig, auf Anhieb zu ersehen, welches Problem gerade geschildert wird, und vor allem, ob der Mitarbeiter am anderen Ende der Telefonleitung auch das tut, was man vorgeschlagen hat. Um auch damit besser umgehen zu können, kann mit Z.E.N.works ein Remote-Control-Mechanismus eingerichtet werden. Man ist dann in der Lage, sich bei Bedarf auf die Workstation des Anwenders aufzuschalten. Das heißt, man bekommt den Inhalt des Bildschirms auf den eigenen Schirm übertragen, kann Tastatureingaben machen und so arbeiten, als würde man sich direkt vor Ort beim Anwender befinden. Man kann auch beobachten, ob die Bildschirmeingaben korrekt ausgeführt werden etc.

Beachtet werden muß nur, daß es sich bei Remote Control um Komponenten handelt, die in der Regel vom Betriebsrat genehmigt werden müssen, da immer wieder die Gefahr der Mitarbeiterkontrolle angeführt wird. Aus Sicherheitsgründen kann man jedoch das System so einrichten, daß der Anwender den Remote-Control-Zugang bestätigen muß, so daß ein willkürliches »Beobachten« nicht möglich ist. Um zu erkennen, daß der Administrator oder das Help Desk seine Remote-Control-Funktion auch wieder abgebaut hat, existiert ein optisches Signal am Bildschirm. Der Benutzer kann eine Remote-Control-Sitzung jederzeit von sich aus abbrechen.

Alle bisher realisierten Projekte mit Z.E.N.works sind auf ein breites und positives Echo gestoßen, da man bereits im Starter Kit viele Möglichkeiten hat, die man in allen anderen Fällen zum Teil teuer bezahlen muß. Mit den kostenpflichtigen optionalen Funktionen wird das Ganze nur noch komplettiert.

20.4 Erweiterte Sicherheit

Auf die von NetWare bislang unterstützten Sicherheitsmechanismen und -funktionen bin ich bereits ausführlich eingegangen. Für NetWare 5 wurden weitere zusätzliche Sicherheitsfunktionen eingeführt, die bei Bedarf genutzt werden können.

20.4.1 Kryptografische Dienste

NetWare 5 beinhaltet kryptografische Dienste, die man als Novell International Cryptographic Infrastructure (NICI) bezeichnet. NICI ermöglicht es den Entwicklern, die Controlled Cryptography Service (CCS) APIs einzusetzen, um kryptografische Mechanismen in die eigenen Anwendungen einzubauen. NICI erlaubt es zudem, eine einzige Anwendung zu schreiben, die anschließend in unterschiedlichen Ländern eingesetzt werden kann, unabhängig davon, welche Gesetze zur Kryptographie im jeweiligen Land existieren. So ist es z.B. möglich, eine Anwendung zu schreiben, die den 128-Bit-Schlüssel zur kryptografischen Verschlüsselung verwendet, die aber, wenn sie nicht in den USA eingesetzt wird, auf den 40-Bit-Schlüssel zur Verschlüsselung zurückgreift.

20.4.2 Secure Authentication Services (SAS)

NetWare 5 beinhaltet SAS, eine Infrastruktur zur Unterstützung bereits existierender und zukünftiger Mechanismen zur Authentication, wie z.B. Biometric- und Token-Authentication-Systeme. Durch SAS unterstützt NetWare 5 auch SSL v3, so daß Entwickler SAS APIs einsetzen können, um Anwendungen zu schreiben, die eine verschlüsselte SSL-Verbindung aufbauen können. In Verbindung mit dem Einsatz von NICI kann gewährleistet werden, daß die SSL-Verbindungen den gesetzlichen Bestimmungen im jeweiligen Land entsprechen.

20.4.3 Public Key Infrastructure Services (PKIS)

Die Unterstützung von PKIS ermöglicht es, serverseitige Zertifikate auszusenden. Die Zertifikate basieren auf dem X.509-v3-Standard, der eine sichere Lightweight-Directory-Access-Protocol-(LDAP-)Verbindung unter Nutzung der Secure-Socket-Layer-v3-Verschlüsselung (SSL v3) aufbauen kann. Diese Netzwerkzertifikate sind ein relativ neuer Weg für Client- und Server-Strukturen, die Identität eines Anwenders als echt zu verifizieren. Allerdings kann die Abhängigkeit von Drittanbietern zur Erzeugung dieser Sicherheitsnachweise ein teures und sehr komplexes Umfeld nötig machen. Die PKIS-Unterstützung von Novell erlaubt es, solche Zertifikate über die NDS selbst zu erstellen und ihre eigene Zertifizierungsinstanz zu werden. Gleichzeitig bleibt aber auch die Möglichkeit bestehen, bei Bedarf weiterhin mit externen Sicherheitseinrichtungen wie Entrust zu arbeiten. Novell wird in NetWare 5 standardmäßig auch auf dem Client Sicherheitsprodukte von Entrust mit Hilfe von LDAP v3 unterstützen.

20.5 Installation und Upgrade

Setzen Unternehmen zur Kommunikation mit neuen Anwendungen auf LDAP, sind die Netze oftmals empfindlicher gegen Eindringlinge von außen. Um dies zu verhindern, wird NetWare 5 SSL v3 für sichere LDAP-Verbindungen integrieren. Zudem erlaubt ein erweitertes Novell Directory Services Interface eine einfachere Administration. Die NDS liefern die Lösung für weltweit arbeitende Unternehmen, die den höchstmöglichen Sicherheitsstandard benötigen, auch wenn sich dieser von Land zu Land erstreckt. Heute müssen Entwickler eine Vielzahl von unterschiedlichen Anwendungen für die verschiedenen Verschlüsselungsstandards liefern. Mit NetWare 5 liefert Novell erstmalig eine internationale Verschlüsselungsstruktur, die Entwickler für einen angemessenen Sicherheitsstandard in ihrer Anwendung – je nach Region, in der die Anwendung verwendet wird – nutzen können. Hierzu muß nicht einmal die Verschlüsselung in die Anwendung eingebunden werden. Dies ist nur deshalb möglich, weil die NDS ihren Sicherheitslevel innerhalb der Anwendung dynamisch den Vorschriften der Region anpassen können. Anwendungen, die die internationale NDS-Architektur nutzen, müssen lediglich einen einzigen Test durchlaufen. Software-Entwickler werden so von langwierigen Nachweisen für eine Exporterlaubnis befreit, da die Architektur von Novell bereits für den Export genehmigt ist (PKIS).

20.5 Installation und Upgrade

Für die Installation von NetWare 5 hat Novell eine der wesentlichsten Änderungen durchgeführt: Eine Standardinstallation läuft mit Hilfe einer grafischen Oberfläche ab. Da NetWare 5 eine leistungsfähige Java-Plattform zur Verfügung stellt, hat man nicht nur die Verwaltung über ConsoleOne als Java-Anwendung implementiert, sondern auch die Installation von NetWare 5 über eine Java-Anwendung realisiert. Hinzu kommt, daß NetWare 5 mit einer sehr guten automatischen Hardware-Erkennung ausgestattet ist, so daß der größte Teil der installierten Hardware im Server selbst erkannt wird. Für jede erkannte Hardware (Plattencontroller, Netzwerkadapter etc.) wird auch automatisch die zu ladende Treiberdatei angegeben. Neben der Installation eines vollständig neuen Servers muß aber auch noch die Möglichkeit gegeben sein, Vorgängerversionen (NetWare 3, NetWare 4.x) auf NetWare 5 umzustellen.

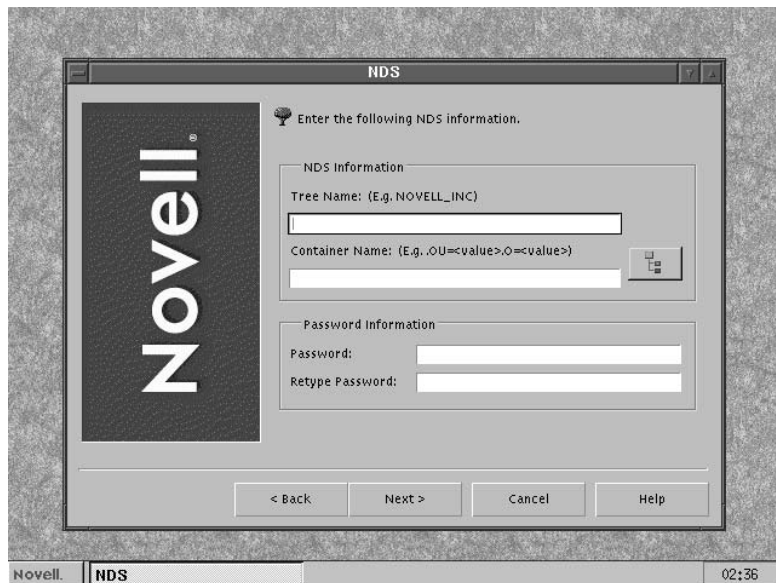
Hierfür stehen als Upgrade-Option die Across-the-Wire-Methode und der In-Place-Upgrade zur Verfügung. Wenn die Hardware-Plattform für den Server nicht geändert wird, dann empfiehlt sich der In-Place-Upgrade. Der bestehende Server wird in diesem Fall regulär beendet und mit der neuen NetWare-5-CD ausgestattet. Anschlie-

20 NetWare 5

Send wird das Install-Programm aufgerufen und die Option des Server-Updates ausgeführt. Alle anderen Eingaben erfolgen in der Regel von selbst, oder der Administrator wird durch das Installationsprogramm nach den notwendigen Parametern gefragt.

Soll für den NetWare 5 Server eine neue Hardware eingesetzt werden, dann wird auf dieser neuen Maschine NetWare 5 installiert und anschließend von einer Workstation aus der Across-the-Wire-Upgrade angestoßen. Um alle diese Aufgaben zu vereinfachen, hat Novell einen grafischen Upgrade Wizard entwickelt. Dieses Utility führt den Update der NetWare 3 Source Bindery (einschließlich der Druckerdefinitionen) und des Dateisystems durch, so daß diese Informationen anschließend auf dem NetWare 5 Server verfügbar sind. Damit Sie sich einen Eindruck davon machen können, wie die grafische Installation abläuft, sehen Sie in Abbildung 20.8 die notwendige Eingabe für den Baum-Namen und den Server Context, wenn ein NetWare 5 Server installiert wird. In Abbildung 20.9 ist dargestellt, wie die Auswahl des Zeitserver durchgeführt wird.

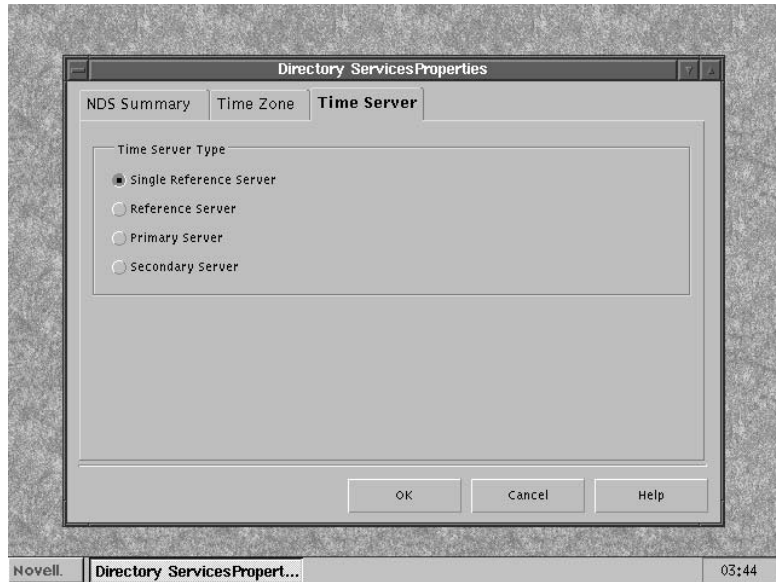
Abbildung 20.8
Installation
NetWare 5 Server



Man erkennt bereits an diesen kleinen Beispielen, daß die grafische Installation von NetWare 5 wesentliche Vorteile bietet. Ebenso wird die Verwaltung der Netzwerkumgebung mit Hilfe der ConsoleOne direkt am Server positive Effekte für den Netzwerkverwalter aufweisen. Ermöglicht werden diese neuen grafischen Oberflächen am Server durch die Unterstützung einer vollständigen Java-Plattform.

20.6 Java-Unterstützung

Abbildung 20.9
Auswahl des
Zeitservers



20.6 Java-Unterstützung

NetWare 5 wird mit der zur Zeit schnellsten Java-Umgebung ausgeliefert. Unabhängige Tests durch die Key Labs und der Einsatz der bekannten VolanoMark Benchmark haben NetWare 5 bestätigt, daß die Java Virtual Machine (JVM) um ein vielfaches schneller ist als zum Beispiel die Java-Implementierung auf einer Windows-NT-Server-Plattform. NetWare 5 wird mit den folgenden Java-basierenden Komponenten ausgeliefert:

- Novell JVM für NetWare und der Just in Time Compiler in Verbindung mit dem Java Naming Directory Interface (JNDI) und den Java Class Libraries erlauben es, Java-basierende Applets und Anwendungen am Server laufen zu lassen.
- Der NetWare Servertop stellt die grafische Oberfläche am Server zur Verfügung und beinhaltet ein Server-Management-Programm. Dieses wird automatisch bei der Installation von NetWare 5 installiert und beinhaltet ConsoleOne als Server Management Utility.

Der Novell Object Request Broker (ORB) stellt Möglichkeiten zur Verfügung, CORBA-konforme Java-basierende Anwendungen auf dem NetWare Server laufen zu lassen.

Die Novell JVM für NetWare besteht aus einer Vielzahl von NLMs, die es ermöglichen, daß auf dem NetWare Server Java-basierende An-

wendungen und Applets laufen können, einschließlich Multi-Threads-Anwendungen und Anwendungen, die eine grafische Oberfläche nutzen.

Auf der JVM kann jede Anwendung laufen, die als hundertprozentig Pure-Java-zertifiziert ist, so wie dies von JavaSoft beschrieben ist. Anwendungen, die keine hundertprozentige Pure-Java-Unterstützung bieten können, müssen für NetWare portiert werden. NetWare 5 beinhaltet den Just in Time Compiler (JIT) von Symantec, um die Performance von Java-basierenden Anwendungen zu erhöhen. Um Novell JVM einsetzen zu können, müssen mindestens 48 Mbyte Hauptspeicher eingebaut sein; man sollte jedoch mindestens 64 Mbyte installieren, wobei ich festgestellt haben, daß 128 Mbyte und mehr besser ist.

Das Hauptziel der Java-Technologie besteht in der Philosophie »Write Once, Run Anywhere«, die mit der Java-Implementierung unter NetWare 5 hervorragend unterstützt und realisiert worden ist. Um die Java-Techniken noch besser unterstützen zu können, hat sich Novell bereiterklärt, auf folgenden Gebieten die Java-Entwicklung fortzuführen:

- Java Telephony Services
- Java Management Services
- Java Internationalization Services
- Java Speech Services
- Java Directory Services
- Java Distributed Printing Services
- Java Workgroup Collaboration Services

Es sei nochmals erwähnt, daß die Java-Unterstützung von NetWare 5 die Möglichkeiten zur Verfügung stellt, Java Applets auf der Server Console zu aktivieren, Java-Anwendungen im X-Windows-Format einzusetzen – mit vollständiger Maus- und grafischer Unterstützung. Zudem können mehrere Java-Anwendungen aktiv auf dem Server eingesetzt werden, während zusätzlich andere Anwendungen ausgeführt werden.

Neben dieser Java-Technologie unterstützt NetWare 5 auch noch unterschiedliche Script-Sprachen, um damit einfach und bequem Anwendungen mit diesen Script-Sprachen erstellen zu können. Zu diesen Script-Sprachen gehören Perl5, NetBasic 6.0, NetBasic 7.0 und JavaScript.

20.7 Third-Party Add-ons

In Zusammenarbeit mit einer Vielzahl anderer Hersteller wird NetWare 5 mit Zusatzanwendungen ausgestattet, die eine vollständige NDS-Unterstützung bzw. -Integration bieten können. Im Lieferumfang von NetWare 5 ist Oracle8 in einer 5-User-Version enthalten, so daß es bei der Entwicklung von Datenbanken unter anderem möglich ist, durch die vollständige NDS-Integration die NDS zu nutzen, um den Zugriff auf die Unternehmensdatenbanken zu steuern.

Ein anderes Datenbanksystem, mit dem Novell schon seit langer Zeit arbeitet und entsprechende Unterstützung anbietet, ist Btrieve. Bestimmte Komponenten von NetWare nutzen Btrieve, um damit interne Aufgaben erledigen zu können.

Als Web-Server stellt Novell standardmäßig den FastTrack Server von Netscape zur Verfügung. Durch die Integration in die NDS werden das Arbeiten und die Verwaltung wesentlich einfacher. Zu den unterstützten erweiterten Technologien des FastTrack Server zählen NDS, LDAP, Common Gateway Interface (CGI), PERL und NetBasic.

20.8 Cluster-Technologie

Mit Einführung von NetWare 5 wird die Weiterentwicklung von NetWare 4, SFT III, nicht mehr durchgeführt. Um jedoch zukünftig die Sicherheitsanforderungen erfüllen und noch mehr Flexibilität erreichen zu können, geht Novell bei seinen neuen Entwicklungen sehr stark in Richtung Cluster-Technologie. Um jedoch auch preiswertere Sicherheitsmechanismen zur Verfügung stellen zu können, ist Novell zusätzlich mit Vinca eine Kooperation eingegangen: Man wird die sogenannte Standby-Server-Technologie weiter forcieren. Auf die Standby-Server-Technologie soll jedoch an dieser Stelle nicht näher eingegangen werden.

Ziel der Cluster-Technologie ist es, ein System aufzubauen, das folgende Funktionen erfüllen kann:

- Verbesserte Verfügbarkeit
- Verbesserte Performance
- Stellt sich wie ein System dar
- Bietet hohe Skalierbarkeit
- Unterstützung von Load Balancing
- Einfache Verwaltung

20 NetWare 5

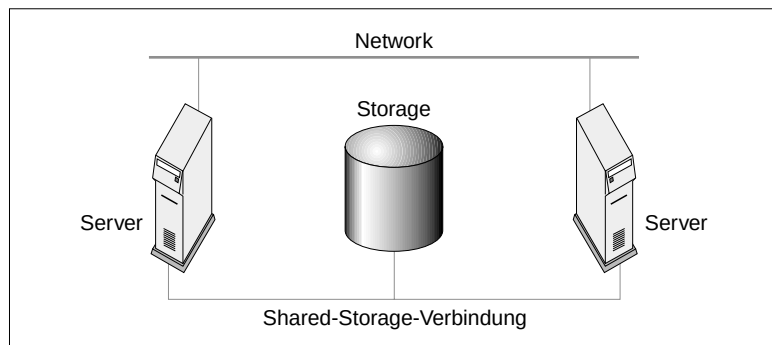
Durch die Entwicklung der Cluster-Technologie beabsichtigt Novell eine Systemlösung zu liefern, die gewährleistet, daß das System 24 Stunden am Tag, 7 Tage in der Woche und 365 Tage im Jahr (und wenn ein Schaltjahr ist, eben 366 Tage) verfügbar ist.

Die Planung von Novell sieht vor, die Cluster-Technologie in zwei Phasen zu implementieren. Der Codename für die Cluster-Technologie ist Orion. Die erste Phase mit Orion I ist verfügbar, und Orion II steht kurz vor der Auslieferung.

Orion I

In Abbildung 20.10 ist dargestellt, wie man sich den Aufbau von Orion I vorstellen muß. Es handelt sich um eine Cluster-Lösung für zwei Server.

Abbildung 20.10
Orion I



Zu beachten ist dabei, daß die Server zwar gemeinsam auf den Storage-Pool, aber nicht gemeinsam auf den gleichen Plattenbereich zugreifen, d.h., jedem Server sind seine eigenen Volumes zugewiesen, mit denen dieser dann arbeiten muß. Der Schreib- und Lesevorgang auf die Volumes kann immer nur vom entsprechenden Server aus durchgeführt werden. Daneben gilt für Orion I, daß beide Server gleichzeitig aktiv sind und Dienste im Netzwerk zur Verfügung stellen können, daß das Umschalten auf den anderen Server automatisch erfolgt und deshalb kein manueller Eingriff notwendig ist und daß das gesamte System gegen Hard- und Software-Ausfälle geschützt ist. Ein wesentlicher Vorteil gegenüber SFT III ist auch, daß die Hardware der beiden Server nicht identisch sein muß. Die Kosten für das Gesamtsystem sind im Vergleich zu einer SFT-III-Lösung wesentlich günstiger, da man zwei gleichzeitig aktive Server hat im Gegensatz zu SFT III, bei der ein Server aktiv ist und der zweite Server standby auf seinen Einsatz warten muß. Weitere Vorteile von Orion I sind:

20.8 Cluster-Technologie

- Unterstützung für einen gemeinsamen Storage Pool
- Unterstützung des Wiederanlaufs von Anwendungen
- Unterstützung von Symmetric Multiprocessing (SMP)

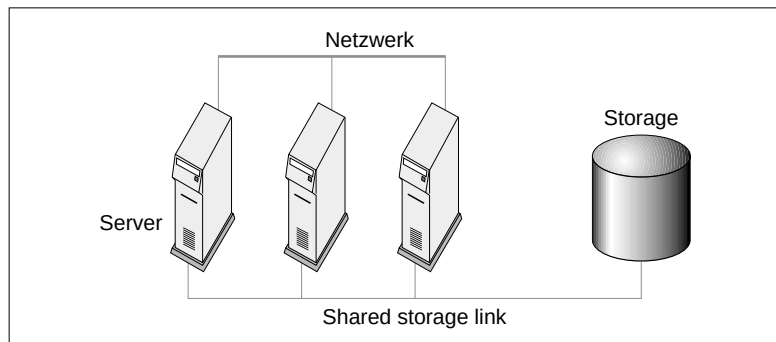
Zu den Einschränkungen von Orion I gehören:

- Beim Ausfall eines Servers ist der Inhalt der Cache-Informationen, die noch nicht auf die Platte des Servers geschrieben worden sind, verloren. Nur die Daten auf den Platten des ausgefallenen Servers können durch den anderen Server bedient werden.
- Es handelt sich um kein Single System Image (SSI), so wie dies bei SFT III der Fall ist.
- Es werden nur zwei Server unterstützt.
- Es gibt noch kein dynamisches Load Balancing.

Orion II

Abbildung 20.11 zeigt, wie man sich die Multiple-Server-Cluster-Technologie von Orion II vorstellen muß. Die Anzahl der Server, die unter Orion II unterstützt werden, hängt von der eingesetzten Shared-Storage-Lösung ab. So bietet z.B. der Fiber Channel von Compaq die Unterstützung von maximal sieben Servern.

Abbildung 20.11
Orion II

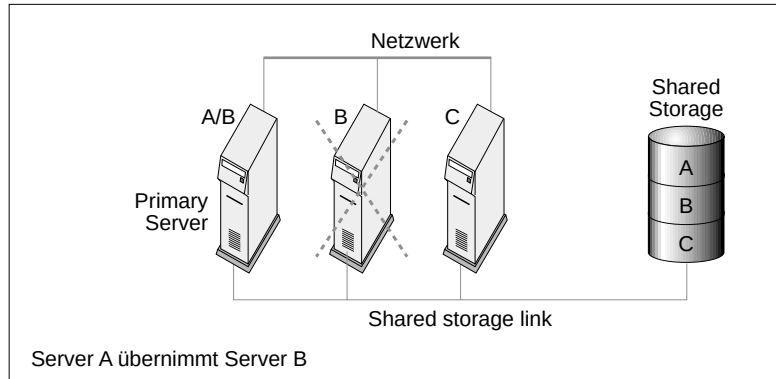


Genau wie bei Orion I sind die Server zwar am gleichen Storage-Pool angeschlossen, jedoch sind jedem Server die eigenen Volumes zugewiesen, auf die von den anderen Servern nicht zugegriffen werden kann. Nur der Server, dem die Volumes zugewiesen sind, ist in der Lage, im Normalbetrieb lesend und schreibend auf die Volumes zuzugreifen.

In Abbildung 20.12 ist dargestellt, was im Falle eines Server-Ausfalls passiert.

20 NetWare 5

Abbildung 20.12
Server-Ausfall
unter Orion II



Wenn man davon ausgeht, daß, wie in Abbildung 20.12 dargestellt, Server B ausfällt, dann wird ein Entscheidungsprozeß durchgeführt, der bestimmt, wer die Aufgaben des ausgefallenen Servers B übernehmen soll. Wird entschieden, daß diese Aufgabe von Server A übernommen wird, dann wird Server A neuer Eigentümer der Volumes, die bislang von Server B verwaltet worden sind. Wenn auch noch Server C ausfällt, dann muß Server A auch noch die Verwaltung der Volumes von Server C übernehmen. Sobald ein ausgefallener Server wieder verfügbar ist, erhält dieser automatisch die Kontrolle für seine Volumes zurück. Das alles passiert für den Benutzer vollkommen transparent.

Der wesentliche Unterschied von Orion I zu Orion II besteht in der größeren Anzahl unterstützter Server in einem Cluster und der Tatsache, daß alle Server im Cluster gleichzeitig aktiv sind und daß man den Mount-Vorgang für die Volumes nochmals beschleunigt hat.

Die Einschränkungen für Orion II sind:

- Beim Ausfall eines Servers ist der Inhalt der Cache-Informationen, die noch nicht auf die Platte des Servers geschrieben worden sind, verloren. Nur die Daten auf den Platten des ausgefallenen Servers können durch den anderen Server bedient werden.
- Es handelt sich um kein Single System Image (SSI), so wie dies bei SFT III der Fall ist.
- Es gibt noch kein dynamisches Load Balancing.

Die nachfolgende Tabelle zeigt die wichtigsten Eigenschaften, die Novell hinsichtlich Ausfallsicherheit in Verbindung mit SFT III, Standby Server und Cluster-Technologie bieten kann. Zusätzlich findet man noch die Vergleichswerte zum Microsoft-Cluster.

20.8 Cluster-Technologie

*Tabelle 20.1
Vergleich der
Lösungen zur
Steigerung der
Ausfallsicherheit*

	MS Cluster Server	Novell SFT III	Novel Standby Server	Orion Phase I	Orion Phase II
Anzahl Server im Cluster	2	2	2 oder mehr	2	2 oder mehr
Kommunikations-mechanismen für die Server untereinander	Ethernet	Mirrored server link	Ethernet und andere Standardnetzwerkadapter	Ethernet und andere Standardnetzwerkadapter	Ethernet und andere Standardnetzwerkadapter
TCP/IP-Unterstützung	Ja	Ja	Ja	Ja	Ja
Unterstützung TCP/SPX	Nein	Ja	Ja	Ja	Ja
Shared Disk	Ja SCSI	Nein	Nein	Ja SCSI und Fibre	Ja SCSI, Fibre und SSA
Unterstützung für den Einsatz lokaler Platten	Nein	Ja	Ja	Nein	Ja
Wiederanbindung Workstation	Automatisch	Automatisch und sofort	Automatisch	Automatisch	Automatisch
Unterstützung großer Entfernungen	Nein	Ja	Ja	Ja	Ja
Flexible Hardware-Konfiguration	Nein	Nein	Ja	Ja	Ja
Single System Image	Nein	Ja	Nein	Nein	Nein
Seit mehr als 2 Jahren am Markt	Nein	Ja	Ja	Nein	Nein

Die zukünftige Weiterentwicklung für die Cluster-Technologie stellt sich Novell wie folgt vor:

- Dynamisches Load Balancing
- Noch größere Skalierbarkeit
- Unterstützung verteilter Java-Anwendungen
- Shared-Memory-Unterstützung
- Wide Area Cluster (WAC)
- Verbessertes Disaster Recovery

Es gibt jedoch noch keine definitiven Termine, wann mit diesen verbesserten Lösungen zu rechnen ist. Es ist auch geplant, die Cluster-Technologie Orion I und Orion II sowohl für NetWare 4 als auch für NetWare 5 verfügbar zu machen.

Dieses Kapitel hat gezeigt, mit welchen neuen Konzepten und Systemen Novell das neue Betriebssystem NetWare 5 ausgestattet hat und in welche Richtung zukünftige Entwicklungen gehen werden. Ein anderer wichtiger Hersteller von Netzwerkbetriebssystemen ist Microsoft mit Windows NT Workstation bzw. Windows NT Server. Die nächsten Kapitel sind deshalb dafür gedacht, diese beiden Systeme näher zu betrachten. Danach möchte ich noch auf die Entwicklungen eingehen, die Microsoft im Zuge der Windows-NT-5.0-Technologie realisiert.

21 NDS für andere Plattformen

Das Ziel von Novell ist es, Directory Services für eine Vielzahl anderer wichtiger Plattformen zur Verfügung zu stellen. Hierzu zählen zur Zeit unter anderem Windows NT Server, SUN Solaris, Linux und OS/390. Für Windows NT Server und SUN Solaris hat Novell die Portierung der NDS selbst durchgeführt. Für OS/390 ist IBM verantwortlich, und für Linux wird die Portierung von Caldera durchgeführt. In diesem Kapitel sollen die beiden Produkte NDS for NT (NDS4NT) und NDS for Solaris (NDS4SOLARIS) näher dargestellt werden. Beide Produkte stehen derzeit in der Version 2.0 zur Verfügung. Es stellt sich die Frage, wieso NDS4SOLARIS bereits in der Version 2.0 bereitgestellt wird. Die Erklärung ist ganz einfach: NDS4SOLARIS ist im Prinzip die gleiche Entwicklung wie NDS4NT 2.0, deshalb hat man hierfür gleich dieselbe Versionsnummer vergeben.

21.1 NDS for NT

Die Anforderung, in einem heterogenen Netzwerk sowohl NetWare als auch NT Server zu betreiben, wird immer größer. Mit den Novell Directory Services wird ein einfaches, aber leistungsfähiges Werkzeug zur Verfügung gestellt, um für diese heterogene Umgebung einen Single Point of Administration durchführen zu können. Zudem hat der Benutzer den Single Point of Login, wodurch das Netzwerk zuverlässiger, skalierbarer und sicherer wird. Als weitere Vorteile können aufgeführt werden:

- Die Entwicklung von NT-Anwendungen wird einfacher, da man sich um das NT-Server-Management nicht mehr kümmern muß.
- Die Verfügbarkeit und Produktivität wird erhöht, da die doppelte Verwaltung von Benutzer-Accounts und das doppelte Anmelden am System (NetWare und NT Server) entfällt. NDS for NT ist die erste Anwendung, die einen Single Sign-on sowohl für NetWare als auch für NT-Server-Benutzer zur Verfügung stellt.

Novell hat NDS for NT entwickelt, um Firmen eine effektive Verwaltung der NT Server und NT-Applikationen zu ermöglichen. Durch NDS for NT wird die Domänen-Datenbank in die NDS integriert. Auf diese Art und Weise wird es dem Netzwerkverwalter ermöglicht, alle Funktionen der NT-Domäne über die NDS zu verwalten. Zudem wurde das Konzept so ausgelegt, daß jede Anwendung, die Zugriff auf die NT-Domänen-Informationen benötigt, diese über die NDS erhält, ohne daß an der Anwendung etwas geändert werden muß.

21 NDS für andere Plattformen

In der Version 2.x benötigt NDS for NT noch mindestens einen NetWare Server, um eingerichtet werden zu können. In einem Folge-Release soll jedoch NDS for NT als native Lösung zur Verfügung gestellt werden, bei der es dann möglich ist, NDS for NT auf einem NT Server zu installieren, ohne hierfür einen NetWare Server im Hintergrund zu haben.

Zu beachten ist, daß NDS for NT nur auf NT-Servern installiert werden kann, die als PDC (Primary Domain Controller) oder BDC (Backup Domain Controller) eingerichtet worden sind. NDS for NT kann somit nicht auf Member-Servern (Standalone Server) oder gar NT Workstations installiert werden. In einem bereits installierten NT-Umfeld müssen keinerlei Änderungen auf den Workstations durchgeführt werden. Aus der Sicht der Microsoft Clients oder Microsoft-Anwendungen, die über Domänenmechanismen arbeiten, bedeutet dies, daß sich für diese Umgebungen nichts ändert. Das heißt, für diese Umgebungen bleibt alles so, wie es war, da der Einsatz von NDS for NT für diese Umgebung transparent bleibt. Alle Workstations und Anwendungen funktionieren genauso weiter, wie dies vor der Installation von NDS for NT auch der Fall war.

Die Vereinfachung des Netzwerkzugriffs in einer NetWare-/Windows-NT-Umgebung wird unter anderem durch die einzige globale Identität erreicht, die für jeden Benutzer im gesamten Netzwerk existiert. Als Ergebnis davon muß der Benutzer beim Anmelden seinen Namen und sein Paßwort nur einmal eingeben. So muß nach der Installation von NDS for NT nur ein Benutzer-Account eingerichtet werden, wohingegen ohne NDS for NT ein Benutzer-Account unter NetWare und ein Benutzer-Account unter Windows NT gepflegt werden müßte. Ebenso wird es einfacher, mit Einführung von NDS for NT die Paßwörter der Benutzer zu pflegen. Ohne NDS for NT hat jeder Benutzer-Account unter NetWare und unter Windows NT jeweils ein eigenes Paßwort, das sich jeder Benutzer merken und beim Anmeldevorgang eingeben muß.

NDS for NT erlaubt es auch, NDS-Replicas auf einen Windows NT Server abzuspeichern. Dadurch kann zusätzliche Ausfallsicherheit gewährt werden. Außerdem dient dies unter anderem auch dazu, den Zugriff auf NDS-Informationen zu erhöhen, wenn z.B. in der Außenstelle nur ein Windows NT Server installiert ist, den man mit NDS for NT ausgestattet hat. Da auf diesem Windows NT Server NDS-Replicas abgelegt werden können, müssen notwendige Informationen der NDS zur Authentifizierung nicht über die WAN-Strecke transportiert werden, da diese direkt über die Replica auf dem Windows NT Server bedient werden können.

21.1.1 Arbeitsweise von NDS for NT

Nach der Installation von NDS for NT auf dem Windows NT Server werden alle Benutzer- und Anwendungsanforderungen, die an die Windows-NT-Domänendatenbank gestellt werden, an die NDS weitergereicht. NDS for NT ist dafür verantwortlich, die »Umleitung« der Anforderungen an die NDS durchzuführen. Die Client Software und die Anwendungen müssen hierbei nicht modifiziert werden – dies ist einer der großen Vorteile, die damit verbunden sind. Die Praxis zeigt, daß mit Installation von NDS for NT Anwendungen weiterhin so arbeiten, als wäre eine »echte« Windows-NT-Server-Domäne vorhanden. Um die Arbeitsweise von NDS for NT besser zu verstehen, ist es notwendig, den Authentifizierungsvorgang von NDS for NT näher zu betrachten.

Sowohl Windows NT Workstations als auch Windows NT Server haben eine Sicherheitsdatenbank, die auch als SAM-Datenbank (Security Account Manager) bezeichnet wird. Die SAM-Datenbank wird in einem sicheren Bereich der Windows NT Registry gespeichert. Auf die Daten der SAM-Datenbank kann nur auf zweierlei Arten zugegriffen werden, wobei für NDS for NT nur eine Art von Interesse ist:

Verwendung der Windows NT Application Programming Interfaces (APIs), um die SAM-Datenbank zu lesen oder zu schreiben.

Wenn eine Anwendung die Windows NT APIs benutzt, um lesend und schreibend auf die SAM-Datenbank zugreifen zu können, dann werden hierfür zwei DLLs benutzt: SAMSRV.DLL und SAMLIB.DLL. Die Kommunikation der Anwendung mit der SAM-Datenbank wird dabei wie folgt durchgeführt:

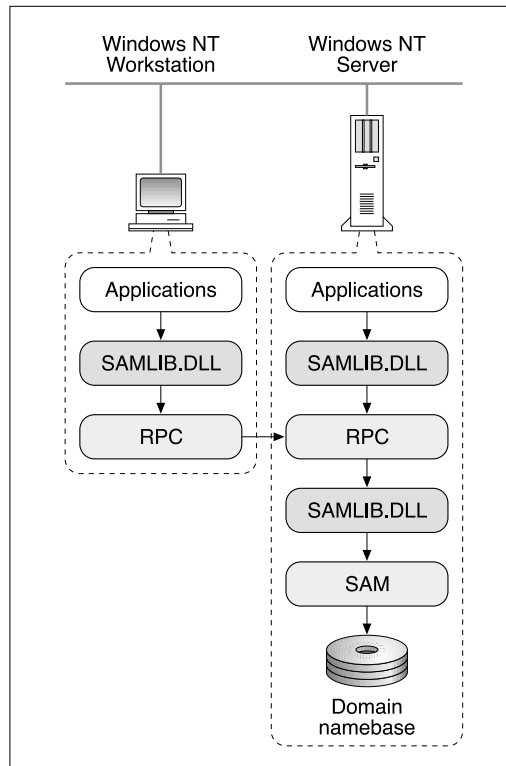
- Die Anwendung führt einen API Call durch, um Benutzer, Gruppen, Server oder Workstations in der SAM-Datenbank zu erstellen, zu löschen oder zu ändern.
- Intern wendet sich Windows NT an die SAMLIB.DLL, um die Anforderung zu erfüllen.
- Die SAMLIB.DLL hingegen schickt sogenannte Remote Procedure Calls (RPCs) an die SAMSRV.DLL, um die Anforderungen auszuführen.
- Die SAMSRV.DLL führt die Kommunikation mit der SAM-Datenbank durch, damit die Änderungen oder ganz einfachen Anfragen an die SAM-Datenbank durchgeführt werden können.

In Abbildung 21.1 ist dargestellt, wie die Kommunikation dieser beiden Module aus der Sicht eines Windows NT Server und aus der Sicht einer Windows NT Workstation aussieht, um auf die SAM-Da-

21 NDS für andere Plattformen

tenbank eines Windows NT Server zuzugreifen, wenn dieser als PDC bzw. BDC definiert ist. Während dieses Vorgangs schreibt und liest nur die SAMSRV.DLL Informationen aus der SAM-Datenbank. In einer Domänen-Konfiguration ist die SAMSRV.DLL auf dem PDC bzw. BDC vorhanden.

Abbildung 21.1
Kommunikation
mit der Domäne



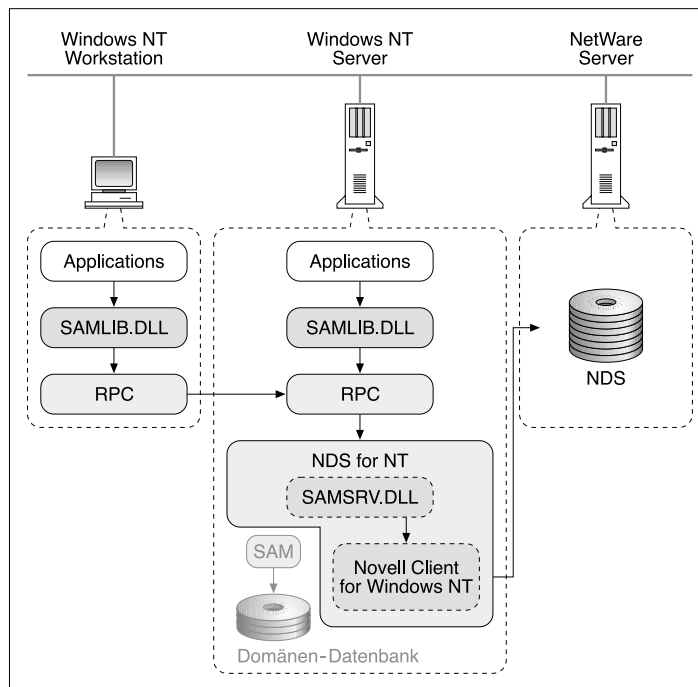
Die Rolle der SAMSRV.DLL unter NDS for NT sieht dabei wie folgt aus:

Wenn eine Domäne eingerichtet wird, dann hat Windows NT auf jeder Workstation und jedem Server in der Domäne sowohl die SAMSRV.DLL als auch die SAMLIB.DLL abgelegt. Jedoch wird nur die SAMSRV.DLL auf dem PDC bzw. BDC dazu verwendet, um die Benutzerauthentifizierung in der Domäne durchzuführen. Wenn sich ein Benutzer in der Domäne anmeldet, dann authentifiziert sich der Client des Benutzers an der Domäne, indem ein RPC-Aufruf an die SAMSRV.DLL am PDC bzw. BDC gegeben wird.

21.1 NDS for NT**NDS for NT und
die SAMSRV.DLL**

Nach diesen kurzen Erläuterungen fällt es nicht mehr schwer, das Prinzip von NDS for NT zu verstehen. NDS for NT ermöglicht es, daß ein PDC bzw. BDC in der Lage ist, mit einer anderen SAM-Datenbank zu arbeiten. Die Kommunikation mit der SAM-Datenbank erfolgt ausschließlich über die SAMSRV.DLL. Dies macht sich NDS for NT zunutze, indem Novell die SAMSRV.DLL so umgeschrieben hat, daß der Zugriff nicht mehr auf die SAM-Datenbank erfolgt, sondern auf die NDS zugegriffen wird. Dadurch werden alle Anforderungen zur Authentifizierung und Management-Anforderungen umgeleitet zur NDS und nicht mehr direkt von der SAM-Datenbank bedient. In Abbildung 21.2 ist dargestellt, wie die neue PDC- bzw. BDC-Architektur unter NDS for NT aussieht.

Abbildung 21.2
NDS-for-NT-
Architektur



Zusätzliche Objekte und Erweiterungen der Properties bestimmter Objekte in der NDS gewähren die volle Funktionsfähigkeit von NDS for NT in Verbindung mit allen Domänenanforderungen, die von Clients gestellt werden. Es ist sogar möglich, die Verwaltung der »Domäne« wie gewohnt über den Benutzermanager für Domänen durchzuführen. Statt jedoch in die SAM-Datenbank zu schreiben, werden alle Änderungen der Domäne in der NDS durchgeführt. Es gibt jedoch einige Besonderheiten zwischen Windows NT Server und NetWare, die durch den Einsatz von NDS for NT gelöst werden mußten.

21.1.2 Verwendung von Paßwörtern unter NDS for NT

Wenn NDS for NT die NDS dazu verwendet, um alle Domäneninformationen zu erhalten, dann wird ein Benutzerobjekt für jeden Benutzer nur noch einmal eingerichtet. Ab diesem Zeitpunkt kann dieses Benutzerobjekt verwendet werden, um sowohl unter NetWare als auch unter Windows NT Server den Anmeldevorgang durchführen zu können, und zwar automatisch mit nur einer Anmeldung. Hierzu werden jedoch zwei Paßwörter benötigt: eines für NetWare und eines für Windows NT Server. Dies liegt darin begründet, daß NetWare und Windows NT unterschiedliche Methoden zur Verwendung und Handhabung von Paßwörtern verwenden.

Paßwörter unter Windows NT

Wenn ein Windows NT Server (PDC oder BDC) die Authentifizierung für einen Benutzer durchführt, dann wird ein Hash-Algorithmus verwendet, um das Paßwort am Client zu verschlüsseln, bevor dieses zum Server weitergeleitet wird. Der Server empfängt das verschlüsselte Paßwort und vergleicht es mit dem abgespeicherten Paßwort, das mit dem gleichen Hash-Algorithmus erzeugt worden ist. Ist das Paßwort gültig, wird der Zugang zum Server erlaubt. Ist das Paßwort nicht richtig, wird der Zugang zum Server untersagt. Der Windows NT Server kann ein mit dem Hash-Algorithmus abgespeichertes Paßwort nicht entschlüsseln, d.h. der Vorgang ist nicht reversibel. Der Server vergleicht nur zwei Hash-Informationen miteinander, um festzustellen, ob der Benutzer das Paßwort korrekt eingegeben hat.

Paßwörter unter NetWare

Für die Authentifizierung unter NetWare in der NDS muß auch der Benutzer ein Paßwort eingeben. An dieser Stelle tritt jedoch der Unterschied zum Windows NT Server bzw. zur Authentifizierung in einer Windows-NT-Domäne auf. Auch die NDS nutzt einen Hash-Algorithmus für das Paßwort, um die Identität des Benutzers festzustellen, es wird jedoch anschließend der Private Key des Benutzers auf den Client der Workstation übertragen. Nachdem der Private Key übertragen ist, kann der Anmeldeprozeß in der NDS vollständig durchgeführt werden, indem sogenannte Credentials erzeugt werden. Diese Credentials hängen dabei unter anderem von der Anmeldesession ab und gewährleisten dadurch, daß die Credentials wirklich eineindeutig sind, um somit Manipulationen beim Anmeldevorgang unterbinden zu können.

NDS verwendet diese erzeugten Credentials anschließend auch dazu, um einen Benutzer transparent auf andere Server zu authentifizieren, wenn Zugriffe auf Server innerhalb eines NDS-Baumes durchgeführt werden, an denen der Benutzer bislang noch nicht authentifiziert worden ist. Auf diese Art und Weise wird sichergestellt,

21.1 NDS for NT

daß der Benutzer sein Paßwort nur einmal eingeben muß, aber zur weiteren Authentifizierung keine Paßwortübertragungen durchgeführt werden, um dadurch die größtmögliche Sicherheit gewährleisten zu können.

Für die Authentifizierung in der NDS verwendet Novell ein RSA-Verfahren (Rivest-Shamir-Adleman-Algorithmus). RSA basiert dabei auf einem Private-Public-Key-Schlüsselpaar, um diese Credentials zu erzeugen. Bevor die Credentials erzeugt werden können, muß der Private Key auf den Client geladen werden, wie vorher bereits beschrieben.

Verwaltung beider Paßwort- typen

Da Windows NT und die NDS (NetWare) unterschiedliche Hash-Algorithmen verwenden, um einen Benutzer zu authentifizieren, muß NDS for NT jedes Paßwort separat behandeln. Wenn ein Benutzer sowohl in der NDS als auch in einer Domäne authentifiziert werden soll, dann speichert NDS for NT zwei Paßwörter: ein Paßwort für die NDS-Authentifizierung und ein Paßwort für die Authentifizierung in der Domäne. Diese Paßwörter werden im jeweiligen Benutzerobjekt in der NDS gespeichert.

Um zu vermeiden, daß der Anwender zwei Paßwörter eingeben muß, stellt Novell zwei Lösungen zur Verfügung.

Mit dem Einsatz von NDS for NT kann über das grafische Administrationsprogramm NWADMIN (bzw. NWADM32) das Paßwort eines Benutzers geändert und synchronisiert werden, so daß in der NDS und unter Windows NT das gleiche Paßwort verwendet wird.

Wenn ein Benutzer sein Paßwort ändert, sorgt NDS for NT für die notwendige Synchronisation der Paßwörter.

Mit NDS for NT ist es auch unerheblich, wie vielen Domänen ein Benutzer angehört, der Benutzer hat immer das gleiche Paßwort und nur einen Benutzer-Account.

21.1.3 Security IDs unter NDS for NT

Für die Sicherheit unter Windows NT wird eine Security ID (SID) und Resource ID (RID) verwendet, um Benutzer und Ressourcen zu identifizieren, die Zugriff auf das Netzwerk benötigen. Wenn einem Objekt in einer Windows-NT-Umgebung z.B. Rechte auf Dateien gegeben werden, verwendet Windows NT Server die SID bzw. RID, um das Objekt zu identifizieren. Diese Security IDs bieten auch die Berechtigung, Netzwerkdienste zu nutzen. Da die SAM-Datenbank unter NDS for NT nicht mehr verwendet wird, werden die SIDs und RIDs für Domänen, die über die NDS gepflegt werden, auch in der NDS gespeichert. Wenn ein Dienst einen Request durchführt, um zu prüfen,

21 NDS für andere Plattformen

ob der Benutzer bereits in der Domäne authentifiziert ist, wird die SID des Benutzers aus der NDS gelesen und ein Token generiert, um die weiteren Sicherheitsprüfungen durchführen zu können.

21.1.4 Installation NDS for NT

Für die Installation von NDS for NT müssen die folgenden Voraussetzungen geschaffen werden:

- PDC oder BDC unter Windows NT Server 4.0 mit Service 3 oder höher, Windows NT Server 3.51 mit Service Pack 5.
- Auf dem Windows NT Server muß das File System NTFS eingerichtet sein.
- Wenn auf dem Windows NT Server eine Replica gespeichert werden soll, dann sollte der Server mit mindestens 32 Mbyte Hauptspeicher ausgestattet sein, besser sind jedoch 64 Mbyte Hauptspeicher oder mehr.

Für die Installation von NDS for NT muß man administrative Rechte sowohl auf dem Windows NT Server als auch in der NDS haben.

Zur Installation von NDS for NT muß genügend freier Plattenplatz existieren. Hierzu sollten die aktuellen Spezifikationen gelesen werden, da sich dies von Zeit zu Zeit ändert, je nachdem, welche Version von NDS for NT eingesetzt wird.

Wenn in einem Netzwerk auch NetWare 4.11 integriert ist, dann muß der Support Pack 6 oder höher installiert sein.

NDS for NT unterstützt auch NetWare 5 – entweder über IPX- oder IP-Protokoll.

NDS for NT sollte zuerst auf dem PDC und dann auf den BDCs installiert werden.

Um eine reibungslose Domänenverwaltung zu gewährleisten, muß NDS for NT innerhalb einer Domäne sowohl auf dem PDC als auch auf allen BDCs eingerichtet werden.

Die Installation von NDS for NT ist relativ unproblematisch, wenn die vorher erwähnten Voraussetzungen eingehalten werden. Die Installation von NDS for NT läuft dabei in unterschiedlichen Phasen ab, die nachfolgend näher erläutert werden sollen:

Zur Installation von NDS for NT muß man auf dem Windows NT Server als Administrator oder Benutzer mit administrativen Rechten angemeldet sein. Anschließend startet man das Programm WINSETUP (für den Fall, daß der Autorun-Mechanismus nach dem Einlegen der CD nicht funktionieren sollte). Wird die NDS for NT Option ausge-

21.1 NDS for NT

wählt, werden die notwendigen Dateien auf den Windows NT Server kopiert (einschließlich einer neuen SAMSRV.DLL). Bevor jedoch mit der weiteren Installation von NDS for NT begonnen werden kann, muß ein spezieller NetWare Client auf den Windows NT Server installiert werden. Dieser spezielle Client ermöglicht es, daß die SAM-Anfragen an den Windows NT Server an die NDS weitergeleitet werden. Nach der Installation des neuen Clients muß der Server neu gebootet werden.

Nach dem Neustart wird der Anmeldevorgang am NT Server (Administrator-Berechtigter) und in der NDS (Admin-Berechtigter auf [Root]) notwendig. Ist dies erfolgreich geschehen, wird automatisch der Object Wizard (SAMMIG.EXE) gestartet. Über den Object Wizard wird es ermöglicht:

- Objekte der Domäne in die NDS zu übernehmen.
- eine NDS-Replica auf einen Windows NT Server zu installieren.
- wenn NDS for NT bereits installiert worden ist, diese über den Object Wizard auch wieder zu entfernen bzw. auch nur die Replica zu entfernen.

Es erfolgt dann die Aufforderung, den Baum auszuwählen, in dem NDS for NT integriert werden soll. Daraufhin wird geprüft, ob das NDS-Schema bereits erweitert worden ist. Ist dies nicht geschehen, muß die Erweiterung des NDS-Schemas bestätigt werden. Als nächstes muß der Container ausgewählt werden, in dem das Domänenobjekt installiert werden soll. Zusätzlich muß ein Container festgelegt werden, in dem neue Benutzer eingerichtet werden sollen. Diese Angabe wird nur benötigt, damit NDS for NT in der Lage ist, NDS-Benutzer-Objekte einzurichten, wenn diese über den Domänen-Manager für Benutzer durchgeführt wird. Dabei ist es nicht notwendig, daß der Context für das Domänenobjekt mit dem Default User Context übereinstimmt, da diese beiden Angaben vollkommen unabhängig voneinander sind. Bei diesen Angaben sollte auch darauf geachtet werden, daß die Option »Force password synch« aktiviert ist. Dies ist notwendig, damit eine Paßwortsynchronisation zwischen dem NDS- und dem Windows-NT-Server-Paßwort durchgeführt wird.

Als nächsten bekommt man die Option, die NDS nach bestehenden Benutzern zu durchsuchen, die den gleichen Namen haben wie Benutzer in der Domäne. Hierzu muß der Context angegeben werden, ab dem die Suche durchgeführt werden soll. Nach einem erfolgreichen Suchvorgang erhält man für die einzelnen Benutzerobjekte in einer Tabelle folgende Möglichkeiten angeboten, wie mit den Benutzer-Accounts verfahren werden soll:

21 NDS für andere Plattformen

- **Create As:** Einen Domänenbenutzer-Account mit diesem Namen in der NDS einrichten (d.h. es wurde kein dazugehöriger Benutzername in der NDS gefunden).
- **Associate With:** Es wurde ein NDS-Benutzer-Account gefunden. Die beiden Objekte werden zusammengeführt, d.h., es erfolgt ein Merge der beiden Objekte. Dieser Merge vereinfacht es somit auch, wenn mehrere Domänen nacheinander in die NDS integriert werden sollen.
- **Don't Move:** In diesem Falle wird der Benutzer-Account der Domäne nicht in die NDS übernommen.

Nachdem die Objekte transferiert worden sind, erhält man eine Statistik, aus der zu ersehen ist, wie viele Benutzer-Accounts, Gruppen-Accounts und Computer-Konten transferiert worden sind.

Um die vollständige Funktionsfähigkeit von NDS for NT im Vergleich zur Domänen-Arbeitsweise aufrechterhalten zu können, ist es notwendig, daß NDS for NT auch in der Lage ist, Computer-Konten zu verwalten. Hierzu gehört auch die Option, globale und lokale Gruppen verwalten zu können. All dies erfolgt über das spezielle für NDS for NT eingerichtete Domänenobjekt. Das heißt, nach der Installation von NDS for NT existiert ein spezielles Domänenobjekt, in dem alle diese Informationen eingerichtet und verwaltet werden.

Am Schluß erhält man die Möglichkeit, eine Replica auf den Windows NT Server zu installieren. Wird auf dem Windows NT Server eine Replica installiert, dann erscheint der Windows NT Server als Server-Objekt im gleichen Container, in dem auch das Mbyte eingerichtet worden ist.

Wenn die Installation vollkommen abgeschlossen ist, muß man den Windows NT Server neu starten; erst dann wird die neue SAMSRV.DLL aktiviert, und alle Anforderung an die Domäne werden nicht an die SAM-Datenbank, sondern an die NDS weitergeleitet.

Damit die Installation vollständig abgeschlossen werden kann, müssen noch die NT Administration Tools eingerichtet werden. Hierzu gehören:

- **Domain Object Wizard:** Hiermit können NDS-Replicas hinzugefügt oder entfernt werden. Es ist aber auch möglich, NDS for NT vom Windows NT Server vollständig zu entfernen.
- **NDS Manager:** Hiermit können NDS-Partitionen und -Replicas eingerichtet und verwaltet werden.
- **NetWare Administrator for Windows NT:** Hiermit erfolgt die Verwaltung der NDS, einschließlich der gesamten Umgebungen für Domänen und alles, was dazugehört.

21.1 NDS for NT

- Novell Login: Dieses Tool kann genutzt werden, um sich in der NDS und am NT Server mit einem Namen und einem Paßwort anzumelden (sofern die Paßwörter synchronisiert worden sind).
- Novell Send Message: Hiermit können kurze Nachrichten an Benutzer geschickt werden, die in der NDS angemeldet sind.

Um die Installation durchführen zu können, wählt man im Hauptmenü, das nach dem automatischen Starten der NDS for NT CD aktiviert oder durch den Aufruf ADMNSETUP.EXE erreicht wird, die Option Admin Utilities aus.

Es wurde bereits mehrfach darauf hingewiesen, daß NDS for NT vor allem darauf abzielt, die Netzwerkverwaltung in einer heterogenen NetWare- und Windows-NT-Server-Domänen-Umgebung zu vereinfachen. Zur Verwaltung von Benutzern dient dazu entweder das Verwaltungsprogramm NWADMN32.EXE oder wie gewohnt der Benutzermanager für Domänen. In der Regel wird man sich jedoch auf den Einsatz von NWADMN32.EXE beschränken, da dieses NetWare Tool doch die meisten und elegantesten Möglichkeiten bietet. Beim Einsatz von NWADMN32.EXE muß man dabei zwei unterschiedliche Arten unterscheiden, wie eine Benutzerverwaltung durchgeführt werden kann:

- Domänenorientierte Verwaltung
- Benutzerorientierte Verwaltung

Es sei nochmals darauf hingewiesen, daß zur Verwaltung der Benutzer mit dem NWAdmin-Tool zuerst ein Benutzerobjekt in der NDS existieren muß oder neu einzurichten ist. Dabei muß das Benutzerobjekt nicht im gleichen Container existieren, in dem das Domänenobjekt für die Verwaltung der Windows-NT-Server-Domäne installiert worden ist.

Domänenorientierte Verwaltung

Bei diesem Ansatz wird das Domänenobjekt in der NDS ausgewählt, zu dem der Domänen-Benutzer hinzugefügt werden soll, und man wählt die Option Details, um weitermachen zu können. Jetzt wählt man die Option Domain Members aus der Liste der Detail Page und drückt die Option Add. Man wählt daraufhin den Benutzer aus der NDS aus, der der Domäne hinzugefügt werden soll (man kann mit den herkömmlichen NWAdmin-Mechanismen auch mehrere Benutzerobjekte gleichzeitig auswählen). Ein erfolgreiches Hinzufügen kann ganz einfach überprüft werden, indem man auf dem NT Server den Benutzermanager für Domänen aufruft. Es müßte dann der neu aufgenommene Benutzer in der Domäne erscheinen. Sollen Benutzer über das NWAdmin-Tool aus der Domäne wieder entfernt werden, wählt man einfach die Member List-Option der entsprechenden Domäne bzw. des NDS-Domänenobjekts, markiert den oder die

21 NDS für andere Plattformen

Benutzer, die gelöscht werden sollen, und drückt anschließend die Taste **[Entf]**. Auch hier kann zur Überprüfung einer erfolgreich durchgeführten Aktion wieder der Benutzer-Manager für Domänen herangezogen werden, um festzustellen, ob der Löschvorgang erfolgreich gewesen ist.

Zur Erinnerung: Wenn NDS for NT auf einem Windows NT Server installiert ist, dann meinen NT Server Tools wie Benutzermanager für Domänen oder Server Manager, daß die Informationen aus der SAM-Datenbank kommen. In Wirklichkeit stammen alle Informationen aus der NDS, da durch NDS for NT die Anfragen an die NDS weitergeleitet werden.

Benutzerorientierte Verwaltung

Bei diesem Ansatz wird ein bestehendes oder ein eben neu eingerichtetes Benutzerobjekt ausgewählt. Anschließend wird nach dem Aufruf von Details für das ausgewählte Benutzerobjekt die Option Domain Access ausgewählt. Daraufhin erhält man eine Liste aller Domänen, zu denen dieses Benutzerobjekt gehört. Daraufhin wählt man die Option Add, und dann in der NDS das Domänenobjekt aus, von dem dieser Benutzer Mitglied werden soll. Man erkennt, daß es auf diese Art und Weise sehr einfach ist, zu einem Zeitpunkt einen Benutzer zu mehreren Domänen gleichzeitig hinzuzufügen. Das Löschen eines Benutzers aus einer Domäne ist genauso einfach realisierbar, indem man in der List der Domänenzugehörigkeiten die entsprechende Domäne und Delete auswählt.

Das Hinzufügen von Domänenbenutzern zu einer Domänengruppe ist genauso einfach wie das Hinzufügen eines Benutzers zu einer Domäne. Auch dies kann domänenorientiert innerhalb des Domänenobjekts oder benutzerorientiert für ein ausgewähltes NDS-Benutzerobjekt erfolgen.

21.1.5 Management Tools für NDS for NT

Neben der einfachen Verwaltung der gesamten Domänenumgebung über das NWAdmin-Tools stellt NDS for NT auch eine Vielzahl von Tools zur Verfügung, die weitere nützliche Mechanismen bereitstellen, um die Netzwerkverwaltung in einer Mischumgebung durchführen zu können.

NT File Share Management

NDS for NT bietet die Möglichkeit, die Verwaltung von NT File Shares vollständig über das NWAdmin-Tool durchzuführen. Dies bietet den großen Vorteil, daß sowohl die Benutzerverwaltung als auch die NT-File-Share-Verwaltung über ein einziges Tool durchgeführt werden können. Um dieses Tool aufzurufen, wählt man das Domä-

21.1 NDS for NT

nenobjekt in der NDS aus, um dafür die Option Details zu aktivieren. In der Page List wählt man dann die Option NT Tools. Daraufhin werden eine Vielzahl von NT Tools angezeigt:

- File and Folders Sharing Wizard
- Server Manager
- User Manager for Domains
- Event Viewer
- Help-Unterstützung für Event Viewer, Server Manager, User Manager

Für die NT-Share-Verwaltung aktiviert man das Tool File and Folder Sharing Wizard. Befindet sich der Share auf dem Computer, auf dem Sie gerade arbeiten, wählen Sie die Option »On my Computer«, ansonsten die Option »On another Computer«. Daraufhin muß der entsprechende Server ausgewählt werden, um auf dem Computer das Verzeichnis zu finden, für das ein Share definiert werden soll. Ist das Verzeichnis gewählt, müssen noch die notwendigen Share-Berechtigungen definiert werden, um die Definition vervollständigen zu können. Derzeit können nur »Users of Microsoft Windows« für den Zugriff berechtigt werden, da dies die einzige verfügbare Option ist, die man auswählen kann. Es existieren noch grau hinterlegt die Angaben »NetWare users« und »Macintosh users«, diese können jedoch noch nicht aktiviert werden.

Sollen weitere Optionen für den definierten Share festgelegt werden, muß der Server Manager für Domänen eingesetzt werden. Wählt man im Server Manager die Option Shared Directories, kann für einen ausgewählten Share die Option Properties ausgewählt werden, um weitere Einstellungen, wie z.B. Zugriffsberechtigungen etc. festlegen zu können.

Nicht dokumentierte Tools

Wenn auf dem NT Server eine NDS-Replica abgelegt worden ist, dann wird im gleichen Verzeichnis, in dem angegeben wurde, wo diese NDS Informationen zu speichern sind, das Programm NDS-CONS.EXE abgelegt. Dieses Tool kann verwendet werden, um die NDS auf dem NT Server herunterzufahren oder andere hilfreiche Tools einzusetzen. Nach dem Aufruf von NDSCONS.EXE stellt man sofort fest, daß die NDS- und Bindery-Module standardmäßig geladen sind. Der Schalter »Load Module« wird verwendet, um ein weiteres Modul zu aktivieren, wohingegen der Schalter »Unload Module« dazu verwendet wird, ein bereits geladenes Modul wieder zu entladen.

21 NDS für andere Plattformen

Als zusätzlich ladbares Modul steht unter anderem »Dstrace« zur Verfügung, um den Kommunikationsverkehr mit den anderen NDS-Servern im gesamten Netzwerk überwachen und kontrollieren zu können. Ebenso kann ein Modul »Monitor« geladen werden, um alle aktiven Verbindungen am NT Server, auf dem NDS for NT installiert ist, kontrollieren zu können. Mit diesem Modul können auch aktive Verbindungen gelöscht werden.

NDS Manager

Der NDS Manager dient dazu, alle Verwaltungsaufgaben durchzuführen, die mit der NDS zu tun haben. Hierzu zählt unter anderem, den aktuellen Synchronisationsstatus zu prüfen, Partitionen einzurichten, Partitionen aufzuheben, DS-Versionen zu aktualisieren, Replicas auf einem Server zu löschen, Replicas auf einem Server einzurichten, den Merge von Partitionen durchzuführen und eine Vielzahl weiterer Arbeiten, die alle mit der NDS und dem Umfeld der NDS zu tun haben.

21.1.6

Deinstallation von NDS for NT

NDS for NT kann auch wieder deinstalliert werden. Hierzu wird der Domain Object Wizard verwendet, den man bereits zum Zeitpunkt der Installation verwendet hat. Wenn der Domain Object Wizard aktiviert wird, dann wird sofort erkannt, daß NDS-Replicas auf dem Server vorhanden sind. Daraufhin wird man aufgefordert, sich in der NDS zu authentifizieren, und zwar unter einem Benutzernamen, der die notwendigen Rechte hat, um alle Replica-Operationen durchführen zu können. Nachdem die Replicas vom NT Server entfernt worden sind, kann mit der Deinstallation von NDS for NT weitergemacht werden.

Bei der Deinstallation von NDS for NT hat man drei Optionen, wie die Deinstallation durchgeführt werden soll:

- Die Standardoption lautet, alle Domäneninformationen in die SAM-Datenbank zu verschieben, auch die Änderungen, die in der Zwischenzeit über NDS for NT in der NDS für die Domäne eingerichtet worden sind.
- Die Objekte werden auf einen Zustand zurückgesetzt, so wie er vor der Installation von NDS for NT in der SAM-Datenbank existiert hat, außer den Paßwörtern.
- NDS for NT wird deinstalliert, und keine Information der NDS wird in die SAM-Datenbank übernommen.

21.2 NDS for Solaris

Durch NDS for Solaris werden die NDS-Dienste auf einem SPARC Solaris Server bzw. auf einer SPARC Solaris Workstation installiert. Somit agiert ein solches System wie ein Directory Server, so wie dies von einem NetWare 5 Server bzw. NT Server realisiert werden kann. Auffallend dabei ist, daß im Gegensatz zu NDS for NT als Voraussetzung NetWare 5 erfüllt sein muß, um die Integration von NDS for Solaris durchführen zu können. Die Begründung hier ist sehr einfach: Nur NetWare 5 ist in der Lage, eine Native-IP-Implementierung durchzuführen. Da die Kommunikation zwischen der NDS unter NetWare und NDS for Solaris auf Basis von IP durchgeführt wird, kann dies somit nur in einer NetWare-5-Umgebung geschehen. Dies heißt aber nicht, daß das gesamte Netzwerk unter NetWare 5 betrieben werden muß, nur der Server, zu dem NDS for Solaris die NDS-Kommunikation durchzuführen hat, muß unter NetWare 5 und Native IP implementiert sein; einer NetWare-4.11/5-Mischumgebung steht somit nichts im Wege. Im Gegensatz dazu kann NDS for NT sowohl eine IPX- als auch eine IP-Kommunikation mit der NDS durchführen. NDS for Solaris gestattet es auch, NDS-Replicas auf einem Solaris Server bzw. einer Solaris Workstation zu installieren, so wie dies für eine gesamte NDS-Umgebung auf unterschiedlichen NetWare Servern oder auch NT Server mit NDS for NT der Fall ist. Die Vorteile liegen auf der Hand: Man kann NDS-Replicas somit auf Solaris Servern/Workstations installieren, um die Vorteile zu nutzen, Replicas so zu platzieren, daß der Zugriff auf notwendige Informationen der NDS optimiert durchgeführt werden kann. Dies betrifft vor allem die Situation, wenn das Netzwerk und somit auch die NDS über mehrere Standorte verteilt sind.

Durch die Einführung von NDS for Solaris ist man auch in der Lage, Solaris-Benutzer-Accounts in die NDS zu migrieren, so daß Benutzerinformationen nicht mehr doppelt gepflegt werden müssen und vor allem bei der Installation von NDS for Solaris bestehende Benutzer-Accounts übernommen werden können, um eine zusätzliche Erfassung von Benutzer-Accounts zu vermeiden. Mit Hilfe dieser gesamten Produktpalette, die NDS auf unterschiedliche Plattformen zu implementieren, hat dies für den Netzwerkverwalter den großen Vorteil, Benutzer für Zugriffe unter NetWare, NT Server und Solaris nur einmal pflegen zu müssen – und zwar in der NDS als das zentrale Verwaltungstool für die gesamte Pflege der Benutzer-, Gruppen-Accounts und anderer wichtiger Informationen.

21 NDS für andere Plattformen

Durch ein entsprechendes Snap-in-Modul für den NWAdmin32 lassen sich diese Informationen von einer zentralen Stelle aus verwalten. Durch die Einführung von NDS for Solaris verwenden Benutzer die sichere NDS-Authentifizierung statt der herkömmlichen Solaris-Authentifizierungsmethode. Auf diese Art und Weise hat man einen sicheren Weg, alle Zugriffe über die NDS zu vereinfachen und für das gesamte heterogene Netzwerk nutzbar zu machen. Es sei nochmals darauf hingewiesen, daß NDS for Solaris nur über eine Native IP Installation betrieben werden kann und mindestens ein NetWare 5 Server vorhanden sein muß.

21.2.1 Vorteile durch NDS for Solaris

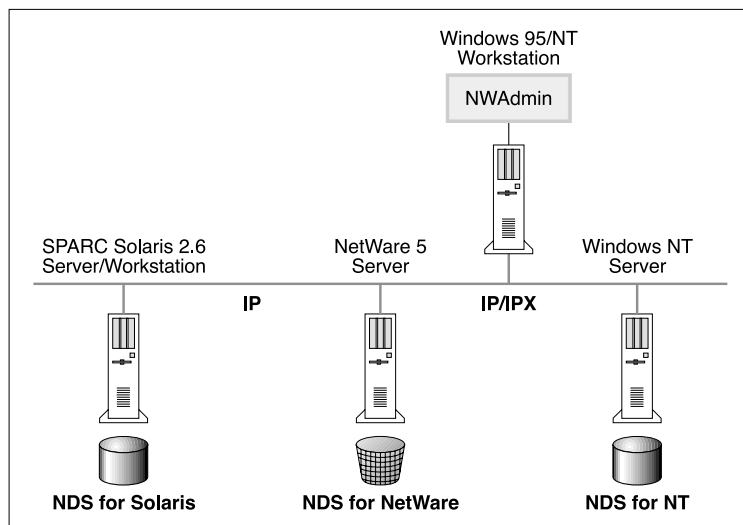
Benutzer-Accounts werden herkömmlicherweise in einem Unix-System in den Dateien `/etc/passwd`, `/etc/groups` und anderen lokalen Dateien gepflegt. In einer kleinen Netzwerkumgebung ist dies auch kein allzu großes Problem. Sobald jedoch die Anzahl Server/Workstations größer wird, steigt damit auch der administrative Aufwand. Die Firma Sun Microsystems Inc. bietet deshalb eine Möglichkeit, über NIS die Verwaltung in einer größeren Unix-Landschaft zu vereinfachen. Unter NIS werden Benutzer, Gruppen und andere Datenbanken, die normalerweise pro Server gepflegt werden, auf einem Master Server gespeichert, um von dort aus die Replizierung der Informationen auf die anderen Server durchführen zu können. NIS ist zwar für eine Vielzahl von Unix-Plattformen verfügbar, aber nicht ganz einfach zu verwalten. Der Netzwerkverwalter muß Benutzer-Accounts oder Gruppen auf einem zentralen Server einrichten bzw. modifizieren und mit Hilfe von NIS Tools den Abgleich mit dem anderen Server durchführen. NIS verwendet eine flache Datenstruktur und erschwert die Administration durch die generelle Zentralisierung der Account-Pflege. Aus diesem Grunde wurde eine Nachfolgeversion NIS+ entwickelt, wodurch eine inkrementielle Replizierung möglich ist und zudem eine hierarchische Namensstruktur zur Verfügung steht. Dadurch wird die Flexibilität wesentlich verbessert. Es bleibt jedoch die Master-Slave-Replizierung, welche administrativ relativ aufwendig ist. Zudem steht NIS+ bei weitem nicht für so viele Unix-Plattformen zur Verfügung, wie dies für NIS der Fall ist.

Die NDS von Novell hingegen ist eine erweiterbare, skalierbare, verteilte und zuverlässige Directory-Services-Struktur, die im wesentlichen auf X.500 basiert. Durch den Einsatz der NDS wird eine Datenbank verwendet, um darin alle Informationen zu speichern und zu pflegen, die zum Betreiben einer gesamten Netzwerkinfrastruktur notwendig ist. Die Unterstützung von sogenannten Directory-Enabled-Anwendungen für die NDS wird zudem immer größer und

21.2 NDS for Solaris

erfreut sich inzwischen eines großen Verbreitungsgrades und vor allem einer sehr großen Akzeptanz am Markt. Über die NDS werden inzwischen nicht nur Benutzer, Gruppen, Server, Volumes, etc. verwaltet, sondern auch Workstations, Applikationen, Systemeinstellungen für NT Workstations und eine Vielzahl weiterer Informationen. Durch die Erweiterbarkeit der NDS, d.h. des NDS-Schemas, ist man sehr schnell in der Lage, neue Informationen in die NDS aufzunehmen. Die Verwaltung des Netzwerks über die NDS kann von jeder beliebigen Stelle aus im Netzwerk durchgeführt werden, da die Synchronisation der NDS und die Replicas auf den einzelnen Servern dafür Sorge tragen, zu jedem Zeitpunkt auf die NDS zugreifen zu können. In Abbildung 21.3 ist dargestellt, wie man sich die einheitliche Verwaltung einer NDS in einer heterogenen Netzwerklandschaft vorstellen muß.

Abbildung 21.3
Einheitliche Verwaltung der NDS
in einem heterogenen Umfeld



Diese flexible Lösung kann derzeit nur Novell liefern. Für den Netzwerkverwalter ergeben sich dadurch die folgenden Vorteile:

- Ein Benutzer-Account für NetWare, NT und Solaris
- NDS als zentrale Stelle zur Verwaltung von NetWare-, NT- und Solaris-Benutzer-Accounts
- NDS-basierende sichere Authentifizierung für Benutzer-Accounts
- Mischumgebung für die Verteilung der NDS (Replicas) auf NetWare-Servern, NT-Servern und Solaris Server/Workstations

21 NDS für andere Plattformen

Für den Benutzer ergeben sich die folgenden Vorteile:

- Er muß sich nur noch einen Benutzernamen und ein Paßwort merken
- Schneller und zuverlässiger Zugriff auf die NDS, da Replicas lokal vorgehalten werden können (Verlagerung der NDS-Informationen dorthin, wo sie benötigt werden)

21.2.2

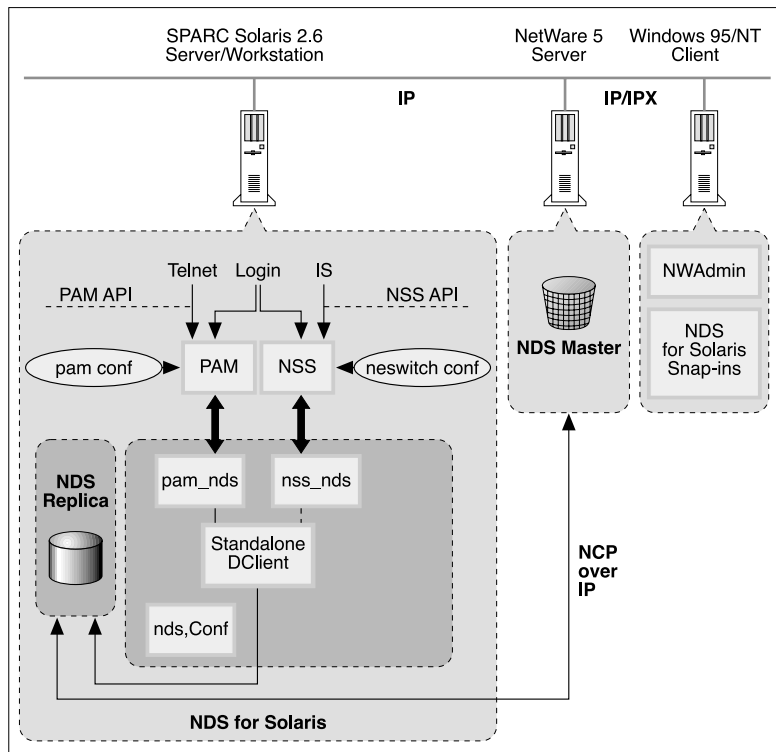
Arbeitsweise von NDS for Solaris

Da die Betriebssystemwelt heterogen bleibt, benötigt man in einem Netzwerk Möglichkeiten, nicht nur einen Single-Sign-on durchzuführen, sondern auch einen Single-Point-of-Administration verfügbar zu machen. Mit NDS for Solaris wird dieser Ansatz auch für diese Unix-Plattform sehr gut machbar. Durch NDS for Solaris werden Benutzer und Gruppen für Solaris in der NDS eingerichtet und verwaltet. Ebenso sind ein Authentication-Modul und ein Name-Service-Modul vorhanden, um eine NDS-Authentifizierung und Name Services für Solaris-Anwendungen zur Verfügung zu stellen. Zur Implementierung dieser beiden Module werden zwei infrastrukturelle Komponenten von Solaris verwendet, die man als Pluggable Authentication Modules (PAM) und Name Service Switch (NSS) bezeichnet und die Standard Programming Interfaces verwenden. Auf diese Art und Weise laufen bestehende Solaris-Anwendungen ohne Modifikation nach der Installation von NDS for Solaris weiter. Da Sun Microsystems Inc. die Systembefehle wie z.B. `login`, `telnet`, `ps`, `ls` etc. so ausgelegt hat, daß diese PAM und NSS nutzen, können diese Befehle und Utilities die NDS-Dienste transparent nutzen. Die Netzwerkverwalter können umgekehrt die Solaris-Benutzer-Accounts und die damit zusammenhängenden Aspekte über den NWAdmin verwalten. Für NDS-Benutzer-Accounts können Solaris-Attribute hinzugefügt werden, wenn diese in der Lage sein sollen, auf Solaris-Systeme zuzugreifen. Ebenso kann die NDS auf einem Solaris-System abgelegt werden, da die Version der NDS for Solaris voll kompatibel ist mit der NDS-Version von NetWare 5. Dadurch können auf einem Solaris-System lokal ein oder mehrere NDS-Replicas abgelegt werden. Die Verwaltung der Replicas auf einem Solaris-System erfolgt dabei über die herkömmlichen NetWare Tools wie NDS Manager von einer Windows Workstation aus. Für den Einsatz von Benutzer-Accounts und Gruppen auf dem Solaris-System ändert sich unter diesem Aspekt nichts. Alle Workstations und Anwendungen funktionieren anschließend genauso, wie dies auch vor der Installation von NDS for Solaris der Fall war. So wie bereits für NDS for NT beschrieben, ist der Einsatz von NDS for Solaris sowohl für Benutzer als auch für Anwender vollkommen transparent.

21.2 NDS for Solaris

Durch die Installation von NDS for Solaris wird das Schema der NDS erweitert, um anschließend alle Solaris-Benutzer- und Gruppen-Attribute verfügbar zu haben. Da es sich bei der NDS um eine globale Datenbank handelt, können Solaris-Benutzer-Accounts und Gruppen ab diesem Zeitpunkt zentral über den NetWare Administrator verwaltet werden, so wie andere Benutzerobjekte auch verwaltet werden. Es steht ein Migrations-Tool zur Verfügung, um bestehende Benutzer- bzw. Gruppen-Informationen aus `/etc/passwd`, `/etc/group`, NIS-Datenbanken und NIS+-Datenbanken in die NDS einfügen zu können. Dadurch wird der Verwaltungsaufwand bei der Migration wesentlich vereinfacht. Bei dieser Migration erfolgt ebenfalls eine Migration der Benutzer-Paßwörter. NDS for Solaris installiert auch eine Read/Write-Replica auf den Solaris-Server. Jedes Solaris-System, auf dem NDS for Solaris installiert wird, erfährt eine Rekonfiguration in der Form, daß ab dem Zeitpunkt der Installation von NDS for Solaris die NDS für die Authentifizierung und den Zugriff auf Benutzerinformationen verwendet wird.

Abbildung 21.4
Architektur von
NDS for Solaris



21 NDS für andere Plattformen

Das Pluggable Authentication Module (PAM) fängt die System Entry Requests zur Authentifizierung eines Benutzers ab und leitet diese an die NDS weiter. Das Name Server-Switch-Modul ist dafür verantwortlich, alle Datenbankzugriffe abzufangen und diese an die NDS weiterzuleiten. Die `pam_nds`- und `nss_nds`-Module verwenden den Directory Client (DClient), um Informationen aus der NDS zu bekommen. Der DClient findet den nächsten NDS-Server und schickt die Anforderung an diesen Server. Wenn die NDS-Replica lokal auf dem Solaris-System installiert ist, dann wird die Dclient-Anforderung lokal aufgelöst und muß nicht weiter über das Netzwerk transportiert werden. Die Architektur von NDS for Solaris ist in Abbildung 21.4 dargestellt.

21.2.3 Einrichtung von NDS for Solaris

Um NDS for Solaris zu installieren, sind die folgenden Schritte notwendig:

- Setup-Programm unter Windows starten
- Install-Programm auf Sun Solaris laufen lassen
- Konfiguration des Produkts

Das Windows-Setup-Programm erweitert das NDS-Schema, um anschließend die notwendigen Solaris-Attribute für Benutzer-Accounts und Gruppen zur Verfügung zu haben. Das Solaris-Install-Programm installiert auf dem Solaris-System die notwendigen Solaris Binaries. NDS for Solaris besteht aus zwei Komponenten: der NDS-User-Account-Management-Komponente und der NDS-Server-Komponente. Wenn die Installation abgeschlossen ist, wird in der Regel das Migrations Tool gestartet, um Benutzer/Gruppen aus der NIS- bzw. NIS+-Datenbank oder den anderen Systemdateien in die NDS zu übernehmen. Ebenso werden dadurch in der NDS Solaris-Client-Objekte eingerichtet. Nach der Migration kann mit der neuen Systemumgebung gearbeitet werden.

21.2.4 Verwaltung der Benutzer-Accounts

Die Solaris-Benutzer-Accounts, Gruppen und Hosts werden als Objekte in der NDS dargestellt. Durch das Snap-in-Modul ist der Netzwerkverwalter in der Lage, über das NWAdmin-Programm nicht nur Benutzer-, Gruppen- und Host-Objekte einzurichten, sondern auch Zugriffsberechtigungen individueller Benutzer auf spezielle Solaris-Systeme zu verwalten. NDS for Solaris kann parallel zu NIS, NIS+ und der Dateiverwaltung von Benutzer-Accounts existieren. Der Netzwerkverwalter kann die Einrichtung so vornehmen, daß ein Teil der Benutzer über die NDS authentifiziert wird und andere hingegen

21.2 NDS for Solaris

über NIS(+). Ebenso ist es möglich, das System so zu konfigurieren, daß die Authentifizierung sowohl in der NDS als auch im NIS(+) durchgeführt wird.

NDS for Solaris stellt das `pam_nds`-Modul zur Verfügung, so daß es möglich ist, daß sich Anwendungen über die NDS authentifizieren können. Wenn die NDS-Authentifizierung durchgeführt ist, hat der Benutzer die gleichen Privilegien und Rechte, wie diese auch von NIS zur Verfügung gestellt werden. Dem Benutzer steht die Solaris Shell wie gewohnt zur Verfügung, das User Profile sieht so aus wie vorher, und an den Zugriffsrechten für Dateien und Druckdienste hat sich auch nichts geändert. Das `pam_nds`-Modul stellt folgende Dienste zur Verfügung:

- Authentifizierung
- Account
- Session
- Password

Diese Dienste stehen für alle Anwendungen zur Verfügung. So stehen zum Beispiel durch den Dienst Password die bekannten NetWare Password Policies zur Verfügung, wie zum Beispiel Ablaufintervall, Paßwortlänge etc., die damit auch für Solaris-Benutzer Gültigkeit haben.

21.2.5 Zusammenspiel mit anderen Novell-Produkten

NDS for Solaris ist nur unter IP einsetzbar. Somit stehen alle Möglichkeiten zur Verfügung, die in Verbindung mit NetWare 5 bereitgestellt werden. Zur Verwaltung der NDS stehen der NWAdmin und der NDS Manager zur Verfügung. Die Kommunikation zwischen der NDS auf einem NetWare 5 Server und der NDS auf dem Solaris-System erfolgt über das IP-Protokoll. In einer Mischumgebung (NetWare 5/NetWare 4.11(4.2)) mit NDS for Solaris sind die folgenden Regeln zu beachten:

- Die Master Replica der Root Partition muß auf einem NetWare 5 Server liegen.
- Wenn eine Replica einer Partition auf einem NetWare 4.11 (4.2) abgelegt ist, dann muß die Master Replica der Partition auf einem NetWare 5 Server liegen. Die ist notwendig, um eine ordnungsgemäße Synchronisation gewährleisten zu können.
- Wenn eine Replica einer Partition auf einem NDS for Solaris System abgelegt ist, dann muß die Master Replica dieser Partition auf einem NetWare 5 Server liegen.
- NDS for Solaris und NetWare 4.11 (4.2) sollten keine Replica der gleichen Partition speichern.

21 NDS für andere Plattformen

Diese Ausführungen haben gezeigt, welche Vorteile die Portierung der NDS auf unterschiedliche Plattformen mit sich bringt. Es sei deshalb an dieser Stelle nochmals aufgezeigt, für welche Plattformen die NDS derzeit zur Verfügung gestellt wird:

NetWare 4, NetWare 5, Microsoft Windows NT Server, IBM OS/390, IBM AIX, Sun Solaris und Linux.

Diese Liste wird in Zukunft mit Sicherheit noch größer werden, um die Vorteile von Directory Services in einer heterogenen Betriebssystemlandschaft immer mehr nutzen zu können.

21.2.6

NDS v8

In den letzten Jahren konnte Novell sehr viel Erfahrung mit Directory Services sammeln. Als Folge davon hat Novell die nächste Generation der NDS entwickelt, die unter der Bezeichnung NDS v8 vertrieben wird und eine Erweiterung der bestehenden NDS darstellt. Durch NDS v8 wird die NDS um Internet- und Enterprise-Directory-Aspekte erweitert, ohne dabei an Funktionalität zu verlieren. Der Schwerpunkt von NDS v8 liegt dabei auf Skalierbarkeit, Performance, LDAP v3 (Lightweight Directory Access Protocol) und Verwaltbarkeit. Im wesentlichen bietet NDS v8 folgende Features:

- Verbesserte NDS-Kapazität für zig Millionen Objekte in einem NDS Baum
- Verbesserte Performance für Lese-, Schreib- und Suchzugriffe auf die NDS
- Management über ConsoleOne
- Verbesserte Lightweight Directory Access Protocol (LDAP) v3 Performance
- Verbessertes DSRepair Utility
- Batch Utility für das Hinzufügen, Ändern und Löschen von NDS-Objekten
- Erweiterte »Naming-Unterstützung« einschließlich »DC=« und uniqueID
- In-Place Upgrade einer bestehenden NDS-Datenbank
- Nur für NetWare 5 Server
- Mischumgebung mit »alter« und »neuer« NDS ist gewährleistet

21.2.7

NDS-v8-Verbesserungen

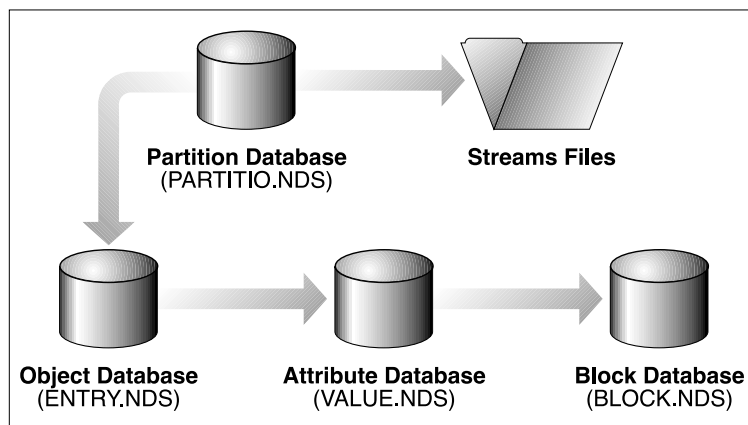
NDS v8 basiert auf dem NetWare 5 Code und kann deshalb auch nur auf einem NetWare 5 Server installiert und eingerichtet werden. NDS v8 unterstützt eine echte Datenbankstruktur-Technologie mit Index-Mechanismen, wodurch sich auch die Performance-Verbesserungen

21.2 NDS for Solaris

ergeben. Die indizierten Werte bestimmen dabei die Zugriffe und Background-Prozesse der NDS. Als Ziel soll erreicht werden, mindestens 200 LDAP v3 Lesezugriffe pro Sekunde zu erreichen. NDS v8 verwendet einen sogenannten Persistent Change Cache. Durch diesen Cache-Mechanismus werden alle durchgeführten Änderungen in einem separaten Bereich gehalten. Sollte der Server während der Durchführung von Änderungen abstürzen, dann wird nach dem Wiederanlauf des Servers die NDS nicht nur schneller geladen, sondern es werden auch die Synchronisationen der Änderungen innerhalb von Sekunden durchgeführt. Als weitere Verbesserung verwendet NDS v8 kein TTS (Transaction Tracking System) mehr, um die Konsistenz der NDS zu gewährleisten. Statt dessen wird das sogenannte Roll-Back-Modell verwendet. Bei diesem Modell wird ein Log File verwendet, um einen Roll Forward für Transaktionen durchführen zu können, für den Fall, daß das Server-System unkontrolliert abstürzt. NDS v8 gestattet es ohne Problem, NDS-Objekte in einer Größenordnung von mehreren Milliarden pro NDS Baum, zig Millionen Objekte pro Server, zig tausend Objekte pro Container und Objektgrößen von bis zu 50 Kbyte zu unterstützen.

Um die wesentlichen Änderungen in der neuen NDS v8 besser verstehen zu können, muß man den Aufbau der alten und der neuen NDS etwas näher betrachten. Die früheren NDS-Versionen verwendeten vier Datendateien und eine Vielzahl von Streams-Dateien, um damit die NDS-Verwaltung durchzuführen. In Abbildung 21.5 ist die alte Struktur dargestellt.

Abbildung 21.5
Die alte NDS-
Struktur



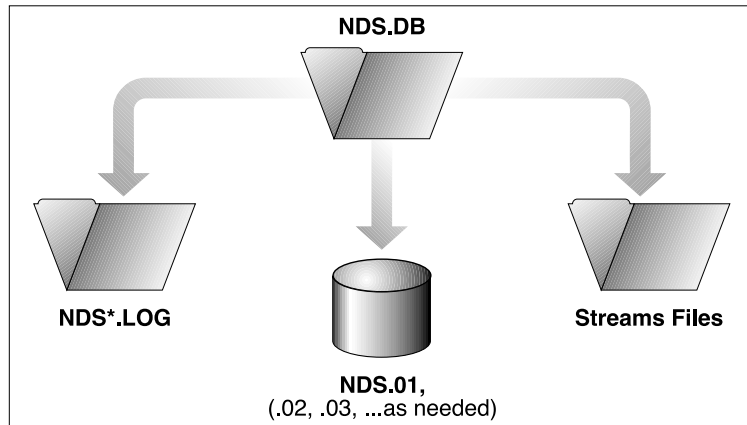
21 NDS für andere Plattformen

In den aufgeführten Dateien werden die folgenden Informationen abgelegt:

- PARTITIO.NDS: Hierin wird eine Liste der NDS-Partitionen gepflegt, einschließlich der System-, Schema-, External-Reference- und Bindery-Partition, die pro NDS-Server existiert.
- ENTRY.NDS: Hierin befindet sich pro Objekt ein Eintrag, der in einer Replica existiert.
- VALUE.NDS: Für jedes Objekt werden darin die Property-Werte gepflegt.
- BLOCK.NDS: Wenn in der VALUE.NDS nicht alle Property-Werte gepflegt werden können, werden diese in der Datei BLOCK.NDS gepflegt – die Pflege von Overflow-Werten.
- Streams: Dateien werden unter Namen bestehend aus hexadezimalen Zahlen abgespeichert und für die Speicherung von Login Scripts oder Print-Job-Konfigurationen benötigt.

Die neue NDS-Struktur unter NDS v8 ist in Abbildung 21.6 dargestellt.

Abbildung 21.6
Die Datenbank-
struktur von
NDS v8



Die Bedeutung der einzelnen Datenbankdateien ist dabei wie folgt:

- NDS.DB: Hierbei handelt es sich um die Kontroll-Datei der Datenbank.
- NDS*.LOG: In dieser Datei werden Transaktionsvorgänge aufgezeichnet, die noch nicht abgeschlossen sind. Bei einem Systemabsturz wird diese Datei verwendet, um die ausstehenden Transaktionen vollständig abschließen zu können, nachdem das abgestürzte System wieder in Betrieb genommen wurde.

21.2 NDS for Solaris

- NDS.01: Hierin befinden sich alle »Records« und »Indizes«, die auf dem Server vorgefunden werden. Wenn diese Datei eine Größe von 2 Gbyte erreicht, wird eine neue Datei NDS.02 für die weiteren Daten erstellt. Erreicht auch diese Datei eine Größe von 2 Gbyte, wird eine Datei NDS.03 erstellt usw.
- Streams: Dateien werden unter Namen bestehend aus hexadezimalen Zahlen abgespeichert und für die Speicherung von Login Scripts oder Print-Job-Konfigurationen benötigt. Im Gegensatz zur alten NDS-Version haben die Streams-Dateien die Extension .NDS.

Um die Performance zu erhöhen, werden in der Datei NDS.01 Indizes gehalten. Diese Indizes beinhalten:

- Attribut-Substring-Indizes für die Felder CN und uniqueID
- Attribut-Indizes für die Object-Class- und dc-Felder (dc=LDAP Domain Container)
- Attribut-Indizes für Strings, die mit CN, uniqueID, Given Name und Surname beginnen.

NDS v8 wird mit dem neuen Tool BULKLOADER ausgestattet. Mit diesem Tool ist man in der Lage, mit Hilfe von LDIF (LDAP Interchange Format) Millionen von Objekten in die NDS einzufügen – in einer Art Batch-Prozedur. LDIF ist das Standard-Format, um Informationen zu importieren bzw. zu exportieren, wenn es sich dabei um Directory Services handelt, die LDAP v3 unterstützen. Das BULKLOADER Tool wird dabei als NLM auf dem Server geladen.

NDS v8 wird auch mit einem neuen DSRepair Utility ausgeliefert, mit dem es möglich ist, die Reparatur auf einer einzelnen Partition durchzuführen, ohne die ganze Datenbank reparieren zu müssen. Unangenehme Nebeneffekte hatte in der Vergangenheit auch die Tatsache, daß die NDS während der Reparatur gesperrt wurde. Dies war vor allem bei großen NDS-Datenbanken eine meist längere Angelegenheit. Mit NDS v8 und dem neuen DSRepair ist man in der Lage, bestimmte Reparaturläufe durchzuführen, ohne die Datenbank sperren zu müssen.

Für die Administration von NDS v8 wird standardmäßig ConsoleOne verwendet. Man kann die Administration zwar noch mit dem NWAdmin32 durchführen, jedoch steht mit der neuen ConsoleOne für NDS v8 eine Vielzahl von neuen Funktionen zur Verfügung, die der NWAdmin32 nicht bieten kann. Die Strategie von Novell ist zudem, ConsoleOne als die neue Administrationsplattform zu verwenden.

21 NDS für andere Plattformen

Die neue ConsoleOne beinhaltet zudem ein LDAP Snap-in, um damit die LDAP-Konfiguration durchführen zu können. Zudem beinhaltet ConsoleOne Snap-ins für das Datei-Management, Objekt-Management und Schema-Management.

Als weitere Ergänzung im Zuge der NDS-v8-Entwicklung wurde ConsoleOne um die folgenden Funktionen erweitert:

- Durchsuchen sehr großer Container: Es können jetzt ohne größeren Performance-Verlust sehr große Container auch sehr schnell durchsucht werden.
- Suche nach individuell angepaßten Sichtweisen: Diese Anzeige von Objekten in ConsoleOne kann durch individuell erstellte Filter und die Angabe von speziellen Attribut-Werten vereinfacht werden.
- Konfiguration der LDAP-Dienste: Mit ConsoleOne können nicht nur die LDAP-v3-Dienste konfiguriert, sondern es kann auch festgelegt werden, mit welchen Berechtigungen Benutzer und Gruppen auf die NDS über LDAP zugreifen dürfen.
- Verwaltung aller NDS-Objekte: Jedes Objekt, das im Schema des NDS-Baumes existiert, kann erstellt, verschoben, umbenannt, gelöscht und geändert werden. Ebenso können gleichzeitig mehrere Objekte modifiziert werden. Für die meisten Objekte gibt es eigene Property-Pages. Wenn es diese Property-Page nicht gibt, kann man die Modifikation über die »Generic«-Other-Page durchführen.
- Erweiterung des NDS-Schemas: Neue Objekte und Attribute können eingerichtet werden.
- Setup Benutzer-Accounts über Templates: Durch das Einrichten von Templates können definierte Vorgaben eingerichtet werden, die jedem neu eingerichteten Benutzer übertragen werden. Es können so ziemlich alle Property-Werte in das Template übernommen werden.
- Steuerung der NDS-Rechtevererbung: Es kann festgelegt werden, ob die Objekte- und Property-Rechte nach unten vererbt werden sollen.
- Verwaltung der NetWare-Dateidienste: Die Dateidienste auf individuellen File-Servern können verwaltet werden. Es können Dateien und Verzeichnisse erstellt, verschoben, gelöscht, umbenannt werden, Attribute können vergeben und geändert werden, Zugriffsberechtigungen für Dateien und Verzeichnisse lassen sich für Benutzer und Gruppen definieren bzw. anpassen.

21.2 NDS for Solaris

Wer sich nicht mit ConsoleOne auseinandersetzen will, um die Verwaltung der NDS durchzuführen, kann immer noch mit dem NWAdmin32 arbeiten. Jedoch hat man dann mit folgenden wesentlichen Einschränkungen zu kämpfen:

- Alle Objekte werden auf der Workstation sortiert.
- Suchergebnisse sind auf maximal 38.000 Objekte beschränkt.
- Trustees eines Objekts sind auf maximal 38.000 beschränkt.

Abschließend sei gesagt, daß die Umstellung von einer früheren NDS-Version auf die neue NDS v8 für einen NetWare 5 Server relativ einfach ist und keine Schwierigkeiten bereitet. Wichtig dabei ist nur, daß man die vorgegebenen Schritte genau einhält, um ungewollte Fehler zu vermeiden.

22

Windows NT

Mittlerweile sind Windows NT und Windows NT Server, beides Microsoft-Produkte, vom Markt nicht mehr wegzudenken. Die Anzahl der Installationen von NT Servern ist in letzter Zeit vor allem durch die Kooperation von SAP und Microsoft stark gestiegen. Die Installation von Windows NT als Workstation-Betriebssystem gewinnt zwar immer mehr an Boden, es gibt aber noch eine größere Anzahl von Windows 3.x Workstations. Die Bedeutung von Windows NT wächst, da viele Unternehmen die Umstellung auf Windows 95 gleich auslassen und statt dessen auf Windows NT umsteigen. Dies wird vor allem unter dem Aspekt interessant, daß mit Einführung von Windows NT Oberfläche und Installation von Windows NT fast genauso aussehen wie bei Windows 95.

Man muß allerdings berücksichtigen, daß die Sicherheitsmechanismen und die Stabilität von Windows 95 nicht mit denen von Windows NT 4 vergleichbar sind, da an Windows NT wesentlich höhere Sicherheitsanforderungen gestellt werden.

Das strategische Ziel von Microsoft liegt auf der Hand: Langfristig gesehen soll es nur noch ein Workstation-Betriebssystem geben, und das wird Windows 2000 heißen. Tatsache ist jedoch, daß die Einführung von Windows 95/98 nur eine Art Übergang zu Windows NT sein soll. Da Windows NT ein echtes 32-Bit-Betriebssystem ist, Windows 95/98 hingegen nicht, könnte das unter Umständen gar nicht mehr so lange dauern. Beeinflußt werden könnte dies auch dadurch, daß Windows NT auf einem Pentium Pro optimal läuft, Windows 95 dagegen langsamer, da es kein echtes 32-Bit-Betriebssystem ist. Man sollte deshalb für Windows 95 bei 80586-Prozessoren bleiben und keine Pentium-Pro-Maschinen verwenden.

Das Ziel der nächsten beiden Kapitel soll sein, Ihnen einen Überblick über die Windows-NT- und Windows-NT-Server-Architektur zu geben. Dabei ist es unerheblich, ob man sich auf die Version 3.51 oder 4.0 festlegt. Da die Unterschiede zwischen Windows NT 4.0 und Windows 3.51 relativ gering sind, zumindest was ihre Funktionen anbelangt, werde ich versuchen, ohne Versionsnummer zu arbeiten. Die wichtigste Neuerung für den Anwender ist die neue grafische Oberfläche. Erwähnt werden soll an dieser Stelle nur noch, daß an den Client-Treibern Änderungen durchgeführt worden sind, so daß es mit Windows NT 4.0 zum Beispiel möglich ist, eine NDS-fähige NetWare-Integration mit dem Microsoft Client durchzuführen

22 Windows NT

und dabei sogar Login Scripts abgearbeitet werden. Dies ist bisher mit der NT Workstation 3.51 nicht möglich.

Nachdem sich IBM und Microsoft getrennt hatten, wurden alle Entwicklungen für OS/2 über Bord geworfen, und es wurde nur noch die Zielrichtung Windows verfolgt. Daraus entstanden im Laufe der Zeit die herkömmlichen Windows-Produktfamilien und Windows NT in Verbindung mit dem Windows NT Server.

Auf Windows 3.x muß nicht näher eingegangen werden. Windows for Workgroups ist so konzipiert, daß einfach und schnell kleine Peer-to-Peer-Netzwerke installiert werden können, damit Ressourcen auf den einzelnen Workstations unter Windows gemeinsam benutzt werden können. Das gleiche gilt für Windows 95; auch hier sind standardmäßige Komponenten enthalten, um kleine Peer-to-Peer-Netzwerke damit aufbauen zu können. Die Vor- und Nachteile dieser kleinen Netzwerke liegen auf der Hand. Anders die Situation bei Windows NT. Es handelt sich dabei um ein vollkommen neu entwickeltes Konzept, nicht nur um leistungsfähige Workstations, sondern auch um eine andere Plattform als den Windows NT Server zu erhalten. Hierzu jedoch später mehr. Zuerst will ich Ihnen das Konzept von Windows NT näher beschreiben und auf die darin integrierten Netzwerkfunktionen eingehen.

22.1 Windows NT Features

Das Betriebssystem Windows NT bietet Produktivität, einfache Handhabung und breite Unterstützung an Software-Applikationen auf Basis eines High-End-Betriebssystems. Es handelt sich um ein skalierbares, robustes und »sicheres« Betriebssystem, das in der Lage sein soll, die gesamte Leistungsfähigkeit der PCs der neunziger Jahre zu nutzen.

Folgende Zusammenstellung soll einen ersten Überblick über die Leistungsfähigkeit von Windows NT bieten:

- *Verbesserte Leistung und Performance*
32-Bit-Betriebssystem, hohe Kapazitäten (4 Gbyte Hauptspeicher, viele Tbyte Plattenkapazität durch 64-Bit-Adressierung, 2 Gbyte virtueller Speicher pro Anwendung).
- *Skalierbarkeit*
Lauffähig auf einer Vielzahl von Plattformen (Intel 386/486/586, Intel Pentium/Pro, MIPS R4000 und DEC Alpha), symmetrisches Multiprocessing, so war es ursprünglich geplant. Eine MIPS-Unterstützung ist inzwischen nicht mehr gegeben, da man diesen Entwicklungsschritt eingestellt hat.

22.1 Windows NT Features

- *Zuverlässigkeit*
Speicherschutzmechanismen, transaktionsorientiertes, recoverfähiges Dateisystem (NTFS), Sicherheit basierend auf C2
- *Einfache Bedienung*
Windows-Oberfläche, in der Version 4 mit der von Windows 95 bekannten Oberfläche.
- *Einfaches Management*
Graphical User Interface Management Tools, Remote Management Tools.
- *Kompatibilität*
Lauffähig sind MS-DOS-, Windows-, 16-Bit- und 32-Bit-Anwendungen, einsetzbar in einer Vielzahl von Netzwerken (Windows for Workgroups, LAN Manager – sofern es die noch gibt –, Novell NetWare, DEC Pathworks und Banyan Vines), Anbindung an Minicomputer und Hosts möglich (TCP/IP-basierend, SNA-Dienste und RPC).
- *Offene Systemarchitektur*
Windows-Open-Service-Architektur, modulares Design von Windows NT.
- *Workgroup-Computing-Mechanismen*
Integrierte Netzwerkfunktion für Workgroup-Computing-Anwendungen (Mail und Scheduling) und die dazugehörigen Administration-Tools.

Zur Entwicklung eines Betriebssystems der Zukunft verpflichtete Microsoft einen der bekanntesten Entwickler auf dem Gebiet der Computertechnologie: David N. Cutler. Cutler ist einer der Entwickler des VMS-Betriebssystems und der MicroVax. David Cutler stellte ein Team von Ingenieuren zusammen, um mit diesen Windows NT (New Technology) zu entwickeln.

Im Vorwort von Helen Custers Buch »Inside Windows NT« schreibt Cutler: »In the summer of 1988, I received an interesting call from Bill Gates at Microsoft. He asked whether I'd like to come over and talk about building a new operating system at Microsoft for personal computers, but I thought this would be a good opportunity to meet Bill and discuss what he had in mind. What Bill had to offer was the opportunity to build another operating system, one that was portable and addressed some of the concerns people had about using personal computers to run mission-critical applications. For me, it meant the chance to build another operating system!«

Die Ziele beim Entwurf von Windows NT beinhalten:

- Erweiterbarkeit
- Portierbarkeit
- Zuverlässigkeit

- Kompatibilität
- Leistungsfähigkeit

22.1.1 Erweiterbarkeit

Der Code des Betriebssystems muß bei Bedarf erweitert werden können, wenn es die Marktgegebenheiten erfordern. Damit dies für Windows NT erreicht werden kann, besteht das Betriebssystem aus einer privilegierten Executive und einer Reihe von nicht privilegierten Servern, die »geschützte Subsysteme« genannt werden. Was heißt dabei privilegiert? Man versteht darunter eine besondere Betriebsart des Prozessors. Die meisten Prozessoren bieten einen privilegierten Modus, in dem ein Programm alle Maschinenbefehle benutzen darf und der Systemspeicher zugänglich ist. Nicht privilegierter Modus bedeutet, daß bestimmte Maschinenbefehle nicht erlaubt sind und der Systemspeicher nicht zugänglich ist. Windows NT bezeichnet den privilegierten Modus als Kernmodus (Kernel Mode) und den nicht privilegierten Modus als Anwendermodus (User Mode).

Das Betriebssystem läuft im Normalfall ausschließlich im privilegierten Modus und die Anwendungen im nicht privilegierten Modus, es sei denn, die Anwendungen rufen Funktionen des Betriebssystems auf. Bei der Konzeption von Windows NT wurde darauf geachtet, daß auch die geschützten Subsysteme im Anwendermodus laufen, genauso wie Anwendungen. Somit können die geschützten Subsysteme geändert werden – es können sogar neue hinzugefügt werden –, ohne die Integrität der Executive zu verletzen, d.h., das Betriebssystem kann leicht erweitert werden.

Zusätzlich zum geschützten Subsystem enthält Windows NT eine Vielzahl weiterer Funktionen, um die Erweiterbarkeit zu unterstützen. Hierzu gehören:

■ *Modulare Struktur*

Die Executive enthält ein Set individueller Komponenten, die mit anderen Komponenten nur über funktionelle Interfaces kooperieren. Neue Komponenten können zur Executive modular hinzugefügt werden, die ihre Arbeit dadurch bewerkstelligen, daß das Interface der existierenden Komponenten aufgerufen wird.

■ *Objekte*

Objekte, abstrakte Datentypen, die nur durch spezielle Sets von Objekt-Diensten manipuliert werden können, ermöglichen es, System-Ressourcen einheitlich zu verwalten. Das Hinzufügen neuer Objekte beeinflusst weder existierende Objekte, noch verlangt es, existierenden Code zu ändern.

22.1 Windows NT Features

■ *Ladbare Treiber*

Das Windows-NT-I/O-System unterstützt Treiber, die im laufenden Betrieb hinzugefügt werden können. Neue Dateisysteme, Devices und Netzwerke können unterstützt werden, indem einfach ein Device-Treiber, File-System-Treiber oder Transport-Treiber geschrieben und zum System hinzugeladen wird.

■ *Remote Procedure Call (RPC)*

Die RPC-Funktionalität ermöglicht es Applikationen, Remote-Dienste aufzurufen, ohne darauf Rücksicht zu nehmen, wo sich diese im Netzwerk befinden. Neue Dienste können auf einer beliebigen Maschine im Netzwerk hinzugefügt werden und sind dann sofort verfügbar für Anwendungen, die auf anderen Maschinen im Netzwerk laufen. Der Einsatz als Exchange Server Client wird davon auch profitieren.

22.1.2 Portierbarkeit

Portierbarkeit bedeutet, daß das gesamte Betriebssystem auf eine andere Maschine übertragen werden kann, die andere Prozessorarchitekturen einsetzt, indem der Code von Windows NT nur geringfügig angepaßt werden muß. Durch den strukturellen Aufbau von Windows NT ist das relativ einfach möglich.

Windows NT ist fast vollständig in C geschrieben. Für die Entwicklung von Windows NT hat man sich vor allem deshalb für C entschieden, weil es weitgehend standardisiert ist und für eine Vielzahl von Rechnerwelten C-Compiler und Entwickler-Tools angeboten werden. Assembler ist nur in den Systemteilen eingesetzt worden, die direkt mit der Hardware des Rechners zusammenarbeiten müssen oder auf Grund von Performance-Gewinn unbedingt in dieser Sprache erstellt werden mußten. Der nicht portierbare Code von Windows NT ist in den Komponenten, die ihn benutzen, sorgfältig isoliert. Zusätzlich zu C und Assembler sind einige Teile auch in C++ geschrieben. Dies betrifft vor allem die grafische Komponente der Windows-Umgebung und Teile der Netzwerkschnittstelle.

Bestimmte Low-Level-Teile des Betriebssystems müssen auf prozessorabhängige Datenstrukturen und Register zugreifen. Der Code, der dies durchführt, ist aber in kleinen Modulen enthalten, die einfach und schnell gegen entsprechende Module für andere Prozessoren ersetzt werden können.

Zusätzlich zu der Abhängigkeit von bestimmten Prozessoren müssen für die Portierung auch noch andere Abhängigkeiten vom Zielsystem berücksichtigt werden. Windows NT bringt den systemabhängigen Code in einer DLL unter, die als HAL (Hardware Abstraction Layer) bezeichnet wird. Die HAL verbirgt die Hardware (Cache oder I/O In-

22 Windows NT

errupt Controller) durch eine Low-Level-Software, so daß der darüberliegende Code nicht geändert werden muß, wenn eine andere Plattform portiert wird. Windows NT wurde so konzipiert, daß es einfach auf Maschinen eingesetzt werden kann, die einen linearen 32-Bit-Adreßraum und virtuelle Speicherverwaltung verwenden.

Derzeit kann Windows NT auf Intel 386/486/586-, Intel-Pentium/Pro-Prozessoren, MIPS-R4000-Risc-Architekturen und DEC-Alpha-Rechner eingesetzt werden. Jede Windows-NT-Plattform bietet das gleiche User Interface und unterstützt 16-Bit- und 32-Bit-Windows-Anwendungen, MS-DOS-Programme und POSIX-konforme Applikationen.

22.1.3 Zuverlässigkeit

Bereits beim Entwurf von Windows NT wurde darauf geachtet, ein robustes System zu entwickeln, das vorhersagbar auf Fehlersituationen reagiert. Es schützt sich selbst und die Anwender aktiv vor zufälligen oder absichtlichen Versuchen, entweder durch den Anwender oder durch Applikationen, das System zu sabotieren.

Windows NT benutzt dabei eine strukturierte Ausnahmebehandlung zur Erkennung von Fehlersituationen und deren einheitlicher Bearbeitung. Es ist dies der primäre Schutz von Windows NT gegen Hard- und Software-Fehler. Entweder verursacht das Betriebssystem oder der Prozessor eine Ausnahmebedingung, wenn ein abnormales Ereignis eintritt. Daraufhin wird der Code zur Bearbeitung dieser Ausnahmesituation automatisch aktiviert, um sicherzustellen, daß kein unentdeckter Fehler das System zerstört oder dem Anwender ein vermeidbarer Schaden entsteht.

22.1.4 Kompatibilität

Software-Kompatibilität für ein Betriebssystem zu gewähren ist kein einfaches Aufgabengebiet. Kompatibilität zeichnet sich für ein Betriebssystem vor allem dadurch aus, daß Programme ausgeführt werden können, die für ein anderes Betriebssystem oder für die Vorgängerversion des Betriebssystems geschrieben worden sind. Für Windows NT nimmt die Kompatibilität mehrere Formen an. Es geht dabei um die Frage der Binär- oder Sourcecode-Kompatibilität. Binärkompatibel heißt, daß ein Programm, so wie es ist, auf einem anderen Betriebssystem laufen kann. Sourcecode-kompatibel bedeutet, ein Programm muß neu kompiliert werden, bevor es auf dem neuen Betriebssystem laufen kann.

22.1 Windows NT Features

Die Frage der Binär- oder Sourcecode-Kompatibilität zu bestehenden Systemen hängt von verschiedenen Bedingungen ab. Einer der wichtigsten Faktoren ist die Architektur des Prozessors. Verwendet der Prozessor denselben Befehlssatz, eventuell mit einigen Erweiterungen, und stimmt die Speicheradressierung mit dem alten Prozessor überein, kann Binärkompatibilität erreicht werden.

Mit der Binärkompatibilität ist es problematischer, wenn es sich um unterschiedliche Prozessortypen handelt. Da jede Prozessorarchitektur normalerweise eine eigene Maschinensprache verwendet, kann die Binärkompatibilität zwischen unterschiedlichen Architekturen nur durch den Einsatz eines Emulationsprogramms erzielt werden. Dieses Emulationsprogramm bildet die Maschinensprache des einen Prozessors in den Befehlssatz des anderen Prozessors ab. Existiert dieser Emulator nicht, muß das Programm neu kompiliert und neu gebunden werden – das bedeutet in den meisten Fällen neue Fehlersuche beim Einsatz des Programms auf dem neuen Prozessor.

Durch den Einsatz geschützter Subsysteme (Protected Subsystems) stellt Windows NT auch für andere Anwendungen andere Laufzeitumgebungen zur Verfügung als diejenigen, die sich auf das primäre API stützten; es handelt sich dabei um WIN32 API. Auf den Intel-Prozessoren bieten die Windows-NT-geschützten Subsysteme Binärkompatibilität für bestehende Microsoft-Anwendungen, einschließlich MS-DOS, 16-Bit-Windows und OS/2. Auf der MIPS-Risc-Architektur wird die Binärkompatibilität für MS-DOS, 16-Bit-Windows und LAN-Manager durch einen Emulator erreicht. Zudem bietet Windows NT Sourcecode-Kompatibilität für POSIX-Anwendungen, die sich an die POSIX-Schnittstellen halten, wie sie vom IEEE-1003.1-Standard festgelegt worden sind.

Zur Programmierschnittstellen-Kompatibilität unterstützt Windows NT zusätzlich bestehende Dateisysteme für MS-DOS (FAT), OS/2 HPFS, CD-ROM CDFS und das neue NTFS (NT File System). NTFS bietet eine Vielzahl von Sicherheitsmechanismen, die von bisherigen Dateisystemen nicht geboten werden können. Ich werde an anderer Stelle auf diese Funktionen zurückkommen.

22.1.5

Leistungsfähigkeit

Die Leistungsfähigkeit eines Betriebssystems hängt nicht nur von der Geschwindigkeit des Prozessors ab. Daß Ihr MS-DOS auf einem 486/66-MHz-Rechner schneller ist, hängt sicher von der besseren Performance des Prozessors ab. Wenn man jedoch bedenkt, daß MS-DOS im 8086-Modus auf diesem Prozessor läuft und somit gar nicht die eigentlichen Leistungsmerkmale des 486 nutzen kann, kommt man

22 Windows NT

von selbst darauf, daß mit MS-DOS nur ein Bruchteil der Leistungsfähigkeit genutzt wird. Es wurde bereits bei der Entwicklung und Konzeption von Windows NT großer Wert darauf gelegt, ein performantes Betriebssystem zu erhalten, das alle Möglichkeiten des Prozessors voll nutzen kann.

Dieses Ziel wurde durch die folgenden integrierten Prozesse erreicht:

- Beim Entwurf der einzelnen Komponenten von Windows NT stand deren Leistungsfähigkeit im Vordergrund. Systemteile, die besonders kritisch bezüglich Geschwindigkeit sind, wurden mit Hilfe spezieller Performancetests geprüft und entwickelt. Systemaufrufe, Page Faults in der Speicherverwaltung und andere kritische Anwendungen wurden immer wieder optimiert, um die besten Ergebnisse zu erzielen.
- Die geschützten Subsysteme (Servers), die Betriebssystemaufgaben erfüllen, müssen sehr oft miteinander und mit Client-Anwendungen kommunizieren. Um zu gewährleisten, daß diese Kommunikationsaufgaben die Performance nicht beeinträchtigen, wurde als integraler Bestandteil des Betriebssystems ein sehr schneller Mechanismus zur Übergabe von Nachrichten implementiert. Dieser wird als *Local Procedure Call* (LPC) bezeichnet.
- Jedes geschützte Subsystem, das eine Betriebssystemumgebung bereitstellt (Environment Subsystem), wurde so konzipiert, daß die am häufigsten benutzten Systemdienste so schnell wie möglich verarbeitet werden.
- Windows NT beinhaltet standardmäßig Netzwerkfunktionen. Die kritischen Komponenten der Netzwerksoftware von Windows NT sind fester Bestandteil des privilegierten Teils des Betriebssystems, da dadurch die größtmögliche Performance erreicht werden kann. Das heißt, diese Netzwerkfunktionen müssen nicht mehr als Treiber oder Anwendung zum Windows-NT-Betriebssystem hinzugefügt werden.

22.2 Systemübersicht

Unter einem Betriebssystem wird ein spezielles Programm verstanden, das eine Umgebung zur Verfügung stellt, in der Programme auf einem Computer ablaufen können. Den Programmen wird somit auch der Zugriff auf den Prozessor, auf I/O Devices und andere Systemumgebungen ermöglicht und erleichtert. Die ersten Betriebssysteme waren sehr einfach gestaltet, die heutigen Systeme werden immer mächtiger und leistungsfähiger. Dies gilt auch für Windows NT. Für das Konzept von Windows NT hat man mehrere Betriebssysteme kombiniert, um ein Optimum an Leistung erzielen zu können.

22.2 Systemübersicht

Für Anwender bieten Betriebssysteme heute zwei wichtige Dienste:

- Die Verwendung der Hardware wird wesentlich erleichtert. Das heißt, der Anwender bekommt aufgrund der heutigen Anwenderoberflächen vom darunterliegenden Betriebssystem gar nichts mehr mit. Diese Situation wurde bereits sehr früh herbeigeführt. Einfache anwenderfreundliche Oberflächen wie der Norton Commander führten sehr rasch dazu, daß Anwender gar nicht mehr wissen, wie zum Beispiel eine Diskette auf dem herkömmlichen DOS-Prompt zu formatieren ist oder der Inhalt des Directory angezeigt werden kann.
- Das Betriebssystem verteilt den Zugriff auf die Hardware-Ressourcen auf das oder die laufenden Programme. Ganz wichtig ist dieser Vorgang für Multitasking-Betriebssysteme. Windows NT, ebenfalls ein Multitasking-Betriebssystem, teilt die Arbeiten in Prozesse auf, wobei jedem Prozeß Hauptspeicher, Systemressourcen und mindestens ein Thread (ausführbare Einheit innerhalb eines Prozesses) zugewiesen werden. Das Betriebssystem führt dabei den Thread für eine kurze Zeit aus und wechselt dann zum nächsten Thread. Auf diese Weise entsteht der Eindruck, daß die aktiven Programme alle gleichzeitig laufen würden, obwohl es in Wirklichkeit eine Quasi-Parallelität ist, da nur ein Prozessor verwendet wird. Anders sieht das jedoch aus, wenn das Betriebssystem eine Multiprozessor-Unterstützung aufweist, wie sie auch von Windows NT angeboten wird.

Windows NT benutzt folgende Modelle:

- Client/Server-Modell, um für die Anwender unterschiedliche Betriebssystemumgebungen bereitstellen zu können (Windows, MS-DOS, OS/2 und POSIX).
- Objekte, um die Systemressourcen einheitlich verwalten zu können und sie dem Anwender verfügbar zu machen.
- Das SMP (Symmetric Multiprocessing) ermöglicht es Windows NT, auf Rechnern mit mehreren Prozessoren eingesetzt zu werden, um die optimale Performance zu erzielen.

22.2.1 Client/Server-Modell

Der Systemcode eines Betriebssystems kann ganz unterschiedlich aufgebaut werden. Die meist in kleinen Betriebssystemen wie MS-DOS eingesetzte Form ist die Aufteilung des Betriebssystems in eine Reihe von Prozeduren, wobei jede Prozedur von der anderen Prozedur aufgerufen werden darf. Diese Form wird auch als monolithische Struktur bezeichnet. Die Erweiterung solcher Strukturen kann zu gewaltigen Problemen führen, da die Änderung einer Prozedur

22 Windows NT

an irgendeiner Stelle in anderen Teilen des Betriebssystems zu Fehlern führen kann, auch wenn kein direkter Zusammenhang zu erkennen ist.

Es gilt jedoch auch in monolithischen Systemen, daß die Anwendungen vom Betriebssystem getrennt werden. Das Betriebssystem läuft im privilegierten Prozessormodus (Kernel Mode) und hat erlaubten Zugriff auf Systemdaten und Hardware; hingegen laufen die Anwendungen im nicht privilegierten Prozessormodus (User Mode) mit einer begrenzten Anzahl Interfaces und einem beschränkten Zugriff auf Systemdaten.

Ruft ein Programm, das im Anwendermodus läuft, einen Systemdienst auf, fängt der Prozessor den Aufruf ab und schaltet den aufrufenden Thread in den Kernel Mode. Wenn der Systemdienst beendet ist, schaltet das Betriebssystem den Thread wieder in den Anwendermodus und der Anwender kann mit seiner Arbeit weitermachen.

Ein anderer Ansatz wird darin gesehen, das Betriebssystem in Module aufzuteilen, wobei in den einzelnen Modulen verschiedene Schichten implementiert sind. Jedes Modul stellt einen Satz Funktionen zur Verfügung, die von anderen Modulen aufgerufen werden können. Der Code in einer bestimmten Schicht ruft aber nur Funktionen von darunterliegenden Schichten auf.

Ein Vorteil dieser Schichtenstruktur kann darin gesehen werden, daß jede Codeschicht nur den Zugriff auf die darunterliegenden Schnittstellen und Datenstrukturen durchführt, die für die Arbeit benötigt werden. Der Programmcode mit uneingeschränkten Möglichkeiten für das Betriebssystem wird dadurch verringert. Zudem wird durch diese Struktur auch eine einfache Fehlerlokalisierung und -suche ermöglicht, da man in der untersten Schicht beginnt und dann die Suche Schicht für Schicht nach oben fortsetzt. Eine Schichtenbildung vereinfacht auch die Erweiterung des Betriebssystems, da eine ganze Schicht ausgetauscht werden kann, ohne die anderen Bereiche des Systems dadurch zu beeinflussen.

Die dritte Möglichkeit, ein Betriebssystem aufzubauen, erfolgt nach dem Client/Server-Modell. Die Idee, die man dabei zugrunde gelegt hat, ist, das Betriebssystem in mehrere Prozesse aufzuteilen, wobei in jedem Prozeß eine bestimmte Anzahl Dienstleistungsfunktionen implementiert sind – z.B. Speicherverwaltung, Prozessorverwaltung oder Prozeßsteuerung. Jeder Server läuft im Anwendermodus und führt eine Programmschleife aus, in der überprüft wird, ob ein Client eine seiner Dienstleistungen angefordert hat. Der Client – entweder eine andere Betriebssystemkomponente oder ein Anwendungsprogramm – fordert einen Dienst an, indem eine Nachricht an den Server geschickt wird.

22.2 Systemübersicht

Ein Betriebssystem-Kernel (Microkernel), der im Kernel Mode läuft, gibt die Nachricht an den Server weiter. Der Server führt die Operation durch; das Ergebnis wird mit einer neuen Nachricht über den Microkernel an den Client weitergegeben.

Durch diesen Ansatz wird ein Betriebssystem geschaffen, dessen Komponenten klein und abgeschlossen sind. Da jeder Server als eigener Anwendungsprozeß läuft, kann ein einzelner Server ausfallen oder neu gestartet werden, ohne daß das restliche Betriebssystem zerstört oder es zu einem Absturz des Gesamtsystems führen würde. Es ist auch denkbar, daß unterschiedliche Server in einer Multiprozessorumgebung auf unterschiedlichen Prozessoren laufen oder auf unterschiedlichen Computern bereitgestellt werden (Netzwerkfunktionalität in Windows NT). Dadurch sind solche Betriebssysteme hervorragend für den Einsatz in verteilten Umgebungen geeignet.

In der Praxis gibt es ein breites Spektrum unterschiedlicher Implementierungen dieser Betriebssystemform. Die einen führen weniger Arbeiten im Kernel Mode aus, wohingegen andere Konzepte mehr Arbeit in diese Ebene verlagern. Das Mach-Betriebssystem, das an Unix angelehnt ist, und ebenfalls eine Client/Server-Architektur aufweist, enthält einen Minimalkern, der sich um Thread Scheduling, Nachrichtenverarbeitung, virtuelle Speicherverwaltung und den Device Driver kümmert. Alle anderen Dinge wie Application Programming Interfaces (APIs), Dateisysteme und Netzwerkdienste laufen im User Mode.

Die Struktur von Windows NT nutzt sowohl die Konzepte des Schichtenmodells als auch die des Client/Server-Modells. Der Teil von Windows NT, der im Kernel Mode läuft, wird als NT Executive bezeichnet. Dieser Teil besteht aus einer Reihe von Komponenten, die sich um die virtuelle Speicherverwaltung, Objekt-Verwaltung (Ressource-), I/O- und Dateisystem (einschließlich Netzwerktreiber), Interprocess Communication und Teile des Sicherheitssystems kümmern. Die Zusammenarbeit zwischen diesen Teilen ist eher modular als geschichtet: Jede Komponente ruft die andere Komponente über einen sorgfältig definierten Satz interner Routinen auf.

Der Schichtenmodellansatz kommt für das I/O-System der NT Executive und für tiefere Schichten von NT – NT Kernel und Hardware Abstraction Layer (HAL) – zum Einsatz. Alle anderen Komponenten der Executive liegen in Schichten über diesen beiden Komponenten.

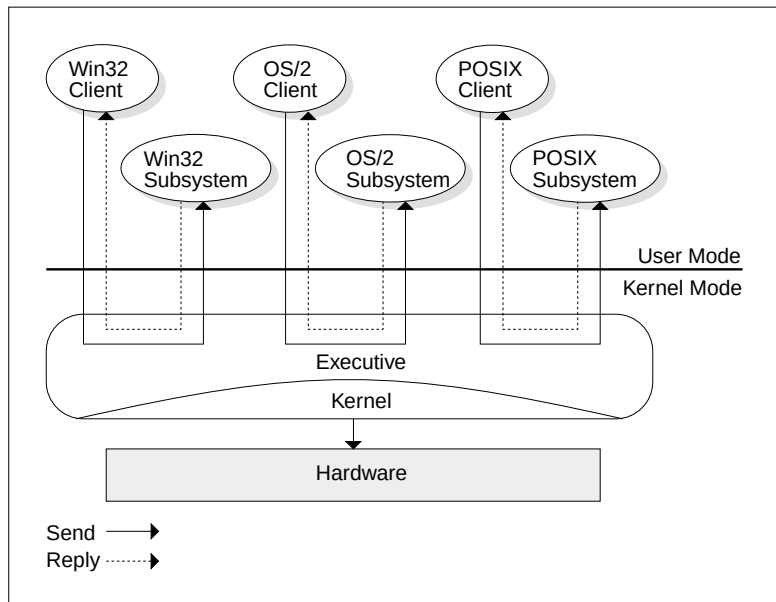
Der NT Kernel führt auf den unteren Ebenen Betriebssystemfunktionen durch, die auch im Microkernel von Client/Server-Betriebssystemen vorzufinden sind. Es handelt sich dabei vor allem um Thread Scheduling, Interrupt und Behandlung von Ausnahmebedingungen

22 Windows NT

sowie Multiprozessor-Synchronisation. Zudem wird eine Reihe von Funktionen und Basisobjekten angeboten, die vom Rest der Executive für die Implementierung von Konstrukten auf höherer Ebene benötigt werden.

Unterhalb des Kernels befindet sich die HAL Dynamic Link Library (HAL DLL). Dabei handelt es sich um eine Schicht hardware-spezifischen Codes, der den Kernel und den Rest der NT Executive vor rechner-spezifischen Hardware-Unterschieden schützt und somit NT hardware-unabhängig macht. Die Portierung auf eine andere Plattform geschieht in der Regel nur durch Austausch der HAL. Die HAL greift direkt auf die Hardware zu. In der nachfolgenden Abbildung ist die Client/Server-Struktur von Windows NT gezeigt.

Abbildung 22.1
Client/Server-
Struktur von
Windows NT



Windows NT benutzt das Client/Server-Modell in erster Linie für die APIs und die anderen Dinge, die man als Betriebssystemumgebung bezeichnen kann. Obgleich das Win32 Protected Subsystem (Server) die Anwenderschnittstelle bereitstellt und den Hauptbestandteil des Betriebssystems bildet, können die anderen Server in die Executive eingehängt und bei Bedarf geladen werden. Die Server kommunizieren mit Anwendungsprozessen durch eine Nachrichtenübertragung in der NT Executive.

22.2 Systemübersicht

Der Einsatz eines Client/Server-Modells bietet unter anderem folgende Vorteile:

- Es vereinfacht die Basis des Betriebssystems, die NT Executive. Ein Ziel von Windows NT ist die Bereitstellung von Win32, MS-DOS, 16-Bit-Windows, POSIX und OS/2 APIs. Die Verlagerung jeder API in einen eigenen Server vermeidet Konflikte und Mehrfachimplementierungen von Teilen des Betriebssystems und ermöglicht ein einfaches Hinzufügen neuer APIs.
- Die Zuverlässigkeit wird erhöht. Jeder Server läuft in einem eigenen Prozeß, hat einen eigenen Adreßraum und ist somit vor den anderen Prozessen geschützt. Da die Server im Anwendermodus laufen, haben sie zudem keine Möglichkeit, direkt auf die Hardware zuzugreifen oder Speicheroperationen der Executive durchzuführen – ein Problem, das man von MS-DOS kennt.
- Es kommt somit von allein der Mechanismus verteilter Systeme zustande. Da vernetzte Rechner nach dem Prinzip des Client/Server-Modells arbeiten und Nachrichtendienste verwenden, um miteinander zu kommunizieren, können lokale Server sehr einfach Nachrichten an Remote-Rechner versenden. Clients müssen von daher gar nicht wissen, wo sich die Dienste befinden und ausgeführt werden: local oder remote.

Um die Flexibilität von Windows NT zu erhöhen, hat man sich bei der Konzeption für den Einsatz eines Objektmodells entschieden. Wie dieses Modell aussieht und welche Vorteile damit verbunden sind, soll nachfolgend näher erläutert werden.

22.2.2 Objektmodell

Wie aus den bisherigen Beschreibungen zu ersehen ist, liegen die Schwierigkeiten vor allem darin, ein leistungsfähiges und flexibles Betriebssystem zu entwickeln. Statt zu versuchen, ein System von oben nach unten zu entwerfen, konzentriert man sich beim objektorientierten Entwurf zuerst auf die Daten, die von der Software bearbeitet werden müssen. Für ein Betriebssystem haben diese Daten die Form von Systemressourcen: Dateien, Prozesse, Speicherblöcke etc.

Das Ziel ist, ein System um diese Daten herum zu entwerfen, das leicht geändert werden kann. Ein Weg, wie objektorientierte Software den Änderungsaufwand minimiert, liegt darin, die physikalische Darstellung von Daten innerhalb von Objekten zu verbergen. Ein Objekt ist dabei als Datenstruktur zu verstehen, deren physikalisches Format hinter einer Typdefinition verborgen wird. Es beinhaltet eine Anzahl formaler Properties (Attributes genannt) und kann durch eine Anzahl von Diensten manipuliert werden.

22 Windows NT

Windows NT benutzt Objekte, um Systemressourcen darzustellen. Alle Systemressourcen, die von mehr als einem Prozeß benutzt werden können, einschließlich Dateien, gemeinsamem Speicher und physikalischen Endgeräten, sind als Objekte implementiert und mit Hilfe von Objektdiensten manipuliert. Dieser Konzeptansatz verhindert Auswirkungen von Änderungen, die im Laufe der Zeit im Betriebssystem durchgeführt werden. Zieht eine Hardware-Änderung zum Beispiel die Änderung des Betriebssystems nach sich, müssen nur das Objekt, das die Hardware-Ressource repräsentiert, und die Dienste, die für das Objekt möglich sind, geändert werden. Der Code, der dieses Objekt nur benutzt, bleibt unverändert.

Genauso einfach können neue Ressourcen in das System aufgenommen werden, ohne daß der bestehende Code geändert werden muß.

Neben diesen Vorteilen durch die geringen Änderungen im Betriebssystem bietet das Objektmodell auch noch andere Vorteile:

- Der Zugriff und die Manipulation der Ressourcen sind vereinheitlicht. Das Objektmodell erzeugt, löscht und benutzt ein Ereignisobjekt auf die gleiche Weise wie ein Prozeßobjekt, nämlich durch eine Objektnummer. Da jede Ressource als Objekt verwaltet wird, kann man die Ressourcen sehr einfach überblicken, indem man die Anlage und den Einsatz der Objekte verfolgt.
- Der Einsatz der Sicherheitsvorkehrungen ist einfacher, da alle Objekte in der gleichen Weise geschützt werden. Wenn irgend jemand versucht, auf ein Objekt zuzugreifen, wird das Sicherheitssystem zwischengeschaltet, das die Gültigkeit der Operation überprüft. Dabei ist es unerheblich, ob es sich um ein Objekt, einen Teil gemeinsamen Speichers oder um einen Kommunikationsport handelt.
- Objekte sind ein bequemes und einheitliches Mittel zur gemeinsamen Nutzung von Ressourcen zwischen zwei oder mehr Prozessen. Zur Bearbeitung aller Objekttypen reicht der Einsatz der Objektnummern. Zwei Prozesse benutzen gemeinsam ein Objekt, wenn beide eine Nummer hierfür anfordern. Das Betriebssystem kann überprüfen, wie viele Nummern für ein Objekt geöffnet sind, um festzustellen, ob das Objekt gerade benutzt wird. Das Betriebssystem kann dann das Objekt löschen, wenn es nicht mehr benötigt wird, da keine Nummer mehr dafür geöffnet ist.

22.2.3

Symmetrisches Multiprocessing

Beim Multitasking teilen sich mehrere aktive Threads einen Prozessor. Besitzt ein Rechner mehr als einen Prozessor, muß das Modell in Richtung Multiprocessing-System angepaßt werden. Ein Rechner mit »x« Prozessoren ist in der Lage, »x« Threads parallel auszuführen. Bei

22.2 Systemübersicht

einem reinen Multitasking-Betriebssystem hat man nur den Eindruck, daß Threads parallel ausgeführt werden, bei einem Multiprocessor-System hingegen geschieht die Abarbeitung tatsächlich parallel. Das Multiprocessing muß in zwei Kategorien aufgeteilt werden, da es zwei Formen gibt: Asymmetrisches Multiprocessing und Symmetrisches Multiprocessing.

- *Asymmetrisches Multiprocessing (ASMP)*

Bei einem ASMP-Betriebssystem wählt das Betriebssystem normalerweise einen Prozessor, auf dem das Betriebssystem läuft, wohingegen die Anwendungen auf dem anderen Prozessor laufen. Eine sinnvolle Lastenteilung ist bei diesem Konzept nicht möglich, da der andere Prozessor von einer Anwendung auch dann nicht genutzt werden kann, wenn er frei ist. Wesentlich effektiver und performanter ist das Konzept des Symmetrischen Multiprocessing.

- *Symmetrisches Multiprocessing (SMP)*

Windows NT baut auf das Konzept des SMP. Dabei ist es möglich, daß das Betriebssystem auf einem beliebigen Prozessor läuft oder auf allen gleichzeitig, dasselbe gilt für den Ablauf der Anwendungen. Die Prozessoren können Speicherbereiche gemeinsam nutzen. Dieser Ansatz nutzt die Prozessoren besser aus, da das Betriebssystem zur Laufzeit einen großen Teil des Rechners beanspruchen kann. Läuft das Betriebssystem hingegen nur auf einem Prozessor, kann es vorkommen, daß der Prozessor die Flut von Anforderungen nicht mehr zeitgerecht bedienen kann und dadurch die Gesamtleistung des Systems leidet. Zudem wird beim SMP-Konzept die Ausfallsicherheit erhöht, da das System auch dann noch weiterlaufen kann, wenn ein Prozessor ausfällt. Die Performance wird dann zwar schlechter, da ein Prozessor weniger zur Verfügung steht, aber wichtiger ist, daß die Arbeit weiter ausgeführt werden kann.

SMP-Betriebssysteme sind in der Regel komplett neu konzipiert und geschrieben, da strenge Codierregeln eingehalten werden müssen, um die korrekte Funktionsfähigkeit sicherstellen zu können. Zudem tritt in Multiprocessing-Systemen eine Vielzahl von Besonderheiten auf, die in Systemen mit nur einem Prozessor nicht berücksichtigt werden müssen. Viele Funktionen sind bei Windows NT entscheidend für den Erfolg eines SMP-Betriebssystems:

- Die Fähigkeit, das Betriebssystem auf jedem freien Prozessor laufen zu lassen, sofern es sich um ein Multiprocessor-System handelt. Mit Ausnahme der Kernel-Komponente, die sich um das Thread Scheduling und um Interrupts kümmert, können alle anderen Teile des Betriebssystems gezwungen werden, den Prozessor freizugeben, wenn ein Thread mit höherer Priorität auftritt.

22 Windows NT

- Mehrere ausführbare Threads innerhalb eines Prozesses ermöglichen es, einen Prozeß und/oder verschiedene Teile (Threads) auf mehreren Prozessoren gleichzeitig laufen zu lassen.
- Es werden Server-Prozesse bereitgestellt, die mehrere Threads nutzen, um Anforderungen von mehr als einem Client gleichzeitig zu bearbeiten.
- Windows NT unterstützt geeignete Mechanismen, um Objekte zwischen Prozessen gemeinsam nutzen zu können und eine flexible Interprocess Communication (Shared Memory und optimierte Nachrichtenübertragung) durchführen zu können.

Nach dieser Darstellung über den Mechanismus von Windows NT sollen im nachfolgenden Abschnitt die wichtigsten Strukturen von Windows NT und eine kurze Darstellung der Bedienung von Windows NT aufgezeigt werden, bevor ich mich dann den Netzwerkfunktionalitäten von Windows NT widmen will.

22.3 Die Struktur von Windows NT

Windows NT wird in zwei Teile gesplittet: den User Mode (Protected Subsystems) und den Kernel Mode (NT Executive). Einen Überblick über diese Aufteilung zeigt Abbildung 22.2.

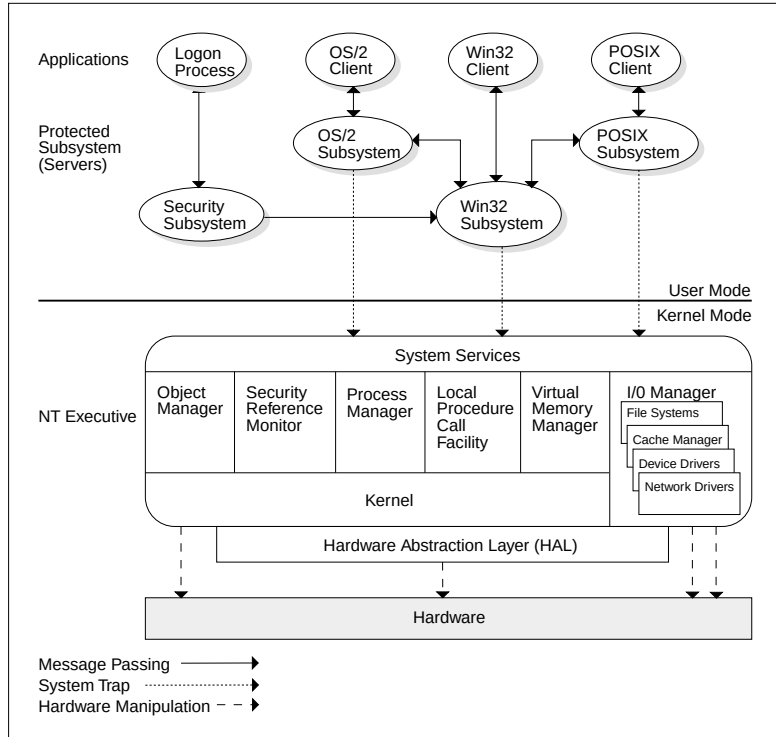
Die Windows NT Server bezeichnet man als geschützte Subsysteme (Protected Subsystems), da jeder in einem eigenen Prozeß abläuft und der davon benutzte Speicher über das Virtual-Memory-System von den anderen Prozessen geschützt wird. Da die Server nicht automatisch gemeinsamen Speicher nutzen, kommunizieren sie über Nachrichtenaustausch miteinander. Wie bereits erwähnt, ist die Executive als Betriebssystemkomponente in der Lage, eine beliebige Anzahl Server zu bedienen. Aufgrund ihrer Wichtigkeit sollen der Mechanismus der Protected Subsystems und die Executive näher betrachtet werden.

22.3.1 Protected Subsystem

Jedes Protected Subsystem stellt einen Satz APIs zur Verfügung, die von Programmen aufgerufen werden können. Wenn eine Anwendung oder ein Server ein API aufruft, wird eine Nachricht an den Server geschickt. Dies geschieht über den Local-Procedure-Call-Mechanismus (LPC) der NT Executive. Der Server antwortet über das Zurücksenden einer Nachricht dem rufenden Client.

22.3 Die Struktur von Windows NT

Abbildung 22.2
Windows NT im
Überblick



Windows NT kennt zwei Protected-Subsysteme: Environment-Subsystem und Integral-Subsystem. Ein Environment-Subsystem ist ein Server, der im User Mode abläuft und die APIs für eine spezielle Umgebung zur Verfügung stellt. Das wichtigste Windows-NT-Environment-Subsystem ist das Win32-Subsystem, das die Microsoft-Windows-32-Bit-API für Anwendungsprogramme zur Verfügung stellt. Zusätzlich stellt das Win32-Environment-Subsystem das GUI von NT zur Verfügung und überwacht jede Anwenderein- und -ausgabe.

Windows NT stellt ebenfalls ein POSIX-Environment-Subsystem, ein OS/2-Environment-Subsystem, ein Windows-16-Bit-Subsystem und ein MS-DOS-Subsystem zur Verfügung. Diese Subsysteme stellen den Anwendungsprogrammen ihre eigenen APIs zur Verfügung, benutzen jedoch zur Ein- und Ausgabe das Win32-Subsystem.

Die restlichen Protected-Subsysteme – die Integral-Subsysteme – sind Server, die wichtige Betriebssystemfunktionen übernehmen und ausführen. Eines der wichtigsten Integral-Subsysteme bildet das Security-Subsystem. Das Security-Subsystem läuft im Anwendermodus und überwacht die Sicherheitseinrichtungen, die auf dem lokalen Rechner aktiviert worden sind. Es wird zum Beispiel überwacht,

22 Windows NT

welche Anwender mit besonderen Rechten ausgestattet worden sind, auf welche Ressourcen der Zugriff gewährt worden ist und ob Alarmmeldungen und -nachrichten wegen Sicherheitsverletzungen erzeugt werden sollen. Zusätzlich pflegt das Security-Subsystem eine Datenbank, in der User Accounts, Anwendernamen, Paßwörter, Gruppen, in denen die Anwender Mitglied sind, oder Sonderrechte, die die Anwender besitzen, gespeichert werden. Nur so können die notwendigen Sicherheitsanforderungen erfüllt werden. Sie werden später sehen, daß Sie auf dem Windows-NT-System unterschiedliche Anwender einrichten können, die die Berechtigung haben, an diesem Rechner zu arbeiten. Je nach Berechtigungen kann der jeweilige Anwender auf mehr oder weniger Ressourcen zugreifen. Das heißt, daß mit Windows NT bereits die lokalen Daten vor unberechtigten Zugriffen geschützt werden können – unter DOS konnte das nur mit Zusatzsoftware erreicht werden.

Im Integral-Subsystem sind bereits die Komponenten der Netzwerksoftware von Windows NT enthalten. Zwei wichtige und interessante Funktionen sind dabei der Workstation Service und der Server Service. Jeder dieser beiden Dienste, oft als Netzwerk-Subsystem bezeichnet, ist ein User-Mode-Prozeß, der APIs implementiert hat, um auf den LAN-Manager-Netzwerk-Redirector und Server zugreifen und diesen verwalten zu können. Beim Redirector handelt es sich um eine Netzwerkkomponente, die dafür verantwortlich ist, I/O-Anforderungen über das Netzwerk zu transportieren, wenn die Dateien oder Endgeräte, auf die zugegriffen werden soll, nicht lokal vorhanden sind. Der Server ist dabei auf einem Remote-Rechner installiert und empfängt diese Anforderung. Sowohl der NT-Server-Redirector als auch der NT-Server-Dienst (mit eingeschränkten Funktionalitäten im Vergleich zum Original-NT-Server) sind bereits als Dateisystem-Driver implementiert. Somit kann Windows NT nicht nur als Workstation im Netzwerk eingesetzt werden, sondern bereits Server-Funktion im Netzwerk übernehmen. Die volle Leistungsfähigkeit als Server im Netz erhält Windows NT jedoch erst durch den Windows NT Server, der separat bezogen und installiert werden muß. Hierzu jedoch später mehr.

22.3.2

Executive

Die Windows NT Executive ist der Kernel-Mode-Teil und selbst, außer für das User Interface, ein vollständiges Betriebssystem. Die Executive besteht aus einer Vielzahl von Komponenten, wobei jede zwei Funktionen wahrnehmen muß: System Services, die vom Umgebungs-Subsystem und anderen Executive-Komponenten aufgerufen werden können, und Internal Routines, die nur den Komponenten innerhalb der Executive zur Verfügung gestellt werden.

22.3 Die Struktur von Windows NT

Obwohl die Executive API-ähnliche System Services zur Verfügung stellt, unterscheidet sie sich grundsätzlich vom Umgebungs-Subsystem. Die Executive läuft nicht die ganze Zeit als eigenständiger Prozeß. Die Executive wird erst im Kontext eines bestehenden Prozesses zum eigenständigen Prozeß, indem der Prozeß einen ausführenden Thread übernimmt, sobald wichtige Systemereignisse auftreten. Ruft ein Thread zum Beispiel eine Systemfunktion auf und der Prozessor fängt diesen Aufruf ab oder ein externes Gerät unterbricht den Prozessor, dann erhält der Kernel die Kontrolle über den dazugehörigen Thread.

Der Kernel ruft den passenden Code zur Bearbeitung des Ereignisses auf, führt ihn aus und gibt die Kontrolle an den Code zurück, der vor der Unterbrechung lief.

Executive-Komponenten sind weitgehend unabhängig voneinander, d.h., jede benutzt und erstellt die eigenen Datenstrukturen, die benötigt werden. Da die Schnittstellen zwischen den Komponenten sorgfältig festgelegt sind, ist es möglich, eine Komponente vollständig aus dem Betriebssystem zu entfernen und durch eine andere zu ersetzen. Sofern die neue Version alle notwendigen System Services zur Verfügung stellt und die internen Schnittstellen richtig bedient werden, läuft das Betriebssystem wie zuvor. Die Pflege des Betriebssystems ist ebenfalls einfacher wie bisher, da die NT-Executive-Komponenten in einer vorhersagbaren Art und Weise zusammenarbeiten.

Folgende Übersicht soll die Aufgaben der Executive-Komponenten verdeutlichen.

- *Object Manager*
Erzeugt, verwaltet und löscht Objekte der Executive – abstrakte Datentypen, die benutzt werden, um Betriebssystemressourcen darzustellen.
- *Security Reference Monitor*
Zwingt zu Sicherheitsvorkehrungen am lokalen Computer. Er überwacht die Betriebssystemressourcen, führt Run-Time-Objekt-Schutz und Auditing aus.
- *Process Manager*
Erzeugt und schließt Prozesse und Threads. Zudem setzt er die Bearbeitung von Threads aus oder nimmt sie wieder auf und verwaltet die Informationen über Windows-NT-Prozesse und Windows NT Threads.
- *Local Procedure Call (LPC)*
Transportiert Nachrichten zwischen Client-Prozessen und Server-Prozessen auf dem lokalen Rechner. Bei LPC handelt es sich um eine flexible und optimierte Version der Remote-Procedure-Call-Architektur (RPC), einem Industriestandard zur Kommunikation zwischen Clients und Servern über das Netzwerk.

22 Windows NT

■ *Virtual Memory Manager (VM)*

Zuständig für die Implementierung von virtuellen Speichern; eine Speicherverwaltung, die große und private Adreßräume für jeden Prozeß zur Verfügung stellt und gewährleistet, daß die Speicherbereiche gegenüber allen anderen Prozessen geschützt sind. Ist der Speicherbedarf zu groß, überträgt der VM-Manager ausgewählten Speicherinhalt auf Platte und lädt diesen Bereich wieder in den Hauptspeicher zurück, wenn er wieder benötigt wird. Dieses Verfahren wird als Paging bezeichnet.

■ *Kernel*

Reagiert auf Interrupts und Ausnahmebedingungen, führt die Thread-Verwaltung durch, synchronisiert die Aktivitäten mehrerer Prozessoren und stellt eine Vielzahl elementarer Objekte und Schnittstellen bereit, die vom Rest der NT Executive benutzt werden, um Objekte auf höherer Ebene einzurichten.

■ *I/O-System*

Dabei handelt es sich um eine Gruppe von Komponenten, die verantwortlich dafür sind, den Input von Devices und den Output zu Devices durchzuführen. Das I/O-Subsystem besteht aus folgenden Subsystemen:

– *I/O-Manager*

Stellt geräteunabhängige Input/Output-Funktionen zur Verfügung und errichtet ein I/O-Modell für die NT Executive.

– *File Systems*

NT Driver, die dateiorientierte I/O-Anforderungen annehmen und sie in I/O-Anforderungen umwandeln, die an ein bestimmtes Device gebunden sind.

– *Netzwerk-Redirector und Netzwerk-Server*

File System Driver, die Remote-I/O-Anforderungen zu einem Rechner im Netzwerk übertragen und auch solche Anforderungen von einem anderen Rechner empfangen können (wenn Windows NT selbst Server-Aufgaben bereitstellt).

– *Windows NT Executive Driver*

Hierbei handelt es sich um Driver auf der unteren Ebene, die direkt auf die Hardware zugreifen, um Ausgaben auf das physikalische Device oder das Netzwerk zu schreiben oder Eingaben von einem physikalischen Device oder dem Netzwerk zu lesen.

– *Cache-Manager*

Der Cache-Manager verbessert die Performance von dateiorientierten I/O, indem die zuletzt gelesenen Informationen im Speicher behalten werden. Der Cache-Manager nutzt die Paging-Funktionen des VM-Managers, um die Änderungen im Hintergrund automatisch auf Platte zu schreiben.

22.3 Die Struktur von Windows NT

Dieser Mechanismus kann durchaus mit dem Caching-Mechanismus von NetWare verglichen werden.

■ *Hardware Abstraction Layer (HAL)*

Eine Code-Schicht zwischen der Executive und der Hardware-Plattform, auf der Windows NT läuft. Sie verbirgt die hardwareabhängigen Einzelheiten, wie I/O-Schnittstellen, Interrupt Controller und Multiprocessor-Communication-Mechanismen, so daß Windows NT durch Austausch der HAL einfach auf andere Rechnerplattformen portiert werden kann. Die Komponenten der Executive erreichen maximale Portabilität, indem nicht direkt auf die Hardware zugegriffen wird, sondern die Routinen der HAL aufgerufen werden, wenn hardwareabhängige Informationen benötigt werden.

Windows NT zeichnet sich als portierbares Betriebssystem dadurch aus, daß es den hardwareabhängigen Code so gering wie möglich hält. Somit wird der Aufwand zur Anpassung an eine andere Plattform relativ gering. Man kommt jedoch nicht umhin, prozessorabhängigen Code (z.B. für Intel 486/586, DEC Alpha oder MIPS R4000) einzusetzen. Dieser liegt in den untersten Ebenen des NT Kernel sowie kleine Anteile im VM-Manager. Diese Komponenten, vor allem der Kernel, verbergen die Prozessorunterschiede vor dem Rest des Betriebssystems.

Rechnerabhängiger Code, d.h. Code, der abhängig von der Rechnerplattform ist, wird bei NT in der HAL eingebettet und von jedem Rechnerhersteller, der Windows NT unterstützen will, zur Verfügung gestellt. Zwar enthalten auch Device Driver geräteabhängigen Code, aber prozessorabhängiger und rechnerabhängiger Code wird dadurch vermieden, daß NT-Kernel-Routinen und HAL-Routinen aufgerufen werden.

Da Sie nun in etwa wissen, wie die einzelnen Komponenten von Windows NT aufgebaut sind und zusammenarbeiten, sollen im nächsten Abschnitt ein paar interessante und wichtige Eigenschaften beim Arbeiten mit Windows NT erläutert werden. Die Oberfläche von Windows NT ist derjenigen von Windows 3.1 sehr ähnlich, aber einige Unterschiede gibt es doch. Dies beginnt bereits damit, daß Sie Ihren Windows-NT-Rechner nicht einfach einschalten und anfangen können zu arbeiten. Um Zugriff auf Windows NT zu erhalten, müssen Sie sich zuerst anmelden.

22.4 Die wichtigsten Eigenschaften von Windows NT

Nur manchmal sieht man es Windows NT unmittelbar an, daß es sich um ein neues Betriebssystem handelt. Es gleicht Windows 3.1x und Windows 95 in der Version 4, und tatsächlich ermöglicht es auch den Einsatz reiner Windows-Anwendungen. Hinter der Anwenderoberfläche sieht es jedoch ganz anders aus. Die nachfolgenden Ausführungen zeigen Ihnen, wie die einzelnen Teile von Windows NT zusammenpassen. Dies beginnt bei der Schnittstelle für den Anwender und endet mit der Schnittstelle zur Executive.

22.4.1 Der Logon-Prozeß

Windows NT ist ein sicheres Betriebssystem, das verlangt, für jeden Anwender, der am Windows-NT-Rechner arbeiten kann und darf, einen Account einzurichten. Mit diesem Account ist der Anwender berechtigt, sich unter Windows NT anzumelden, und erhält dann Zugriff auf alle Ressourcen, für die ihm vom Administrator Berechtigungen vergeben worden sind. Sie können sich das in etwa so vorstellen, daß Sie einen Server einrichten, an dem zu einem Zeitpunkt nur ein Anwender arbeiten darf. Mit Hilfe der Netzwerkfunktionen können sich aber auch Anwender über das Netzwerk am Windows-NT-Rechner anmelden, die Zugriff auf die freigegebenen Ressourcen haben möchten.

Jeder User Account wird somit mit einem Sicherheitsprofil verknüpft – einer Sammlung von sicherheitsrelevanten Informationen, die in einer Systemdatenbank gespeichert werden. Das Security-Subsystem arbeitet mit diesen Informationen, um feststellen zu können, ob es sich beim angemeldeten Anwender auch um denjenigen Anwender handelt, der auf die Ressourcen zugreifen darf. Die Systemkomponenten, die mit dem Logon-Prozeß verknüpft sind, heißen: Security-Subsystem, Win32-Subsystem.

Ein Prozeß des Sicherheitssystems, Logon-Prozeß genannt, wartet auf die Eingaben eines Anwenders. Es können mehrere Logon-Prozesse aktiv sein, jeder für eine eigene Klasse von Logon Devices – z.B. die Kombination Tastatur/Maus oder die Netzwerkverbindung. Ein Thread im Prozeß stellt fest, wenn ein Anwender Windows NT benutzen will, und verlangt von diesem die Eingabe eines Anwendernamens und, wenn definiert, die Eingabe eines Paßworts.

22.4 Die wichtigsten Eigenschaften von Windows NT

Wenn Sie Windows NT gestartet haben, erscheint ein Fenster am Bildschirm, in dem geschrieben steht, die Tastenkombination **[Alt] + [Strg] + [Entf]** zu drücken, um sich anmelden zu können. Wer DOS gewöhnt ist, wird wissen, daß die Tastenkombination früher zum Warmstart des Systems geführt hat. Jetzt verwenden Sie diese Kombination zum Anmelden unter Windows NT.

Nach Eingabe von Anwendername und Paßwort gibt der Logon-Prozeß die Informationen zum Security-Subsystem weiter, das die Angaben in der Security-Datenbank überprüft. Ist der Logon erfolgreich, errichtet das Subsystem ein Objekt, das diesen Anwender in allen nachfolgenden Transaktionen eindeutig identifiziert. Dieses Objekt, Access Token genannt, ist der Schlüssel zur Sicherheit von Windows NT. Es legt fest, welche Systemressourcen die Threads des Anwenders benutzen dürfen.

Sobald die Identität des Anwenders festgestellt worden ist, erzeugt das Security-Subsystem einen Prozeß, fügt das Access Token an diesen Prozeß an und übergibt ihn an das Win32-Subsystem, das den Win32-Programm-Manager im Adreßraum des Prozesses laufen läßt. Danach ist der Anmeldevorgang für den Anwender vollzogen. Windows NT unterstützt sowohl lokale als auch Remote-Logons. Ein Server, auf dem Windows NT läuft, wird zu einem Zeitpunkt mehrere Logon-Sessions aktiv haben.

Sobald ein Anwender erfolgreich angemeldet ist, übernimmt das Win32-Subsystem die Kontrolle über den Bildschirm und stellt eine Oberfläche zur Verfügung, die ähnlich der von Windows 3.1 ist. Bei genauer Betrachtung stellt man einige Unterschiede fest, die jedoch mit den zusätzlichen Mechanismen von Windows NT im Vergleich zu Windows 3.1 zusammenhängen. Ab diesem Zeitpunkt kann der Anwender Win32-Programme, 16-Bit-Windows-Anwendungen, MS-DOS-, OS/2- und POSIX-Programme starten, sofern die Berechtigungen hierfür existieren.

Bei Windows 95/98 kann dieser Logon-Prozeß abgebrochen werden, wobei für den Anwender anschließend ein Standard-Profile geladen wird. Für Windows NT kann der Logon-Vorgang nicht unterbunden werden; diese Hürde ist zu nehmen. Steht Ihnen unter Windows 95/98 die gesamte lokale Platte zur Verfügung, so können auf der NT Workstation nur die Daten gesehen werden, für die der angemeldete Anwender auch Berechtigungen erhalten hat. Deshalb auch die wesentlich höhere Sicherheit im NT-Workstation-Betriebssystem.

22.4.2 Environment-Subsysteme

Das Win32-Environment-Subsystem stellt das Windows NT User Interface zur Verfügung. Es überwacht nicht nur den Bildschirm, sondern auch die Tastatur, die Maus und andere Input Devices, die am NT-Rechner angeschlossen sind. Nicht bei allen Anwendungen handelt es sich um Win32-Anwendungen. Die Überwachung von Nicht-Win32-Anwendungen wird nicht vom Win32-Subsystem durchgeführt. Startet der Anwender ein Programm, das das Win32-Subsystem nicht erkennt, bestimmt das Subsystem, um welche Art Anwendung es sich handelt, und ruft daraufhin entweder ein anderes Subsystem auf, um die Anwendung laufen zu lassen, oder initialisiert eine DOS-Umgebung, in der das Programm gestartet wird.

Jedes Environment-Subsystem stellt APIs bereit, die von der Client-Anwendung benötigt werden. Das Win32-Subsystem bietet 32-Bit-Windows-API-Routinen, und das OS/2-Subsystem stellt OS/2-APIs zur Verfügung. Die Anwendungen können aber nicht APIs aus verschiedenen Subsystemen mischen, da jedes Subsystem anders arbeitet und anders konzipiert ist. Ein File Handle, vom Win32-Subsystem erstellt, kann nicht für das POSIX-Subsystem umgesetzt werden.

Die Emulationen für MS-DOS- und 16-Bit-Windows-Anwendungen werden durch ein Subsystem verfügbar gemacht, das als Virtual DOS Machine (VDM) bezeichnet wird. Diese VDM stellt eine komplette MS-DOS-Umgebung zur Verfügung. Es lassen sich jedoch nicht alle von MS-DOS bekannten Befehle aufrufen. Genaue Angaben bezüglich dieser Einschränkungen sind der Dokumentation zu entnehmen. MS-DOS- und 16-Bit-Windows-Anwendungen laufen in VDMs, die wiederum als Clients auf dem Win32-Subsystem laufen. Jede MS-DOS-Anwendung läuft in einem eigenen VDM-Prozeß. Windows-3.1-Anwendungen werden als MS-DOS-Anwendungen angesehen, deshalb teilen sich alle Anwendungen unter dem emulierten Windows 3.1 eine VDM.

Da das Win32-Subsystem alle Bildschirmausgaben durchführt, müssen die anderen Environment-Subsysteme die Bildschirmausgaben der Anwendung dem Win32-Subsystem übergeben. Läuft in einer VDM eine 16-Bit-Windows-Anwendung, wird die Bildschirmausgabe in Win32-Aufrufe übersetzt und über eine Nachrichtenübertragung an das Win32-Subsystem übergeben. Das OS/2- und POSIX-Subsystem wie auch jede VDM, in der eine MS-DOS-Anwendung läuft, übergeben die zeichenorientierte Ausgabe zum Win32-Subsystem und zeigen die Ausgaben in einem zeichenorientierten Bildschirm an, der als Console bezeichnet wird.

22.4 Die wichtigsten Eigenschaften von Windows NT

Ein Environment-Subsystem kann zu einem gegebenen Zeitpunkt eine Vielzahl von Client-Anwendungen unterstützen. Jedes Subsystem kümmert sich um seine Clients und die globalen Informationen, die von allen Clients gemeinsam benutzt werden. Obwohl mehrere Subsysteme und VDMs aktiv sein können, bleibt Win32 das einzige Environment-Subsystem, das man zu Gesicht bekommt. Der Anwender hat den Eindruck, daß alle Anwendungen unter Windows NT laufen.

22.4.3 Native Service

Unter Native Service sind die Basisdienste von Windows NT zu verstehen. Environment-Subsysteme implementieren ihre API-Routinen durch den Aufruf von NT-Basisdiensten, System Services, die von individuellen Komponenten der NT Executive bereitgestellt werden.

Wenn ein Subsystem einen NT-Basisdienst aufruft, erkennt die Hardware den Aufruf und übergibt die Kontrolle an die NT Executive. Der Dienst läuft dann im Kernel Mode. Da die Basisdienste von verschiedenen Environment-Subsystemen benutzt werden, müssen sie sehr allgemein gehalten sein. Sie müssen flexibel sein und dürfen keine unnötig eingebauten Beschränkungen haben. Sie dürfen keine Nebeneffekte nach sich ziehen, die mit den verschiedenen anderen Environment-Subsystemen in Konflikt geraten könnten.

Flexibilität besteht unter anderem in der Fähigkeit, mit jedem beliebigen Prozeß zu arbeiten, der vom Anwender angegeben wird. Die Hauptanwender der Windows-NT-Basisdienste sind die Protected Subsystems, DLLs und Komponenten der NT Executive.

22.4.4 Objekte

Die meisten Windows-NT-Basisdienste sind Object Services, das heißt, daß sie irgendwelche Dinge mit Objekten der NT Executive durchführen. Gemeinsam nutzbare Ressourcen, einschließlich Prozessen, Threads, Dateien und gemeinsam verwendetem Speicher, sind als Objekte in der NT Executive implementiert. Dadurch wird es dem Betriebssystem ermöglicht, die Vorteile der Ähnlichkeiten von Ressourcen zu nutzen und gemeinsamen Code zu verwenden, wann immer dies möglich ist, um die Objekte zu verwalten.

Zusätzlich zur Verwaltung der Ressourcen und der Regelung zur gemeinsamen Nutzung von Ressourcen ist das Object System auch wichtigster Bestandteil für die Ressourcensicherheit. Wenn ein Thread ein NT-Objekt öffnet, wird das NT-Sicherheitssystem aktiviert. Zu jedem Objekt gehört eine kleine Datenbank, genannt Ac-

cess Control List (ACL), die festlegt, welche Threads Zugriff auf das Objekt haben und was mit diesem Objekt gemacht werden darf. Öffnet ein Thread ein Objekt, gibt er die Operation an, die ausgeführt werden soll.

22.4.5 Virtueller Speicher

Unter Windows NT laufen Anwendungen in einer Betriebssystemumgebung, die sich wie Windows, MS-DOS, POSIX oder OS/2 verhält. Der Trick dabei ist, alle Arten von Anwendungen lauffähig zu machen, ohne die Anwendung selbst neu schreiben zu müssen. Jedes Windows-NT-Environment-Subsystem sorgt dafür, daß die Clients den Speicher so sehen, wie ihn die Applikation auf dem Originalsystem vorfinden würde. Bei der Speicherarchitektur von Windows NT handelt es sich um einen virtuellen Speicher mit einem flachen, linearen Adreßraum, in dem mit 32-Bit-Adressen gearbeitet werden kann.

Während der Laufzeit übersetzt der VM-Manager die virtuellen Adressen in die physikalischen Adressen, an denen die Daten tatsächlich gespeichert sind. Durch die Überwachung der Umrechnung der Adressen kann vom Betriebssystem garantiert werden, daß einzelne Prozesse nicht überlagert oder Teile des Betriebssystems überschrieben werden.

Der virtuelle Adreßraum, der von jedem Prozeß genutzt werden kann, beträgt 4 Gbyte, wobei 2 Gbyte als Speicher für die Anwendung zur Verfügung stehen und 2 Gbyte als Systemspeicher genutzt werden können. 4 Gbyte Speicher ist bei weitem mehr, als heutzutage physikalisch im Rechner eingebaut sind. Ist der physikalische Speicher voll, lagert der VM-Manager Teile des Hauptspeichers auf Platte aus (Paging). Das Paging von Daten auf Platte setzt physikalischen Hauptspeicher frei, so daß dieser freie Speicher für andere Prozesse oder auch den gleichen Prozeß zur Verfügung steht.

Unter Windows NT liegt der Systemcode im oberen virtuellen Speicher, wohingegen Anwendungen und Daten im unteren virtuellen Speicherbereich abgelegt werden. Threads, die im User Mode laufen, können den Systemspeicher nicht direkt nutzen. Ein Teil des Speichers, als Nonpaged Pool bezeichnet, wird nie auf Platte ausgelagert und enthält einige Objekte und Datenstrukturen, die für Windows NT besonders wichtig sind.

Der andere Teil des Systemspeichers, als Paged Pool bezeichnet, kann auf Platte ausgelagert werden. Der gesamte User-Memory-Bereich kann auf Platte ausgelagert werden.

22.4.6 I/O- und Dateisysteme

So wie für den Speicher bieten Environment-Subsystems alle I/O-Möglichkeiten, die von der Applikation erwartet werden. Die Implementierung dieser Mechanismen erfolgt auch wieder durch Aufruf der NT-I/O-Basisdienste. Das Basis-I/O-System benutzt ein asynchrones I/O-Modell, aber es stellt Systemdienste zur Verfügung, die einem Environment-Subsystem den Einsatz eines asynchronen oder synchronen Modells ermöglichen. Asynchrone I/Os bedeuten für den Aufrufer, eine I/O-Operation anzufordern und andere Arbeiten durchzuführen, solange das Device mit der Übertragung der Daten noch nicht fertig ist. Das I/O-System informiert den Aufrufer automatisch, wenn der I/O abgeschlossen ist, so daß die weitere Verarbeitung durchgeführt werden kann.

Da I/O Devices generell langsamer sind als die Prozessoren, kann ein Programm, das mehrere I/Os durchführt, seine Geschwindigkeit erhöhen, indem asynchrone I/Os ausgeführt werden.

Windows NT unterstützt eine Vielzahl von Dateisystemen, einschließlich FAT-Dateisystemen (File Allocation Table), HPFS-Dateisystemen (High Performance File System) und ein neues Dateisystem für Windows NT: NTFS (NT File System). NTFS bietet als Dateisystem wesentlich mehr Möglichkeiten und Funktionen, als sie von FAT oder HPFS zur Verfügung gestellt werden können. Hierzu zählen folgende Eigenschaften:

- File System Recovery (ermöglicht eine schnelle Restaurierung der Daten auf der Platte nach einem Systemfehler)
- Unterstützung großer Plattenkapazitäten von bis zu 2^{64} Byte bzw. 17 Milliarden Gbyte
- Sicherheitseinrichtungen auf Directory- und Dateiebene
- Unicode-Dateinamen, womit es möglich wird, Dateien von einem Computer auf einen anderen Computer zu übertragen, ohne die Dateinamen zu verändern
- Unterstützung der POSIX-Betriebssystemumgebung, einschließlich Hard Links, case-sensitiven Namen und Informationen darüber, wann die Datei das letzte Mal geöffnet worden ist
- Funktionen für zukünftige Erweiterungen wie zum Beispiel transaktionsorientierte Operationen, um fehlertolerante Anwendungen zu unterstützen, anwendergesteuerte Versionsnummern für Dateien, flexible Optionen für Dateinamen und Dateiattribute sowie Unterstützung für die wichtigsten File-Server wie Novell, AppleShare oder SUN NFS.

Je nach Anforderung ermöglicht es der I/O Manager Device Driver, daß File Systems dynamisch geladen oder entladen werden. Die Driver sind modular und können übereinander geladen werden. Dadurch ist es möglich, daß unterschiedliche Dateisysteme den gleichen Harddisk Driver aufrufen, um auf Dateien zugreifen zu können. In Abbildung 22.2 wird das dargestellt.

Das Schichtenmodell für die Driver bietet zudem die Möglichkeit, zusätzliche Driver in die Hierarchie einzufügen.

Soweit zu den wichtigsten Merkmalen und Funktionen von Windows NT. Es wurde bereits mehrfach erwähnt, daß Windows NT eingebaute Netzwerkfunktionalitäten besitzt. Diese Funktionalitäten eignen sich jedoch nur für den Aufbau kleinerer Netzwerke, da sonst der Verwaltungsaufwand viel zu groß würde. Die volle Leistungsfähigkeit als Serverbetriebssystem erhält Windows NT nur durch den Einsatz und die Installation von Windows NT Server.

22.5 Die Netzwerkfunktionalitäten von Windows NT

Bei allen bisherigen Netzwerklösungen von Microsoft mußten die Netzwerkfunktionen für das Betriebssystem und den Rechner zusätzlich installiert werden. Obwohl man den LAN Manager als Netzwerkbetriebssystem bezeichnet hat, ist der LAN Manager nichts anderes gewesen als eine Ansammlung spezieller Anwendungen und Treiber, durch deren Installation auf OS/2 oder Unix Netzwerkfunktionen und -fähigkeiten implementiert wurden. Dadurch wurden Funktionen wie User Accounts, Ressourcen-Sicherheit und Intercomputer-Kommunikation mit Hilfe von Mail Slots oder Pipes über das Netzwerk erreicht.

Unter Windows NT ist die Netzwerksoftware nicht mehr länger als Add-on zum Betriebssystem implementiert. Statt dessen ist sie integraler Bestandteil der NT Executive. Die genauen Funktionen, die damit verbunden sind, sollen an anderer Stelle erläutert werden. Was ist jedoch unter der eingebauten Netzwerkfunktionalität von NT zu verstehen?

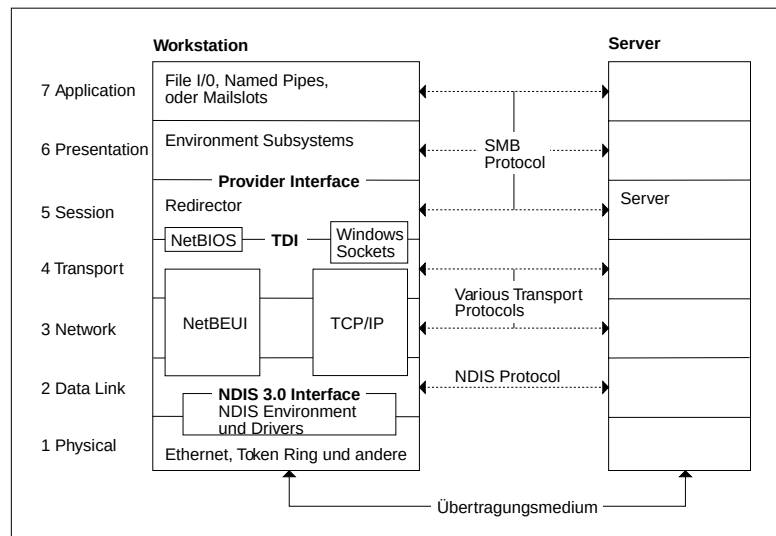
Zunächst sind die Peer-to-Peer-Netzwerkmechanismen von NT zu nennen, über die auch Windows for Workgroups verfügt. Windows NT ist mit Eigenschaften ausgestattet, die das Kopieren von Dateien, E-Mail oder das Drucken auf Netzwerkdruckern ermöglichen, ohne daß der Anwender zusätzliche Server-Software und Treibersoftware installieren muß. Einzige Voraussetzung ist, daß der Rechner, auf

22.5 Die Netzwerkfunktionalitäten von Windows NT

dem Windows NT eingerichtet wird, mit einer Netzwerkkarte ausgestattet ist, damit beim Installieren und Einrichten von Windows NT bereits die korrekten Eingaben für das Netzwerk gemacht werden können.

In Kapitel 9 wurde ausführlich über die Aufgaben und Funktionen des ISO-Schichtenmodells berichtet. Durch die nachfolgende Abbildung sollen Sie einen Eindruck davon erhalten, wie die Netzwerkkomponenten von Windows NT in das ISO-Schichtenmodell eingeordnet werden können.

Abbildung 22.3
ISO-Schichtenmodell und Windows-NT-Netzwerkfunktionen



User-Mode-Anwendungen (z.B. Win32 I/O APIs) führen einen Remote-I/O-Request aus, indem die Basis-NT-I/O-Dienste aufgerufen werden. Daraufhin errichtet der I/O-Manager ein I/O-Request-Paket (IRP) und gibt die Anforderung an einen der eingerichteten File System Driver, in diesem Fall den Windows NT Redirector. Der Redirector gibt das Paket an die darunterliegenden Driver (Transport Driver) weiter, die es bearbeiten und auf das Netzwerk geben. Wenn das Paket das Zielsystem erreicht, wird es vom Transport Driver empfangen und durchläuft eine Vielzahl weiterer Driver.

Der Zugriff einer Applikation auf Netzwerkressourcen kann auf mehrere Arten erfolgen:

- *Win32 I/O API*

Die I/O-Routinen führen das normale Öffnen, Schließen, Lesen, Schreiben sowie andere Funktionen durch. Der Durchgriff über das Netzwerk kann nur erfolgen, wenn die Datei oder Named

22 Windows NT

Pipe, auf die zugegriffen werden soll, auf einem Remote-Rechner existiert. Dies bedeutet, daß es sich bei dem Dateinamen um einen Uniform-Naming-Convention-Namen handelt oder der Dateiname mit einem Laufwerksbuchstaben beginnt, der auf einen Remote-Rechner verweist.

- *Win32 Network API (WNet)*

Diese Routinen sind hilfreich für Anwendungen, z. B. Windows NT File Manager, die die Verbindung zum Remote-Dateisystem aufbauen oder dieses nach bestimmten Dateien durchsuchen. Die WNet-Routinen können benutzt werden, um auf Microsoft-Dateisysteme oder andere Dateisysteme wie NetWare oder Vines zuzugreifen.

- *Win32 Named Pipe and Mailslots API*

Named Pipes bieten eine Schnittstelle auf höherer Ebene, die Daten zwischen zwei Prozessen austauschen können, ohne Rücksicht darauf, ob der andere Prozeß lokal oder remote ist. Mailslots sind mit Named Pipes vergleichbar, mit dem Unterschied, daß sie statt einer 1:1-Kommunikation zwischen Sender- und Empfänger-Mailslots eine 1:m- oder m:1-Kommunikation ermöglichen. Mailslots sind hilfreich, wenn Broadcast-Nachrichten an mehrere Prozesse weitergegeben werden müssen.

- *NetBIOS API*

Dieses API bietet Abwärtskompatibilität für jene MS-DOS-, 16-Bit-Windows- und OS/2-Anwendungen, die Datenströme direkt über das Netzwerk transportieren. Es wird von Windows NT auch eine neue 32-Bit-Version unterstützt.

- *Windows Socket API*

Dieses neue API stellt 16-Bit- und 32-Bit-Sockets zur Verfügung, ein Unix-ähnliches Interface für Internetworking. Windows NT bietet auch Code auf unteren Ebenen, der Unix-Anwendungen unterstützt, und ermöglicht es Windows NT, einfach in einem WAN-Internetwork zu kooperieren.

- *Remote Procedure Call (RPC)*

Mit dieser Library und dem Compiler wird es Programmierern erleichtert, verteilte Anwendungen zu schreiben.

Jedes API findet seinen Weg im Netzwerk auf unterschiedliche Art und Weise. Zum Beispiel: NetBIOS DLLs über den NetBIOS Driver oder Windows Sockets DLLs über den Windows Sockets Driver, wobei diese wiederum über das Transport Driver Interface an das Netzwerk übergeben werden.

22.5.1 Eingebaute Netzwerkkomponenten

Zu den wichtigsten Netzwerkkomponenten von Windows NT gehören der Redirector und der Netzwerk-Server. Durch die Implementierung des Redirectors und des Servers als File System Driver werden diese zum Bestandteil der NT Executive.

Redirector

Der Netzwerk-Redirector stellt die Mechanismen zur Verfügung, die für Windows NT notwendig sind, um auf Ressourcen zugreifen zu können, die sich auf einem anderen Server befinden. Der Windows NT Redirector kann auf Remote-Dateien, Named Pipes und Remote-Drucker zugreifen. Da der Redirector das SMB-Protokoll implementiert hat, kann er mit existierenden MS-NET- (sofern es diese noch gibt) und LAN-Manager-Servern arbeiten. Umgekehrt können MS-DOS-, Windows- und OS/2-Systeme auf Windows NT zugreifen, sofern auf den Clients die entsprechende Redirector-Software installiert ist und für Windows NT der Server Service aktiviert ist.

Sicherheitsmechanismen tragen Sorge dafür, daß nur berechtigte Anwender den Logon am Windows NT Server durchführen können. Der Redirector versendet und empfängt SMB-Daten, um seine Arbeit ausführen zu können.

22.5.2 Server

Wie der Redirector ist auch der Windows NT Server für hundertprozentige Kompatibilität mit existierenden MS-NET- und LAN-Manager-SMB-Protokollen geschrieben worden. Auf diese Weise ist es dem Windows NT Server möglich, Requests zu bearbeiten, die nicht von einem anderen Windows-NT-System stammen, sondern von anderen Stationen, die die LAN-Manager-Software installiert haben. Ebenso wie der Redirector ist der Server als File System Driver implementiert.

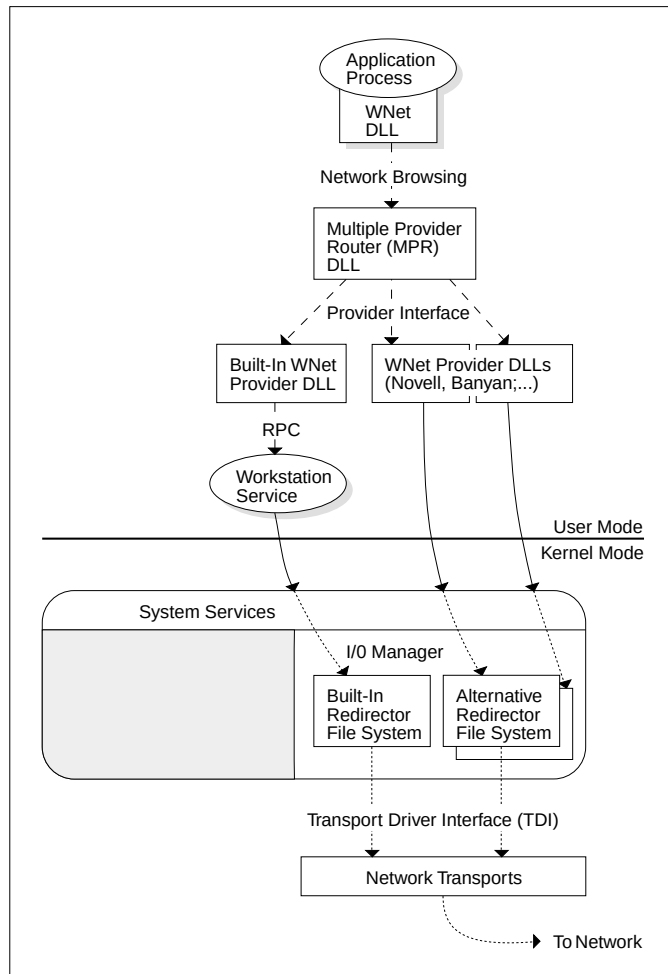
Lassen Sie sich nicht verwirren, wenn etwas als Server bezeichnet wird, obwohl es nicht als Server-Prozeß implementiert ist. Dadurch daß der Windows NT Server als Driver direkt in der Executive implementiert ist, kann der NT Cache Manager direkt aufgerufen werden, was die Performance wesentlich erhöht. Obwohl der Windows NT Server als File System Driver installiert ist, können andere Server entweder als Driver oder als Server-Prozeß eingerichtet werden.

Windows NT stellt eine offene Architektur dar, die nicht nur die Einbindung in Netzwerke mit SMB-Protokoll ermöglicht, sondern Windows NT auch als Client für andere Netzwerke einsetzbar macht

22 Windows NT

(Unix, NetWare, Vines). Die Win32-WNet-Funktionen ermöglichen es Anwendungen (einschließlich dem Windows File Manager), die Verbindung zu Netzwerk-Ressourcen herzustellen, z.B. zu File-Server und Drucker. Diese Funktionen ermöglichen auch das Durchsuchen von beliebigen Remote-Dateisystemen. Da das API aufgerufen werden kann, um auch auf anderen Netzwerken mit unterschiedlichen Transportprotokollen arbeiten zu können, muß Software vorhanden sein, um die Anforderung korrekt über das Netzwerk zu verschicken und das Ergebnis zu verstehen, das vom Remote-System zurückkommt. In der nachfolgenden Abbildung ist dargestellt, welche Software für diese Mechanismen verantwortlich ist. Alle renommierten Hersteller wie Banyan und Novell haben die Absichtserklärungen abgegeben, entsprechende Software zu entwickeln.

Abbildung 22.4
Einbindung in
eine heterogene
Welt



22.5 Die Netzwerkfunktionalitäten von Windows NT

Unter einem Provider ist Software zu verstehen, die Windows NT als Client in einem Netzwerk einrichtet. Aufgaben, die vom WNet Provider ausgeführt werden, sind das Aufbauen und Auflösen einer Netzwerkverbindung, das Drucken auf einem Netzwerkdrucker und die Übertragung von Daten. Der eingebaute WNet Provider enthält ein DLL, die Workstation-Dienste und den eingebauten Redirector. Andere Netzwerkhersteller müssen nur ein entsprechendes DLL und einen Redirector gemäß den Anforderungen des Netzwerkbetriebsystems dieses Herstellers zur Verfügung stellen.

Der in Abbildung 22.4 dargestellte Multiple Provider Router DLL muß entscheiden, auf welches Netzwerk zugegriffen werden soll, wenn die Win32 WNet API ein Remote-Dateisystem verwenden will.

Damit die Daten den richtigen Server erreichen und dieser auch das eintreffende Paket versteht, benötigt Windows NT ein entsprechendes Transportprotokoll (oder auch mehrere davon).

22.5.3 Transport-Protokolle

In Windows NT sind auch die Transport-Protokolle als Treiber installiert; sie können wie Redirector und Server geladen und entladen werden. In einem herkömmlichen Netzwerkmodell muß der Redirector, der ein bestimmtes Transport-Protokoll verwendet, wissen, welchen Typ Input dieser Protokolltreiber erwartet. Er schickt dann die Anforderungen in diesem Format zu ihm. Die unteren Schichten des Redirector müssen umgeschrieben werden, um die für jeden Transport unterschiedlichen Transfermechanismen zu unterstützen.

Windows NT umgeht dieses Problem, indem eine einzige Programmierschnittstelle zur Verfügung gestellt wird – für Redirector und andere Netzwerk Driver auf höherer Ebene. Diese wird als Transport Driver Interface bezeichnet (TDI). Das TDI ermöglicht es dem Redirector und den Servern, unabhängig vom eingesetzten Transportmechanismus zu bleiben.

Das TDI stellt einen Satz Funktionen zur Verfügung, mit denen der Redirector genutzt werden kann, um also jeden Datentyp transportieren zu können. Das TDI unterstützt sowohl verbindungslose als auch verbindungsorientierte Übertragung. Microsoft unterstützt standardmäßig folgende Transportprotokolle:

- *NetBEUI (NetBIOS Extended User Interface)*

Dieses LAN-Transport-Protokoll wurde von IBM entwickelt und von Microsoft erweitert.

- *TCP/IP (Transmission Control Protocol/Internet Protocol)*
Ein meist in der Unix-Welt eingesetztes Protokoll. Dieses ermöglicht Windows NT, auf Unix Hosts zu arbeiten (Terminalemulation, FTP etc.). Das TCP/IP-Transportprotokoll arbeitet in einer Streams-kompatiblen Umgebung.
- *IPX/SPX (Internet Packet Exchange/Sequenced Packet Exchange) NW-Link-Protokoll*
Transport-Protokolle, die von Novell für NetWare eingesetzt werden. Damit kann Windows NT vollständig in eine NetWare-Umgebung eingegliedert oder auch als eigenständiges System mit diesem Protokoll implementiert werden.
- *AppleTalk*
Transport-Protokoll zur Einbindung in eine Apple-Umgebung.

Bei der Entwicklung der Transport-Driver kann entschieden werden, ob diese für eine Streams-Umgebung konzipiert oder als monolithischer Driver wie NetBEUI gestaltet werden sollen.

In den folgenden Ausführungen möchte ich Ihnen zeigen, wie Sie die Windows-NT-Netzwerkfunktionen einsetzen können. Dabei geht es nicht nur um die integrierten Netzwerkfunktionen von Windows NT, sondern auch um die Möglichkeiten, die mit Hilfe des Windows NT Server geboten werden.

22.6 Der Einsatz der Windows-NT-Netzwerkfunktionen

Aus den bisherigen Kapiteln wissen Sie inzwischen, welche Komponenten für den Aufbau von Netzwerken notwendig sind. Um die Netzwerkfunktionen von Windows NT nutzen zu können, benötigen Sie mindestens zwei Rechner, passende Netzwerkadapter und Kabel, um diese verbinden zu können, und natürlich Windows NT als jeweils eigene Lizenz pro Rechner. Daß auch noch andere Server-Systeme unterstützt werden, wurde bereits erläutert.

Netzwerke können auf unterschiedliche Weise klassifiziert werden. Die eine Möglichkeit ist, die Klassifikation anhand der Topologie und der Transportprotokolle durchzuführen – das wurde bereits ausführlich besprochen. Es ist auch möglich, die Klassifikation durch die Aufgaben, die die Rechner im Netzwerk erhalten, durchzuführen: Client, Server oder beides gleichzeitig. Windows NT unterstützt zwei Arten von Netzwerkstrukturen: Distributed Networks und Dedicated Server Networks. Eine dritte Art Netzwerktyp wird als Domain Network bezeichnet. Das Domain-Network-Konzept wird jedoch nicht standardmäßig von Windows NT unterstützt. Diese Funktion erhält Windows NT erst mit der Installation von Windows NT Server.

22.6 Der Einsatz der Windows-NT-Netzwerkfunktionen

Die Unterschiede dieser Konzepte sollen nachfolgend erläutert werden, damit Sie einen Eindruck bekommen, wann sich welche Funktion für welchen Einsatz am besten eignet.

Distributed Networks

Ein Distributed Network besteht aus mindestens zwei Computern, die miteinander vernetzt sind, wobei jeder dieser Computer als Server und Workstation gleichzeitig fungieren kann. Das gleiche Prinzip erreichen Sie auch durch den Einsatz von Windows for Workgroups. Dadurch, daß jeder oder zumindest ein Teil der Rechner als Server und Workstation eingerichtet wird, können die Daten im Netzwerk vollkommen verteilt werden deshalb auch die Bezeichnung Distributed Network.

Problematisch dabei ist jedoch, daß auf jedem Server die Anwender separat für sich eingerichtet werden müssen, um anderen Stationen bzw. Anwendern im Netzwerk die Berechtigung, auf Daten des Servers zuzugreifen, zu geben. In kleinen Netzwerken ist dieses Konzept noch empfehlenswert, es sollte jedoch bei großen Netzwerken nicht mehr verwendet werden. Hier ist entweder das Konzept des Dedicated Server Network oder das Domain Network zu empfehlen. Die Gefahr beim Distributed Network liegt eindeutig darin, daß die Daten im Lauf der Zeit vollkommen zerklüftet im Netzwerk verteilt sind. Ein Problem tritt bereits auf, wenn ein Mitarbeiter seinen Rechner mit der Server-Funktion nicht gestartet hat und Sie auf Daten dieses Servers zugreifen wollen. Noch schlimmer wird es, wenn ein Anwender mit seiner eigenen Arbeit fertig ist, seinen Rechner abschaltet und dieser Rechner als Server im Netz arbeitet, auf dem momentan auch noch ein anderer Anwender Daten bearbeiten will. Bei diesem Konzept stehen jedoch nicht nur die Platten der definierten Server zur Verfügung, sondern auch die in den jeweiligen Rechnern installierten Drucker. Ein gemeinsames Ressourcen-Sharing ist somit relativ einfach. Der Aufwand zum Einrichten und Verwalten der Anwender mit all den dazugehörigen Zugriffsberechtigungen ist als ziemlich hoch einzuordnen.

Aus diesen kurzen Beschreibungen dürfte bereits ersichtlich sein, daß dieses Netzwerkprinzip wirklich nur im Notfall eingesetzt werden sollte.

Dedicated Server Network

Bei diesem Netzwerkkonzept wird ein Rechner als reiner Server definiert und eingerichtet. Es kann aber auch mehr als ein Server im Netzwerk vorhanden sein. Der grundsätzliche Unterschied zum vor-

22 Windows NT

her beschriebenen Konzept liegt darin, daß der oder die Server nicht mehr gleichzeitig als Workstation eingesetzt werden. Wenn man das Konzept von Banyan Vines oder Novell NetWare betrachtet, sieht man, daß diese Systeme genau nach diesem Prinzip arbeiten. Das Konzept von Windows NT ist zwar primär das des Distributed Network, aber Windows NT läßt sich auch als Dedicated Server Network nutzen. Man muß nur gewährleisten, daß auf dem Server kein normaler Anwender mehr arbeitet. Die Vorteile sind darin zu sehen, daß die Anwenderverwaltung zentralisiert auf diesem Server durchgeführt wird und auch die Datenhaltung und -verwaltung stärker zentralisiert abläuft. Nachteilig ist, daß beim Einsatz mehrerer Server im Netz, auf denen alle Anwender arbeiten dürfen, diese mehrfach eingerichtet und verwaltet werden müssen.

Probleme dieser Art weist auch NetWare 3 auf, sie werden durch NetWare 4 jedoch behoben. Für Windows NT wird Abhilfe durch Windows NT Server geschaffen, das so erhaltene Netzwerk wird als Domain Network bezeichnet.

Domain Network

Um die Verwaltung der Anwender im Netzwerk zu erleichtern, wird von Microsoft das Domain-Controller-Konzept zur Verfügung gestellt. Dieses Konzept wird ausführlich im nachfolgenden Kapitel erklärt. Windows NT selbst unterstützt dieses Konzept standardmäßig nicht. Der Domain Controller muß auf einem NT Server installiert werden. Ein Computer, auf dem Windows NT läuft, kann aber Mitglied einer NT Domain sein und ist besonders dafür ausgestattet, Mitglied einer Windows NT Server Domain zu sein.

Zusammengefaßt heißt das: Meist sind Distributed Networks, bei denen sich dieser Einsatz lohnt, klein und einfach. Nicht selten werden die anfänglichen Installationen auf diese Weise durchgeführt, weil man sich erst an das Arbeiten im Netzwerk gewöhnen will. Oft geht es auch nur darum, Ressourcen auf den einzelnen Rechnern gemeinsam nutzen zu können.

Nicht zu unterschätzen ist dabei, daß in der Regel jeder einzelne Anwender Kenntnisse über die Server-Funktion des Rechners besitzen muß, um im laufenden Betrieb eventuelle Anpassungen der Anwenderberechtigungen und des Ressourcen-Sharing durchführen zu können. Unübersichtlichkeit droht da. Sollte ein Administrator die einzelnen Server im Netzwerk verwalten müssen, ist er ziemlich ausgelastet, um alles funktionsfähig zu halten.

Die Leistungsfähigkeit des Computers, der sowohl Server als auch Workstation sein soll, muß entsprechend groß sein, damit keine Be-

22.6 Der Einsatz der Windows-NT-Netzwerkfunktionen

einträchtigung für den Serverbetrieb und den Workstationbetrieb zu befürchten ist. Es ist zu überlegen, ob sich diese generelle Investition auch wirklich rechnet.

Der Einsatz des Dedicated-Server-Konzepts ist in der Regel wesentlich effizienter, da die Verwaltung und Administration sehr viel einfacher durchzuführen ist. Durch die Zentralisierung der Verwaltung (User, Groups, Ressourcen) ist die Übersichtlichkeit im gesamten Netzwerk viel größer. Die Verwaltung des Netzwerks kann von einem Administrator übernommen werden, wobei es trotzdem eine oder mehrere Personen geben muß, die sich mit der Installation des Netzwerks gut auskennen. Dies gilt jedoch generell für jede Netzwerkinstallation. Nachteilig bei Dedicated-Server-Systemen ist die mehrfache User-Verwaltung, wenn also ein und derselbe Anwender auf mehreren Servern im Netzwerk Zugriffsberechtigungen erhält. Administration und Pflege werden aufwendiger und schwieriger.

Bei einem Domain Network handelt es sich um eine spezielle Form des Dedicated Server Network. Wie aus der Erklärung über das Domain-Konzept beim Windows NT Server zu sehen ist, kennt das Domain-Konzept einen Primary Domain Controller, auf dem alle Informationen abgelegt und verwaltet werden, die mit der Verwaltung des Netzwerks zu tun haben. Ein Anwender muß in einem solchen Netzwerk nur noch einmal eingerichtet werden, und er erhält damit Zugriff auf alle anderen Server im Domain-Netzwerk.

Ein Domain Administrator für den Windows NT Server kann für jeden Anwender ein Profile einrichten und verwalten, mit dem festgelegt wird, wie Windows NT selbst einzurichten ist, wenn sich der Anwender in einer Windows NT Server Domain anmeldet.

Windows NT stellt eine Reihe von Möglichkeiten zur Verfügung, den Rechner als Workstation oder Server im Netzwerk einzurichten. Diese sollen jetzt näher betrachtet werden.

■ *Installation des Netzwerkadapter-Drivers*

Jeder Rechner im Netzwerk muß mit einer Netzkarte ausgestattet werden, damit er im Netzwerk auch betrieben werden kann. Die Karte allein reicht jedoch nicht aus. Die passenden Device Driver für Netzkarte und Betriebssystem müssen installiert werden, um die Kommunikation im Netzwerk zu ermöglichen. Windows NT unterstützt bereits eine Vielzahl herkömmlicher Netzwerkadapter. Man sollte sich jedoch vorher vergewissern, ob der Hersteller der Karte eine entsprechende Driver-Software zur Verfügung stellt oder ob die Unterstützung der Karte bereits in Windows NT enthalten ist. Hierzu existieren Kompatibilitätslisten, aus denen diese Informationen zu entnehmen sind.

22 Windows NT

■ *Installation und Binding der Netzwerk-Protokoll-Software*

Der Kartentreiber ermöglicht nur die Kommunikation von Windows NT mit der Karte. Zusätzliche Software (z. B. Protokoll-Software) ist notwendig, um der Karte die Kommunikation mit dem Netzwerk, also mit anderen Systemen im Netzwerk, zu ermöglichen. Diese Software wird als Transport-Software bezeichnet. Sie wird entweder mit der Karte ausgeliefert oder ist im Lieferumfang von NT enthalten.

■ *Directory und Printer Sharing*

Wenn die Installation der Netzwerkkarte und der Transport-Software erfolgreich durchgeführt worden ist, steht die Netzwerkfunktion zur Verfügung. Die hauptsächlichen Aufgaben für das Arbeiten im Netzwerk sind dabei der gemeinsame Zugriff auf Directories, Dateien und Drucker. Diese Ressourcen werden von Serversystemen zur Verfügung gestellt, die auch gleichzeitig Workstation-Funktion haben können (Dedicated Server).

■ *Verbindung zu Remote-Directories und -Druckern*

Der Zugriff auf Remote-Directories und -Drucker hat nur dann Sinn, wenn der Anwender selbst Zugriff auf diese Ressourcen gewährt bekommt. File-Manager und Print-Manager erleichtern es unter Windows NT ungemein, Zugriff auf Remote-Directories und -Drucker zu nehmen.

■ *Anwenderzugriff auf Shared Resources*

Der gemeinsame Zugriff auf Ressourcen bedeutet noch nicht, daß alle Anwender uneingeschränkten Zugriff auf diese Ressourcen haben. Windows NT ermöglicht es Ihnen, festzulegen, welche Anwender auf Shared Resources zugreifen können und mit welchen Rechten auf diese Ressourcen zugegriffen werden darf.

Mit Hilfe einer Anwenderverwaltung unter Windows NT ist es möglich, User Accounts einzurichten, mit denen festgelegt wird, welche Ressourcen auf diesem Computer vom User benutzt werden dürfen. Für den Account wird festgelegt, welchen Grad der Verwaltung dieser Anwender für die Ressourcen und den Computer selbst erhält. Mit dem User Account kann man sich entweder direkt am Windows-NT-Rechner anmelden, oder die Anmeldung kann über das Netzwerk von einem anderen Rechner aus erfolgen.

Über den File-Manager kann definiert werden, wie Anwender auf Shared Directories zugreifen können. Auf Laufwerken, die mit NTFS-Dateisystem eingerichtet worden sind, sind zusätzliche Optionen möglich, die später besprochen werden sollen.

Über den Print-Manager kann festgelegt werden, welche Anwender auf die Drucker zugreifen können.

22.7 Andere Betriebssysteme und deren Einsatz im Netz mit Windows NT

- *Überwachung der Anwenderzugriffe für Shared Resources*
Vollständige Sicherheit bedeutet bzw. verlangt die Überwachung der Anwenderaktivitäten auf dem Server, damit festgestellt werden kann, wer versucht, die Sicherheitseinrichtungen von NT zu umgehen. Zudem können mit dem Utility-User-Manager und File-Manager Security-Auditing-Mechanismen aktiviert und mit dem Event Viewer die Audit-Log-Dateien ausgewertet werden. Mit dem Event Viewer können auch Datensätze angezeigt werden, in denen wichtige Systemmeldungen abgespeichert sind.
- *Überwachung der Verbindungen zu Shared Resources*
Mit dem Utility Control Panel kann eingesehen werden, welche Anwender gerade an dem Computer arbeiten, also angemeldet sind, Shared Resources können aufgelistet werden, und es kann angezeigt werden, welche Anwender mit diesen Shared Resources gerade arbeiten. Es können auch die Dateien angezeigt werden, die gerade von Remote-Anwendern benutzt werden. Es ist auch möglich, einzelne oder alle diese Anwender vom Computer zu trennen und die von diesen Anwendern geöffneten Dateien schließen zu lassen.
- *Electronic Mail und Group Scheduling*
Ein immer wichtigerer Aspekt für den Einsatz von Netzwerken ist die Möglichkeit, Nachrichten und Informationen zwischen Anwendern auszutauschen. Ein häufig eingesetztes Mittel, um Nachrichten, Texte und Dokumente von einem Rechner zu einem anderen Rechner zu versenden, ist Electronic Mail. Eine ähnliche Anwendung steckt hinter Group Scheduling. Hierbei geht es jedoch mehr um den Einsatz eines gemeinsamen Terminkalenders, der die Terminplanung vereinfacht. Microsoft Mail und Schedule+ sind als Standardprogramme verfügbare Anwendungen, die in Windows NT enthalten sind.

22.7 Andere Betriebssysteme und deren Einsatz im Netz mit Windows NT

Windows NT ist konzipiert, um mit einer Vielzahl anderer Systeme gemeinsam im Netz eingesetzt werden zu können. Die Netzwerkfunktionen basieren auf den Funktionen des LAN-Manager-Betriebssystems. Daher ist Windows NT, laut Aussage von Microsoft, vollständig kompatibel zu Rechnern, die eine andere Form der LAN-Manager-Software einsetzen oder ähnliche Betriebssysteme im Einsatz haben.

22 Windows NT

Computer mit folgenden Software-Produkten können gemeinsam mit Windows NT im Netzwerk eingesetzt werden und auf die Ressourcen von Windows NT zugreifen, wenn auf dem NT-System der Server aktiviert worden ist:

- MS-DOS und Windows für MS-DOS, wenn darauf die entsprechende Software installiert ist, um auf NT Server oder Windows NT zugreifen zu können,
- Microsoft Windows for Workgroups und
- OS/2, wenn darauf der LAN-Manager installiert ist.

Wichtig ist dabei, daß alle Rechner die gleiche Kommunikationssoftware nutzen, damit sie untereinander kommunizieren können. Windows NT selbst kann auch auf Ressourcen anderer Systeme zugreifen, wenn die entsprechende Kommunikationssoftware eingerichtet ist bzw. zur Verfügung steht. Windows NT kann als Client für Windows for Workgroups, Windows NT Server oder auch Novell NetWare eingesetzt werden.

Da Windows NT multiprotokollfähig ist, können auch andere Kommunikationsmechanismen eingesetzt werden. NT wird standardmäßig mit TCP/IP ausgeliefert – somit ist es möglich, daß der Windows NT Client die Verbindung zu einem Unix Host herstellt und als Terminal fungiert oder FTP oder r-Utilities ausführt.

Man muß aber auch für Windows NT eine sorgfältige Planung durchführen und festlegen, welche NT-Rechner Workstation, Server oder beides sein sollen, welche Anwender auf welchen Rechnern auf welche Ressourcen mit welchen Zugriffsrechten eingerichtet werden müssen. Das heißt, für den Einsatz von Windows NT als Server-Betriebssystem ist mit der gleichen Sorgfalt die Planung und Installation durchzuführen, wie dies bereits für NetWare angesprochen wurde (und für NT-Server noch erläutert wird), da ansonsten das Chaos im Netzwerk vorprogrammiert ist.

22.8 Sicherheitsmechanismen von Windows NT

Wie bei allen bisher besprochenen Netzwerkbetriebssystemen bietet auch Windows NT entsprechende Mechanismen, um Zugangs- und Zugriffsschutzmechanismen im Netzwerk gewähren zu können. Es wäre fatal, wenn man von jedem Rechner im Netz auf die Daten eines Windows-NT-Systems zugreifen könnte, sobald die Serverfunktion aktiv ist. Es müssen Maßnahmen zur Verfügung stehen, mit denen man Vorkehrungen treffen kann, um zu bestimmen, welche

22.8 Sicherheitsmechanismen von Windows NT

Anwender auf einen Server Zugriffsrechte haben, welche Zugriffsrechte festgelegt werden und auf welche Ressourcen Zugriffsrechte vergeben werden sollen.

Die gesamten Sicherheitsvorkehrungen auf Directory- und Datei-Ebene können bei Windows NT nur dann ausgeführt werden, wenn das neue Dateisystem NTFS eingesetzt wird. Windows NT unterstützt zwar auch das FAT- und das HPFS-Dateisystem, aufgrund der Vorteile, die NTFS bietet, es ist aber anzuraten, bei der Installation ausschließlich dieses neue Dateisystem auf den Platten zu konfigurieren. Man kann jedoch auch eine Mischung der Dateisysteme durchführen, wenn NT installiert wird. Ich werde Ihnen nur die Sicherheitsvorkehrungen aufzeigen, die Ihnen das NTFS-Dateisystem bietet. Vorab soll ein kleiner Vergleich der drei Dateisysteme durchgeführt werden:

NTFS

Vorteile

Unterstützung der vollen Windows-NT-Sicherheitsmechanismen, so daß ausgereifte Zugriffsberechtigungen auf Datei- und Directory-Ebene vergeben werden können. Die uneingeschränkten Zugriffsrechte auf Dateiebene sind nur mit dem NTFS-Dateisystem möglich. Das heißt, Zugriffsrechte auf Dateiebene sind mit HPFS- oder FAT-Dateisystem unter Windows NT nicht möglich. NTFS unterstützt die Fault-Tolerant-Möglichkeiten von Windows NT, um eine automatische Fehlerkorrektur auf Dateien oder NTFS-Partitionen durchzuführen.

NTFS unterstützt Datei- und Directory-Namen beliebiger Länge und erlaubt fast jedes Zeichen. Zudem werden auch die Extended File Attributes unterstützt, die bereits vom HPFS-Dateisystem bekannt sind. Damit auch DOS-Anwender im Netz auf solche Dateinamen zugreifen können, werden automatisch entsprechende DOS-Namen eingerichtet (vergleichbar mit dem Name Space Support von NetWare). MS-DOS-Programme können auf NTFS-Dateien zugreifen, wenn diese Programme unter Windows NT ablaufen.

Nachteile

Das NTFS-Dateisystem wird derzeit nur von Windows NT unterstützt. Wird der Windows-NT-Rechner unter einem anderen Betriebssystem gestartet (z.B. DOS oder OS/2), können diese Betriebssysteme nicht auf die NTFS-Partitionen zugreifen. Dies muß unter Betrachtung der Sicherheit jedoch nicht unbedingt als Nachteil angesehen werden. Auf eine Platte mit NetWare-Partition kann auch nur NetWare zugreifen und sonst kein anderes Betriebssystem, und das ist auch gut so. In den jetzigen Versionen ist es nicht möglich, eine Floppy-Disk mit NTFS-Dateiformat zu formatieren. Windows NT formatiert, liest und beschreibt Disketten nur im FAT-Dateisystem-Format.

22 Windows NT

FAT

Vorteile

Auf die Dateien und Directories kann unter MS-DOS und OS/2 zugegriffen werden. Da NT auch dieses Format unterstützt, ist natürlich auch von Windows NT aus der Zugriff auf diese Dateien möglich.

Auf dem Laufwerk C muß eine DOS-Partition eingerichtet sein, wenn der Computer auch unter MS-DOS von der Platte aus gestartet werden soll. Floppy-Disks oder wechselbare Festplatten, die gemeinsam im Netzwerk benutzt werden sollen, müssen das FAT-Dateisystem nutzen. An dieser Stelle sei angemerkt, daß Windows NT, vergleichbar mit NetWare v4.0, eine automatische Unterstützung des CDFS-Dateisystems (CD-ROM-Dateisystems) beinhaltet. Auf eine CD-ROM kann somit ohne zusätzlichen Installationsaufwand von allen Anwendern im Netzwerk zugegriffen werden.

Nachteile

Dateien einer FAT-Partition können unter Windows NT nicht mit den Sicherheitsmechanismen und Fault-Tolerant-Mechanismen von NT geschützt werden. Dateien und Directories einer FAT-Partition unterliegen der herkömmlichen 8.3-Konvention (achtstelliger Dateiname und dreistellige Extension).

HPFS

Vorteile

Unterstützung längerer Dateinamen (siehe Beschreibung des NT-Servers) und verbesserte Fehlerkorrekturmechanismen, als dies im FAT-Dateisystem der Fall ist.

Nachteile

Keine automatische Erzeugung von gültigen DOS-Dateinamen. Dateien auf einer HPFS-Partition können nicht mit allen Sicherheitsmechanismen von NT geschützt werden.

Soll der eingesetzte Rechner ausschließlich als Server oder Workstation für Windows NT verfügbar gemacht werden, ist auf alle Fälle bei der Installation das NTFS-Dateisystem einzurichten. Es ist jedoch auch möglich, eine FAT- oder HPFS-Partition in ein NTFS-Dateisystem umzuwandeln. Man kann aber eine NTFS-Partition nicht in eine FAT- oder HPFS-Partition umwandeln.

Windows NT unterstützt folgende Mechanismen, um Sicherheit für das System zu gewährleisten:

- Unterstützung eines UPS (Uninterruptable Power Supply)
- Für einen PC bietet Windows NT die bislang besten Mechanismen, um Sicherheit auf Anwenderebene gewährleisten zu können. Für ein Server-Betriebssystem sind die Mechanismen jedoch zwingend. Wenn Windows NT als Workstation eingesetzt werden

22.8 Sicherheitsmechanismen von Windows NT

soll, benötigt man auf keinen Fall mehr zusätzliche Software, um Zugangsschutz für diesen Rechner einzuführen, so wie dies unter DOS z.B. mit SafeGuard realisiert werden muß. Es sei nochmals darauf hingewiesen, daß dieser Schutz erst dann vollständig eingerichtet werden kann, wenn die Partitionen mit NTFS-Format eingerichtet sind.

- Eingebaute Backup-Mechanismen ermöglichen einen einfachen und schnellen Backup auf Band. Das ist für eine Workstation nicht zu vernachlässigen und schon gar nicht für NT, wenn es als Server genutzt wird.

Beim Einrichten der Sicherheitsvorkehrungen für Windows NT ist Ihnen sehr viel Freiheit gegeben, um das System absolut sicher oder weniger sicher einzurichten. Um jedoch ein großes Maß an Sicherheit zu erhalten, sollten Sie sich zum einen mit den Möglichkeiten vertraut machen und daraufhin entscheiden, welche Mechanismen für Ihre Umgebung am besten geeignet sind. Zum anderen sollte man darauf achten, die gesamten Möglichkeiten in ihrer einfachsten Form zu verwenden, d.h. die eingebauten Methoden so zu nutzen, daß sie das Arbeiten soweit wie möglich vereinfachen. Sie werden nachfolgend feststellen, daß sich die Konzepte von Windows NT nur geringfügig von anderen Netzwerkbetriebssystemen unterscheiden. Es liegt schon aufgrund der Anforderungen der Anwender auf der Hand, daß die Unterschiede nicht mehr als marginal sein können.

Windows NT nutzt drei wichtige Sicherheitsmethoden:

- *User Identification and Authentication*

Es kann auf einem Windows-NT-Rechner als lokaler oder Remote User nur derjenige arbeiten, für den ein User Account eingerichtet worden ist und die entsprechenden Rechte vergeben wurden, um auf Ressourcen zugreifen zu dürfen. Der Anwender-Account, also Name und eventuell Paßwort, müssen bekannt sein, damit eine Anmeldung am System erfolgen kann (siehe die Beschreibung des Logon-Vorgangs bei Windows NT). Solange der User Account und das Paßwort den Mitarbeitern einer Firma nicht bekannt sind, ist auch die Sicherheit im Netzwerk gewährleistet. Es ist leider nicht selten so, daß User Accounts in Firmen sehr vielen bekannt sind und somit die Sicherheitsvorkehrungen nicht beachtet werden.

- *Ausgereifte Zugangskontrollen*

Sicherheit ist mehr, als nur den Zugang einer Person zu bestimmen. Hierzu gehören auch die Festlegungen, auf welche Ressourcen Zugriffe gewährt werden sollen und mit welchen Rechten die Zugriffe durchgeführt werden können und dürfen. Damit nicht jeder seine eigenen Konfigurationen ändern kann, gibt es normale

22 Windows NT

Anwender und Administratoren bzw. Rechte eines Administrators, die ein Anwender haben kann. Die Festlegung der Rechte und der Umgebung für einen Anwender wird vom Administrator in einem Netzwerk bzw. für einen Windows-NT-Rechner definiert.

■ *Accounting*

Vollständige Sicherheit kann nur dann garantiert werden, wenn auch die Möglichkeit besteht, nachzuvollziehen, welche Aktionen ein Anwender durchgeführt hat. Nicht selten werden aus Versehen Dateien gelöscht, da ein Anwender das Recht dazu hatte. Um überprüfen zu können, von wem diese Datei gelöscht wurde, werden solche Vorgänge in einer Accounting-Datei gespeichert, die bei Bedarf ausgewertet werden kann. Diese Funktion stößt jedoch bei Betriebsräten größerer Unternehmen immer wieder auf Widerstand, da nach deren Meinung dadurch eine verstärkte Mitarbeiterkontrolle möglich ist. Es ist jedoch verwunderlich, daß auf Host-Systemen die Mechanismen akzeptiert werden, im PC-Netzwerk ihnen aber mehr Aufmerksamkeit geschenkt wird, obwohl hier Sicherheitsvorkehrungen genauso wichtig und notwendig sind.

Sicherheitsmechanismen sind jedoch nur so gut oder so schlecht, wie man sich an deren Einsatz hält und ihn durchführt. Ich habe schon eine Vielzahl installierter, meist kleinerer Netzwerke gesehen, in denen alle Mitarbeiter Administrator-Rechte haben, da der Aufwand zum Einrichten und Verwalten dadurch einfacher wird. Dies widerspricht jedoch vollständig den Zielen, die mit Netzwerken und den eingebauten Sicherheitsvorkehrungen erreicht werden sollen.

Was wird unter Windows NT unter einem User Account verstanden und welche Informationen werden dort abgespeichert bzw. können dort abgespeichert werden? Der Mechanismus ist durchaus vergleichbar mit den Methoden von NetWare, LAN Server, Vines oder Unix.

Der User Account ist eine Verwaltungseinheit in Windows NT, über die bestimmt wird, welche Rechte beim Anmelden mit diesem Account zu Verfügung gestellt werden. Jeder Anwender, der unter Windows NT oder einem Server arbeiten darf, muß einen User Account haben. In einem User Account von Windows NT werden folgende Informationen gespeichert:

- Der Anwendername, mit dem der Account identifiziert wird. Normalerweise verwendet man als *User-Account-Namen* den Vor- oder Nachnamen einer Person. Es kann jedoch auch eine beliebige Zeichenfolge verwendet werden. Man sollte nur darauf achten, den User-Account-Namen nicht zu lang zu machen oder zu kompliziert zu gestalten, da man sich mit diesem Namen am System anmelden muß.

22.8 Sicherheitsmechanismen von Windows NT

- Bei Bedarf kann der vollständige Name des Anwenders für dessen User Account eingetragen werden, damit eine leichtere Identifizierung möglich ist, vor allem bei späteren Auswertungen.
- Eine aussagefähige Beschreibung für den User Account, z. B. den Arbeitstitel dieser Person oder einen zweckgebundenen Namen für diesen Account.
- Das *Paßwort* für diesen User Account. Beim Einrichten des Account sind mehrere Möglichkeiten vorhanden, die Verwendung der Paßwörter zu definieren (z. B. Ablaufdatum).
- Man sollte darauf achten, ob der Account *disabled* ist oder nicht. Ist ein Account disabled, kann man sich unter diesem Namen nicht mehr am System anmelden. Wenn aus Sicherheitsgründen das Anmelden eines Anwenders für bestimmte Zeit unterbunden werden soll, muß man nicht den gesamten Anwender löschen (auch dann ist ein Anmelden mit diesem Account nicht mehr möglich), sondern man sperrt einfach den Zugriff für diesen Account und kann den Account selbst bei Bedarf wieder freigeben.
- Die *Gruppenzugehörigkeiten* für diesen Account. Die Steuerung der Rechtevergabe im Netzwerk über Gruppen ist eine sinnvolle, hilfreiche und flexible Möglichkeit, strukturiert und übersichtlich Rechtedefinitionen durchzuführen. Erfolgt die Rechtevergabe über Gruppen, erhält ein Anwender auf eine Ressource Rechte, sobald er Mitglied einer Gruppe ist, in der die Rechte für diese Ressource definiert worden sind. Die explizite Vergabe der Rechte direkt auf der Anwenderebene kann somit reduziert werden. Direkte Rechtevergabe explizit im User Account selbst wird nur dann durchgeführt, wenn die Rechtevergabe nicht über geeignete Gruppenelemente möglich ist.
- Vorgänge, die beim Initialisieren des Accounts zum Logon-Zeitpunkt festgelegt werden sollen bzw. beim Einrichten des Anwenders. Hierbei handelt es sich vor allem um das Einrichten eines *Home Directory* und das Einrichten eines *Logon Script* (unter NetWare als Login Script und beim NT Server als Profile bezeichnet).

22.8.1

Paßwörter unter Windows NT

Beim Einrichten eines Anwenders bzw. bei der nachträglichen Pflege hat man unter Windows NT im User Manager Utility die Möglichkeit, folgende Restriktionen für die Verwendung von Paßwörtern zu definieren:

- *Gültigkeitsdauer*
Festlegung, wie lange ein Paßwort gültig ist, bis Windows NT den Anwender auffordert, ein neues Paßwort festzulegen (never oder 1-999 Tage).

22 Windows NT

■ *Gültigkeitsdauer für Änderung*

Hiermit wird festgelegt, wie lange ein Anwender warten muß, bis ein neu vergebenes Paßwort geändert werden darf. Da der Anwender die Möglichkeit hat, bei Bedarf sein Paßwort zu ändern, wird hiermit eine Schranke auferlegt, wie lange ein Paßwort bestanden haben muß, bevor eine vorzeitige Änderung durchgeführt werden kann (immediately oder 1-999 Tage).

■ *Minimale Länge des Paßworts*

Ein Paßwort muß mindestens die angegebene Anzahl Zeichen haben, damit es von NT akzeptiert wird. Paßwörter die kürzer sind, werden abgewiesen (Blank Passwords oder 1-14 Zeichen).

■ *Eindeutigkeit des Paßworts*

Hiermit legt man fest, wie viele unterschiedliche Paßwörter benutzt werden müssen, bevor ein älteres Paßwort wieder verwendet werden kann. Es wird im Prinzip die Größe des Ringpuffers definiert, in dem die verwendeten Paßwörter abgelegt werden, um deren Eindeutigkeit zu garantieren (keine History-List führen oder ein bis acht Paßwörter aufzeichnen).

Beim Einrichten eines User Account haben Sie zudem die Möglichkeit, folgende Maßnahmen für das Paßwort zu definieren:

■ *User Must Change Password at Next Logon*

Beim nächsten Logon wird der Anwender bereits aufgefordert, ein neues Paßwort zu vergeben. Diese Option kann nur beim erstmaligen Einrichten des Anwenders vergeben werden. Die anderen unten aufgeführten Möglichkeiten können individuell auch für bestehende Accounts gesetzt werden.

■ *User Cannot Change Password*

Dem Anwender wird das Recht entzogen, sein Paßwort zu ändern. Die Vergabe eines neuen Paßworts kann nur vom Administrator oder einem Äquivalent durchgeführt werden.

■ *Password Never Expires*

Das Paßwort für diesen Account läuft nie ab und muß somit nie geändert werden.

22.8.2

Default Accounts

Bei der Installation von Windows NT werden drei Standard-Accounts eingerichtet. Die individuelle Anpassung kann nach der Installation vom Administrator durchgeführt werden.

■ *System Administrator Account*

Hierbei handelt es sich um einen Account, der unter dem Namen Administrator eingerichtet wird. Jeder Anwender, der in der Lage ist, sich mit diesem Namen unter NT anzumelden (oder an einem Server), hat die vollen Rechte auf das System. Er kann auf

22.8 Sicherheitsmechanismen von Windows NT

alle Ressourcen zugreifen und neue Anwender oder Gruppen einrichten sowie Rechtevergaben hierfür festlegen. Bestehende Anwender oder Gruppen können individuell geändert werden. Mit diesem Account sollte deshalb, wie bei allen anderen Systemen auch, sehr vorsichtig umgegangen werden.

■ *System Guest Account*

Dabei handelt es sich um einen User Account mit dem Namen Guest, der ebenfalls bei fast allen Netzwerkbetriebssystemen eingerichtet wird. Dieser Anwender-Account dient nur dazu, einen Anwender einfache Dinge auf dem System durchführen zu lassen. Anrichten können solche Anwender nichts, da die Rechte sehr eingeschränkt sind.

■ *Initial User Account*

Dies sind vom Administrator individuell eingerichtete Anwender, die mit den notwendigen Rechten ausgestattet werden, um auf entsprechende Ressourcen zugreifen zu können. Standardmäßig werden diese Anwender der Gruppe Power User zugewiesen. Welche Aufgaben damit verbunden sind, werden Sie anschließend erfahren. Bei Bedarf kann diese Berechtigung entzogen bzw. jeder Anwender mit zusätzlichen Gruppenzugehörigkeiten ausgestattet werden.

Jedes Netzwerkbetriebssystem enthält einen User Account, der mit allen Rechten ausgestattet ist. Die Namensgebung ist von System zu System verschieden, der Aufgabenbereich jedoch überall ähnlich. Der Systemadministrator von Windows NT oder ein Anwender, der Mitglied der Gruppe Administrator ist, kann folgende Aufgaben durchführen:

- Einrichten, Ändern oder Löschen von User Accounts
- Einrichten, Ändern oder Löschen von Gruppen
- Hinzufügen oder Entfernen von Gruppenzugehörigkeiten für User Accounts
- Hinzufügen von Special Rights für eine Gruppe
- Ändern der Betriebssystemsoftware
- Einrichten oder Ändern von Anwendungssoftware
- Einrichten oder Ändern von Device Drivern
- Formatieren der Festplatte
- Setup für den Rechner durchführen, damit eine Remote-Administration möglich ist

Wenn ein Anwender unter Windows NT eingerichtet wird, können unter anderem ein Logon Script und ein Home Directory für diesen Anwender definiert werden. Mit diesen beiden Einrichtungen können die Umgebungsbedingungen für jeden einzelnen User festgelegt werden, die zur Verfügung stehen, wenn sich dieser unter

22 Windows NT

Windows NT anmeldet. Zusätzlich zum Gebrauch von Home Directory und Logon Script kann bestimmt werden, wie die Computer-Konfiguration für jeden Anwender auszusehen hat. Dies geschieht durch ein Initial Profile für den Anwender.

Von jedem Anwender, der sich an Windows NT anmeldet, behält Windows NT Informationen über die Änderungen, die er für bestimmte Voreinstellungen durchgeführt hat, speichert diese Informationen in einer Datenbank beim Abmelden des Anwenders und stellt die gleiche Umgebungsbedingung für diesen Anwender wieder her, wenn er sich erneut am System anmeldet. Hierbei kann es sich um die Farben, die Gestaltung der Fenster u. ä. handeln. Windows NT sichert und restauriert folgende Anwendereinstellungen, wenn man sich unter Windows NT anmeldet:

- *Program Manager*
Alle Einstellungen, überwacht durch die Save Settings Option beim Verlassen des Program Manager, einschließlich Programm-Gruppen und Items
- *File Manager*
Alle Einstellungen, überwacht durch die Option Save Settings beim Verlassen des Programms
- *Windows NT Command Prompt*
Alle Windows-Einstellungen
- *Print Manager*
Alle Druckerverbindungen und Einstellungen
- *Control Panel*
Farbe, Maus, Desktop, Sound, International-Einstellung, Tastatureinstellungen und User-Environment-Variablen
- *Accessories and Applications*
Alle Anwendereinstellungen für Windows NT Accessories und für Windows-Anwendungen, die Anwendereinstellungen speichern können
- *Windows NT Help*
Alle Marken, die gesetzt worden sind (Einmerkungen = Bookmarks)
- *Applications*
Alle Voreinstellungen (Windows-Position, vorher geöffnete Dateien etc.), die von der Applikation gesichert werden können

Da der Anwender in der Lage ist, diese Einstellungen selbst zu ändern, können Sie es nicht vermeiden, daß die Oberfläche von Windows NT für jeden Anwender im Lauf der Zeit anders aussehen wird. Sollen jedoch bestimmte Programmteile von Windows NT nicht verfügbar sein (z.B. File Manager), müssen diese Programmteile mit Hilfe der Sicherheitsmechanismen auf Dateiebene blockiert werden, um einen Zugriff zu unterbinden.

22.8 Sicherheitsmechanismen von Windows NT

Für jeden Anwender kann also eine individuelle Arbeitsumgebung geschaffen werden. Dies ist vor allem dann interessant, wenn sich an einem Windows-NT-Arbeitsplatz mehrere Anwender nacheinander anmelden können und jeder von diesen seine eigene Umgebung zur Verfügung gestellt bekommt. Das gilt natürlich auch, wenn ein Remote Login an einer Windows-NT-Servermaschine erfolgt bzw. der Windows NT Server auf einem oder mehreren Windows-NT-Rechnern installiert ist.

Sie können bereits aus diesen Ausführungen ersehen, daß eine Verwaltung im Distributed Network Environment (Workgroups) sehr aufwendig werden kann, da jeder Windows NT Server seine eigenen Informationen sammelt und speichert. Um auf unterschiedlichen Windows NT Servern die gleiche Umgebung zur Verfügung zu haben, müssen wesentlich mehr Anpassungen durchgeführt werden. Anders wird es aussehen, wenn der Windows NT Server zum Einsatz kommt, der mit einem Domain-Konzept ausgestattet ist.

Ein weiteres wichtiges Instrument zum Einrichten, Verwalten und Überwachen der Zugangsberechtigungen unter Windows NT ist das Konzept der Gruppendefinitionen. Windows NT kennt nach der Installation bereits eine Vielzahl von Gruppen, mit der ein Administrator die Möglichkeit hat, bestimmte Arbeitsberechtigungen für User zu bestimmen.

Nach der Installation existieren folgende Gruppen: Users, Power User, Administrator, Backup Operator, Guests, Interactive Users, Network Users, Everyone und Creator/Owner. Jeder Anwender, der unter Windows NT arbeiten soll, sollte auch Mitglied der Gruppe Users sein, da damit grundlegende Rechte zum Arbeiten unter Windows NT vergeben werden.

Wenn ein Anwender Mitglied der Gruppe Power User ist, hat er die Möglichkeit, festzulegen, welche Directories als Shared Directories im Netzwerk freigegeben werden sollen. Da man diese Aufgabe nicht herkömmlichen Anwendern überlassen will, aber für die Durchführung solcher Aufgaben auch keinen Administrator-Status vergeben möchte (ein Administrator kann wesentlich mehr durchführen als ein Power User), gibt es unter Windows NT die Gruppe Power User.

Mit dieser Gruppenzugehörigkeit können und dürfen folgende Aufgaben durchgeführt werden:

- *Shared Directories im Netzwerk*

Festlegung, welche Directories als Shared Directories im Netzwerk verfügbar gemacht werden, bzw. Aufheben eines Shared Directory im Netzwerk. Zudem können Permissions für diese

22 Windows NT

Shared Directories definiert werden, die festlegen, mit welchen Rechten auf diese Directories und die darin befindlichen Dateien zugegriffen werden darf.

■ *Installation, Teilen und Verwalten von Druckern*

Mitglieder der Gruppe Power User können Shared Printer im Netzwerk definieren. Damit können Drucker eingerichtet und verwaltet werden.

■ *Einrichten, Ändern und Löschen von User Accounts*

Die Festlegung von Shared Resources im Netzwerk nützt relativ wenig, wenn nicht auch festgelegt werden kann, welche Anwender darauf zugreifen dürfen. Anwender mit diesen Gruppenrechten können neue Anwender einrichten, ändern oder auch wieder löschen. Anwender, die von einem anderen Anwender eingerichtet worden sind, können von diesem nicht geändert, geschweige denn gelöscht werden.

■ *Setzen der internen Uhr*

Ein User Account, der zur Gruppe Power User gehört, hat die Berechtigung, die interne Uhr auf dem Rechner zu setzen.

Auf die einzelnen Aufgaben, die ein User durchführen kann, wenn er zur Gruppe Administrator Group gehört, brauche ich nicht näher einzugehen, da das auf der Hand liegt. Die Bedeutung der anderen Gruppen bedarf keiner weiteren Erklärung, da sich deren Funktion aus dem Namen bereits ersehen läßt. Wesentlich wichtiger ist es jedoch, zu erfahren, welche Möglichkeiten bei der Vergabe von Zugriffsrechten auf Directory- und Dateiebene zur Verfügung stehen. Dies soll jetzt gezeigt werden.

22.8.3 Zugriffsrechte für Directories und Dateien

Bei der Vergabe von Zugriffsrechten muß man zwischen Standardrechten und Special-Access-Rechten unterscheiden.

Windows NT weist bei der Festlegung der Rechte für Directories eine Besonderheit auf, die bereits von Vines bekannt ist. Für ein Directory können Standardrechte definiert werden, die einer neu eingerichteten Datei in diesem Directory übertragen werden. Wenn jedoch ein Subdirectory in diesem Directory eingerichtet wird, erhält es die Rechte, die im Parent definiert worden sind. Die Standardrechtebestimmung für neu eingerichtete Dateien funktioniert nur auf Dateiebene.

Standardrechte für Directories

Windows NT kennt sechs Standardrechte, die für ein Directory definiert werden können, um festzulegen, mit welchen Rechten auf das Directory und die darin befindlichen Dateien zugegriffen werden

22.8 Sicherheitsmechanismen von Windows NT

kann. Die Rechte können auf Dateiebene zusätzlich explizit nochmals anders gesetzt werden als für das Directory selbst. Zu diesen sechs Rechten zählen:

No Access	Mit diesem Recht werden dem Anwender die Dateien im Directory nicht angezeigt. Zudem erhält der Anwender das Standarddateirecht No Access für alle Dateien, die nachträglich in diesem Directory eingerichtet worden sind.
List	Hiermit hat der Anwender das Recht, die Dateien im Directory angezeigt zu bekommen. Zudem erhält er Zugriff auf die Subdirectories in diesem Directory. Der Anwender kann jedoch keine Dateien einrichten und hat standardmäßig nicht das Recht, Dateien in diesem Directory zu benutzen, wenn sie von anderen Anwendern neu eingerichtet worden sind.
Read	Das Read-Recht erlaubt es dem Anwender, Dateien in diesem Directory angezeigt zu bekommen, und er erhält Zugriff auf Subdirectories in diesem Directory. Der Anwender kann keine neuen Dateien erstellen und erhält für neu eingerichtete Dateien anderer Anwender das Standard-Read-Recht. Ein Vergleich mit der Directory-Access-Tabelle im Handbuch ergibt, daß dieses Recht in seiner Bedeutung fast identisch ist mit dem List-Recht. Der Unterschied besteht nur in der Vergabe des Dateirechts für neu erstellte Dateien.
Add	Dieses Recht befähigt einen Anwender, in einem Directory neue Dateien zu erstellen, der Anwender kann jedoch den Inhalt des Directory nicht sehen. Der Anwender erhält automatisch keine Rechte, auf Dateien in diesem Directory zuzugreifen. Dies gilt auch für Dateien, die der Anwender selbst erstellt hat.
Add & Read	Damit erhält der Anwender die gleichen Rechte, die für das Read-Recht beschrieben sind, zusätzlich kann er neue Dateien einrichten. Der Anwender erhält automatisch das Standard-Read-Recht für jede neu erstellte Datei in diesem Directory.
Change	Mit diesem Recht kann ein Anwender in dem Directory neue Dateien erstellen und sich Dateien und Subdirectories in diesem Verzeichnis anzeigen lassen. Zudem können die Directory-Attribute angezeigt und geändert werden. Der Anwender erhält für alle neu eingerichteten Dateien das Standard-Change-Recht.
Full Access	Mit diesem Recht kann der Anwender Dateien erstellen, sich Dateien auflisten lassen, Attribute und Rechte für das Directory anzeigen lassen und diese ändern sowie Owner für das Directory werden. Werden im Directory neue Dateien eingerichtet, wird dem Anwender das Standard-Full-Access-Recht für diese Dateien zugewiesen.

22 Windows NT

Neben diesen Standard-Directory-Rechten kennt Windows NT auch noch Special-Access-Rechte für Directories. Worin liegt der Unterschied zwischen beiden?

Standard-Directory-Rechte schützen den Zugriff auf Directories, so wie dies auch bei Special-Access-Rechten der Fall ist. Bei den Standard-Directory-Rechten handelt es sich jedoch um eine Kombination vordefinierter Rechte der Special-Access-Rechte und der Special-File-Access-Rechte. Im Gegensatz zu den Standardrechten wird beim Einsatz der Special-Access-Rechte keine Voreinstellung der Rechtevergabe vorgenommen, die ein Anwender erhält, wenn neue Dateien im Directory eingerichtet werden.

Ich habe bei der Einführung in die NT-Rechte bereits darauf hingewiesen, daß NT eine Funktion zur Verfügung stellt, mit der man für einen Anwender und eine Gruppe festlegen kann, welche Rechte vergeben werden, wenn eine neue Datei im Directory eingerichtet wird. Bei der Vergabe der Rechte für neue Dateien entnimmt NT die Informationen beim Einsatz der Special-Access-Rechte aus dieser Definition. Man sollte deshalb beim Einsatz dieser Special-Access-Rechte für Directories dafür Sorge tragen, daß Default-Special-File-Access-Rechte definiert sind.

Special-Access-Rechte für Directories

Read	Ein Anwender kann sich die Namen der Dateien und die Attribute des Directory anzeigen lassen.
Write	Es dürfen neue Dateien eingerichtet und die Attribute des Directory geändert werden.
Execute	Mit diesem Recht hat der Anwender die Berechtigung, den Directory-Baum zu durchsuchen, er kann also auch den Inhalt des Subdirectory sehen.
Delete	Wenn das Directory leer ist, hat der Anwender das Recht, es zu löschen. Ist das Directory nicht leer, muß er auch noch das Recht besitzen, die Dateien und Subdirectories zu löschen.
Change Permissions	Hiermit können die Berechtigungen für das Directory geändert werden. Der Anwender hat aber nicht das Recht, Zugriffsberechtigungen für Subdirectories und Dateien zu ändern.
Take Ownership	Der Anwender kann sich mit diesem Recht zum Owner der Datei machen. Es besteht somit die Gefahr, daß der frühere Owner des Directory jede besondere Beziehung zum Directory oder gar den Zugriff auf dieses Directory verliert.

Ein Stufe tiefer können Sie auch noch den direkten Zugriff auf Dateiebene festlegen.

22.8 Sicherheitsmechanismen von Windows NT

Standardrechte für Dateien

Mit den Dateirechten wird festgelegt, wie auf Dateien zugegriffen werden kann. Insgesamt stehen Ihnen vier Standardrechte für Dateien zur Verfügung:

No Access	Der Anwender hat kein Recht auf diese Datei. Dieses Recht überschreibt jedes andere Recht, das ein Anwender für die Datei hat. Hat ein Anwender direkt das Read-Recht für die Datei erhalten, gehört aber zu einer Gruppe, die für diese Datei das No-Access-Recht zugewiesen bekommen hat, kann der Anwender die Datei nicht mehr öffnen und lesen, da das Read-Recht nicht mehr gilt.
Read	Mit diesem Recht kann der Anwender die Datei öffnen und den Inhalt der Datei bearbeiten. Handelt es sich bei der Datei um ein Programm, verleiht dieses Recht auch die Berechtigung, das Programm auszuführen. Nicht erlaubt ist es, Änderungen in der Datei durchzuführen und den neuen Inhalt abzuspeichern. Wenn jedoch die Read-Berechtigung existiert, kann die Datei kopiert oder eine durchgeführte Änderung mit neuem Namen abgespeichert werden. Mit dem Read-Recht hat der Anwender auch die Möglichkeit, sich die Dateiattribute und Berechtigungen anzeigen zu lassen und auch den Owner der Datei zu sehen.
Change	Dieses Recht enthält die gleichen Berechtigungen wie das Read-Recht, mit der zusätzlichen Möglichkeit, Änderungen in der Datei abzuspeichern. Mit der Change-Berechtigung kann die Datei auch gelöscht werden.
Full Access	Dieses Recht vergibt die volle Kontrolle über eine Datei. Neben der Berechtigung, die Datei zu lesen, auszuführen und den Inhalt der Datei zu ändern, bestehen auch die Rechte, die Dateiberechtigungen zu ändern, und sogar die Möglichkeit, den Anwender als neuen Owner für die Datei einzutragen.

Sie werden feststellen, daß diese Berechtigungen in der Regel genügen, um ausreichenden Schutz für Dateien zu definieren. Es kann jedoch sein, daß diese Möglichkeiten nicht hinreichen, um Ihre Dateien ausreichend zu schützen. Wenn das der Fall ist, nutzen Sie die Mechanismen, die Windows NT mit den Special-Access-Rechten für Dateien zur Verfügung stellt.

Special-Access-Rechte für Dateien

Read	Das Special-Access-Read-Recht unterscheidet sich vom Standard-Read-Recht dahingehend, daß hiermit nicht die Berechtigung vergeben wird, eine Programmdatei auszuführen, also ein Programm zu starten (.COM, .EXE oder .BAT). Hierfür gibt es ein eigenes Recht.

22 Windows NT

Write Das Special-Access-Write-Recht berechtigt den Anwender zum Öffnen der Datei und dazu, Änderungen der Datei auf die Platte zurückzuschreiben. Solange dieses Recht nicht mit dem Special-Access-Read-Recht kombiniert ist, kann der Anwender aber keine Daten von der Datei lesen, und so wird der Anwender entweder den gesamten Inhalt der Datei ersetzen oder Daten an die Datei anfügen, in Abhängigkeit der Applikation, die mit dieser Datei arbeitet.

Im Gegensatz zum Standard-Access-Recht Change, erlaubt das Special-Access-Recht Write nicht, die Datei zu löschen. Ein Anwender kann aber die Datei öffnen, um ihren Inhalt zu ersetzen und sie dann schließen, ohne neue Daten zu schreiben – es entsteht also eine leere Datei. Vorsicht beim Umgang mit diesem Recht! Damit können Daten verlorengehen.

Execute Hiermit wird der Anwender berechtigt, ein Programm auszuführen. Dieses Recht muß in Kombination mit dem Special-Access-Recht Read für eine Programmdatei vergeben werden, wenn der Anwender auch das Recht haben soll, ein Programm zu starten.

Delete Dieses Recht berechtigt einen Anwender, eine Datei aus dem Directory zu löschen. Ein Anwender benötigt dieses Recht, um eine Datei entweder zu löschen oder für die Datei einen Move durchzuführen.

Change Permissions Dieses Recht erlaubt dem Anwender, die Rechte für die Datei zu ändern, einschließlich der Rechte, die einen Zugriff auf die Datei für den User verhindern würden. Ein Anwender, dem dieses Recht für die Datei verliehen wird, hat im Prinzip die volle Kontrolle über die Datei, da sogar die Dateiberechtigung geändert werden und man sich selbst als Owner für die Datei eintragen kann.

Take Ownership Der Anwender kann mit diesem Recht zum Owner der Datei werden. Wird der Anwender neuer Owner der Datei, verliert der frühere Owner jeglichen speziellen Bezug zu dieser Datei und kann daran gehindert werden, Zugriff auf diese Datei zu nehmen.

Dateiattribute

Neben der Vergabe von Zugriffsberechtigungen bietet Windows NT auch die Möglichkeit, für Dateien Attribute zu vergeben. Dieser Mechanismus ist jedoch bei weitem nicht so stark ausgeprägt wie zum Beispiel bei NetWare.

Folgende Dateiattribute stehen unter Windows NT zur Verfügung:

R (Read Only) Die Datei kann nur gelesen werden. Auch wenn der Anwender Schreibberechtigung besitzt, kann eine Datei, die dieses Attribut besitzt, nicht mehr geändert werden.

22.9 Plattenverwaltung unter Windows NT

- A (Archive)** Eine Datei, die seit dem letzten Backup geändert worden ist, erhält das Archive-Attribut zugewiesen. Das macht Windows NT ohne Ihr Zutun. Somit ist es möglich, statt einen erneuten Full Backup durchzuführen, einen Incremental Backup anzustoßen, bei dem nur die Dateien gesichert werden, deren Archive-Attribut gesetzt ist. Beim Backup dieser Dateien wird dieses Attribut wieder zurückgenommen.
- H (Hidden)** Die Datei erscheint nicht mehr beim Auflisten des Directory-Inhalts, wenn der DIR-Befehl auf Command-Line-Ebene durchgeführt wird. In einem Windows-NT-Fenster werden Dateien mit diesem Attribut nur dann angezeigt, wenn man explizit angibt, auch Hidden-Dateien sehen zu wollen.
- S (System)** Die Datei wird als Systemdatei identifiziert. Sie wird beim DIR-Befehl nicht angezeigt. Im Directory-Fenster von Windows NT erscheint die Datei nur dann, wenn man explizit angibt, auch solche Dateien sehen zu wollen.

Sie haben jetzt einen umfassenden Überblick über Windows NT erhalten, der Ihnen helfen sollte, Ihnen einen Gesamteindruck von den Möglichkeiten dieses Systems zu bieten. Bevor ich Ihnen die grundsätzlichen Eigenschaften für den Windows NT Server darstellen will, soll abschließend erläutert werden, wie beim Einrichten von Windows NT die Konfiguration der Festplatten durchgeführt werden kann.

Das ist notwendig, um sich einen Eindruck über die Flexibilität dieser Mechanismen machen zu können, wenn man Windows NT als Server einsetzen will und um so mehr, wenn man das Windows-NT-Server-System installieren will.

22.9 Plattenverwaltung unter Windows NT

Die Plattenverwaltung unter Windows NT kann als sehr flexibel bezeichnet werden. Auf dem freien Platz einer Platte können bis zu vier Partitionen eingerichtet werden. Zudem haben Sie die Möglichkeit, mehrere logische Laufwerke im freien Bereich einer Extended Partition zu definieren.

Im freien Bereich einer Platte können folgende Einrichtungen durchgeführt werden:

- Single Primary Partition
- Bis zu vier Additional Partitions
- Extended Partition mit einer beliebigen Anzahl logischer Laufwerke
- Andere Windows-NT-Typen, Volume-Sets und Stripe-Sets

22 Windows NT

Zum besseren Verständnis hier einige Erklärungen zu den verwendeten Bezeichnungen und Möglichkeiten.

Free Space	Ein nicht benutzter Teil auf der Platte, der partitioniert werden kann. Free Space innerhalb einer Extended Partition ist zum Einrichten logischer Laufwerke verfügbar. Free Space, der sich nicht innerhalb einer Extended Partition befindet, ist zum Einrichten von Partitionen verfügbar, wobei eine maximale Anzahl von vier erlaubt ist.
Partition	Der Teil einer Platte, der als eigene separate physikalische Einheit behandelt werden kann. Eine Partition wird normalerweise als Primary oder Extended Partition bezeichnet.
Primary Partition	Der Teil einer Platte, der für ein Betriebssystem markiert werden kann. Es können bis zu vier Primary Partitions pro physikalischer Platte benutzt werden (bis zu drei, wenn eine Extended Partition eingerichtet ist). Eine Primary Partition kann nicht in Subpartitionen unterteilt werden.
Extended Partitions	Wird auf dem Free Space einer Platte eingerichtet und kann unterteilt werden in null oder mehrere logische Laufwerke. Der Free Space einer Extended Partition kann auch benutzt werden, um Volume Sets oder andere Volume-Typen zu definieren oder um Fault Tolerant Volumes einzurichten. Nur eine der vier Partitionen, die pro Platte erlaubt sind, kann als Extended Partition eingerichtet werden. Es muß keine Primary Partition vorhanden sein, um eine Extended Partition einrichten zu können.
Volume	Ein Volume ist eine Partition oder eine Ansammlung von Partitionen, die für die Verwendung eines Dateisystems formatiert worden ist. Einem Windows NT Volume kann ein Laufwerksbuchstabe zugewiesen werden, der zum Einrichten von Directories oder Dateien genutzt werden kann.

Besonders interessant ist bei Windows NT das Einrichten von Volume Sets. Man kann damit eine wesentlich effizientere Ausnutzung des gesamten verfügbaren freien Speicherplatzes auf der Platte erreichen. Man richtet Volumes ein, indem man die unterschiedlich großen Free-Space-Bereiche von bis zu acht Platten in einem logischen Volume Set zusammenfaßt und danach wie eine einzelne Partition betrachtet.

Eine Alternative besteht darin, sogenannte Stripe Sets zu definieren. Das Einrichten von Stripe Sets ist mit einem Volume Set vergleichbar, hier existieren aber zusätzliche Einschränkungen. Jede Partition in einem Stripe Set muß sich auf einer eigenen Platte befinden. Die Anzahl der Platten ist auf acht beschränkt. Beim Einrichten von Stripe Sets werden die Free-Space-Bereiche von bis zu acht Platten zu ei-

22.9 Plattenverwaltung unter Windows NT

nem gesamten Volume zusammengefaßt, wobei der Disk-Manager beim Einrichten der Stripe Sets die Größe der einzelnen Partitionen in etwa angleicht.

Die Daten können somit in »Stripes« auf die einzelnen Partitionen geschrieben werden. Dadurch können I/O-Befehle gleichzeitig durchgeführt werden, wodurch der Durchsatz wesentlich erhöht wird.

Ich habe versucht, bis zu diesem Punkt alle wichtigen und interessanten Eigenschaften von Windows NT und den damit verbundenen Netzwerkfähigkeiten darzustellen. Es gäbe noch eine Vielzahl weiterer Informationen, die in Windows NT eingebaut und ebenso interessant sind. Sie vorzustellen ist innerhalb des Rahmens dieses Buchs nicht zu leisten. Auf jeden Fall handelt es sich bei Windows NT um ein leistungsfähiges Betriebssystem mit einer Oberfläche, die vielen bereits bekannt ist. Es wurden Funktionen und Mechanismen eingebaut, die sowohl für ein Netzwerkbetriebssystem zur Verfügung stehen, aber auch dann eingesetzt werden können, wenn Windows NT als reines Workstation-Betriebssystem eingesetzt wird.

Windows NT kann ohne Zweifel als Alternative zu Unix, OS/2 oder Windows 95/98 betrachtet werden. Die Akzeptanz bei den Anwendern wird zeigen, welches dieser Systeme in Zukunft auf dem Markt bestehen wird. Windows NT als Arbeitsplatzsystem für normale Routinearbeiten zu verwenden, dürfte zwar leicht überzogen sein, da die Anforderungen mit einem 16-Mbyte-Hauptspeicher (besser sind 32 Mbyte) und mindestens 500-Mbyte-Plattenkapazität ziemlich hoch sind. Wer jedoch echtes Multitasking haben will – mit der Option auf Multiprocessing –, mit der Möglichkeit, alle herkömmlichen Programme unter DOS, Windows etc. nach wie vor einzusetzen, der ist mit Windows NT auf alle Fälle gut bedient. Bevor man jedoch die Entscheidung trifft, seinen Arbeitsplatz auf Windows NT umzustellen, sollte man die sich im Einsatz befindenden Anwendungen ausführlich testen. Die Praxis zeigt immer wieder, daß zwar theoretisch alle Anwendungen unter Windows NT laufen müßten, aber bei der einen oder anderen Anwendung kann es dann doch vorkommen, daß NT scheitert, außer es gibt eine echte NT-Anwendung als Ersatz. Die optimale Performance von NT kann auf Dauer nur dann erzielt werden, wenn alle Anwendungen 32-Bit-NT-Anwendungen sind.

Abschließend sei erwähnt, daß die neue Windows-NT-4-Version durch ihre neue Oberfläche sehr überzeugt und langfristig gesehen das bessere Windows sein wird.

22 Windows NT

Beim Testen der Windows-4-Version fielen die folgenden Punkte besonders auf:

- Das Einrichten erfolgt immer noch über drei Boot-Disketten oder beim Aufruf von WINNT mit dem Parameter /B, wobei dann alle notwendigen Installationsdateien temporär auf die Platte geschrieben werden. Voraussetzung ist hier natürlich, daß es sich um eine CD-Version handelt.
- Die Installation ist anschließend sehr einfach, da die automatische Hardware-Erkennung inklusive der Interrupts etc. sehr gut funktioniert.
- Nachdem die Daten übertragen sind und das Basisbetriebssystem installiert ist, erfolgt ein Neustart des Rechners, und die von Windows 95/98 bekannte grafische Installation beginnt.
- Das HPFS-Dateiformat von OS/2 wird nicht mehr unterstützt. Wer mit diesem Dateisystem bei einem Upgrade konfrontiert ist, sollte vorher das mit NT 3.51 ausgelieferte Konvertierungsprogramm eingesetzt haben, mit dem HPFS-Partitionen in das NTFS-Format konvertiert werden.
- Die Unterstützung von NT als Client für unterschiedliche Netzwerkbetriebssysteme wurde weiter verbessert.

Mit Auslieferung von Windows NT 4 dürfte die Entscheidung noch leichter fallen, von Windows 3.x auf NT umzusteigen, unter dem Aspekt, daß man die Windows-95/98-Umstellung auslassen will. Solange es sich nur um einzelne PCs handelt, ist das kostenmäßig auch noch nicht tragisch. Wenn es jedoch darum geht, mehrere, vor allem ältere Rechner umzustellen, zieht das immer Investitionen im Bereich der Hardware nach sich. Das betrifft vor allem den Hauptspeicher und die Platten in der NT Workstation. Im schlimmsten Fall muß der komplette Rechner getauscht werden. Die Anforderungen an eine Windows-95/98-Umgebung sind nicht ganz so anspruchsvoll.

23

Windows NT Server

Im Kapitel über Windows NT haben Sie gesehen, daß Sie damit nicht nur ein Workstation-Betriebssystem, sondern zugleich auch ein Netzwerkbetriebssystem zur Verfügung haben. Zu beachten ist dabei nur, daß jede Windows NT Workstation einen eigenen Server darstellt. Das heißt, jeder Anwender, der die Berechtigung erhalten soll, auf Ressourcen einer Windows NT Workstation zuzugreifen, muß auf jeder Windows NT Workstation als Benutzer eingerichtet und verwaltet werden. Zum Verwalten eines Benutzers zählt dabei unter anderem auch die Vergabe von Zugriffsberechtigungen auf die einzelnen Ressourcen. Die Arbeitsweise ist dabei durchaus vergleichbar mit Windows for Workgroups oder Personal NetWare von Novell (von der man immer weniger hört). Die Leistungsfähigkeit von Windows NT ist aufgrund der Plattform und des internen Aufbaus wesentlich größer.

Wenn es jedoch darum geht, einen zentralen Server zur Verfügung zu stellen, der nicht nur leistungsfähiger, sondern auch sicherer und einfacher für das Verwalten von Benutzern und den dazugehörigen Ressourcen ist, reicht Windows NT nicht mehr aus. Hierfür bietet Microsoft das erweiterte System Windows NT Server an. Das nachfolgende Kapitel soll Ihnen alle notwendigen Informationen bieten, mit denen Sie einen Eindruck über die Arbeitsweise, den Aufbau und die Funktionalitäten von Windows NT Server erhalten.

Windows NT Server ist ein Netzwerkbetriebssystem für den Einsatz auf Servern in lokalen Netzwerken. Es bietet unter anderem die Leistungsstärke, einfache Handhabung und Erweiterbarkeit von Windows NT, ergänzt um weitere Merkmale wie zentrale Sicherheitsverwaltung, Benutzerverwaltung und verbesserte Fehlertoleranz. Windows NT Server ist somit nicht mehr als Workstation-Betriebssystem gedacht, sondern als reines Server-Betriebssystem. Das fällt unter anderem auch dadurch auf, daß Sie bei der Installation von Windows NT die Konfiguration einer Netzwerkkarte deaktivieren können. Beim Installieren von Windows NT Server kann diese Option nicht umgangen werden. Somit kann Windows NT als reines Workstation(s)-Betriebssystem ohne Netzwerkanbindung konfiguriert werden. Für Windows NT Server hingegen ist ein Netzwerkananschluß zwingend.

Im Gegensatz zu Windows NT kann sich nicht mehr jeder definierte Anwender an diesem Rechner anmelden. Hierauf wird später eingegangen. Die Netzwerkfunktionen von Windows NT Server sind in

23 Windows NT Server

das Betriebssystem integriert und nicht als Add-on zu sehen, im Gegensatz zur bisherigen LAN-Manager-Philosophie. Dadurch lassen sich die Netzwerkfunktionen bequemer einsetzen und verwalten. Auf den ersten Blick sind beim Betrachten der Bildschirmoberflächen keine allzu großen Unterschiede zwischen Windows NT und Windows NT Server zu sehen. Die generellen Unterschiede stellt man erst dann fest, wenn man mit dem System arbeitet. Inzwischen ist es ja bekannt, daß aus einer Windows NT Workstation durch das Ändern von nur ein paar Byte in der Registry eine Windows-NT-Server-Maschine gemacht werden kann, es fehlen dann nur noch die Server-Programme für die Verwaltung, wie z.B. der Benutzermanager für Domänen etc. Es sei jedoch darauf hingewiesen, daß man eine unberechtigte Modifikation im Betriebssystem durchführt, die rechtlich nicht erlaubt ist. Man sollte somit von einer solchen Änderung Abstand nehmen.

23.1 Windows NT Server – ein Überblick

Genauso wie Windows NT gibt es auch Windows NT Server in einer Version 4. Die größten Änderungen betreffen dabei vor allem die grafische Oberfläche, da auch sie an Windows 95/98 angepaßt worden ist. Ebenso ändern sich die Installationsroutinen, wobei diese immer einfacher werden. In der Regel werden so ziemlich alle Hardware-Komponenten erkannt und dem Anwender für die Installation zur Auswahl gegeben. Da Windows NT Server in der Version 4 auch die Einstellungen der Hardware-Komponenten sehr gut erkennt, muß dort fast nur noch bestätigt werden, was vom Installationsprogramm vorgeschlagen wird.

Windows NT Server ist ein plattformunabhängiges und erweiterbares Netzwerkbetriebssystem für Server, die auf den Prozessorfamilien 386, 486 oder Pentium bzw. Pentium/Pro laufen können, zudem werden RISC-, MIPS- und DEC-Alpha-Systeme unterstützt. Somit ist man auch beim Einsatz von Windows NT Server nicht von einer Prozessorarchitektur abhängig, sondern kann den Prozessor auswählen, der, bezogen auf die jeweiligen Anforderungen, die beste Leistungsfähigkeit bietet.

Am Rande sei erwähnt, daß für Windows NT Server nicht unter einem 586-Prozessor mit mindestens 90 MHz begonnen werden sollte. Wenn das auch stark von der Netzwerkumgebung (Anzahl der Anwender, Applikationen etc.) abhängt, so hat sich doch gezeigt, daß man mit dieser Ausstattung sehr gut bedient ist. Als Hauptspeicher sollten mindestens 32 Mbyte vorhanden sein, mehr Hauptspeicher ist aber auf alle Fälle von Vorteil, da Sie damit die Performance wesent-

23.1 Windows NT Server – ein Überblick

lich steigern können. Durch die Erweiterbarkeit für ein symmetrisches Multiprocessing kann je nach Anwendungsfall die für die jeweilige Umgebung am besten abgestimmte Serverplattform konfiguriert werden. Wie NetWare oder Windows NT auch, arbeitet Windows NT Server intern mit einer vollständigen 32-Bit-Architektur. Dadurch, daß auch die Möglichkeit besteht, mehrere Threads gleichzeitig auszuführen, sind Anwendungsprogramme entsprechend leistungsfähig einsetzbar und zu konzipieren. Das Betriebssystem und jede Anwendung arbeiten in voneinander getrennten Adreßräumen. Somit sind diese voneinander abgeschirmt, und der Absturz des Servers durch ein unkontrolliertes Schreiben einer Anwendung in einen Adreßraum, in dem das Betriebssystem liegt, kann nicht erfolgen. Zu den wesentlichen Merkmalen von Windows NT Server gehören:

Offene Netzwerkarchitektur

Windows NT Server unterstützt die beiden Standards NDIS (Network Driver Interface Specification) und TDI (Transport Driver Interface). NDIS ist ein Interface-Standard für die Kommunikation zwischen den Netzwerkkartentreibern und Netzwerkprotokollen. NDIS ermöglicht auf diese Weise eine flexible Kommunikation von Netzwerkkartentreibern und Protokollen, und es muß nicht für jede im Einsatz befindliche Adapterkarte eine speziell angepaßte Version des Protokolls geschrieben werden. Zudem ist es damit möglich, mit einer einzigen Netzwerkkartentreiber mehrere Protokolle zu bedienen. Wenn beim Windows NT Server von NDIS die Rede ist, sollte das unter NetWare mit ODI verglichen werden – zwei Standards, die sich am Markt etabliert haben und die im Prinzip das gleiche leisten können. Im Lieferumfang von Windows NT Server sind folgende Netzwerkprotokolle enthalten, die dem NDIS-Standard entsprechen: NetBEUI (NetBIOS Extended User Interface), TCP/IP (Transmission Control Protocol/Internet Protocol), Microsoft NWLINK (NetWare Link Protokoll) und DLC (Data Link Control Protocol).

Die TDI-Schnittstelle arbeitet zwischen dem Netzwerkprotokoll und der oberen Ebene der Netzwerksoftware (Server und Redirector). Durch die TDI-Schnittstelle müssen Redirector und Server nicht direkt mit den Netzwerkprotokollen kommunizieren bzw. überhaupt nicht über die verwendeten Protokolle informiert sein. Somit kann mit Windows NT Server ein anderes Protokoll oder sogar ein anderer Server und Redirector eingesetzt werden. Zudem werden damit auch RPC-Anwendungen (Remote Procedure Calls), NetBIOS-Anwendungen und Windows-Sockets-Anwendungen unterstützt.

Netzwerkinstallation

Damit nicht bei jeder Installation der Windows NT Workstation Disketten gewechselt und nicht jede Workstation mit einem CD-ROM-Laufwerk ausgestattet werden muß, und damit die Installation beschleunigt wird, empfiehlt es sich, an einem Windows NT Server ein CD-ROM-Laufwerk zu installieren, für das auch die Treiber unter Windows NT Server zur Verfügung stehen. Wenn Sie dann die CD für Windows NT in das CD-ROM-Laufwerk einlegen, können Sie von der neuen Workstation die Verbindung zum Windows NT Server aufbauen und das Installationsprogramm WINNT.EXE aufrufen. Eine andere Möglichkeit besteht darin, sämtliche Dateien der CD auf die Platte des Servers zu kopieren.

Integrierte Sicherheitsfunktionen

Ebenso wie bei Windows NT sind die zusätzlichen Sicherheitsfunktionen, die Windows NT Server zur Verfügung stellt, in das Betriebssystem integriert worden. Hierzu zählen unter anderem die Vergabe von Rechten auf Dateien und Directories (nur optimal einsetzbar, wenn das NTFS-Dateisystem eingesetzt wird), die Festlegung grundlegender Systemfunktionen (z.B. das Einstellen der Systemuhr oder der Shut Down des Servers) und eine Vielzahl wichtiger Sicherheitseigenschaften. Ein Teil dieser Funktionen kann durch einen eigenen Mechanismus überwacht werden (Auditing).

Zentrale Benutzerverwaltung

Damit Benutzer Zugriff auf Windows-NT-Ressourcen erhalten, müssen sie auf diesem Server eingerichtet sein. Das ist vergleichbar mit NetWare 3.12, einer zentralen Benutzerdatenbank (Bindery) pro Server. Mit der Einführung von NetWare 4.x ist dieses Problem dank der NDS, einer globalen, verteilten und replizierbaren Datenbank, behoben. Windows NT Server bietet einen ähnlichen Mechanismus, d.h. eine zentrale Benutzerdatenbank, durch Einführung von Domains. In einer Domain können mehrere Server zusammengefaßt werden, um einen Benutzer nur noch einmal einrichten zu müssen und ihm damit Zugriff auf alle freigegebenen Ressourcen der Server innerhalb der Domain zu geben. Die Anmeldung des Benutzers muß dabei nur einmal erfolgen. In einem Netzwerk unter Windows NT Server können mehrere Domains eingerichtet sein. Damit ein Benutzer, der in Domain A definiert worden ist, auch auf Ressourcen der Domain B zugreifen kann, ohne einen weiteren Anmeldevorgang durchführen zu müssen, wurde das Prinzip der sogenannten Trusted Domains implementiert. Welche Vorteile das bringt und mit welchem zusätzlichen Aufwand dies unter Umständen verbunden ist, soll an anderer Stelle ausführlicher erläutert werden.

23.1 Windows NT Server – ein Überblick

Verwalten von Windows NT Workstations

Durch die Einführung von Benutzerprofilen unter Windows NT Server ist es möglich, Benutzern auf einer Windows NT Workstation genau die Umgebung zur Verfügung zu stellen, die von ihnen benötigt wird. Das Benutzerprofil für den Windows NT Server ist nicht zu verwechseln mit einem Login Script, so wie dies unter NetWare, Vines und natürlich auch für den Windows NT Server zur Verfügung steht.

Die Definition von Benutzerprofilen erlaubt es auch, die Möglichkeiten, die ein Benutzer auf einer Windows NT Workstation hat, einzuschränken. Somit kann der Anwender bestimmte Programmgruppen nicht ändern oder bekommt Programmgruppen, die er nicht benötigt oder gar nicht sehen soll, überhaupt nicht angezeigt. Das Benutzerprofil für einen Benutzer kann auf einem Windows NT Server gespeichert werden und enthält Angaben der bevorzugten Arbeitsumgebung, Einstellungen der Netzwerkverbindungen, Programmgruppen, und, wenn notwendig, auch noch die Bildschirmfarben. Ein Benutzerprofil wird beim Anmelden des Benutzers an einer beliebigen Windows NT Workstation ausgeführt. Sie kennen vielleicht den Ärger, den Sie als Netzwerkverwalter für Windows-Arbeitsplätze haben, wenn der Anwender seine Einstellungen der Programmgruppen ändert oder Anwendungen sieht, die sich unter Windows nicht so ohne weiteres ausklammern lassen. Benutzerprofile ermöglichen es Ihnen, Verwaltungsaufgaben und -einschränkungen für Windows NT Workstations, bezogen auf einen einzelnen Benutzer, individuell festzulegen.

Druckerverwaltung

Die Handhabung der Druckerverwaltung unter Windows NT Server ist im Vergleich zu früher wesentlich besser. Somit ist es für den Administrator einfacher, Drucker im Netzwerk einzurichten und zu verwalten. Auch der Anwender hat es leichter, das Netzwerk nach vorhandenen Druckern zu durchsuchen und Verbindungen zu diesen herzustellen. Hinzu kommt, daß Benutzer auf einer Windows NT Workstation, die Verbindungen zu Druckern herstellen, welche auf einem Windows NT Server eingerichtet sind, keinen eigenen Druckertreiber für den jeweiligen Drucker installiert haben müssen. In diesem Fall wird der auf dem Windows NT Server installierte Druckertreiber verwendet. Das gilt jedoch nur für Windows-NT-Arbeitsplätze.

Performance-Überwachung

Für jeden Server im Netzwerk ist es wichtig und nützlich zu erkennen, an welcher Stelle Leistungsengpässe auftreten. Jedes der bislang beschriebenen Netzwerkbetriebssysteme (NetWare, Vines) bietet hierfür eine Vielzahl von Informationen. Auch Windows NT Server bietet einen Performance Monitor, auf dem die einzelnen Leistungsparameter des Servers überprüft und überwacht werden können. In der Summe können Sie aus mehr als hundert Optionen auswählen und sich diese grafisch am Bildschirm darstellen lassen. Hierzu gehören unter anderem Informationen über die Server-Auslastung im Netzwerk, die Auslastung der Plattenlaufwerke, die Prozessorbelastung oder auch Statistiken über Server und Workstations. Mit dem System-Monitor ist es auch möglich, gleichzeitig von mehr als einem Server oder einer Windows NT Workstation entsprechende Leistungsdaten zu erhalten und angezeigt zu bekommen. Somit kann man ohne großen Aufwand die Leistung und Auslastung von mehreren Servern (oder auch Windows NT Workstations) verfolgen und vergleichen.

Aktivitäten im Netzwerk überwachen

Unter Windows NT Server steht Ihnen ein Tool zur Verfügung, das als Server-Manager bezeichnet wird. Hiermit können Sie Informationen abfragen, um zu sehen, wer auf dem Server angemeldet ist, welche Directories zur gemeinsamen Benutzung freigegeben sind und vieles andere mehr. Damit können aber nicht nur die entsprechenden Informationen von Windows-NT-Server-Systemen abgefragt und überprüft werden, sondern auch von im Netzwerk installierten Windows NT Workstations. Über den sogenannten Event Viewer werden Ihnen alle aufgetretenen Ereignisse angezeigt. Dabei können Sie auch wieder auswählen, ob Sie Windows NT Server oder Windows NT Workstations überprüfen und kontrollieren möchten.

Da Sie nun einen groben Überblick über Windows NT Server erhalten haben und im Kapitel 22 Windows NT als Workstation-Betriebssystem bereits erläutert wurde, möchte ich Ihnen im nachfolgenden Abschnitt die grundsätzlichen Unterschiede zwischen Windows NT und Windows NT Server aufzeigen. Danach werde ich auf spezielle Eigenschaften, die für den Aufbau von Netzwerken unter Windows NT Server notwendig sind, näher eingehen.

23.2 Windows NT und Windows NT Server im Vergleich

Es sei nochmals erwähnt, daß Windows NT Server eine noch leistungsfähigere Version von Windows NT ist. Windows NT Server umfaßt alle Einrichtungen und Funktionen von Windows NT und darüber hinaus unterschiedliche Erweiterungen, die es erst zum Netzwerkbetriebssystem für lokale Netzwerke machen. Die hierfür wichtigste Eigenschaft, die es zu einem Netzwerkbetriebssystem für einen oder mehrere Server macht, ist die Möglichkeit, Domains einzurichten und zu verwalten. Damit wird die Administration von Benutzern und Gruppen zentralisiert und verbessert. Das heißt, die Arbeit für den Netzwerkverwalter wird dadurch wesentlich vereinfacht.

Unter einer Domain ist eine Gruppe von Servern zu verstehen, für die eine gemeinsame Datenbank von Benutzer- und Gruppen-Accounts mit den dazugehörigen Sicherheitsfestlegungen verwaltet wird. Egal wie viele Server in der Domain definiert sind, das Benutzer- und Gruppen-Account muß nur einmal eingerichtet werden, damit es alle Server in der Domain erkennen und den Zugriff für den Account mit den hierfür definierten Rechten zulassen.

Wenn in einem Netzwerk mehr als eine Domain eingerichtet wird, können sogenannte Trusted Domains definiert werden. In diesem Fall erkennen die Server der einen Domain die Accounts der anderen und ermöglichen dann den Zugriff auf eigene Ressourcen. Daher müssen die Accounts nur einmal eingerichtet werden, um Zugriff auf Ressourcen in allen anderen Domains (sofern diese als Trusted Domains eingerichtet sind) zu ermöglichen. Das ist vergleichbar mit dem StreetTalk-Konzept von Vines oder der NDS von NetWare 4.x. Sie werden jedoch sehen, daß mit den Domains und Trusted Domains andere Konzepte realisiert worden sind, als dies bei Vines oder NetWare 4.x der Fall ist. Die Vorteile für die Anwender sind darin zu sehen, daß durch einen einzigen Login im Netzwerk der Zugriff auf alle freigegebenen Ressourcen ermöglicht wird. Es wird sich zeigen, daß der Planungsaufwand auch für das Trusted-Domain-Konzept in Verbindung mit Windows NT Server nicht unerheblich ist, vor allem dann nicht, wenn es sich um größere Netzwerke mit einer Vielzahl von Servern handelt.

Ein weiterer Unterschied zu Windows NT ist darin zu sehen, daß Windows NT Server erweiterte Fault-Tolerance-Mechanismen unterstützt. Hierzu zählen unter anderem das Disk-Mirroring (RAID Level 1) und die Disk-Stripe-Sets mit Parität (RAID Level 5). Beim Disk-Mirroring werden Daten, die auf die eine Platte geschrieben werden,

23 Windows NT Server

automatisch auch auf die gespiegelte Platte geschrieben. Somit sind auf beiden Platten identische Datenbestände vorhanden. Fällt eine Platte aus, kann mit dem Datenbestand der zweiten Platte ohne Unterbrechung weitergearbeitet werden. Disk-Striping mit Parität ist derzeit die modernste Technologie, um fehlertolerante Systeme zu installieren. Hierbei wird jedes logische Volume auf verschiedene Festplatten verteilt. Wenn eine der Festplatten ausfällt, dann können die darauf gespeicherten Informationen mit Hilfe der Daten und Paritätsinformationen auf den anderen Platten rekonstruiert werden. Dieses Verfahren darf nicht verwechselt werden mit dem Verteilen der Volumes unter NetWare auf mehrere physikalische Platten. Wenn im Fall von NetWare bei Verteilung der Volumes über mehrere Platten eine Platte ausfällt, dann ist das gesamte Volume nicht mehr verfügbar.

Für Windows NT Server steht zudem ein Mechanismus zur Verfügung, der als Directory Replication bezeichnet wird. Dabei ist auf einem Server das Original abgelegt (Export-Server), und einen anderen Windows NT Server oder Windows-NT-Rechner legen Sie als Import-Computer fest. Wenn Sie dann Änderungen in Dateien durchführen, die auf dem Originalverzeichnis liegen (Export-Server), werden diese automatisch auf alle festgelegten Import-Computer übertragen. Durch die Directory-Replication können Sie Dateien automatisch auf mehrere Computer in Ihrem Netzwerk verteilen. Somit können Sie gewährleisten, daß alle Dateien, verteilt auf mehreren Computern, den aktuellen Stand haben. Die Reproduktion wird auch dann ausgeführt, wenn Dateien im Exportverzeichnis hinzugefügt oder gelöscht werden.

Die Directory Replication ist auch beim Laden von Dateien hilfreich. Wenn mehrere Benutzer auf eine Gruppe von Dateien zugreifen müssen, dann können die Dateien zum Laden auf verschiedene Computer verteilt werden. Hierzu konfigurieren Sie einen Server als Export-Server und die anderen Computer als Import-Computer. Auf den Export-Server kopieren Sie dann die Originalversion der Dateien. Somit muß nur eine Kopie der einzelnen Dateien verwaltet werden, und jeder Import-Computer ist im Besitz einer identischen Kopie dieser Dateien. Damit das Ganze funktioniert, hat jeder Export-Server eine Liste von Computern, auf denen die Kopien der Unterverzeichnisse gespeichert werden sollen, und jeder Import-Computer verwaltet eine Liste von Computern, von denen Original-Verzeichnisse empfangen werden. Eine Windows NT Workstation verfügt nur über den Mechanismus, Import-Informationen zu verwalten; die Workstation legt also fest, von welchem Windows-NT-Server-Dateien im Zuge der Directory Replication empfangen werden.

23.3 Netzwerksicherheit

Zwei weitere Dienste, die standardmäßig im Lieferumfang von Windows NT Server enthalten sind, beinhalten Windows NT Services for Macintosh und Windows NT Remote Access Services. Für Windows NT Workstations stehen diese beiden Dienste nicht zur Verfügung. Mit Windows NT Services for Macintosh stellt Windows NT Server Dienste zur Verfügung, die Macintosh-Rechnern den Zugriff auf Daten des Servers ermöglichen. Mit den Windows NT Remote Services wird es Ihnen ermöglicht, die Verbindung zum Server über Modemstrecken aufzubauen.

23.3 Netzwerksicherheit

Windows NT Server bietet eine Vielzahl von Sicherheitsmechanismen. Hiermit können Sie steuern, was ein Benutzer im Netzwerk machen darf. Basis für dieses Sicherheitssystem ist die benutzerdefinierte Zugriffskontrolle. Ausgewählten Benutzern können Zugriffe auf bestimmte Ressourcen und das Ausführen bestimmter Aktionen erlaubt werden. Wie bei NetWare können dabei die Zugriffsberechtigungen für das Dateisystem nicht nur auf Directory-Ebene, sondern bis auf Dateiebene festgelegt werden. Durch die eingebaute Netzwerkfunktionalität ist es möglich, den Zugriff auf Ressourcen direkt an der Windows-NT-Server-Station zu sichern und nicht nur den Zugriff über das Netzwerk (d.h. von einer Workstation aus). Somit ist es nur bestimmten Benutzern erlaubt, sich direkt an der Windows-NT-Server-Station anzumelden und direkt an dieser Station zu arbeiten.

Durch das Domain-Konzept ist es für große Netzwerke auch möglich, Server in Domains zusammenzufassen und User Accounts nur einmal einzurichten und zu verwalten. Durch das Einrichten von Trusted Domains kann das auch übergreifend für eine Netzwerkkumgebung mit mehreren Domains aufgebaut werden.

23.3.1 Domains und Trusted Domains

Beim Verwalten von mehreren Servern im Netzwerk bilden Domains die grundlegende Einheit im Zusammenhang mit Netzwerksicherheit und zentraler Verwaltung. Unter einer Domain versteht man eine Gruppe von Servern, die unter Windows NT Server betrieben werden. Da alle Windows NT Server einer Domain dieselbe Gruppe von User Accounts kennen – es wird für sie nur eine zentrale Datenbank gepflegt –, müssen die Informationen eines Benutzers nur einmal eingerichtet werden, damit der Benutzer auf allen anderen Servern innerhalb der Domain bekannt ist.

23 Windows NT Server

Besteht das Netzwerk aus mehreren Domains, können Trusted Domains definiert werden, das heißt, Informationen über User Accounts werden an die anderen Domains weitergeleitet. Somit muß der Benutzer nur in einer Domain eingerichtet worden sein, um auf Ressourcen zugreifen zu können, die in den anderen Domains vorzufinden sind. Bei genauer Planung der Domains und Trusted Domains ist der Benutzer über eine einmalige Definition im gesamten Netzwerk bekannt. Dies ist vergleichbar mit StreetTalk von Vines oder NDS von NetWare 4.x, Sie werden jedoch noch sehen, daß der Aufwand zum Einrichten dieser Mechanismen im Vergleich zu Vines und NetWare 4.x wesentlich aufwendiger ist.

Domain – die elementare Verwaltungseinheit

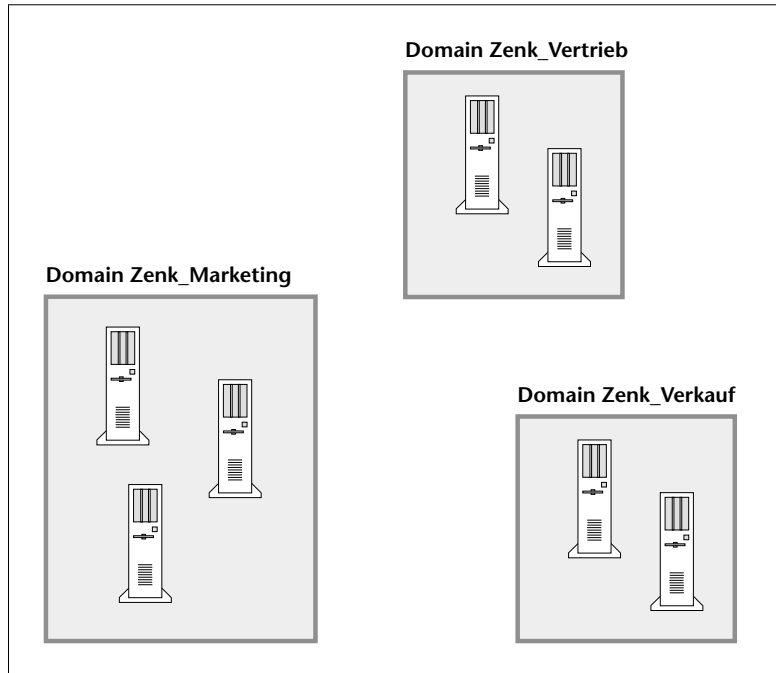
Die Zusammenfassung von Servern in Domains ist nicht nur für Netzwerkverwalter von Vorteil, sondern auch für alle Benutzer, die innerhalb einer Domain arbeiten. Die Server in der Domain stellen eine Verwaltungseinheit mit einem gemeinsamen Sicherheitssystem und mit gemeinsamen User Accounts dar. In jeder Domain existiert eine Datenbank mit User Accounts, Gruppendefinitionen und Sicherheitseinrichtungen. Alle weiteren Server in der Domain, auf denen Windows NT Server installiert ist, erhalten eine Kopie dieser Datenbank. Somit muß vom Netzwerkverwalter nur eine Datenbank gepflegt werden. Jeder Benutzer benötigt nur ein User Account und einen Login innerhalb der Domain, um auf alle verfügbaren Ressourcen, für die er Rechte hat, Zugriff zu haben.

In Abbildung 23.1 ist dargestellt, wie ein Netzwerk in mehrere Domains unterteilt werden kann. Zu beachten ist dabei, daß jede Domain im Netzwerk einen eindeutigen Namen erhalten muß.

Um die Übersichtlichkeit zu erhöhen, werden dem Benutzer beim Durchsuchen der Domains nach verfügbaren Ressourcen nicht alle Netzwerkserver und -drucker auf einmal gezeigt, vielmehr sind diese nach den Domains geordnet. Nach Auswahl der Domain werden dann alle in dieser Domain verfügbaren Server und Drucker aufgelistet. Das Konzept der Domains ist vergleichbar mit Workgroups unter Windows NT oder Windows for Workgroups. Der große Unterschied besteht jedoch darin, daß innerhalb einer Workgroup auf jedem Server die User Accounts und Gruppen pro Server separat verwaltet werden müssen.

23.3 Netzwerksicherheit

Abbildung 23.1
Aufteilung des
Netzwerks in meh-
rere Domains



Trusted Domain – Verbindung zwischen Domains

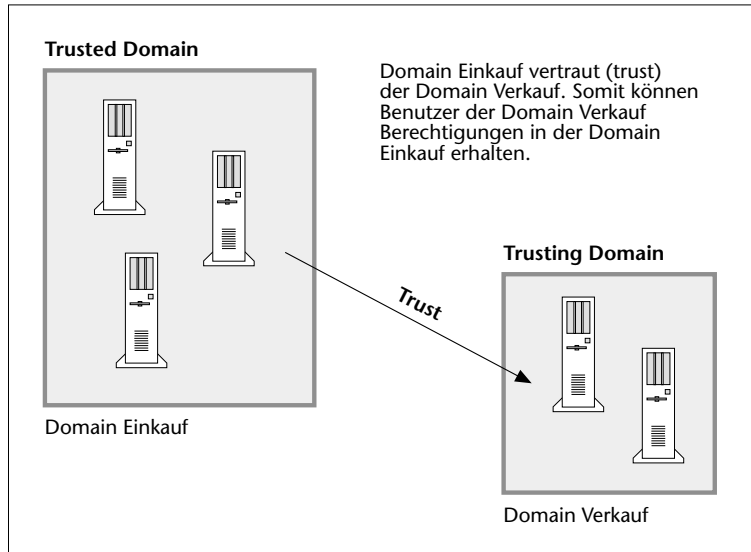
Beim Einrichten von Domains hat jede Domain eine zentrale Datenbank, um User Accounts, Gruppen etc. verwalten zu können. Sollen nun übergreifende Zugriffe auf Ressourcen anderer Domains ermöglicht werden, ohne daß der Benutzer noch einmal in der anderen Domain eingerichtet werden muß, bietet Windows NT Server den Aufbau sogenannter Trusted Domains.

Durch das Einrichten von Trusted Domains, d.h. den Aufbau von Beziehungen zwischen Domains in einem Netzwerk, wird es ermöglicht, User Accounts und globale Gruppen einer Domain auch in einer anderen Domain zu verwenden, in der diese User Accounts und globalen Gruppen nicht explizit definiert worden sind. Damit wird die Verwaltung des Netzwerks wesentlich erleichtert, weil, insgesamt betrachtet, User Accounts, Gruppen etc. nur einmal eingerichtet werden müssen. Das heißt, dem Benutzer können Ressourcen im gesamten Netzwerk über eine einmalige Definition verfügbar gemacht werden. Wenn Sie eine Beziehung zwischen zwei Domains erstellen, dann vertraut die eine Domain (Trusting Domain) der anderen Domain (Trusted Domain). In Abbildung 23.2 ist das Konzept einer Trusted Domain dargestellt.

23 Windows NT Server

Die Trusting Domain erkennt alle User Accounts und globalen Gruppen der Trusted Domain. Diese Accounts können innerhalb der Trusting Domain vollwertig verwendet werden. Eine Beziehung zwischen Domains kann einseitig oder gegenseitig eingerichtet werden. Eine gegenseitige Beziehung bedeutet dabei, daß Domain A der Domain B vertraut und Domain B der Domain A.

Abbildung 23.2
Einrichten von
Trusted Domains



Der Aufbau von Trusted Domains ist nicht transitiv. Das heißt, wenn die Domain Verkauf der Domain Einkauf vertraut und die Domain Einkauf der Domain Marketing vertraut, bedeutet dies nicht, daß die Domain Verkauf auch der Domain Marketing vertraut. Für den Fall, daß die Domain Verkauf auch der Domain Marketing vertrauen soll, um Benutzern der Domain Marketing Berechtigungen in der Domain Verkauf zuweisen zu können, müßte eine zusätzliche Trusted-Domain-Beziehung zwischen Verkauf und Marketing definiert werden.

**Aufbau einer
Domain**

In einer Domain muß mindestens ein Server unter Windows NT Server installiert sein. Dieser Server muß als Domain Controller arbeiten und verwaltet das Original der Benutzer- und Gruppendatenbank.

In der Domain selbst können dann noch weitere Windows NT Server, LAN-Manager-2.x-Server, Windows NT Workstations und andere Clients installiert werden. Der Domain Controller in einem Windows-NT-Server-Netzwerk muß ein Windows NT Server sein. Alle Änderungen in der Benutzer- und Gruppendatenbank für die Domain müssen auf dem Domain Controller durchgeführt werden. Über die Anwendung User Manager for Domains wählen Sie zum

23.3 Netzwerksicherheit

Hinzufügen oder Ändern von Informationen nur die Domain aus, in der diese Änderungen durchzuführen sind. Die Änderungen werden automatisch, ohne daß Sie davon etwas bemerken, an den Domain Controller der Domain weitergeleitet. Somit ist es nicht möglich, Änderungen in einer Benutzer- und Gruppendatenbank durchzuführen, die nicht auf einem Domain Controller liegt.

Auf den zusätzlichen Windows-NT-Server-Systemen, die Sie in der Domain einrichten können, wird eine Kopie der Benutzer- und Gruppendatenbank abgespeichert. Die anderen Windows NT Server fordern den Domain Controller alle fünf Minuten auf, eventuell durchgeführte Änderungen bekanntzugeben. Es werden dabei nur die Änderungen gesendet und aktualisiert. Alle Server unter Windows NT Server innerhalb einer Domain können Login-Anforderungen bearbeiten. So kann jeder Windows NT Server die Korrektheit der Login-Anforderung prüfen. Damit fungieren die anderen Windows NT Server als Backup Domain Controller, so wie dies unter LAN-Manager 2.x der Fall ist.

Aus Sicherheitsgründen wird empfohlen, in einer Domain mehr als einen Windows NT Server zu installieren, sofern es Ihre Netzwerkgröße zuläßt. Sollte in einem solchen Fall der Domain Controller ausfallen, kann ein anderer Windows NT Server zum neuen Domain Controller gemacht werden. Zudem kann in größeren Netzwerken der Anmeldevorgang mehrerer Benutzer auf unterschiedliche Server verteilt werden. Existieren in einem Netzwerk mehrere Domain Controller (primäre Domain Controller und Backup Domain Controller), dann kann der Logon-Vorgang auch auf diese Domain Controller aufgeteilt werden. Sollte ein Netzwerk über WAN-Strecken verbunden und die Domain über diese verteilt sein, ist es aus Performance-Gründen zu empfehlen, in der Außenstelle einen eigenen Backup Domain Controller zu installieren. Zudem darf nicht vergessen werden, daß beim Ausfall der WAN-Strecke kein Login über den Domain Controller möglich ist, für den Fall, daß kein eigener Backup Domain Controller installiert ist. Es gibt also sowohl Performance- als auch Ausfallsicherheitsgründe für die Installation mehrerer Backup Domain Controller.

Windows NT Workstations können im Netzwerk entweder zum Mitglied einer Domain oder zum Mitglied einer Workgroup gemacht werden. In der Regel wird man die Windows NT Workstations zum Mitglied der Windows NT Server Domain machen, weil nur dann die Möglichkeit besteht, sich von der Windows NT Workstation aus mit einem User Account in der Domain anzumelden. Zu beachten ist dabei, daß eine Windows NT Workstation keine Kopie der Benutzer- und Gruppendatenbank erhält.

23 Windows NT Server

Ist eine Windows NT Workstation Mitglied einer Workgroup, besitzt die Workstation eine eigene Benutzer- und Gruppendatenbank und verarbeitet Anmeldevorgänge selbst. Die Windows NT Workstations verwenden keine gemeinsame Benutzer- und Gruppendatenbank. Das heißt, jeder Windows-NT-Rechner hat seine eigenen Informationen über Benutzer, Gruppen und die Rechte, die Benutzern und Gruppen für Ressourcen des Windows-NT-Rechners vergeben worden sind.

23.3.2

Modelle für Domains

Der Aufbau eines Domain-Modells ist entscheidend für das Arbeiten und Verwalten von Netzwerken unter Windows NT Server. Dabei wird nicht nur der Verwaltungsaufwand reduziert, sondern auch gewährleistet, daß alle Benutzer im Netzwerk arbeiten können, indem Domains so eingerichtet werden, daß alle Benutzerkonten und globalen Gruppen in allen Domains Gültigkeit haben. Man unterscheidet hierbei vier Modelle, um Domains aufzubauen: Single Domain, Master Domain, Multiple Master Domain und Complete Trust Domain.

Single-Domain-Modell

Wird ein Netzwerk mit relativ wenigen Benutzern eingerichtet und es besteht keine Notwendigkeit, das Netzwerk aus organisatorischen Gründen zu unterteilen, dann kann das Single-Domain-Modell eingesetzt werden. In diesem Fall besteht das Netzwerk aus nur einer einzigen Domain. Alle Benutzerkonten und globalen Gruppen (Erklärung siehe nachfolgend) werden innerhalb dieser Domain eingerichtet. Da nur eine Domain eingerichtet wird, besteht keine Notwendigkeit, Trusted Domains zu definieren – es besteht aber auch keine Möglichkeit hierfür.

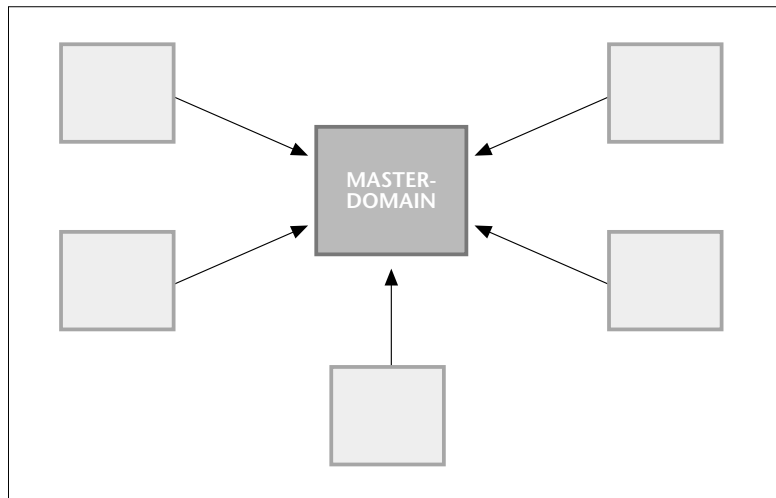
Sind in einem Netzwerk mehrere Server installiert oder gibt es in Ihrem Unternehmen mehrere Abteilungen, ist es wahrscheinlich, daß es sich beim Single-Domain-Modell nicht um die beste Lösung handelt. Unterteilen Sie das Netzwerk in solchen Fällen in mehrere Domains. Der Benutzer durchsucht das Netzwerk zuerst auf Domain-Ebene, wählt eine Domain aus und sieht dann die in der ausgewählten Domain enthaltenen Ressourcen. Wenn nur eine Domain eingerichtet ist, können die definierten Netzwerkverwalter jederzeit alle Server in der Domain administrieren, da die Möglichkeit zur Verwaltung der Server auf Domain-Ebene vergeben wird. Wenn das Netzwerk in Domains unterteilt wird, legt man fest, daß Administratoren für die Domain nur deren Server verwalten können und dürfen.

23.3 Netzwerksicherheit

Master-Domain-Modell

Muß das Netzwerk aufgrund der Größe und der organisatorischen Gegebenheiten in mehrere Domains aufgeteilt werden, empfiehlt sich das Master-Domain-Modell. In diesem Modell sind die Vorteile der zentralen Verwaltung mit den Vorteilen verbunden, die die Aufteilung in mehrere Domains mit sich bringt. In diesem Modell wird eine Domain für das Netzwerk eingerichtet, in der alle Benutzer und globalen Gruppen des Netzwerks definiert werden. Alle anderen Domains im Netzwerk sind Trusted Domains gegenüber der Master Domain (Trusting Domain). Somit können die Benutzer und globalen Gruppen der Master Domain Berechtigungen für Ressourcen der anderen Domains erhalten. Gehen Sie davon aus, daß in einem Unternehmen die EDV-Abteilung für das gesamte Netzwerk zuständig ist, dann wird die Domain der EDV-Abteilung zur Master Domain. In Abbildung 23.3 ist dieses Prinzip dargestellt.

Abbildung 23.3
Einrichten eines
Master-Domain-
Modells



Stellen Sie sich dabei die Aufgabe der Master Domain so vor, daß diese dazu dient, Benutzer- und Gruppenkonten zentral für das gesamte Netzwerk zu verwalten, unabhängig davon, aus wie vielen weiteren Domains das Netzwerk besteht. Der Aufwand besteht letztendlich darin, die Trusted Domains korrekt einzurichten. Die anderen Domains können als Resource Domains betrachtet werden und verwalten selbst keine eigenen Benutzer- und Gruppenkonten. Kopien der Benutzer- und Gruppendatenbank liegen nur auf den Servern in der Master Domain. Beim Einsatz dieses Modells sollte in der Master Domain aus Sicherheitsgründen mindestens ein zweiter

23 Windows NT Server

Windows NT Server eingerichtet werden, damit gewährleistet ist, daß eine Kopie der Benutzer- und Gruppendatenbank vorhanden ist. Zudem kann der zweite Server beim Ausfall des Domain Controller zum neuen Domain Controller gemacht werden, um das Arbeiten im Netzwerk nicht zu behindern.

Multiple-Master-Domain-Modell

Statt mit einer Master Domain zu arbeiten, kann man auch ein Konzept entwickeln, bei dem mehrere Master Domains eingerichtet werden. Wie beim Master-Domain-Modell dient jede Master Domain hauptsächlich dazu, die Benutzer- und Gruppendatenbank zu verwalten. Jeder Benutzer wird in einer der Master Domains angelegt. Hinter jeder Domain muß man sich eine Vielzahl kleinerer Domains vorstellen, in denen die Ressourcen zur Verfügung gestellt werden. Jede Master Domain räumt der anderen Domain einen Trust ein. Jede kleinere Domain wird als Trust jeder Master Domain definiert. Für diese kleineren Domains muß der Trust jedoch nicht in umgekehrter Richtung definiert werden. Da alle Benutzerkonten des Unternehmens auf den Master Domains verteilt sind und jede kleinere Domain als Trust für jede Master Domain definiert ist, können alle Benutzerkonten innerhalb des Unternehmens und somit im gesamten Netzwerk in allen Domains verwendet werden.

Problematischer wird dabei jedoch der Einsatz globaler Gruppen. Soll eine globale Gruppe Benutzer verschiedener Master Domains beinhalten, so müssen mehrere globale Gruppen eingerichtet werden (eine in jeder Master Domain). Warum das so ist, werden Sie besser verstehen, wenn erklärt worden ist, worin sich globale Gruppen von lokalen Gruppen unterscheiden. In Abbildung 23.4 ist dargestellt, wie ein Multiple-Master-Modell aufgebaut werden könnte.

Sie können anhand von Abbildung 23.4 feststellen, daß der administrative Aufwand zunimmt, je mehr Master Domains definiert werden und je mehr kleinere Domains im Netzwerk vorhanden sind.

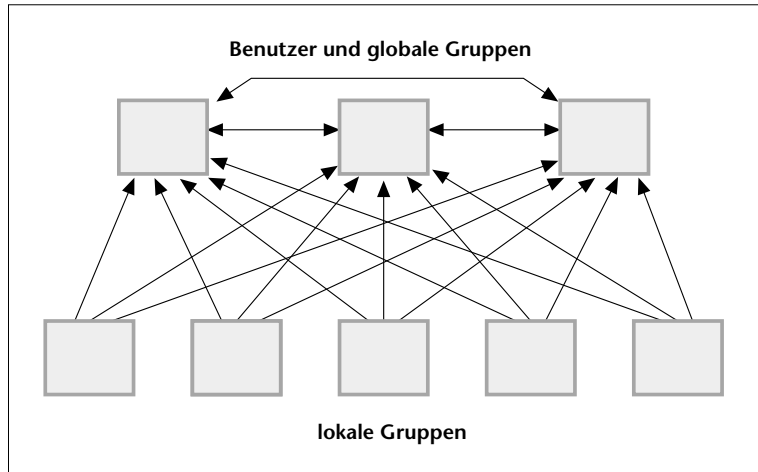
Das aufwendigste Verfahren stellt das Complete-Trust-Modell dar.

Complete-Trust-Modell

Die bisher beschriebenen Modelle dienen vor allem dazu, die Verwaltung der Benutzer zu zentralisieren. Wenn hingegen die Verwaltung nicht mehr zentralisiert sein soll, aber dennoch die Möglichkeit bestehen soll, jede Ressource im Netzwerk jedem Benutzer bereitzustellen, dann müssen Sie das Complete-Trust-Modell verwenden.

23.3 Netzwerksicherheit

Abbildung 23.4
Netzwerkstruktur-
rierung nach dem
Multiple-Master-
Modell



In diesem Modell räumt jede Domain im Netzwerk allen anderen Domains einen Trust ein, d.h., »jeder kennt jeden« bzw. vertraut jedem und ist somit ein Trust des anderen. Auf diese Weise können in jeder Domain eigene Benutzer und globale Gruppen definiert werden. Die darin definierten Benutzer und globalen Gruppen können in jeder anderen Domain benutzt werden. In Abbildung 23.5 ist dargestellt, wie ein solches Modell aussieht.

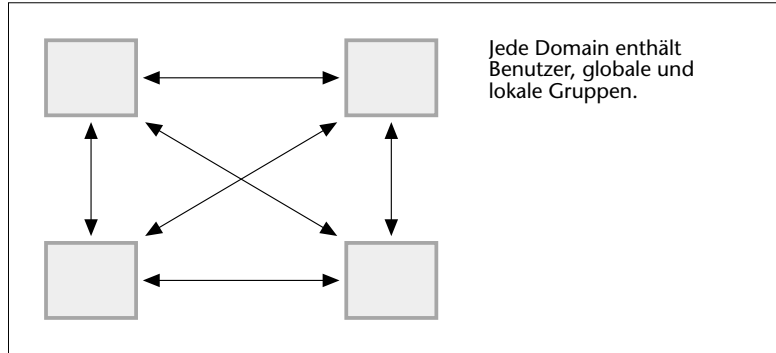
In großen Unternehmen mit einer Vielzahl von Domains ist dieses Modell nicht unbedingt das geeignete. Wenn Sie im Netzwerk n Domains eingerichtet haben, dann müssen bei diesem Modell insgesamt $n \cdot (n-1)$ Trust-Definitionen eingerichtet werden. So erfordern zehn Domains 90 Trust-Definitionen und 30 Domains schon beachtliche 870 Trust-Definitionen.

Um für den Windows NT Server die gleichen funktionellen Vorteile wie für NetWare 4.x oder Vines 5.x zu erhalten, müsste das Complete-Trust-Modell eingesetzt werden. Sie sehen jedoch, daß dies nicht unbedingt sinnvoll und empfehlenswert ist.

Der Einsatz von Windows NT Server erfordert eine detaillierte Planung, um sich für das richtige und sinnvollste Modell zu entscheiden. Bei dieser Entscheidung ist vor allem ausschlaggebend, wie die Verwaltung des Netzwerks, d.h. der Windows NT Server, und folglich die Domain organisiert werden sollen. Auf diese Weise ein X.500-basierendes Modell zu erstellen, dürfte aber schwerfallen. An anderer Stelle werden Sie noch sehen, inwieweit nachträglich Änderungen innerhalb einer Domain möglich sind. Sie müssen dann immer eines dieser Modelle vor Augen haben, um sich über die Konsequenzen im klaren zu sein.

23 Windows NT Server

Abbildung 23.5
Complete-Trust-
Modell



23.3.3

Login unter Windows NT Server

Nach dem Starten von Windows NT Server muß man sich, genauso wie beim Starten von Windows NT, erst daran gewöhnen, daß zum Anmelden die Tastenkombination **Strg** + **Alt** + **Entf** gedrückt werden muß. Unter DOS ist diese Tastenkombination zum Auslösen eines Warmstarts bekannt. Nachdem Sie diese Tastenkombination gedrückt haben, erscheint der Anmeldebildschirm, besser gesagt, das Anmeldefenster. Sie haben in diesem Fenster drei Eingabemöglichkeiten: Benutzername, Domain und Paßwort. Beim Anmeldevorgang ist zu unterscheiden, ob Sie sich an einer Windows NT Workstation oder an einem Windows NT Server befinden. Zuerst soll gezeigt werden, wie vorgegangen werden kann, wenn Ihr Arbeitsplatz eine Windows NT Workstation ist.

Windows NT Workstation

In das Eingabefeld *Benutzername* geben Sie den User Account ein, unter dem Sie sich anmelden wollen. Dazu muß das entsprechende Paßwort eingegeben werden. Die Eingabe in das Feld *FROM* (in der deutschen Version das Feld *AN*) hängt davon ab, wo sich das User Account befindet, unter dem Sie sich anmelden wollen. Befindet sich das User Account in einer Windows NT Server Domain, wählen Sie die entsprechende Domain aus, in der Sie sich anmelden wollen. Beim Auswählen einer Domain werden Benutzername und Paßwort zur Prüfung auf Existenz und Korrektheit an die angegebene Domain gesandt. Ein Server in dieser Domain überprüft den Benutzernamen und das Paßwort in der User-Account-Datenbank der Domain. Werden ein entsprechendes User Account und das Paßwort in der User-Account-Datenbank gefunden, erfolgt die Bestätigung der korrekten Anmeldung für die Workstation bzw. den Benutzer. Gleichzeitig übermittelt der Server notwendige Anmeldeinformationen für

23.3 Netzwerksicherheit

den Benutzer an die Workstation (z.B. das Benutzerprofil und die Umgebungsvariablen). Ab diesem Zeitpunkt ist der Benutzer erfolgreich in der Domain angemeldet und kann mit den für ihn freigegebenen Ressourcen arbeiten.

Der Benutzer auf einer Windows NT Workstation kann aber auch zum Anmelden statt eines User Accounts in der Domain einen lokalen User Account der Windows NT Station auswählen. Hierfür muß im Feld *FROM* der Name der Windows NT Workstation ausgewählt werden. Dann durchsucht Windows NT die eigene lokale User-Account-Datenbank nach dem Benutzernamen und dem angegebenen Paßwort. Sind die Angaben korrekt, wird der Anmeldevorgang durchgeführt, und alle für den Benutzer definierten und freigegebenen Ressourcen werden zur Verfügung gestellt.

Windows NT Server

Der Anmeldevorgang direkt an einer Windows NT Server Workstation ist bis auf eine Ausnahme mit dem vorher beschriebenen Anmeldevorgang identisch. Eine Windows NT Server Station kennt keine direkten lokalen Benutzerkonten, sondern nur die Benutzerkonten der Domain, der dieser Windows NT Server zugewiesen worden ist. Aus diesem Grund kann man sich an einer Windows NT Server Station nur mit einem User Account anmelden, der in der dazugehörigen Domain definiert ist.

Wichtig

Standardmäßig kann sich aus Sicherheitsgründen nicht jeder in der Domain definierte Benutzer direkt an einer Windows NT Server Station anmelden, um diese als Arbeitsplatz zu nutzen. Dieser Anmeldevorgang ist nur Benutzern erlaubt, die der Gruppe Administrators, Server-Operators, Print-Operators, Account-Operators oder Backup-Operators angehören.

Zu beachten ist an dieser Stelle, daß Sie mit der Auslieferung von Windows NT Server keine Workstation-Software direkt auf der CD bekommen, die sie an den Windows NT Server anbinden können. Das heißt, für die Einbindung herkömmlicher DOS-Workstations muß die Treibersoftware nach der Installation des NT Server erst erzeugt werden. Hierzu bietet der NT Server ein eigenes Programm an, um damit auszuwählen, welcher Diskettensatz erzeugt werden soll. Wenn Sie Windows for Workgroups, Windows 95/98 oder auch Windows NT Workstation im Einsatz haben, müssen Sie sich um den Treiber keine Sorgen machen, da dieser in den aufgeführten Produkten enthalten ist. Die Administration von Windows NT Server kann auch nur direkt an der Windows NT Server Station durchgeführt werden oder von einer anderen Windows NT Workstation, wenn Sie

sich die entsprechenden Directories als neues Netzwerklaufwerk auf der Windows NT Workstation definieren. Für Windows for Workgroups gibt es inzwischen einen eigenen Domain Manager zur Verwaltung der Windows NT Server Domains.

23.3.4

Benutzer und Benutzergruppen

Damit ein Benutzer im Netzwerk unter Windows NT Server arbeiten kann, benötigt er ein User Account in der Domain des Netzwerks. Für das User Account werden notwendige Informationen über diesen Benutzer eingerichtet (z.B. Benutzername, Paßwort, Zugriffsberechtigungen und vieles andere mehr). Existieren Benutzer mit ähnlichen Aufgaben oder ähnlichen Anforderungen für Ressourcen, dann können sie in globalen oder lokalen Gruppen zusammengefaßt werden. Durch den Einsatz von Gruppen wird das Verwalten von Rechten und Ressourcenzuteilungen wesentlich vereinfacht. Rechte, die Sie einer Gruppe hinzufügen oder auch abnehmen, gelten für alle bestehenden und zukünftigen Mitglieder dieser Gruppe. Sie sehen, daß dadurch die Administration der Benutzer um einiges vereinfacht werden kann. Windows NT Server unterscheidet zwei Arten von User Accounts: globale und lokale User Accounts. Die lokalen Benutzerkonten sind an dieser Stelle uninteressant, so daß wir uns ausschließlich mit globalen User Accounts beschäftigen wollen. Globale User Accounts werden für Benutzer in der Domain eingerichtet. Lokale User Accounts werden eingerichtet, wenn es sich um Benutzer handelt, die sich aus einer Untrusted Domain anmelden.

Für das Einrichten von Benutzern und Gruppen steht Ihnen ein eigenes Tool, der User Manager for Domains, zur Verfügung. Die Vergabe von Zugriffsberechtigungen für Dateien und Directories erfolgt über den File-Manager. Um Berechtigungen für Drucker zu erhalten, benötigen Sie den Print-Manager, mit dem Sie festlegen, wer auf einem definierten Netzwerkdrucker Druckaufträge ausgeben darf.

Um einen besseren Vergleich mit NetWare oder Vines zu erhalten, soll anschließend kurz dargestellt werden, welche Definitionen Sie für ein User Account durchführen können.

■ *Benutzername*

Eindeutiger Name des Benutzers, unter dem sich dieser in der Domain anmelden muß. Die Vergabe des Benutzernamens hängt davon ab, in welcher Form Sie die Definitionen durchführen möchten.

■ *Paßwort*

Das Paßwort, mit dem sich der Benutzer als Berechtigter ausweisen muß, um den Login auch ausführen zu können. Für Paßwörter können Sie zusätzlich folgende Optionen einrichten: Der Be-

23.3 Netzwerksicherheit

nutzer muß beim nächsten Login das Paßwort ändern, der Benutzer kann sein Paßwort ändern (oder auch nicht), das Paßwort läuft nie ab (oder es wird ein Ablaufintervall für das Paßwort eingerichtet). Im Gegensatz zu anderen Netzwerkbetriebssystemen muß bei Paßwörtern unter Windows NT die Groß-/Kleinschreibung beachtet werden; die Paßwörter können bis zu 14 Zeichen lang sein. Bei Bedarf können Sie festlegen, wie viele frühere Paßwörter sich Windows NT Server für den Benutzer merken soll, damit diese nicht noch einmal verwendet werden.

Um das Einrichten von User Accounts zu vereinfachen, haben Sie die Möglichkeit, für das Erstellen eines neuen User Account ein bestehendes Account zu kopieren. Anschließend ändern Sie die notwendigen Angaben der übernommenen Benutzerdaten. Somit können Sie sich eine oder mehrere User-Account-Vorlagen einrichten, um diese für das Erstellen zukünftiger User Accounts zu verwenden. Damit über diese Vorlagen kein Logon durchgeführt wird, sollten diese gesperrt (disabled) werden.

■ *Full Name*

Bei Bedarf kann ein vollständiger Name des Benutzers eingegeben werden (in der Regel Vor- und Nachname).

■ *Logon-Stunden*

Mit dieser Einrichtung wird definiert, wann sich der Benutzer in der Domain anmelden darf. Wie bei NetWare können Sie für jeden Tag in der Woche unterschiedliche Zeiten definieren. NetWare erlaubt ein Intervall von 30 Minuten, wohingegen beim Windows NT Server in Intervallen von einer Stunde der erlaubte Anmeldezeitraum festgelegt werden kann.

■ *Logon From*

Wenn der Login des Benutzers nicht von jeder Workstation aus im Netzwerk möglich sein soll, dann können Sie bis zu acht unterschiedliche Workstations eingeben, von denen aus sich der Benutzer mit diesem Domain-Account anmelden kann. Standardmäßig darf sich der Benutzer von jeder Workstation aus anmelden, solange Sie dies nicht einschränken.

■ *Ablaufdatum User Account*

Damit können Sie festlegen, wann das eingerichtete User Account ungültig wird. Der Benutzer kann sich ab diesem Zeitpunkt nicht mehr anmelden. Dies ist unter anderem für Mitarbeiter nützlich, die nur eine beschränkte Zeit da sind (z.B. Praktikanten). Damit ist sichergestellt, daß diese User Accounts ab dem festgelegten Datum nicht mehr verwendet werden können. Das User Account wird dadurch jedoch nicht aus der Benutzerdatenbank gelöscht.

23 Windows NT Server

■ *Home-Directory*

Ein Verzeichnis auf dem Server (oder der lokalen Platte der Workstation oder auf einem anderen Server im Netzwerk), das dem Benutzer zur Verfügung steht. Der Benutzer kann selbst festlegen, wer Zugriff auf das Home-Directory haben soll.

■ *Logon Script*

Eine Batch-Datei oder eine ausführbare Datei, die beim Anmelden des Benutzers automatisch ausgeführt wird.

■ *Profile*

Eine benutzerspezifische Datei, die über einen eigenen User-Profile-Editor erstellt werden muß. Es läßt sich damit festlegen, wie die Desktop-Umgebung des Benutzers aussehen soll, wenn sich dieser in der Domain anmeldet. Unter anderem können Sie damit definieren: Programmgruppen, Netzwerkverbindungen, Bildschirmfarben und die Einstellungen, die die vom Benutzer veränderbaren Aspekte der Umgebung festlegen. Somit kann man relativ problemlos festlegen, wie die Umgebung des Benutzers aussehen soll, wenn der Logon in der Domain erfolgt.

■ *User-Account-Typ*

Damit läßt sich festlegen, ob es sich um einen globalen oder lokalen User Account handeln soll. Diese Option ist nur in Windows NT Server Domains verfügbar.

■ *Gruppenzugehörigkeit*

Um die Administration im Netzwerk zu vereinfachen, richten Sie nicht nur Benutzergruppen ein, sondern legen auch fest, für welche Gruppen der Benutzer als Mitglied eingetragen sein soll.

■ *Account Disabled*

Ist diese Option eingeschaltet, kann das User Account nicht mehr für den Logon verwendet werden. Das User Account bleibt in der Datenbank erhalten, ist jedoch gesperrt.

Wie bereits erwähnt, kann der Einsatz von Gruppen dazu verwendet werden, die Administration der Benutzer für die Vergabe von Berechtigungen auf Dateien und Ressourcen zu erleichtern. Hierbei ist zwischen globalen und lokalen Gruppen zu unterscheiden.

■ *Globale Gruppe*

Eine globale Gruppe umfaßt eine Anzahl von User Accounts einer Domain, die unter einem Gruppennamen zusammengefaßt werden. Eine globale Gruppe kann ausschließlich User Accounts einer einzelnen Domain enthalten – und zwar der Domain, in der die globale Gruppe eingerichtet worden ist. Nachdem eine globale Gruppe erstellt worden ist, kann diese global im gesamten Netzwerk verwendet werden. Das heißt, der globalen Gruppe können Rechte der eigenen Domain und von vertrauenden Domains erteilt werden. Als Mitglied einer globalen Gruppe können nur Benutzer eingetragen werden, aber keine anderen lokalen oder globalen Gruppen.

23.3 Netzwerksicherheit

■ *Lokale Gruppen*

Eine lokale Gruppe enthält eine Anzahl von Benutzern und globalen Gruppen aus einer oder mehreren Domains, die unter einem Gruppennamen zusammengefaßt werden. Im Gegensatz zur globalen Gruppe kann eine lokale Gruppe Benutzer und globale Gruppen aus dieser Domain (in der sie eingerichtet ist) und jeder vertrauenden Domain enthalten, aber einer lokalen Gruppe können nur die Rechte und Berechtigungen für Ressourcen der Domain zugewiesen werden, in der sie eingerichtet worden ist. Eine lokale Gruppe kann Benutzer und globale Gruppen, aber keine weiteren lokalen Gruppen enthalten.

Lokale Gruppen sind auch für Windows NT Workstations verfügbar. Eine lokale Gruppe auf einer Windows NT Workstation kann sowohl User Accounts der eigenen Workstation als auch User Accounts und globale Gruppen der Domain der Workstation und aus allen dieser Domain vertrauenden Domains enthalten. Zu Beginn erkennt man keine allzu großen Unterschiede zwischen lokalen und globalen Gruppen. Deshalb soll dies anhand eines Beispiels erläutert werden.

Eine in der Domain Vertrieb erstellte globale Gruppe

- kann nur Benutzer aus der Domain Vertrieb enthalten
- kann in allen der Domain Vertrieb vertrauenden Domains verwendet werden

Eine lokale Gruppe in der Domain Vertrieb

- kann Benutzer und globale Gruppen aus der Domain Vertrieb und allen vertrauten Domains enthalten
- kann nur auf Servern der Domain Vertrieb verwendet werden

Es wird bei der Gegenüberstellung einer globalen Gruppe und einer lokalen Gruppe unterschieden, wo der Gruppe Rechte und Berechtigungen erteilt werden können, also der Gültigkeitsbereich der Gruppe. Lokale Gruppen können zudem globale Gruppen enthalten, wohingegen globale Gruppen weder lokale noch andere globale Gruppen enthalten können. Die User-Account-Datenbank einer Windows NT Workstation kann nur lokale Gruppen enthalten. Globale Gruppen können auf einer Windows NT Workstation nicht eingerichtet werden. Der lokalen Gruppe einer Windows NT Workstation können nur Rechte und Berechtigungen auf dieser Workstation erteilt werden. Selbst dann, wenn die Workstation Teil einer Domain ist, können die lokalen Gruppen einer Windows NT Workstation nicht auf anderen Computern verwendet werden.

23 Windows NT Server

Jeder Windows NT Server besitzt eine bestimmte Anzahl vordefinierter lokaler und globaler Gruppen. Die standardmäßig eingerichteten lokalen/globalen Gruppen sollen nachfolgend näher erläutert werden.

Vordefinierte lokale Gruppen

Administrators Mitglieder dieser lokalen Gruppe haben auf Servern der Domain so gut wie alle Berechtigungen. Sie können User Accounts, globale und lokale Gruppen einrichten, löschen und verwalten, Directories und Drucker für andere Teilnehmer freigeben, Benutzern Berechtigungen für Ressourcen und Rechte zuweisen, und sie können Betriebssystemdateien und Programme installieren. Im Gegensatz zum LAN-Manager 2.x kann der Administrator nicht automatisch auf alle Dateien eines Servers zugreifen. Wenn die Dateiberechtigung einem Administrator keinen Zugriff gewährt, kann der Administrator auf diese Datei auch nicht zugreifen. Jede Datei eines NTFS-Dateisystems hat einen sogenannten Owner, der Berechtigungen für seine Datei festlegen kann. Ein Benutzer, der eine Datei anlegt, wird unter Windows NT Server automatisch zum Owner der Datei gemacht.

Bei Bedarf kann der Administrator das Owner-Recht für eine Datei übernehmen, um dann auf diese zugreifen zu können. Wenn Sie eine Windows NT Workstation einer Domain hinzufügen, wird die globale Gruppe Domain Admins der Domain in die lokale Gruppe Administrators der Windows NT Workstation aufgenommen. Damit können die Mitglieder der Gruppe Domain Admins die Windows NT Workstation verwalten. Um zu verhindern, daß die Domain-Administratoren die Windows NT Workstation eines Benutzers verwalten können, muß die globale Gruppe Domain Admins aus der lokalen Gruppe Administrators der Windows NT Workstation entfernt werden.

Users Die lokale Gruppe Users wird für typische Netzwerkbenutzer verwendet, also Anwender, die im Netzwerk arbeiten müssen. Es sei nochmals darauf hingewiesen, daß herkömmliche Benutzer am Server nur über einen Login an einer Workstation arbeiten können. Ein direkter Login an der Windows NT Server Station ist bestimmten Benutzern mit speziellen Privilegien vorbehalten.

Guests Unter Windows NT Server haben Mitglieder der lokalen Gruppe Guest dieselben Rechte wie Mitglieder der Gruppe Users. Beide Gruppen haben nur das Recht, über den Login auf einer Windows NT Workstation auf den Server zuzugreifen. Ein direktes lokales Anmelden am Server ist ihnen also nicht erlaubt. Herkömmliche Benutzer, die Mitglied der lokalen Gruppe Guest sind, haben weniger Möglichkeiten auf der Windows NT Workstation. Die ausschließliche

23.3 Netzwerksicherheit

Mitgliedschaft in der lokalen Gruppe Guest erlaubt es nicht, die Workstation zu sperren und lokale Gruppen auf der Workstation einzurichten, zu löschen oder zu ändern.

Server Operators

Die lokale Gruppe Server Operators gibt es nur auf einem Windows NT Server und nicht auf einer Windows NT Workstation. Allgemein kann man sagen, daß Mitglieder dieser lokalen Gruppe den Server verwalten dürfen. Mitglieder dieser Gruppe haben bis auf die Einschränkung, keine Sicherheitsverwaltung auf dem Server durchführen zu können, weitgehend die gleichen Möglichkeiten wie Administratoren. Die berechtigten Aufgaben eines Server Operators liegen in der Freigabe von Druckern und Dateien bzw. in der Aufhebung der Freigabe. Der Server darf gesperrt bzw. die Sperre darf übergangen und die Festplatte bei Bedarf neu formatiert werden.

Ein Mitglied der lokalen Gruppe Server Operators kann sich direkt am Windows NT Server anmelden, Dateien des Servers sichern und zurückspielen oder den Server herunterfahren.

Account Operators

Diese Gruppe existiert nur auf einem Windows NT Server. Mitglieder dieser lokalen Gruppe haben die Berechtigung, die Benutzer- und Gruppendatenbank des Servers zu verwalten. Die Berechtigung dieser lokalen Gruppe beinhaltet nahezu alle Konten der Benutzer, daß sie globale sowie lokale Gruppen erstellen, löschen und ändern können. Ausgeschlossen ist die Verwaltung der Benutzerkonten der Administratoren und der lokalen Gruppen-Administratoren, Server Operators, Account Operators, Print Operators und Backup Operators. Zudem ist es einem Mitglied der Gruppe Account Operators nicht erlaubt, Benutzerrechte zu erteilen.

Print Operators

Diese lokale Gruppe gibt es nur auf einem Windows NT Server. Mitglieder der lokalen Gruppe Print Operators dürfen Drucker freigeben, die Freigabe von Druckern aufheben und Drucker verwalten, die am Windows NT Server angeschlossen sind. Print Operators dürfen sich lokal am Windows NT Server anmelden und den Server-Betrieb beenden.

Backup Operators

Mitglieder dieser lokalen Gruppe dürfen die Dateien des Servers sichern und wiederherstellen. Zudem wird damit die Berechtigung vergeben, sich lokal am Server anzumelden und den Server-Betrieb bei Bedarf zu beenden.

Replicator

Diese lokale Gruppe wird nur in Verbindung mit den File-Replication-Diensten benötigt.

Vordefinierte globale Gruppen

Nach der Installation von Windows NT Server sind standardmäßig zwei globale Gruppen eingerichtet.

23 Windows NT Server

Domain Admins In dieser globalen Gruppe ist zu Beginn der Benutzer-Administrator eingetragen. Beim Einrichten zusätzlicher Administratoren sollten diese als Mitglied der Gruppe hinzugefügt werden.

Domain Users Jeder neu eingerichtete Benutzer wird automatisch Mitglied dieser Gruppe.

Die beiden globalen Gruppen Domain Admins und Domain Users können nicht gelöscht werden.

Neben den besprochenen lokalen und globalen Gruppen sind nach der Installation zwei Standardbenutzer definiert: Administrator und Guest.

Das User Account Administrator ist das Benutzerkonto, das Sie nach der Installation eines neuen Servers (oder einer Windows NT Workstation) benötigen, um die ersten Schritte zum Verwalten des Servers durchführen zu können. Dieses Account kann nicht gelöscht oder gesperrt werden. Die Administration des Servers kann also auch nicht aus Versehen lahmgelegt werden.

Das User Account Guest kann dazu verwendet werden, daß sich Benutzer anmelden können, ohne ein eigenes User Account zu besitzen. Das User Account Guest sollte aus Sicherheitsgründen nicht durch zu viele Rechte ergänzt werden. Aus Sicherheitsgründen ist dieses User Account nach der Installation gesperrt. Möchten Sie entsprechende Anmeldungen zulassen, schalten Sie das User Account Guest frei.

23.4 Verwalten der Benutzeraktivitäten

Das Arbeiten der Benutzer im Netzwerk kann auf unterschiedliche Weise geregelt und gesteuert werden. Die dabei wichtigste und am häufigsten verwendete Methode besteht darin, vordefinierte lokale Gruppen zu verwenden. Durch die Zuordnung zu einer dieser Gruppen erhält der Benutzer eine Vielzahl vordefinierter Rechte und die damit verbundenen Möglichkeiten.

Vergessen Sie nicht, sich Gedanken über die Einstellungen bestimmter Festlegungen für das User Account zu machen. Hierzu gehören unter anderem die Beschränkung der erlaubten Logon-Zeit, die Paßworteinschränkungen und unter Umständen die Festlegung, von welcher Workstation der Logon im Netzwerk erfolgen darf.

Die Zugangsberechtigungen für im Netzwerk freigegebene Dateien, Directories und Drucker legen fest, wer auf die Ressourcen mit welchen Berechtigungen Zugriff haben soll. Solche Berechtigungen können lokalen oder globalen Gruppen zugewiesen werden. Durch die Mitgliedschaft in einer Gruppe erhält der Benutzer auch die mit

23.4 Verwalten der Benutzeraktivitäten

ihr verbundenen Rechte vererbt. Man kann jedoch die Berechtigungen auch dem Benutzer direkt zuweisen. Wie bei allen anderen Netzwerkbetriebssystemen sollte man jedoch generell versuchen, Berechtigungen soweit wie möglich über Gruppendefinitionen zu steuern, da dadurch der administrative Aufwand so gering wie möglich gehalten wird.

Wenn ein besonderes Sicherheitsbedürfnis existiert, können Sie bestimmte Aktivitäten eines Benutzers überwachen lassen, da Windows NT Server ein integriertes Auditing-System besitzt. Bei diesem Auditing-System ist zu unterscheiden, ob Benutzer, Dateien oder Directories überwacht werden sollen:

■ *Auditing von Dateien und Directories*

Für Directories (und die sich darin befindenden Dateien und Sub-directories) und Dateien können Sie Benutzer und Gruppen eintragen, wenn Aktivitäten hierfür protokolliert werden sollen. Folgende Ereignisse können protokolliert werden:

Read, Write, Execute, Delete, Change Permissions und Take Ownership.

Dabei muß noch festgelegt werden, ob die oben aufgeführten Ereignisse bei einem Fehlversuch oder einem erfolgreichen Versuch des Zugriffs in das Auditing Log eingetragen werden sollen.

■ *Auditing von Benutzern*

Für jeden einzelnen Benutzer können die folgenden Ereignisse protokolliert werden:

Logon und Logoff, File und Object Access, Use of User Rights, User and Group Management, Security Policy Changes, Restart – Shutdown, Process Tracking.

Auch hier haben Sie wieder die Möglichkeit, den erfolgreichen oder fehlgeschlagenen Versuch der oben aufgeführten Ereignisse protokollieren zu lassen.

Die Vergabe von Zugriffsberechtigungen sollte wie in allen anderen Netzwerkbetriebssystemen auch beim Windows NT Server sorgfältig geplant und ausgeführt werden. Wie bereits erwähnt, sollte man nach Möglichkeit die Vergabe von Zugriffsrechten so oft wie möglich über Gruppendefinitionen steuern. Dadurch behält man einen wesentlich besseren Überblick im Netzwerk, und man kann Änderungen bezüglich der Zugriffsberechtigungen einfacher und schneller durchführen.

Neben der Verwaltung der Benutzeraktivitäten spielt eine sehr wichtige Rolle im Netzwerk die Verwaltung der Benutzerumgebung selbst. Einige Aspekte der Verwaltung sind in den bisher ausgeführten Kapiteln bereits angesprochen worden. Diese Aspekte sollen im nachfolgenden Abschnitt vertieft werden.

23.5 Verwalten der Benutzerumgebung

Eine der Hauptaufgaben beim Einrichten von Netzwerken ist darin zu sehen, die Benutzerumgebung für jeden einzelnen Anwender entsprechend den jeweiligen Anforderungen optimal zu gestalten. Dies ist jedoch mit einem meist beträchtlichen Aufwand verbunden. Windows NT Server bietet unterschiedliche Möglichkeiten, die Umgebung der Workstations für Benutzer zu definieren. Unter anderem können festgelegt werden: Netzwerkverbindungen, verfügbare Anwendungen, Windows-Programmgruppen und die Gestaltung des Windows-Desktops. Damit Sie nicht ständig mit dem Neugestalten dieser Benutzerumgebungen beschäftigt sind, können die eingerichteten Desktop-Konfigurationen gegen Änderungen geschützt werden. Zur effizienten Gestaltung der Benutzerumgebung bietet Windows NT Server den sogenannten User-Profile-Editor. Ein User Profile ist eine Datei, in der Informationen über die Desktop-Umgebung eines Benutzers abgespeichert werden. Dabei kann es sich um Programmgruppen im Programm-Manager, Programme in den Programmgruppen, die Fenstergröße und -position und die Bildschirmfarben handeln. Mit Hilfe der Profiles können auch die Rechte von Benutzern eingeschränkt werden, Änderungen für die Einstellungen der Workstation durchführen zu dürfen.

Ein weiterer wichtiger Aspekt beim Gestalten der Benutzerumgebung ist die Möglichkeit, für einen Benutzer ein Logon Script zu definieren. Wenn für den Benutzer ein Logon Script vorhanden ist, dann wird es beim Anmelden des Benutzers ausgeführt, egal von welcher Workstation aus der Logon erfolgt. Das Logon Script kann eine Batch-Datei mit Betriebssystembefehlen (Herstellen von Netzwerkverbindungen, Starten spezieller Anwendungen oder Netzwerkbefehle) oder ein herkömmliches ausführbares Programm sein.

Damit der Anwender auf dem Server auch noch einen eigenen individuellen Bereich zur Verfügung hat, mit dem er tun und lassen kann, was er will, kann für jeden Benutzer ein Home-Directory eingerichtet werden. Mit dem Home-Directory wird einem Benutzer ein individueller Speicherplatz zugewiesen. Jeder Benutzer kann den Inhalt seines Home-Directory und den Zugriff auf dieses Verzeichnis selbst verwalten.

Daneben können für jede Workstation Umgebungsvariablen definiert werden. Mit diesen Umgebungsvariablen können unter anderem der Suchpfad der Workstation, das Verzeichnis für temporäre Dateien oder ähnliche wichtige Informationen festgelegt werden.

23.5 Verwalten der Benutzerumgebung

In den Benutzerprofilen sind die benutzerspezifischen Einstellungen der Windows-NT-Umgebung gespeichert. Benutzerprofile sind nur für Benutzer auf Windows NT Workstations einsetzbar. An MS-DOS-Workstations können sie nicht verwendet werden. Beim Einsatz von Windows NT Server in Verbindung mit Windows NT Workstations ist zwischen lokalen Profilen und Server-basierenden Profilen zu unterscheiden.

Lokale Profiles auf Windows NT Workstations

Ein lokales Profile wird auf einer Windows NT Workstation automatisch und ohne weiteres Zutun des Netzwerkverwalters angelegt. Immer wenn sich ein Benutzer an einer Windows NT Workstation anmeldet (außer er ist nicht berechtigt, auf das lokale Profile zuzugreifen) und anschließend wieder abmeldet, werden die vom Benutzer definierten Änderungen im lokalen Profile gespeichert.

Zu den im lokalen Profile gespeicherten Informationen gehören Netzwerkverbindungen, Programmgruppen und Programme, Fenstergröße und -position sowie das Aussehen des Desktops. Wenn der Benutzer die nächste Anmeldung wieder auf der gleichen Station durchführt, wird der Benutzer erkannt und das beim letzten Abmeldevorgang des Benutzers von der Workstation angelegte Profile geladen. Durch das Profile wird gewährleistet, daß bei jeder neuen Anmeldung Standardeinstellungen des Benutzers eingerichtet werden. Wenn an einer Windows NT Workstation mehrere Benutzer arbeiten und jeweils unterschiedliche Benutzernamen haben, läßt sich somit für jeden einzelnen Benutzer ein individuelles Profile und damit eine individuelle Umgebung einrichten und schaffen.

Lokale Profiles sind spezifisch für jeden Windows-NT-Arbeitsplatz. Die auf einer bestimmten NT Workstation durchgeführten Einstellungen sind nicht mehr verfügbar, wenn sich der Benutzer an einer anderen NT Workstation anmeldet (sofern er dort als Benutzer eingerichtet ist).

Server-basierende Profiles

In einem Netzwerk mit Servern und Domains unter Windows NT Server können Sie Profiles für Benutzer in Verbindung mit einem User Account in der Domain erstellen und diese Profiles auf einem Server abspeichern. Dadurch haben Sie folgende Vorteile:

- Für jeden Benutzer kann ein eigenes persönliches Profile mit einer speziellen Konfiguration erstellt werden. Dieses Profile wird beim Logon immer dann geladen, wenn sich der Benutzer im Netzwerk anmeldet, egal auf welcher NT Workstation der Logon erfolgt.

23 Windows NT Server

- Anhand des Benutzer-Profiles kann der Zugriff eines Benutzers auf das Profil so beschränkt werden, daß dieser keine Änderungen im Profil vornehmen kann. Somit wird vermieden, daß der Benutzer seine Einstellungen aus Versehen ändert (oder auch bewußt und dadurch gewisse Einstellungen nicht mehr stimmen).
- Beim Einsatz eines Profils für mehrere Benutzer können diesen Benutzern globale Zugriffsrechte erteilt werden, die ihnen zum Beispiel auf eine neue Anwendung oder einen neuen Server Zugriff gewähren, wobei nur das entsprechende Profil geändert werden muß.

Bei Verwendung von Profilen auf einem Windows NT Server muß noch zwischen persönlichen und verbindlichen Profilen unterschieden werden.

Beide Profil-Typen sind zentral auf einem Server abgespeichert. Man weist sie Benutzern zu, indem man jeweils Pfad- und Dateiname des Profils im User Account des Benutzers einträgt. Zu beachten ist dabei, daß zu einem bestimmten Zeitpunkt der Benutzer nur ein aktives Profil haben kann.

Persönliche Profile können vom jeweiligen Benutzer geändert werden. Sie werden automatisch bei jedem Abmeldevorgang aktualisiert und am Server gespeichert. Das heißt, alle Änderungen der benutzerspezifischen Einstellungen werden ohne das Zutun des Benutzers abgespeichert. Beim nächsten Logon des Benutzers wird die zuletzt eingerichtete Umgebung wiederhergestellt.

Verbindliche Profile können vom Benutzer nicht dauerhaft geändert werden. Auch wenn der Benutzer während seiner Arbeit die benutzerspezifischen Einstellungen ändert, werden diese Änderungen beim Abmelden im Benutzer-Profil nicht gespeichert. Beim nächsten Logon werden wieder die ursprünglichen Einstellungen des Benutzer-Profiles verwendet.

Beim Einsatz von sowohl persönlichen als auch verbindlichen Profilen können die Rechte eines Benutzers mit Hilfe folgender Aufgaben beschränkt werden:

- Erstellen von Programmsymbolen
- Erstellen von Programmgruppen
- Ändern des Inhalts von Programmgruppen
- Ändern von Programmeigenschaften
- Ausführen von Programmen im Programm-Manager über die Option *File (Run)*
- Herstellen von Verbindungen zu Netzwerkdruckern (zu anderen als den im Profil angegebenen Druckern)

23.5 Verwalten der Benutzerumgebung

Beim Arbeiten mit Windows NT ist noch die Bedeutung des Standard-Profiles zu berücksichtigen. Auf jeder Windows NT Workstation ist ein Standard-User-Profile gespeichert, das bei der Anmeldung des Benutzers in folgenden Fällen auf der Windows NT Workstation geladen wird:

- Wenn dem User Account noch kein anderes Profile zugewiesen ist und der Benutzer sich das erste Mal an diesem Windows-NT-Rechner anmeldet.
- Wenn der Zugriff auf das zugewiesene Profile des Benutzers nicht erfolgen kann, weil zum Beispiel der Server, auf dem das Profile gespeichert ist, nicht verfügbar ist.
- Wenn die Anmeldung mit dem User Account Guest durchgeführt wird.

Wenn einem User Account kein Profile zugewiesen worden ist, lädt NT beim ersten Logon des Benutzers das Standard-User-Profile dieser NT Workstation. Wenn der Benutzer über ein eigenes lokales Profile verfügen darf, werden beim Abmelden die benutzerspezifischen Einstellungen gespeichert und als lokales Profile für diesen Benutzer abgelegt. Bei jedem weiteren Logon des Benutzers an der gleichen NT Workstation wird dann statt des Standard-User-Profile sein gespeichertes lokales User Profile ausgeführt.

Arbeitsweise von Logon Scripts

Wie bereits erwähnt, handelt es sich beim Logon Script um eine Batch-Datei oder eine ausführbare Datei, die beim Anmelden des Benutzers an einer Windows NT Workstation oder einer MS-DOS Workstation automatisch ausgeführt wird. Mit Hilfe des Logon Script wird in der Regel die Arbeitsumgebung des Benutzers definiert, indem zum Beispiel Netzwerkverbindungen hergestellt und Anwendungen gestartet werden.

Ein Logon Script wird einem User Account durch Angabe eines Pfadnamens und eines Dateinamens zugewiesen. So wird bei jeder Anmeldung das Logon Script geladen und ausgeführt. Auf diese Weise kann jedem Benutzer das eigene Logon Script zugewiesen werden. Dadurch, daß das Logon Script eine herkömmliche Datei ist, kann diese auch für mehrere Benutzer gleichzeitig verwendet werden, sofern die Umgebungen in diesem Fall für alle Benutzer die gleichen sind.

Das Logon Script wird immer von dem Server geladen, der die Anmeldung des Benutzers bearbeitet. Bei Windows NT Server Domains mit mehreren Servern kann ein beliebiger Server in der Domain die Anmeldung des Benutzers durchführen. Damit bei jedem Logon in

der Domain das Logon Script für den Benutzer verfügbar ist, muß es auf allen Servern in der Domain verfügbar sein. Damit Sie nicht explizit jedes Logon Script auf alle anderen Server im Netzwerk kopieren müssen, vor allem unter dem Aspekt, bei Änderungen die Verteilung der Logon Script zu berücksichtigen, empfiehlt sich der Einsatz der Replicator-Dienste von Windows NT Server. Hierfür richten Sie den Server, auf dem das Original-Logon-Script abgespeichert ist, als Export-Server ein, und alle anderen Server sind dann Import-Server für die Logon-Script-Dateien.

23.6 Verwalten von Netzwerkdateien

Eine der Hauptaufgaben von Servern im Netzwerk besteht darin, Benutzern Dateien und Directories zur gemeinsamen Benutzung verfügbar zu machen bzw. bereitzustellen. Wird ein Directory freigegeben, können Benutzer von ihren Workstations aus Verbindungen zu diesem Directory herstellen und auf die Dateien in diesem Verzeichnis zugreifen. Das freigegebene Directory kann so verwendet werden, als wäre es eine andere Festplatte, die dem Benutzer zur Verfügung gestellt wird. In Verbindung mit dem Windows-NT-Dateisystem (NTFS) verbessern sich Leistungsfähigkeit, Zuverlässigkeit und Sicherheit für diese freigegebenen Directories.

Ihnen stehen Möglichkeiten zur Verfügung, Berechtigungen für Dateien und Directories zu vergeben, um damit festzulegen, wer mit welchen Rechten darauf zugreifen darf. Mit NTFS kann bei Bedarf die Berechtigung für jede Datei und jedes Directory unterschiedlich gestaltet werden. Für jede Datei und jedes Directory kann definiert werden, welcher Benutzer und welche Gruppe darauf Zugriff haben soll. Die NTFS-Berechtigungen sind gültig für Benutzer, die sich direkt am Windows NT Server anmelden (sofern sie aufgrund der Gruppenzugehörigkeit dazu berechtigt sind), und für Benutzer, die von einer Workstation aus auf die Datei zugreifen.

Um den Zugriff auf Dateien und Directories noch besser überwachen zu können, kann protokolliert werden, wann ein Benutzer auf eine Datei oder ein Directory zugegriffen hat.

Bei dieser Funktion handelt es sich um einen Mechanismus, der vom Betriebsrat genehmigt werden muß. Solch eine Art der Überwachung greift in den Bereich der Mitarbeiterkontrolle ein und kann deshalb nicht ohne vorherige Zustimmung eingerichtet und aktiviert werden.

23.6 Verwalten von Netzwerkdateien

Jede Datei und jedes Directory hat einen Owner, der den Zugriff auf diese Datei oder das Directory kontrollieren darf. Andere Benutzer können nur dann auf die Datei und das Directory zugreifen, wenn das vom Owner genehmigt wird.

Windows NT Server kann mit unterschiedlichen Dateisystemformaten installiert werden. Die besten Möglichkeiten der Sicherheit und Performance erhalten Sie dann, wenn Sie sich für das Windows-NT-Dateisystem entscheiden (NTFS).

23.6.1 Auswahl des Dateisystems

Der Server unter Windows NT Server kann drei Dateisysteme unterstützen:

- Windows NT File-System (NTFS)
- High Performance File-System (HPFS)
- File Allocation Table (FAT)

Auf den Platten und Partitionen eines Servers unter Windows NT Server können eines oder mehrere dieser Dateisysteme installiert werden. Bei der Installation des Servers müssen Sie sich entscheiden, welches dieser Dateisysteme eingesetzt werden soll.

Bei der Auswahl des Dateisystems sollten Sie sich an folgende Richtlinien halten, um das richtige Dateisystem für den Server zu finden:

1. Wird der Server nicht zusätzlich zu Windows NT Server auch mit MS-DOS oder OS/2 booten, dann verwenden Sie nur das NTFS auf dem Server. Jede andere Entscheidung hat keinen Sinn.
2. Muß der Server zusätzlich auch mit MS-DOS oder OS/2 booten, belassen Sie das aktuelle Dateisystem auf Laufwerk C:. Für die weiteren Partitionen, die für Windows NT Server eingerichtet werden, richten Sie NTFS-Partitionen ein. Sie müssen sich darüber im klaren sein, daß diese NTFS-Partitionen nicht unter DOS oder OS/2 gelesen werden können. Das ist aus Sicherheitsgründen auch gut so. Windows NT Server kann zusätzlich mit vorhandenen FAT- oder HPFS-Partitionen arbeiten.

Die Auflistung unten soll die Vor- und Nachteile der unterschiedlichen Dateisysteme gegenüberstellen, um nochmals zu zeigen, daß NTFS eingesetzt werden sollte, sofern es um die volle Ausnutzung der Sicherheitsmöglichkeiten unter Windows NT Server geht.

Windows-NT-Dateisystem**Vorteile**

Unterstützt die vollständige Sicherheit unter Windows NT Server. Zugriffsberechtigungen können auf Directory- und Dateiebene vergeben werden. Es wird ein Protokoll der Aktivitäten geführt, um die Festplatte nach einem Stromausfall oder anderen Problemen wiederherstellen zu können. Es wird das Fault-Tolerance-System von Windows NT unterstützt. Die Datei- und Directory-Namen können bis zu 256 Zeichen lang sein, und es stehen zusätzliche, erweiterte Dateiattribute zur Verfügung. Es werden automatisch MS-DOS-kompatible Dateinamen generiert, so daß Dateien zur gemeinsamen Benutzung mit MS-DOS-Anwendern freigegeben werden können. Ein Programm, das für ein anderes Betriebssystem erstellt worden ist, kann auf NTFS-Dateien zugreifen, wenn es unter Windows NT gestartet wird. Auf einem Windows-NT-System ist NTFS leistungsfähiger als das FAT oder HPFS-System. Bei der Eingabe von Datei- und Directory-Namen wird zwischen Groß- und Kleinschreibung unterschieden.

Nachteile

Wird nur von Windows NT erkannt. Wenn der Rechner mit einem anderen Betriebssystem gestartet wird (DOS, OS/2), kann dieses Betriebssystem auf die NTFS-Partition nicht zugreifen. Wenn das Laufwerk C: unter NTFS formatiert ist, kann MS-DOS nicht von der Festplatte aus ausgeführt werden.

HPFS-Dateisystem**Vorteile**

Abgestimmt für das Betriebssystem OS/2. Es werden Dateinamen mit bis zu 254 Zeichen unterstützt. Bietet bessere Fehlerkorrekturmechanismen als FAT. Es ist das Dateisystem, welches früher für OS/2-LAN-Manager verwendet worden ist.

Nachteile

Dateien auf einer HPFS-Partition können nicht durch die Sicherheitsmechanismen von Windows NT Server geschützt werden. Auf einer HPFS-Partition können MS-DOS- und Windows-3.1-Anwendungen nicht auf Dateien mit langen Dateinamen zugreifen (oder auf Pfade mit langen Verzeichnisnamen), da HPFS keine automatische Einrichtung von MS-DOS-konformen Dateinamen unterstützt, so wie oben beschrieben.

FAT-Dateisystem**Vorteile**

Es ist das meist verbreitete Dateisystem für PCs. Auch wenn der Rechner mit einem anderen Betriebssystem ausgestattet ist, kann er auf die Dateien zugreifen.

23.6 Verwalten von Netzwerkdateien

Nachteile

Dateien auf einer FAT-Partition sind nicht durch die Sicherheitsmechanismen von Windows NT Server geschützt. Dateinamen auf einer FAT-Partition sind auf eine Länge von acht Zeichen und einer dreistelligen Extension beschränkt. Sicherheitstechnisch gesehen ist eine FAT-Partition weniger robust im Vergleich zu NTFS, d.h., es gibt keine automatische Wiederherstellung von Festplatten.

23.6.2

Freigabe von Dateien/Directories für Anwender im Netzwerk

Wird ein Verzeichnis auf dem Server freigegeben, hat der Benutzer theoretisch Zugriff auf dieses Directory und auf alle darin enthaltenen Dateien und Subdirectories inklusive der darin enthaltenen Dateien. Beim Einsatz des NTFS-Dateisystems ist es möglich, den Zugriff auf einige Directories oder Dateien in dem freigegebenen Directory-Baum zu unterbinden und gleichzeitig andere Directories wieder zugänglich zu machen. Hierbei handelt es sich um die gleichen Möglichkeiten, die bereits für NetWare 3 und NetWare 4 beschrieben worden sind.

Wenn ein Directory auf dem Server für Benutzer freigegeben wird, muß diesem ein Share Name zugewiesen werden. Unter diesem Namen greifen die Anwender auf der Workstation auf dieses Directory zu. Standardmäßig wird als Share Name der Name des Directory verwendet. Sie können den Share Name bei Bedarf jedoch ändern.

Es ist erlaubt, mehrere Directories im gleichen Directory-Baum freizugeben. Dadurch kann der Fall eintreten, daß ein freigegebenes Directory für die Benutzer auf zwei Arten zugänglich ist: als eines der tatsächlich freigegebenen Directories oder als Subdirectory eines anderen freigegebenen Directory.

Herstellen von Netzwerkverbindungen

Normalerweise wird die Verbindung zu einem freigegebenen Directory am Server hergestellt, indem dem freigegebenen Directory ein Laufwerksbuchstabe für die entsprechende Workstation vergeben wird. Mit diesem Laufwerksbuchstaben bezieht sich der Anwender anschließend auf das Directory, für das die Verbindung hergestellt worden ist. Benutzer unter Windows NT oder Windows for Workgroups richten ein Netzwerklaufwerk mit dem File-Manager ein. Ein unter DOS arbeitender Benutzer benötigt für den Zugriff auf Windows NT Server eine installierte LAN-Manager-Workstationsoftware. Zum Verbinden eines Laufwerksbuchstabens mit einem Directory auf dem Windows NT Server muß dann der Befehl NET USE eingegeben werden. Wenn für Windows-NT-Server-Directories Netz-

23 Windows NT Server

werklauferwerke unter DOS, Windows oder Windows for Workgroups hergestellt werden müssen, dann sind dabei folgende Konventionen zu beachten:

- Bei der Vergabe des Share Name sollte der Share Name der MS-DOS-Konvention (8.3-Regel) entsprechen. Für Benutzer unter MS-DOS sind freigegebene Directories nicht zugänglich, wenn der Share Name sich nicht an diese Konvention hält.
- Wird auf ein freigegebenes Directory nur unter Windows NT Workstations zugegriffen, dann darf der Share Name maximal 12 Zeichen lang sein.
- Auf einer NTFS-Partition darf ein Datei- oder ein Directory-Name maximal 256 Zeichen lang sein. Für MS-DOS-Anwender stellt dies in der Regel jedoch kein Problem dar, weil NTFS für die Anzeige gegenüber einem MS-DOS-Anwender eine automatische Namenszuordnung durchführt. Dabei wird für allen Dateien und Verzeichnissen, deren Name nicht dem MS-DOS-Standard entspricht, automatisch ein zweiter, normgerechter Name zugewiesen. Wenn ein MS-DOS-Anwender die Datei oder das Verzeichnis über die Zuweisung als Netzwerklauferwerk anspricht, dann wird der entsprechende MS-DOS-konforme Name angezeigt. Windows-NT-Benutzer hingegen sehen nach wie vor den Ursprungsnamen, d.h. den langen Datei- und Directory-Namen. Zu beachten ist dabei, daß durch NTFS nur für Dateien und Directories mit langen NTFS-Namen der 8.3-Regel entsprechende Namen erzeugt werden. Für Share Names, die nicht MS-DOS-konform sind, werden keine kurzen Namen erzeugt. Diese müssen bereits beim Vergeben korrekt definiert werden, sofern auf das entsprechende freigegebene Directory auch MS-DOS-Anwender zugreifen sollen und werden. Beim Öffnen einer Datei durch eine Anwendung, die keine langen Dateinamen unterstützt, geht der lange Name verloren, sobald die Anwendung eine Änderung in der Datei durchführt und diese auf dem Server wieder abspeichert.

Wenn ein langer Name für eine Datei und ein Directory vergeben wurde, dann verwendet Windows NT Server folgende Regeln, um einen kurzen Namen zu erzeugen:

- Aus dem Namen werden die Leerzeichen entfernt.
- Zeichen, die MS-DOS nicht unterstützt, werden durch einen Unterstrich (_) ersetzt.
- Der Name wird auf die ersten sechs verbleibenden Buchstaben gekürzt (oder alle Zeichen vor dem ersten Punkt im langen Namen, falls sich der Punkt unter den ersten sechs Zeichen befindet). An diese sechs Zeichen werden eine Tilde und eine Zahl angefügt. Beim ersten kurzen Namen, der aus einer Kette von sechs Zeichen erzeugt wird, ist die Zahl eine 1. Werden aus diesen sechs

23.6 Verwalten von Netzwerkdateien

Zeichen weitere Namen generiert, gibt es also den erzeugten kurzen Namen bereits in den ersten sechs Zeichen, dann wird als Zahl die 2 angefügt. Wenn auf diese Weise der 10. Dateiname erzeugt werden soll, dann werden nur 5 Zeichen übernommen, und nach der Tilde wird die Zahl 10 angefügt und so weiter.

- Sind im langen Dateinamen ein oder mehrere Punkte enthalten, auf die noch andere Zeichen folgen, dann wird aus dem letzten Teil des Namens, der dem letzten Punkt folgt, und den ersten drei darauffolgenden Zeichen die Extension für den kurzen Namen gebildet. Zum Beispiel wird der Name ANDREAS.ZENK.TEXTDA-TEI der kurze Name ANDREA~1.TEX gebildet.

Beim Einsatz von Windows NT Server in einer gemischten Umgebung, d.h. Workstations unter Windows NT, MS-DOS und Windows 3.1 (Windows for Workgroups), ist es empfehlenswert, Dateinamen zu verwenden, die entweder in den ersten sechs Buchstaben der DOS-Konvention entsprechen oder gleich vollständig in der 8.3-Konvention abgespeichert werden.

23.6.3 Zugriffsberechtigungen für das NTFS-Dateisystem

Windows NT Server stellt eine Anzahl von Standardberechtigungen zur Verfügung, die für das Festlegen von Zugriffsrechten auf Dateien und Directories definiert werden können. Es handelt sich dabei um eine sinnvolle Kombination von Zugriffsrechten, die durchaus brauchbar sind. Bei Bedarf können jedoch individuell zusammengestellte Berechtigungen separat vergeben werden. Die Standardberechtigungen für Dateien und Directories sollen nachfolgend aufgeführt werden. Dabei gilt: Die in Klammern stehende Zugriffsberechtigung für Directories gibt an, welche Rechte im Verzeichnis für nachträglich erstellte Dateien vergeben werden.

Standardberechtigungen für Directories im NTFS-Dateisystem:

Verzeichnis

Kein Zugriff	(Keine) Der Benutzer darf in keiner Weise auf das Verzeichnis zugreifen, auch dann nicht, wenn er Mitglied einer zugriffsberechtigten Gruppe für dieses Verzeichnis ist.
Anzeigen	(Nicht festgelegt) Der Benutzer darf Dateien und Subdirectories im Verzeichnis nur auflisten und einen Wechsel in ein Subdirectory vornehmen. Der Benutzer hat keinen Zugriff auf neu erstellte Dateien in diesem Directory.
Lesen – RX	(RX) Der Benutzer darf Dateien im Directory lesen und Anwendungen in diesem Directory ausführen.

23 Windows NT Server

Hinzufügen – WX	(Nicht festgelegt) Der Benutzer darf im Directory Dateien anlegen, aber er darf vorhandene Dateien nicht lesen oder ändern.
Hinzufügen & Lesen – RWX	(RWX) Der Benutzer darf im Directory Dateien anlegen und vorhandene Dateien lesen. Das Ändern von Dateien ist nicht gestattet.
Ändern – RWXD	(RWXD) Der Benutzer darf Dateien lesen, hinzufügen, ändern und löschen.
Vollzugriff	(Alle) Der Benutzer darf Dateien lesen und ändern, neue Dateien hinzufügen, Berechtigungen für das Directory und die sich darin befindenden Dateien ändern und das Besitzrecht für Directory und Dateien übernehmen.

Datei

Kein Zugriff	Der Benutzer darf in keiner Weise auf die Datei zugreifen, auch dann nicht, wenn er Mitglied einer Gruppe ist, die Berechtigungen für die Datei besitzt.
Lesen – RX	Der Benutzer darf die Datei lesen. Handelt es sich bei der Datei um eine Anwendung, darf er sie auch ausführen.
Ändern – RWXD	Der Benutzer darf die Datei lesen, ändern und löschen.
Vollzugriff	Der Benutzer darf die Datei lesen, ändern, löschen, Berechtigungen hierfür vergeben und neuer Owner für die Datei werden.

Insgesamt stehen die folgenden Rechte zur Verfügung:

- Lesen (Read)
- Schreiben (Write)
- Ausführen (Execute)
- Löschen (Delete)
- Berechtigungen ändern (Change Permission)
- Besitz übernehmen (Take Ownership)

Wenn die Notwendigkeit besteht, hat man die Möglichkeit, beim Erstellen der Berechtigungen für eine Datei oder ein Directory Zugriffsberechtigungen selbst zusammenzustellen, also nicht nur die vordefinierten Standardrechte (wie vorher beschrieben) zu verwenden. Hierfür gibt es beim Vergabe der Rechte die Option *Special Access*; aus den sechs Rechten können Sie Ihre eigenen Kombinationen bilden.

23.6 Verwalten von Netzwerkdateien

Beim Einrichten des Sicherheitssystems für Directories und Dateien sind folgende Punkte zu beachten:

- Es besteht keine Notwendigkeit, jedem Anwender bzw. jeder einzelnen Gruppe explizit »Kein Recht« für Dateien und Directories zu vergeben. Solange Sie einem Benutzer oder einer Gruppe (der der Benutzer angehört) nicht explizit Rechte vergeben, hat er auch keine.
- Berechtigungen sind additiv zu sehen. Wenn zum Beispiel die Gruppe X Leserecht für die Datei TEXT.DOC hat und Sie geben dem Benutzer Schreibrecht für die gleiche Datei, dann hat der Benutzer somit Lese- und Schreibrecht. Das gleiche gilt, wenn das Recht auf diese Weise an zwei Gruppen vergeben wird und der Benutzer Mitglied beider Gruppen ist.

Eine Ausnahme stellt in diesem Zusammenhang das Recht »Kein Zugriff« dar, durch das alle anderen Berechtigungen wieder aufgehoben werden.

Damit ist es möglich, einer Gruppe das Zugriffsrecht auf eine Datei zu erteilen und gleichzeitig einer anderen Gruppe oder dem Benutzer den Zugriff zu entziehen.

- Standardmäßig übernehmen neue Dateien und Subdirectories die Berechtigungen des Directory, in dem die Datei oder das Subdirectory angelegt worden ist.
- Beim Ändern der Berechtigungen für ein bestehendes Directory kann entschieden werden, ob die Änderungen auf alle Directories und Subdirectories übertragen werden sollen.
- Legt ein Benutzer eine Datei oder ein Directory an, dann wird er als Owner dafür eingetragen. Der Owner hat immer das Recht, die Zugriffsmöglichkeiten auf die Datei oder das Directory zu definieren.

23.6.4 Zugriffsberechtigung beim Freigeben von Directories

In der Regel werden vor der Freigabe von Directories die Zugriffsrechte für Benutzer und Gruppen definiert. Wenn ein Directory freigegeben, d.h., der Shared Name vergeben wird, dann besteht die Möglichkeit, hierfür Freigabeberechtigungen zu definieren. Diese Berechtigungen wirken sich zusätzlich zu den individuellen Berechtigungen aus. Dieser Mechanismus ist vor allem dann von Interesse, wenn Directories auf FAT- oder HPFS-Partitionen freigegeben werden.

23.6.5 Vergeben von Berechtigungen

Bei der Vergabe von Zugriffsberechtigungen muß ausgewählt werden, wem die Berechtigungen erteilt werden sollen. Dabei stellt man fest, daß Windows NT Server intern noch weitere Objekte verwaltet, die sonst an keiner anderen Stelle auftreten.

Berechtigungen können sowohl für vordefinierte lokale Gruppen einer Domain als auch für neu angelegte Gruppen einer Domain vergeben werden. Zudem können Zugriffsberechtigungen für selbst eingerichtete Benutzer und die von Windows NT Server verwalteten »besonderen Benutzer« definiert werden. Zu den »besonderen Benutzern« und deren Eigenschaften zählen:

Everyone	Berechtigungen für dieses Objekt zu vergeben bedeutet, daß alle bereits vorhandenen und zukünftig eingerichteten Benutzer die zuge teilten Rechte besitzen.
System	Dieses Objekt stellt das Betriebssystem des lokalen Computers dar. Nach der Installation von Windows NT und Windows NT Server ent hält SYSTEM Berechtigungen für eine Vielzahl von Verzeichnissen. Diese Berechtigungen sollten auf keinen Fall aufgehoben werden. In der Regel muß für SYSTEM kein Recht mehr vergeben werden, es sei denn, spezielle Server-Dienste benötigen Zugriff auf erstellte Direc tories.
Network	Die hier eingetragenen Rechte erhält der Benutzer (alle bereits vor handenen und zukünftigen), wenn er von einer Workstation aus auf die Datei oder das Directory zugreift.
Interaktiv	Im Gegensatz zu NETWORK erhält der Benutzer die Rechte, wenn er sich direkt am Server mit seiner Kennung anmeldet. Greift ein Be nutzer über das Netzwerk auf eine Datei zu, gelten die Rechte, die in NETWORK vergeben wurden, aber nicht die Rechte, die für INTER AKTIV eingetragen sind. Erfolgt die Anmeldung unter dem gleichen Benutzernamen am Server, dann gelten für ihn die Rechte, die für INTERAKTIV eingetragen, und nicht mehr die Rechte, die in NET WORK festgelegt wurden.
Creator Owner	Dieses Objekt kann nur bei der Vergabe von Berechtigungen für Di rectories verwendet werden. Es steht für alle Benutzer, die nachfol gend Dateien und Verzeichnisse im aktuellen Verzeichnis anlegen. Wenn für ein Directory CREATOR OWNER hinzugefügt wird, erhält jeder Anwender, der eine Datei oder ein Directory in diesem Ver zeichnis anlegt, automatisch die Berechtigungen, die für den Objekt eintrag CREATOR OWNER festgelegt worden sind.

23.6.6 Berechtigungen für FAT- und HPFS-Dateisysteme

Für eine Partition unter einem FAT- oder HPFS-Dateisystem ist es nicht möglich, einzelne Berechtigungen für Dateien oder Directories zu vergeben. Die einzige Möglichkeit, den Zugriff auf ein FAT- oder HPFS-Dateisystem zu beschränken, besteht in der Vergabe von Freigabeberechtigungen, d.h. beim Einrichten eines Shared Name. Die Beschränkungen wirken sich nur auf die Benutzer aus, die über das Netzwerk auf Dateien oder Directories zugreifen. Bei der Freigabe von Directories können Sie einer Gruppe oder einem Benutzer für das Directory eine von vier Berechtigungen vergeben: Vollzugriff, Ändern, Lesen oder kein Zugriff. Es ist nicht notwendig, für jeden Benutzer »kein Zugriff« einzutragen, wenn dieser auf ein freigegebenes Directory keinen Zugriff haben soll. Sie schließen einen Benutzer vom Zugriff auf ein freigegebenes Directory einfach dadurch aus, daß Sie weder für den Benutzer noch für irgendeine Gruppe, in der der Benutzer Mitglied ist, eine Freigabeberechtigung für das Directory vergeben.

23.6.7 Dateibesitzrecht

Jede Datei und jedes Directory besitzt auf einem NTFS-Dateisystem einen Owner (Besitzer). Der Owner steuert die Berechtigungen für die Datei oder das Directory und kann zudem anderen Benutzern Berechtigungen erteilen. Das Konzept des Dateibesitzrechts ermöglicht es dadurch den Benutzern, private und persönliche Dateien auf dem Server auch vor einem Administrator im Netzwerk zu verbergen. Legt der Benutzer eine Datei oder ein Directory an, wird er automatisch zum Owner der Datei oder des Directory. Man sollte sich bei diesem Besitzrecht im klaren sein, daß die meisten Anwendungen in der Regel vom Netzwerkadministrator eingespielt und installiert werden.

Das Besitzrecht kann auf folgende Art und Weise übertragen werden:

- Der aktuelle Owner kann anderen Benutzern die Berechtigung »Besitz übernehmen« erteilen. In diesem Fall können diese Benutzer das Besitzrecht jederzeit übernehmen.
- Ein Administrator kann den Besitz jeder Datei auf dem Server übernehmen.

Ein Administrator kann zwar ein Besitzrecht übernehmen, er kann es jedoch nicht auf andere übertragen. Wenn somit ein Administrator aus Versehen das Besitzrecht für die Datei eines Benutzers übernommen hat, kann er dieses dem ursprünglichen Owner nicht wieder zurückgeben. Stellt ein Anwender fest, daß er nicht mehr Owner der Datei ist, kann er das gegenwärtige Besitzrecht der Datei prüfen, um festzustellen, wer als Owner für die Datei eingetragen worden ist.

23.7 Drucken im Netzwerk unter Windows NT Server

Neben dem Zugriff auf Dateien im Netzwerk besteht eine weitere Aufgabe darin, Druckdienste im Netzwerk bereitzustellen. Dieses Kapitel soll Ihnen die wichtigsten Aspekte aufzeigen, die zur Verfügung stehen, um das Drucken im Netzwerk unter Windows NT Server zu gestalten.

Die Druckdienste von Windows NT Server stellen eine Vielzahl von leistungsfähigen Möglichkeiten zur Verfügung:

- Wenn ein Drucker ausgewählt werden muß, kann das Netzwerk nach verfügbaren Windows-Druckern durchsucht werden, bevor eine Verbindung zu einem dieser Drucker aufgebaut wird. Die Verbindung kann über den Print-Manager oder im Dialogfeld zur Druckereinrichtung direkt innerhalb der Anwendung hergestellt werden.
- Die Druckertreiber müssen nicht auf der lokalen Windows NT Workstation installiert sein, damit der Zugriff auf einen Windows-NT-Netzwerkdrucker möglich ist. Für Windows 3.1x oder Windows 95/98 müssen die jeweiligen Druckertreiber lokal installiert sein.
- Es können auch Drucker auf LAN-Manager-2.x-Print-Servern verwendet werden. In diesem Fall muß der Druckertreiber für diesen Drucker lokal auf der Windows NT Workstation eingerichtet sein.

Jede Windows NT Workstation oder jeder Windows NT Server kann als Print-Server im Netzwerk eingerichtet und als solcher benutzt werden. Sind alle Workstations im Netzwerk mit Windows NT ausgestattet, dann müssen die Druckertreiber nur auf einem Rechner installiert werden, und zwar dem Print-Server.

Beim Einrichten der Druckdienste ist es durchaus möglich, Windows NT gleichzeitig als Print-Server und File-Server einzusetzen. Dateioperationen erhalten generell die höhere Priorität, so daß in der Regel die Druckdienste den Zugriff auf Dateien nicht wesentlich verzögern sollten. Einen Server ausschließlich als Print-Server zu verwenden ist nur dann notwendig, wenn das Druckaufkommen sehr groß ist. Dann könnte man allerdings auch die Entscheidung treffen, das Drucken im Netzwerk auf mehrere Print-Server gleichmäßig zu verteilen. Nicht zu vergessen ist jedoch auch der Sicherheitsaspekt, wenn zu entscheiden ist, welche Station im Netzwerk zum Print-Server gemacht wird. Die Drucker im Netzwerk sollten eigentlich immer verfügbar und für den Anwender zugänglich sein. Beim File-Server hingegen ist es dagegen angebracht, ihn in einem abgeschlossenen Raum aufzustellen.

23.7 Drucken im Netzwerk unter Windows NT Server

Meist werden Netzwerkdrucker nicht am Server oder an der Workstation installiert, sondern direkt in das Netzwerk integriert. Hierfür stellen die unterschiedlichen Hersteller entsprechende externe Print-Server zur Verfügung. Beim Einsatz der externen Print-Server muß entweder das DLC-Protokoll eingesetzt werden, oder man konfiguriert die Print-Server für TCP/IP-Unterstützung. Für den Einsatz von TCP/IP als Protokoll der Netzwerkdruckerunterstützung müssen zusätzliche Mechanismen freigeschaltet werden. Da für das Drucken über TCP/IP das LPR-Protokoll notwendig ist, muß am NT Server nicht nur TCP/IP installiert sein. Zusätzlich ist einzurichten, daß die Unix Print Services unterstützt werden. Ohne diese Konfiguration ist an ein Drucken über das LPR- und TCP/IP-Protokoll nicht zu denken.

Das Einrichten des File-Servers erfordert eine ebenso sorgfältige Planung. Beim Einrichten der Druckerumgebung sind zu unterscheiden: Print-Devices, die am Print-Server oder direkt im Netzwerk angeschlossen sind, und logische Printer, die über den Windows-NT-Print-Manager eingerichtet werden. Das Print-Device ist die echte physikalische Hardware, über die Druckaufträge ausgegeben werden. Der Drucker, der mit dem Print-Manager eingerichtet wird, ist eine Software-Schnittstelle zwischen dem Betriebssystem und dem Print Device. Diese Schnittstelle bestimmt, wohin das Dokument zum Ausdrucken gesendet werden muß, wann es auszudrucken ist und weitere Aspekte der Druckersteuerung.

Wenn der Anwender eine Verbindung zu einem Netzwerkdrucker herstellt, wird tatsächlich die Verbindung zu einem logischen Drucker hergestellt. Durch die unterschiedlichen Möglichkeiten, logische Drucker und Print-Devices miteinander zu verbinden, werden dem Benutzer die Flexibilitäten geboten, das Drucken im Netzwerk so zu gestalten, daß alle Erfordernisse erfüllt werden. Insgesamt stehen folgende Möglichkeiten der Druckerkonfiguration zur Verfügung:

- Ein logischer Drucker bedient ein Print-Device.
- Mehrere logische Drucker bedienen ein Print-Device.
- Ein logischer Drucker bedient mehrere Print-Devices.

Die Flexibilität und Effizienz des Druckens im Netzwerk kann zusätzlich durch verschiedene Konfigurationen der Druckerumgebung optimal angepaßt werden. Diese Funktionen sollen anschließend näher betrachtet werden.

23.7.1 Zurückstellen von Druckaufträgen

Um Drucker optimal auslasten zu können, lassen sich für den logischen Drucker sogenannte Druckzeiten festlegen. Damit legt man fest, in welchen Zeiträumen der Drucker seine Druckaufträge ausgeben soll. Der Print-Spooler nimmt für diesen Drucker zwar jederzeit Druckaufträge an, zum Print-Device werden sie jedoch nur dann geschickt, wenn die angegebenen Druckzeiten erreicht sind. Ist die Druckzeit beendet, werden keine Druckaufträge mehr zum Drucker geschickt, sondern die Druckaufträge werden bis zur nächsten Druckzeit aufgehoben. Damit kann erreicht werden, daß ein Drucker, der tagsüber stark belastet ist, nicht zusätzlich mit weniger wichtigen Druckaufträgen belastet wird. Hierzu wird für den Drucker ein zusätzlicher logischer Drucker definiert, für den eine Druckzeit in der Nacht eingerichtet ist. Weniger wichtige Druckaufträge werden dann über diesen logischen Drucker ausgegeben.

23.7.2 Prioritäten für Drucker vergeben

Im Netzwerk kann es immer wieder vorkommen, daß ein Dokument sofort gedruckt werden muß und deshalb die bereits vorhandenen Druckaufträge umgangen werden sollen. Das kann unter Windows NT erreicht werden, indem logische Drucker mit unterschiedlichen Prioritätsstufen eingerichtet werden. Sind zwei logische Drucker mit demselben Print-Device verbunden, so werden die Druckaufträge zuerst gedruckt, die über den Spooler mit der höheren Priorität an den Drucker geschickt werden. Das System der Druckerprioritäten kann ausgenutzt werden, indem man mehrere logische Drucker einrichtet, die an das gleiche Print-Device angebunden werden.

23.7.3 Einsatz von Print-Pools

Der Print-Pool besteht aus mindestens zwei gleichen Print-Devices, die mit dem gleichen logischen Drucker verbunden sind. Um einen Print-Pool einzurichten, wird zuerst ein logischer Drucker definiert und mit einem Druckerausgang verbunden. Anschließend wird diesem logischen Drucker ein weiterer Ausgabeport zugewiesen. In dieser Konfiguration werden die Print-Devices bestmöglich ausgelastet. Für Print-Pools sind folgende charakteristische Eigenschaften anzuführen:

- Alle Print Devices für den Print-Pool sind vom gleichen Typ und werden wie eine Einheit betrachtet. Alle Druckereinstellungen sind gültig für den gesamten Pool.
- Die Druckeranschlüsse können parallel, seriell oder vom Typ Netzwerk sein. Eine Mischung ist möglich.

23.7 Drucken im Netzwerk unter Windows NT Server

- Kommt ein Druckauftrag im Print-Pool an, dann wird vom Spooler geprüft, an welchem Druckerausgang ein Print Device im Leerlauf ist. Die Anschlüsse werden in der Reihenfolge geprüft, in der sie installiert worden sind. Wenn der Pool aus unterschiedlichen Anschlüssen besteht, sollte darauf geachtet werden, daß der schnellste Anschluß als erster ausgewählt wird, d.h., es sollte die Reihenfolge Netzwerk, parallel und dann seriell berücksichtigt werden.
- Unterbricht ein Print Device das Drucken im Netzwerk, weil zum Beispiel kein Papier mehr im Drucker ist, dann wird nur der Druckauftrag dieses Druckers angehalten. Die anderen Druckaufträge können in der Zwischenzeit über die anderen Print Devices im Print-Pool ausgegeben werden. Der unterbrochene Druckauftrag wird so lange angehalten, bis der Drucker wieder intakt ist.
- Es ist nicht vorherzusehen, welcher Drucker im Pool welchen Druckauftrag ausgeben wird. Ist jedoch der Windows-NT-Message-Service eingerichtet, dann bekommt die Workstation, d.h. der Anwender, eine Nachricht, daß der Druckauftrag ausgegeben ist. In dieser Nachricht wird auch angegeben, an welchem Ausgabeport der Druck ausgegeben wurde. Somit ist feststellbar, welcher Drucker diesen Auftrag gedruckt hat.

23.7.4

Zugriff auf Drucker steuern

Die Benutzung von Druckern unter Windows NT kann dadurch gesteuert werden, daß Sie festlegen, wer die Berechtigung zur Benutzung des Druckers hat. Standardmäßig sind alle freigegebenen Drucker für alle Netzwerkanwender verfügbar. Um Berechtigungen für einen Drucker zu ändern, muß man der Owner des Druckers sein oder die Berechtigung »Vollzugriff« haben. Für die Vergabe von Berechtigungen stehen zur Verfügung:

- Kein Zugriff
- Drucken
- Dokumentenverwaltung (Berechtigung, alle an diesen Drucker gesendeten Aufträge zu verwalten)
- Vollzugriff

Die Berechtigungen sind additiv, außer der Berechtigung »kein Zugriff«, die alle anderen Berechtigungen überschreibt.

Die gesamte Verwaltung der Drucker erfolgt im Print-Manager. Hierzu zählen im Detail:

- Anzeigen aller Drucker und der dazugehörigen Druckaufträge
- Löschen von Druckaufträgen
- Anhalten oder Freigeben eines Druckauftrags
- Erneutes Starten eines Druckauftrags von Anfang an

23 Windows NT Server

- Unterbrechen eines gerade im Druck befindlichen Druckauftrags
- Anhalten eines Druckers und erneutes Starten
- Löschen eines Druckers

Ein lokaler oder entfernter Print-Server kann von jeder beliebigen NT Workstation im Netzwerk verwaltet werden, vorausgesetzt man besitzt hierfür die Berechtigung »Vollzugriff«.

23.8 Fehlertoleranz

Unter Fehlertoleranz versteht man die Fähigkeit des Systems, auch bei Ausfall eines Systemteils weiterzuarbeiten. Fehlertoleranz ist vor allem bei Festplattensystemen erforderlich. Sie kann sich aber durchaus auch auf andere Systemteile beziehen, die gegen Ausfall gesichert sein müssen, damit bei deren Ausfall nicht die Funktionsfähigkeit des Gesamtsystems gefährdet ist. Große Ausfallsicherheit wird durch den Einsatz redundanter Platten-Controller (inklusive Platten) und Stromversorgungen erreicht.

Auch wenn der Server mit redundanter Peripherie ausgestattet ist und somit die Verfügbarkeit so groß wie möglich sein wird, entbindet dies nicht von der regelmäßigen Datensicherung. Der Systemausfall kann ein derartiges Ausmaß haben, daß auch die Redundanz keine Sicherheit mehr bringt und zum Rekonstruieren der Datenbestände auf die letzte Datensicherung zugegriffen werden muß (z.B. aufgrund von Feuer, Wassereinbruch oder ähnlichen Katastrophen). Für solche Fälle sollte die Bandsicherung auf alle Fälle außer Haus aufbewahrt werden. Für den Einsatz fehlertoleranter Festplattensysteme ist ein Standard definiert worden, der in sechs Stufen eingeteilt wird. Diese Stufen werden allgemein als RAID Level (Redundant Arrays of Inexpensive Disks) bezeichnet (Stufe 0 bis Stufe 5). Da darüber immer wieder unterschiedliche Meinungen zu hören sind, sollen diese sechs RAID Levels anschließend näher betrachtet werden.

23.8.1 RAID-Level-Systeme

Die einzelnen RAID Levels sind leider etwas oberflächlich definiert, so daß sich die Geschwindigkeiten und die Art der Plattenzugriffe in den unterschiedlichen Konfigurationen unterscheiden. In Abhängigkeit von der Implementierung können sich Teile der Definitionen durchaus überschneiden, oder sie können kombiniert werden. Zu beachten ist dabei, daß die Fehlertoleranz nicht verfügbar ist, solange ein aufgetretener Fehler nicht behoben wird. Nur wenige RAID-Systeme können es verkraften, daß gleichzeitig zwei Fehler auftreten und das System immer noch lauffähig bleibt.

23.8 Fehlertoleranz

■ *RAID Level 0*

Diese Toleranzstufe wird häufig auch als Festplatten-Striping bezeichnet. Es sei jedoch gleich darauf hingewiesen, daß hierbei keinerlei Ausfallsicherheit vorliegt, dafür aber ein sehr hoher Datendurchsatz erreicht wird. In diesem Fall wird ein Plattensystem (Stripe Set) eingesetzt, bei dem die Daten in Blöcke aufgeteilt und in einer festen Reihenfolge auf alle Platten des Stripe Sets verteilt werden. Das heißt, die Datei ist auf die Anzahl der Platten des Stripe Sets verteilt. Es wird keine Fehlertoleranz geboten. Wenn eine der Partitionen im Stripe Set ausfällt, dann gehen alle Daten verloren. Aus Sicherheitsgründen müßte dieses Verfahren (hoher Durchsatz) mit RAID Level 1 kombiniert werden.

■ *RAID Level 1*

Eine andere Bezeichnung für RAID Level 1 ist Plattenspiegelung. Bei der Plattenspiegelung werden alle Daten, die auf die eine primäre Platte geschrieben werden, gleichzeitig auf eine sekundäre Platte (Spiegelplatte) geschrieben. Man hat also z.B. zwar insgesamt 2 mal 1 Gbyte Plattenkapazität zur Verfügung, aber real zum Arbeiten nur 1 Gbyte Kapazität. Fällt eine Platte aus, arbeitet das System mit der anderen Platte weiter.

■ *RAID Level 2*

Bei diesem Verfahren wird durch Fehlerkorrekturinformationen Redundanz hinzugefügt. Man bedient sich auch hier der Stripe-Technologie, bei der Dateien in einzelne Bytes zerlegt und auf mehrere Platten verteilt werden. Die eingesetzte Methode zur Fehlerkorrektur ist relativ aufwendig und benötigt mehrere Platten für die Speicherung der Informationen zur Fehlerkorrektur.

■ *RAID Level 3*

Dieses RAID Level gleicht RAID Level 2 insofern, als die gleiche Striping-Methode eingesetzt wird. Bei RAID Level 3 wird für die Fehlerkorrektur nur eine Platte für die Paritätsdaten benötigt. Die Ausnutzung der Speicherkapazität beträgt in Abhängigkeit von der Anzahl der eingesetzten Festplatten bis zu 86%.

■ *RAID Level 4*

Bei diesem Verfahren werden die Daten in größere Blöcke oder Segmente eingeteilt, als dies bei RAID Level 2 oder 3 der Fall ist. Es werden immer noch alle Daten zur Fehlerkorrektur auf einer einzigen Platte, getrennt von den Benutzerdaten, gespeichert. Die Ausnutzung der Speicherkapazität hängt auch hier von der Anzahl der Platten pro Stripe-Set ab.

■ *RAID Level 5*

Dieses Verfahren wird als Striping mit Parität bezeichnet und ist heute die am häufigsten eingesetzte Methode (neben RAID Level 1). Ähnlich wie bei RAID Level 4 werden die Daten in großen Blöcken auf alle Platten innerhalb des Stripe Set verteilt. Der Un-

23 Windows NT Server

terschied zu RAID Level 4 liegt beim Abspeichern der Paritätsinformationen; diese werden auf alle Platten verteilt. Datenredundanz wird dadurch gewährleistet, daß die Daten und die Paritätsinformationen so auf die Platten verteilt werden, daß sich die beiden Informationen immer auf zwei unterschiedlichen Plattenlaufwerken befinden. Stripe Sets mit Parität erzielen beim Lesen bessere Leistungen als Spiegelungen. Wenn jedoch ein Teil im Stripe Set fehlt (Ausfall einer Platte), reduziert sich die Leistung, da die Daten über die Paritätsinformation rekonstruiert werden müssen. Die Performance beim Schreiben wird ebenfalls reduziert, da die Paritätsberechnung zusätzlich durchgeführt werden muß.

Generell sollte man beim Einsatz von Plattensubsystemen darauf achten, daß Hardware verwendet wird, die entsprechend leistungsfähig ist, um den größtmöglichen Durchsatz zu erzielen. Die Hauptaufgaben eines Server-Systems liegen im Lesen und Schreiben von Daten. Es sollte für diese Hardware das Optimum gefunden werden, da sich andernfalls die Leistungsfähigkeit des Servers stark reduziert. Abgesehen davon sollten generell alle Hardware-Komponenten optimal aufeinander abgestimmt sein. Was nutzt Ihnen das leistungsfähigste RAID-Level-5-System, wenn es in einen 386-16-MHz-Rechner eingebaut wird.

23.8.2 Unterbrechungsfreie Stromversorgung

Unterbrechungsfreie Stromversorgung (USV) liefert auch dann Strom, wenn die lokale Stromversorgung (über die Steckdose) ausfällt. In der Regel sind solche Systeme dafür ausgelegt, die Stromversorgung über einen längeren Zeitraum zu überbrücken.

Bei den USV-Systemen können Online- und Offline-USV-Anlagen unterschieden werden.

■ *Online USV*

Eine Online USV wird zwischen Steckdose und Server angeschlossen, so daß der Server immer mit Strom versorgt wird. Das heißt, die Stromversorgung des Servers erfolgt nicht mehr über die Steckdose, sondern sie kommt immer von der USV. Durch den Anschluß der USV an die Steckdose wird die USV immer geladen. Durch eine Online USV werden auch Spannungsspitzen, Spannungsschwankungen, Spannungsausfälle und Spannungsrauschen unterbunden. Bei dieser Methode ist auch keine Schaltzeit zu berücksichtigen (im Vergleich zur Offline USV), da beim Ausfall der Spannung nur das Aufladen der Batterie in der USV ausbleibt.

23.8 Fehlertoleranz

■ *Offline USV*

Beim Anschluß einer Offline USV erhält der Server die Spannungsversorgung über die Steckdose und bei Ausfall der Spannung über die USV-Anlage. Das heißt, bei Bedarf (Stromausfall) wird auf den USV-Betrieb umgeschaltet. Solange die Spannung aus der Steckdose zur Verfügung steht, verbindet die USV die Spannung der Steckdose mit dem Server und überwacht die Spannung. Die USV-Stromversorgung bleibt somit im Mitlaufbetrieb (d.h. immer bereit, um Strom zu liefern), und die Batterie bleibt geladen. Wenn die Spannung in der Steckdose ausfällt oder die Spannung auf einen voreingestellten Wert sinkt, schaltet die USV die Spannungsversorgung auf USV-Betrieb um. Dies muß so schnell geschehen, daß das Netzteil des Servers davon nicht beeinträchtigt wird und ohne Unterbrechung weiterarbeiten kann.

■ *Zusammenarbeit von USV und Windows NT Server*

Beim Einsatz einer USV-Anlage muß darauf geachtet werden, daß sie auch vom Netzwerkbetriebssystem unterstützt wird. Nur in diesem Fall können die gesamten Vorteile vollständig genutzt werden. Hierzu zählt unter anderem, daß Benutzer automatisch darüber informiert werden, wenn der Server auf USV-Betrieb läuft und bald heruntergefahren werden sollte oder wenn die normale Stromversorgung wiederhergestellt ist und somit der Server nicht mehr heruntergefahren werden muß.

Während eines Stromausfalls unterbricht der USV-Dienst sofort den Server-Dienst, wodurch die Herstellung neuer Verbindungen durch neue Benutzer verhindert wird. Anschließend sendet der USV-Dienst eine Nachricht an alle noch aktiven Benutzer, um über den Ausfall der Spannung zu informieren. Der USV-Dienst wartet eine vorher festgelegte Zeit, innerhalb derer der Benutzer aufgefordert wird, sich abzumelden und seine Arbeit zu beenden.

Wird die Stromversorgung in dieser Zeit wiederhergestellt, werden die Benutzer darüber informiert, und es wird Ihnen mitgeteilt, daß der normale Betrieb wieder aufgenommen wurde. Der Anschluß der USV erfolgt über COM1, ..., COM4, in Abhängigkeit davon, wie Sie das System konfigurieren.

Standardmäßig sind im Lieferumfang von Windows NT Server-Dienste enthalten, die im nächsten Abschnitt näher betrachtet werden sollen. Es handelt sich dabei um Remote Access Services, Macintosh Services und TCP/IP-Unterstützung.

23.9 Remote Access Services (RAS)

Die RAS-Dienste von Windows NT Server bestehen aus zwei Komponenten:

- *RAS-Server*

Ein Server, der es einem externen Computer ermöglicht, sich in ein Netzwerk einzuwählen, um damit arbeiten zu können.

- *RAS-Client*

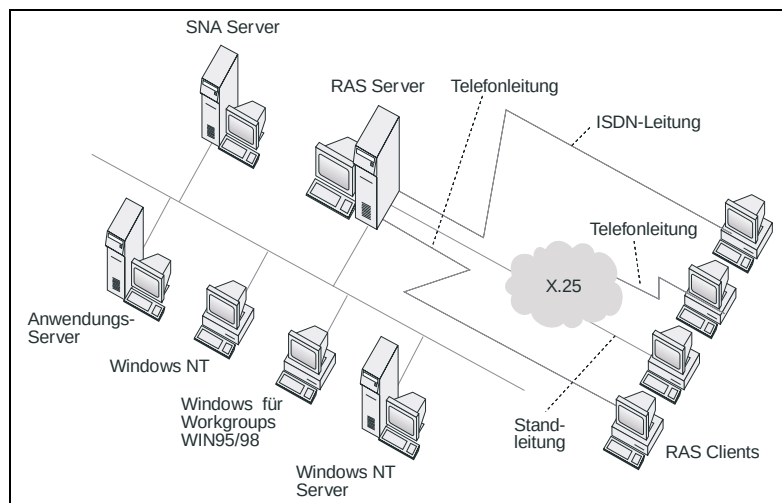
Ein Computer, der sich in einem RAS-Server einwählt.

Als RAS-Client bezeichnet man einen Computer, der nicht direkt in das Netzwerk eingebunden ist. Sobald der Anschluß hergestellt ist, ist die Telefonverbindung für den Anwender vollkommen transparent. Das heißt, vom RAS-Client aus kann der Benutzer die zum Netzwerk gehörenden Ressourcen einsehen und so auf diese zugreifen, als würde er sich direkt im Netzwerk (physikalisch eingebunden) befinden. Auf diese Weise dient der RAS-Server als Gateway zwischen dem RAS-Client und dem Netzwerk.

Zu den RAS-Diensten gehört ein Telefonbuchprogramm, mit dem die Namen und Telefonnummern von Remote-Netzwerken verwaltet werden können. Ein Client kann damit einfach und bequem Verbindungen zu Remote-Netzwerken aufbauen und wieder beenden.

Das Administrationsprogramm für die RAS-Dienste ermöglicht es Ihnen, RAS-Server und -Benutzer von einem beliebigen Rechner (Windows NT Workstation) aus im Netzwerk zu überwachen. In Abbildung 23.6 sind alle unterstützten Möglichkeiten zur Remote-Einbindung dargestellt.

Abbildung 23.6
RAS-Dienste unter
Windows NT
Server



23.10 Services for Macintosh

Folgende Eigenschaften stehen mit den RAS-Diensten zur Verfügung:

- Transparenter Zugriff für Außendienstmitarbeiter auf das Netzwerk
 - Unterstützung von Named Pipes, Remote Procedure Call (RPC) und der LAN-Manager-Schnittstelle für Anwendungsprogrammierung (LAN Manager Application Programming Interface)
 - Zugriff von Clients auf Anwendungsserver wie SQL-Server, SNA-Server für Windows NT oder Lotus Notes
- Unterstützung für normale Telefonleitungen, ISDN und X.25
- Unterstützung für Modemkomprimierung und Modem-Fehlerkorrektur
- Software-Komprimierung
- Zugriffsüberwachung
 - Integration in die Zugriffsüberwachung von Windows NT Server
 - Domain-bezogene Zugriffsüberwachung (auch in Trusted Domains)
 - Verschlüsselte Authentifizierung zum Zeitpunkt des Verbindungsaufbaus
 - Rückrufmodus für zusätzliche Sicherheit oder zur Kostenübernahme
 - Zentrale Verwaltung der Server und der Benutzer
- Pro Server sind bis zu 256 Verbindungen gleichzeitig möglich
- Unterstützung für über 100 Modems

Mit diesen Diensten haben Sie eine sehr gute Möglichkeit, Remote-Anbindungen für das Netzwerk vorzunehmen. Da die Sicherheitsanforderungen in keiner Weise verletzt werden, ist eine Integration von Remote-Anwendern problemlos möglich.

23.10 Services for Macintosh

Im Lieferumfang von Windows NT Advanced Server ist das Produkt Services for Macintosh enthalten. Hiermit kann eine Integration von Macintosh-Rechnern in das Netzwerk erreicht werden, die damit die Möglichkeit haben, auf Dateien und Drucker zuzugreifen, die von Windows NT Server verwaltet werden. Der Windows NT Server verhält sich den Macintosh-Rechnern gegenüber wie ein AppleShare Server.

23 Windows NT Server

Somit muß auf den Macintosh-Rechnern keine zusätzliche Software installiert werden. Durch den Einsatz von Services for Macintosh stehen Ihnen zur Verfügung: gemeinsame Nutzung von Dateien und Druckern, vereinfachte Verwaltung und Unterstützung von Apple-Talk Routing.

Gemeinsame Nutzung von Dateien

Die Dateisysteme von MS-DOS, OS/2 und Windows NT unterscheiden sich zwar grundsätzlich vom Macintosh-Dateisystem, dennoch können mit Hilfe von Services for Macintosh PC-Anwender (mit den oben aufgeführten Betriebssystemen) und Macintosh-Anwender mit allen auf dem Server befindlichen Dateien gemeinsam arbeiten. Sowohl für Macintosh-Anwender als auch für andere Benutzer werden die Dateien in der gewohnten Form und Umgebung dargestellt (Native Form). Das heißt, jedes System arbeitet beim Zugriff auf Dateien mit seinen gewohnten Betriebssystemoberflächen.

Wenn Sie Anwendungen einsetzen, die für DOS-, OS/2-, Windows NT und Macintosh-Workstations zur Verfügung stehen, kann ein gemeinsamer Zugriff auf Dateien noch einfacher gestaltet werden, da diese Anwendungen dateiformatkompatibel sind. In anderen Fällen müssen unter Umständen Dateiformatkonvertierungen durchgeführt werden. Damit ein Macintosh-Benutzer auf Directories und Dateien zugreifen kann, muß der Netzwerkverwalter das jeweilige Verzeichnis als Datenträger für den Macintosh bestimmen.

Da für den Macintosh andere Konventionen bezüglich der Verwendung von Dateinamen existieren, muß bei Bedarf eine Umsetzung der Dateinamen erfolgen.

Hierbei sind zwei Arten der Umsetzung zu unterscheiden:

- Verwaltung und Darstellung von Macintosh-Dateinamen für die unterschiedlichen Benutzer
- Darstellung der längeren NTFS-Namen mit mehr als 32 Zeichen für die Macintosh-Anwender

Die Umsetzungsroutinen sind dabei wie folgt zu verstehen:

- Ein nach der FAT-Dateinamenskennung vergebener Dateiname wird für NTFS- und Macintosh-Anwender in unveränderter Form angezeigt.
- Ein Dateiname, der im Rahmen der Begrenzung des Macintosh-Betriebssystems mit 31 Zeichen eingegeben worden ist, wird für NTFS-Anwender in unveränderter Form angezeigt. Für MS-DOS-Anwender wird der Dateiname in der bereits beschriebenen Form konvertiert.

23.10 Services for Macintosh

- Ein Dateiname, der im Rahmen der NTFS-Begrenzung mit 256 Zeichen eingegeben worden ist, wird in unveränderter Form angezeigt, sofern der Name nicht länger ist als 31 Zeichen. Andernfalls muß für den Macintosh-Anwender eine Konvertierung in Kurzform erfolgen.

Gemeinsame Nutzung von Druckern

In Services for Macintosh sind Funktionen enthalten, die es ermöglichen, daß Macintosh- und PC-Anwender Druckaufträge an jeden Drucker übertragen können, der an einem Windows NT Server angeschlossen ist, also auch zu Druckern, die als LaserWriter im AppleTalk-Netzwerk installiert sind. Dadurch sind folgende Vorteile gegeben:

- Macintosh-Anwender können PostScript-Druckaufträge auf Nicht-PostScript-Druckern, die direkt an den Windows NT Server angeschlossen sind, drucken. Für den Macintosh-Anwender erscheinen diese Drucker wie herkömmliche LaserWriter-Drucker.
- PC-Benutzer können Druckaufträge an PostScript-Drucker im AppleTalk-Netzwerk übertragen. Sie können auch den Status der Druckaufträge vom eigenen Arbeitsplatz aus überprüfen und abfragen.
- Macintosh- und PC-Druckaufträge werden zwischengespeichert, bevor sie zum Drucker weitergeleitet werden. Macintosh- und PC-Benutzer können somit Druckaufträge zum Drucker übertragen und mit der normalen Arbeit weitermachen, wenn die Übertragung beendet ist. Das heißt, es muß nicht bis zur endgültigen Ausgabe des Druckauftrags gewartet werden, um die Arbeit am PC oder Macintosh fortsetzen zu können.

Netzwerksicherheit

Unter Windows NT Server und Services for Macintosh wird die Netzwerksicherheit für Macintosh-Anwender genauso wie für PC-Benutzer realisiert. Services for Macintosh setzt die Benutzeridentifizierung, Authentifizierung und Berechtigungen so um, daß die Integrität des Servers, unabhängig von der verwendeten Workstation, erhalten bleibt.

Beim Einsatz von Services for Macintosh wird mit der gleichen Benutzerdatenbank gearbeitet, die Windows NT Server auch für die anderen Benutzerumgebungen benötigt und verwaltet. Auf einem Macintosh-Arbeitsplatz kann man sich somit mit einem bereits installierten Benutzerkonto anmelden, sofern man Name und Paßwort kennt. Sie müssen nur für neue Anwender für Macintosh-Rechner eigene Konten einrichten.

23 Windows NT Server

Das Macintosh-System kennt eine etwas andere Art der Berechtigung, als diejenige, die vom Windows NT Server zur Verfügung gestellt wird. Mit Hilfe von Services for Macintosh wird jedoch gewährleistet, daß eine korrekte Umsetzung der Berechtigungen erfolgt. Der Vollständigkeit halber sollen nachfolgend die hierfür geltenden Änderungen dargestellt werden, ohne daß darauf näher eingegangen würde, da dies wiederum mit den Berechtigungsmechanismen von AppleShare zusammenhängt.

In Macintosh-Systemen können für Directories die folgenden Berechtigungen vergeben werden:

Dateien sehen	Hiermit ist es einem Benutzer erlaubt, sich die Dateien im Directory (bei Macintosh spricht man von einem Ordner) anzeigen zu lassen und sie auch lesen zu dürfen.
Ordner sehen	Hiermit darf ein Benutzer im Ordner enthaltene weitere Ordner sehen.
Ändern	Damit ist es einem Benutzer erlaubt, den Inhalt der Dateien im Ordner zu ändern, Dateien umzubenennen oder zu verschieben, neue Dateien anzulegen und vorhandene Dateien zu löschen.
Bewegen, Umbenennen und Löschen unmöglich	Hiermit wird das Ausführen dieser Aktionen in einem Ordner nicht erlaubt. Ein Macintosh-Anwender kann diese Berechtigungen nicht mehreren Benutzern und Gruppen erteilen. Statt dessen können die Berechtigungen drei Kategorien (Vergleich mit Unix-Rechten) von Benutzern zugewiesen werden:
Eigentümer	Der Benutzer, der den Ordner angelegt hat, kann oben aufgeführte Rechte erhalten.
Mitbenutzer (Benutzer oder Gruppe)	Der hier aufgeführten Gruppe oder dem hier aufgeführten Benutzer können oben aufgeführte Rechte vergeben werden.
Jeder	In dieser Rubrik vergebene Rechte sind für alle Benutzer im Netzwerk gültig. Dies ist so, wie wenn Sie beim Windows NT Server Rechte für Everyone vergeben. Man sollte deshalb auch hier mit diesem Objekt sehr vorsichtig umgehen.

23.11 TCP/IP-Umgebung für Windows NT Server

TCP/IP zählt zu den am meisten eingesetzten Protokollen, wenn es darum geht, die Kommunikation in einem heterogenen Netzwerk zu ermöglichen. Normalerweise muß man sich dieses Protokoll als Zusatz für das jeweilige Betriebssystem separat beschaffen. Nicht so für Windows NT Server.

Sie haben damit eine Protokollwelt integriert, mit der es möglich ist, die Grundfunktionen in TCP/IP-basierenden Umgebungen durchzuführen. Zudem kann das Protokoll NetBIOS auch über dieses Protokoll abgehandelt werden. Zusätzlich zum TCP/IP ist auch ein SNMP Agent enthalten, um mit Hilfe von SNMP-basierenden Netzwerkmanagementsystemen Informationen des Windows NT Server abfragen zu können.

Beim Konfigurieren der TCP/IP-Umgebung sind alle Möglichkeiten enthalten, die man von allen bekannten TCP/IP-Produkten bereits kennt (inklusive die Festlegung von Domain Name Servern etc.).

Neben den wichtigsten und bekannten TCP/IP-Anwendungen, z. B. Ping-Befehl, Finger etc., ist auch ein FTP-Programm und FTP-Daemon enthalten; Sie finden die Befehle Rexec, Rsh und Telnet. Telnet dient dazu, über Terminalemulation zum Beispiel auf einer Unix-Maschine zu arbeiten. Nicht vergessen werden darf das einfache Datentransferprogramm Tftp. Ebenso müßten NFS-Dienste separat von einem Dritthersteller beschafft werden. Da die TCP/IP-Umgebung von Windows NT Server einige Besonderheiten aufweist, sollen diese nachfolgend erläutert werden.

IP-Adressierung

Eine IP-Adresse besteht immer aus 4 Byte und setzt sich aus einer Netzwerk-ID und einer Host-ID zusammen. Aus historischen Gründen haben sich für die IP-Adressen drei IP-Adreß-Klassen ergeben. Unterschieden werden müssen die Class-A-, Class-B- und Class-C-Adressen. Es gibt zwar auch noch die Class-D- und Class-E-Adressen, diese sind in der Praxis jedoch weniger von Bedeutung.

Wenn man die 4 Byte einer IP-Adresse näher betrachtet, stellt man fest, daß man bei den 4 Byte wissen muß, wie groß der Anteil der Netzwerk-ID ist und wie groß der Anteil der Host-ID. Wir gehen exemplarisch von folgender IP-Adresse aus:

aa.bb.cc.dd

23 Windows NT Server

Bei einer Class-A-Adresse werden das erste Byte für die Netzwerk-ID und die restlichen drei Byte für die Host-ID verwendet. In diesem Fall wird das Byte aa für die Netzwerk-ID verwendet, der Rest steht für die Adressierung der Hosts im Netzwerk zur Verfügung.

Wird eine Class-B-Adresse eingesetzt, dann sind bezogen auf unser Beispiel die Byte aa und bb für die Netzwerkadresse zu verwenden, wohingegen die Byte cc und dd für die Host-IDs verwendet werden.

Bei einer Class-C-Adresse werden die Byte aa, bb und cc für die Netzwerkadresse verwendet, und das Byte dd steht für die Host-IDs zur Verfügung.

In der Regel wird die Adresse wie folgt eingegeben:

153.10.134.19

Um jetzt zu wissen, was den Netzwerkanteil bildet und was den Hostanteil, wird eine Netmask angegeben. Für die Adresse 153.10.134.19 wäre dies die Netmask ff.ff.0.0. In Abhängigkeit der IP Class stehen folgende Adressen zur Verfügung:

Class	Von	Bis	Netz-ID	Host-ID
A	1	126	126	16.777.214
B	128	191	16.384	65.534
C	192	223	2.097.152	254

Die Netz-ID 127 ist standardmäßig für interne Mechanismen von TCP/IP reserviert und darf nicht verwendet werden.

Wenn unter IP ein Endgerät adressiert werden muß, ist es notwendig, die dafür vergebene IP-Adresse zu kennen. Da man sich in einem großen Netzwerk nie alle IP-Adressen vollständig merken kann, gibt es die Möglichkeit, statt herkömmlicher Adressen sprechende Namen zu verwenden. Hierfür wird ein Datei HOSTS angelegt, in die eingetragen wird, welchen Namen eine IP-Adresse erhalten soll. Der Inhalt der HOSTS-Tabelle kann wie folgt aussehen:

```
152.100.12.10    zenka    andreaszenk
152.100.12.11    zenkr    rosemariezenk
```

Ab diesem Zeitpunkt kann das Endgerät direkt über den definierten Namen angesprochen werden. Zu beachten ist dabei, daß jeder IP-Host eine eigene Host-Tabelle hat und somit für jede IP-Adresse ein anderer Name verwendet werden könnte. Wenn man diese Unordnung zulassen würde, hätte man das Problem, daß auf jedem IP-Host ein und dasselbe Endgerät einen anderen Namen haben würde.

23.11 TCP/IP-Umgebung für Windows NT Server

In der Regel muß für einen IP-Host die IP-Adresse einzeln konfiguriert werden. Ebenso müßte die HOSTS-Tabelle einzeln gepflegt werden. Um das zu vereinfachen, bietet Microsoft einen separaten DNS-Server an, mit dem es möglich ist, die Zuordnung von Namen und IP-Adressen im Netzwerk zu zentralisieren. Damit man sich um die Konfiguration der IP-Adressen nicht mehr kümmern muß, steht ein DHCP-Mechanismus (Dynamic Host Configuration Protocol) zur Verfügung, der die zentrale Vergabe der IP-Adressen im Netzwerk durchführt. Die Vorgängervariante von DHCP war der sogenannte BOOTP-Server. Da Windows NT beim Auffinden von Servern, d.h. für den Anmeldevorgang, einen NetBIOS Broadcast verwendet, hat man schlechte Karten, wenn Netzwerke über Router gekoppelt sind. Wie Sie inzwischen wissen, transportieren Router keinen Broadcast. Auf DHCP und WINS soll in den folgenden Abschnitten näher eingegangen werden.

Vor diesen Ausführungen noch einige Worte zum Routing unter Windows NT Server: In einen Windows NT Server können mehrere Netzwerkkarten eingebaut werden, um über einen NT Server mehrere Netzwerke koppeln zu können. Beim Einsatz von TCP/IP ist der NT Server selbst nicht in der Lage, ein dynamisches Routing durchzuführen. Daher ist es notwendig, dem NT Server statische Routing-Tabellen zu definieren. Solange das nicht geschehen ist, weiß der NT Server nicht, wohin Datenpakete für andere Netzwerke zu transportieren sind. Microsoft sollte an dieser Stelle noch etwas tun, um das Arbeiten des IP-Routers dynamisch zu realisieren.

DHCP

Die dynamische Konfiguration der IP-Adressen erleichtert einem Netzwerkverwalter das Arbeiten im Netzwerk, da die IP-Endgeräte nicht mehr manuell konfiguriert werden müssen. Bevor DHCP eingesetzt werden kann, muß dieser Dienst zuerst auf dem NT Server installiert werden. Nach der Installation von DHCP muß die Umgebung konfiguriert werden. Zu den Konfigurationen zählen die Angabe des IP-Adreßbereichs und die dazugehörige Netmask. Auf diese Weise kann genau festgelegt werden, welche IP-Adressen verfügbar sind und vergeben werden dürfen.

Damit der IP Client die IP-Adresse erhält, muß ihm nur noch der DHCP Server eingetragen werden. Nachdem dem Client die IP-Adresse zugewiesen worden ist, erfolgt ein Eintrag beim DHCP Server, welcher MAC-Adresse die IP-Adresse gegeben worden ist. Somit ist gewährleistet, daß der IP Client immer die gleiche IP-Adresse erhält und keine Doppelbelegung auftritt. Wenn die IP-Adresse für den Client vergeben ist, erfolgt beim nächsten Start der Workstation am

23 Windows NT Server

DHCP Server die Prüfung, ob für die MAC-Adresse bereits ein IP-Eintrag existiert. Ist die Antwort positiv, wird die eingetragene IP-Adresse verwendet, ansonsten teilt DHCP dem Client eine neue IP-Adresse zu.

WINS

Jedem Windows NT Server und jeder Windows NT Workstation wird bei der Installation ein eindeutiger Name zugewiesen. Beim Arbeiten auf der Workstation oder auf dem Windows NT Server wird mit diesen vergebenen Namen gearbeitet. Das Namenssystem von Microsoft-Netzwerken basiert somit auf NetBIOS-Namen. Solange sich im Netzwerk keine Router befinden, funktioniert dieses Verfahren sehr gut. Eine wesentliche Einschränkung der NetBIOS-Namensauflösung in einer TCP/IP-Umgebung besteht darin, daß die Auflösungsanforderung, die über einen Broadcast erfolgt, nicht über Router transportiert wird. Das bedeutet, daß Windows NT Server, die hinter einem IP Router liegen, nicht gesehen werden können. Zur Lösung dieses Problems kann man jede NT Workstation mit einer LMHOSTS-Tabelle ausstatten. In dieser Tabelle werden NetBIOS-Namen der Windows NT Server (auch Windows NT Workstation) und die dazugehörigen IP-Adressen eingetragen. Dieses Verfahren ist ähnlich der Host-Tabelle für das normale TCP/IP.

Da es sich hierbei wieder um separate Konfigurationen pro Workstation und auch pro NT Server handelt, empfiehlt sich dieser Vorgang vor allem in einem großen Netzwerk nicht. Die bessere Alternative hierzu ist der Einsatz eines WINS Server.

Der WINS Server (Windows Internet Name Service Server) pflegt eine zentrale Tabelle, mit der die Auflösung von NetBIOS-Name und IP-Adresse durchgeführt wird, damit der Client in der Lage ist, das Zielsystem zu adressieren. Die einzige Voraussetzung nach dem Installieren der WINS-Dienste ist, auf dem Client die Eintragung durchzuführen, welcher WINS Server verwendet werden soll. Aus Sicherheitsgründen kann man einen primären und einen sekundären Server definieren. Wenn im Netzwerk IP Clients verwendet werden, die es nicht ermöglichen, bei der IP-Konfiguration einen WINS Server einzutragen, muß in diesem Segment ein WINS Proxy installiert werden. Dieser WINS Proxy hat die Aufgabe, die NetBIOS-Namensauflösung über den WINS Server durchzuführen – für alle Clients in diesem Segment, die keinen eigenen WINS-Eintrag haben können.

Es sei an dieser Stelle darauf hingewiesen, daß die Konfiguration von TCP/IP, DHCP, WINS und DNS nicht ganz unproblematisch ist. Alle Konfigurationen müssen im Rahmen einer Gesamtplanung de-

23.12 NetWare-Einbindung

finiert und festgelegt werden. Hierzu zählt auch die Festlegung notwendiger Namenskonventionen, so daß sprechende NetBIOS-Namen und auch für TCP/IP entsprechende Namen verwendet werden.

Nach diesen Ausführungen über die TCP/IP-Problematik in einem Windows-NT-Server-Netzwerk sollen Sie zum Abschluß noch einen Überblick darüber erhalten, wie Windows NT und Windows NT Server in eine NetWare-Umgebung eingebunden werden können.

23.12 NetWare-Einbindung

Für Windows NT Server und somit auch für Windows NT bietet sowohl Novell als auch Microsoft selbst Treibersoftware an, mit denen diese Systeme als Clients in eine NetWare-Umgebung integriert werden können. Mit beiden Produkten ist es im ersten Ansatz möglich, die Verbindung zum NetWare Server aufzubauen, einen Login durchzuführen und auf Dateien zuzugreifen, für die man entsprechende Rechte erhalten hat. Es ist auch möglich, mit den Menüsystemen unter NetWare zu arbeiten, um die Administration von NetWare auch von einer NT Workstation aus durchführen zu können. Alle angebotenen Produkte sind für NetWare 3.x und NetWare 4 optimal einzusetzen. Für NetWare 4 sind die entsprechenden Treiber inzwischen auch in der Lage, die NDS-Funktion zu unterstützen. Zu beachten ist noch, daß ein Windows NT Server selbst nicht mit einer Client-Software ausgestattet werden kann, sondern die Anbindung immer über das NetWare Gateway realisiert werden muß. In diesem Fall baut der NT Server eine Verbindung zum NetWare Server auf, und alle Clients im NT-Netzwerk können über die Verbindung auf den NetWare Server zugreifen.

Sie haben jetzt einen ausführlichen Überblick über Windows NT Server erhalten. Sowohl für Windows NT als auch für Windows NT Server sind die Anforderungen an die Hardware, die ein leistungsfähiges System sicherstellen, noch ziemlich groß. Dies betrifft vor allem den Hauptspeicherausbau. Ein NT-Arbeitsplatz unter 16 Mbyte Hauptspeicher und einem 486-Rechner mit 33 MHz ist nicht zu empfehlen. Für den Windows NT Server sollten Sie durchaus die doppelte Hauptspeicherkapazität einbauen und einen 586-Rechner mit 90 MHz installieren. Nur so kann gewährleistet werden, daß ein Arbeiten mit diesem System auch Spaß macht. In allen anderen Fällen sind die Wartezeiten beim Starten des Systems und vor allem beim Ausführen von Anwendungen viel zu lange.

Im großen und ganzen kann gesagt werden, daß mit Windows NT Server ein leistungsfähiges Netzwerkbetriebssystem zur Verfügung

23 Windows NT Server

steht. Mit Einführung von Windows NT 4 und Windows NT Server 4 wird das Arbeiten, Konfigurieren und Verwalten von Windows NT nochmals erleichtert. Zur Abrundung der Windows-NT-Server-Umgebung fehlt jetzt nur noch die Implementierung der Directory Services. Bis jetzt ist nur bekannt, daß man an einer entsprechenden Version arbeitet, aber es ist kein genauer Auslieferungstermin angegeben. Solange sich der Anwender mit der dann doch aufwendigeren Domain-Struktur zufriedengibt, kann auch das mit entsprechender Zeitverzögerung erfolgen, ohne daß allzu großer Druck gemacht werden muß. Microsoft sollte mit etwas mehr Engagement an den Directory Services arbeiten und vor allem auch darauf achten, daß die Zusammenarbeit mit NetWare 4 problemlos realisiert werden kann. Es wäre unschön, wenn es wieder eine eigene Variante von Directory Services geben würde. Die damit verbundenen Schwierigkeiten kennt man aus den Produktentwicklungen der Vergangenheit zu gut.

Es sei nochmals darauf hingewiesen, daß die Strategie von Microsoft »Windows« heißt.

24

Windows 2000

Auf die Auslieferung von Windows 2000 wird schon seit längerem gewartet. Allerdings wurde von Microsoft der Auslieferungstermin immer wieder verschoben, Angaben über genaue Gründe fehlen jedoch. Zum Zeitpunkt der Entstehung dieses Buches gab es unterschiedliche Betaversionen. Vom Erfolg dieser Betaversionen hängt der genaue Auslieferungstermin von Windows 2000 ab. Über diese neue Version von Microsoft wurde zwar schon viel geschrieben, jedoch sollte man einige Aspekte detailliert betrachten: Es sind nicht nur Vorteile zu erkennen. An der einen oder anderen Stelle gibt es auch kleine Haken, die man in dieser Form von einer neuen Betriebssystem-Version nicht erwartet hätte.

Es ist inzwischen hinreichend bekannt, daß mit Windows NT 4.0 die Verwaltung von Multi-Server-Netzwerken äußerst aufwendig wird. Dies liegt unter anderem an der flachen Verwaltungsstruktur, die dem Domänen-Konzept bzw. -Prinzip zugrunde liegt. Alle Verwaltungseinheiten (Benutzer, Lokale und Globale Gruppen) werden in einem »Topf« verwaltet. Je größer die Anzahl der Benutzer- und/oder Gruppen-Konten ist, die man über eine Domäne verwalten muß, desto unübersichtlicher wird das Ganze. Um sich von einer solchen »flachen« Struktur zu lösen, hat Microsoft das Konzept der Vertrauensstellungen eingeführt. Auf diese Art und Weise können unterschiedliche Domänenmodelle eingeführt werden, auf die ich bereits eingegangen bin. Aber auch hier stellt man fest, daß man sehr schnell die Übersicht verlieren kann und der Verwaltungsaufwand schnell und stetig wachsen wird. Das notwendige Einrichten der Vertrauensstellungen tut hier ein übriges. Ebenso ist es mit den Domänenmodellen nicht ohne weiteres möglich, Subadministratoren einzurichten, es sei denn, man richtet in jedem Sub-Admin-Bereich eigene Domänen mit eigenen Administratoren ein. Innerhalb einer Domäne kann man zwar einen Account Operator einrichten, dieser ist dann jedoch in der Lage, die gesamten Benutzer-Konten in der Domäne zu verwalten. Für alle anderen Operator-Funktionen verhält es sich genauso, d.h., die Flexibilität von Windows NT 4.0 läßt an der einen oder anderen Stelle durchaus zu wünschen übrig, da die administrativen Möglichkeiten zum Teil sehr eingeschränkt sind. Ein noch höherer Aufwand entsteht, wenn Vertrauensstellungen zwischen Domänen eingerichtet und gepflegt werden müssen. Beachtet werden muß dabei, daß Vertrauensstellungen immer zwischen zwei Domänen eingerichtet werden müssen und keine transitiven Beziehungen unterstützt werden. Wenn also die Domäne A der Domäne B

vertraut und B wiederum der Domäne C vertraut, dann bedeutet dies unter Windows NT 4.0 nicht, daß die Domäne A auch der Domäne C vertraut. Dies ist auch der Grund, warum mit diesem Domänenmodell immer nur zwei Ebenen-Modelle aufgebaut werden können. Ein weiteres Handicap für eine flexible Verwaltung ist die Tatsache, daß man für Windows NT 4.0 eine Vielzahl unterschiedlicher Menüs benötigt, um die Verwaltung durchführen zu können.

All dies soll mit Windows 2000 Server wesentlich einfacher, übersichtlicher und besser werden. Windows 2000 wird mit einer großen Anzahl Neuerungen ausgestattet werden, die sich jedoch nicht nur auf die Verwaltung auswirken, sondern auch auf die Sicherheit von Windows 2000 und das gesamte Umfeld.

Alle in diesem Kapitel aufgeführten Informationen wurden aufgrund der Beta-Version von Windows 2000 und den im Internet zur Verfügung gestellten Informationen ermittelt. Es ist also durchaus möglich, ja sogar ziemlich sicher, daß sich im Final-Release von Windows 2000 Änderungen ergeben werden. Ich möchte deshalb in den nachfolgenden Ausführungen die bislang ermittelten Produkteigenschaften von Windows 2000 kurz beschreiben und anschließend auf ein paar wichtige Funktionen näher eingehen (z.B. Active Directory).

Windows 2000 wird eine Vielzahl neuer und wichtiger Funktionen enthalten, die es zu einem leistungsstarken Betriebssystem für Workstation und Server macht. Die erweiterten Funktionen von Active Directory, Dynamic DNS, Microsoft Management Console sowie zahlreiche andere Funktionen stellen ein hervorragendes Toolkit für die Entwicklung und Verwendung verteilter Anwendungen zur Verfügung.

24.1 Windows 2000 Management

Es wurde in den einleitenden Ausführungen bereits darauf hingewiesen, daß Windows NT 4.0 in einer Multi-Server Umgebung sehr umständlich und aufwendig verwaltet werden muß. Da es inzwischen das kurzfristige Ziel ist, die Verwaltung so wenig aufwendig wie möglich zu machen, ist für Windows 2000 eine Vielzahl neuer Komponenten eingeführt worden, die ich nachfolgend näher beschreiben will.

24.1.1 Active Directory

Das meist diskutierte System für Windows 2000 ist das Konzept der Active Directories, ein vollständig neuer Aspekt für die Verwaltung der Ressourcen unter Windows 2000 – ein Ersatz für das bisherige Domänen-Konstrukt. Active Directory stellt den neuen Verzeichnisdienst für Windows 2000 dar. Die Directory Services liegen in ähnlicher Form vor, wie sie im X.500-Standard definiert sind. In den Active Directories werden alle Informationen über die Objekte (Ressourcen) im Netzwerk gespeichert. Administratoren, Entwickler und Anwender können auf die gesamten Informationen relativ problemlos zugreifen und damit arbeiten. Active Directory stellt einfache, einheitliche und offene Schnittstellen zur Verfügung, mit deren Hilfe häufig ausgeführte Verwaltungsaufgaben wie z.B. das Hinzufügen neuer Benutzer, das Verwalten von Druckern und das Suchen nach Ressourcen in einer verteilten Computerumgebung ausgeführt werden können. Zudem wird es dadurch für Entwickler einfacher, ihre Anwendungen in einen Verzeichnisdienst einzubinden, um auf alle diese Informationen zugreifen zu können. Die Entwickler arbeiten mit einem Set »Schnittstellen für Verzeichnisdienst-Programme« unabhängig von den installierten Verzeichnisdienst-Programmen.

Active Directory ist ein Verzeichnisdienst mit den folgenden Funktionen:

- Flexible hierarchische Struktur
- Effiziente Multimaster-Replikation
- Differenzierte Sicherheitsverteilung
- Programmierschnittstellen der höchsten Ebene, auf die mit jeder Sprache zugegriffen werden kann (Active Directory Services Interfaces – ADSI)
- Erweiterbares Schema für neue Objekte und Eigenschaften von Objekten
- LDAP-3-Unterstützung, für den Zugriff auf Active-Directory-Informationen
- Integrierter Dynamic-DNS-Server
- Unterstützung von COM/DCOM- und Java-Klassen

24.1.2 Erweiterte Suchfunktionen

Mit Hilfe der Active-Directory-Funktionen ist es wesentlich einfacher, Benutzer, Dateien oder auch Drucker im Netzwerk zu finden. So gibt es zum Beispiel im »Start-Fenster« die Option Suchen, mit der wiederum »In the Directory...« ausgewählt werden kann. Man muß dann eingeben, welchen Objekttyp man sucht und welchen Namen das Objekt hat, nach dem gesucht werden soll. Auffallend ist dabei, daß

die auswählbaren Objekte nicht erweiterbar sind, d.h., falls die Active-Directory-Struktur um Objekte erweitert worden ist, wird die Suchfunktion nicht automatisch um diese neuen Objektklassen erweitert.

24.1.3 Dynamic DNS

Windows NT 4.0 benötigt bislang den Einsatz von WINS-Diensten, um in einem Netzwerk mit Routern die IP-Adresse eines Servers oder einer Workstation ausfindig machen zu können. Dies liegt daran, daß Windows NT 4.0 immer noch NetBIOS Broadcast verwendet, um den Namen eines Endgeräts in eine entsprechende Adresse auflösen zu können. Da es sich hierbei um Broadcasts handelt, die nicht über Router transportiert werden, hat Microsoft den WINS-Dienst eingeführt, der sich dieser Problematik annimmt. Windows 2000 hingegen wird Native-IP unterstützen und WINS nur noch in einer gemischten NT 4.0/NT 5.0-Umgebung nutzen. In einer reinen Windows-NT-5.0-Umgebung arbeitet NT ohne NetBIOS-Mechanismen und nutzt für die Kommunikation zwischen Client und Server bzw. Server und Server herkömmliche IP-Mechanismen, so wie dies für NetWare 5 auch der Fall ist. Wie später noch zu sehen sein wird, ist der wesentliche Kommunikationsmechanismus für Active Directory DNS, so wie man dies bereits aus der Internet bzw. Intranet-Technologie kennt.

Der Microsoft Domain Name Server (DNS) bietet die Funktion, dynamische Updates für DNS durchzuführen, um von anderen Netzwerkdiensten wie z.B. Active Directory, Dynamic Host Configuration Protocol (DHCP) und Microsoft Windows Internet Naming Service (WINS) die notwendigen Informationen automatisch eintragen zu können. Auf diese Art und Weise erhält man eine flexible und robuste Lösung für die Registrierung und das Auffinden von Ressourcen im Netzwerk. Dynamic DNS (DDNS) senkt dadurch die Verwaltungskosten für Netzwerke erheblich, da es nur noch in den seltensten Fällen notwendig ist, die DNS-Datenbank – außer wenn die Konfiguration eines DNS-Clients geändert wird – manuell zu bearbeiten. Damit sinkt auch das Risiko von Fehlern, die sich bei einer manuellen Konfiguration einschleichen können.

24.1.4 Speicherverwaltung

Die Speicherverwaltung von Windows 2000 wurde soweit verbessert, daß ein Netzwerkverwalter Online-Aufgaben durchführen kann, ohne das System abschalten oder die Arbeit von Benutzern unterbrechen zu müssen (um z.B. ein Laufwerk zu erstellen, zu er-

24.1 Windows 2000 Management

weitere oder zu duplizieren). Zudem können Netzwerkverwalter Daten auf einer Vielzahl magnetischer oder optischer Speichermedien sichern. Verwaltungsaufgaben, wie das Einrichten oder das Entfernen von Medien- oder Laufwerksfunktionen, werden bei Windows 2000 von einem Dienstprogramm NTMS (Windows NT Media Service) ausgeführt. Dieses Dienstprogramm stellt eine Schnittstelle für automatische (robotergesteuerte) Medienwechsler und Medienbibliotheken zur Verfügung; es ermöglicht mehreren Anwendungen den gleichzeitigen Zugriff auf lokale Bibliotheken sowie Band- oder Diskettenlaufwerke und steuert entfernbare Medien innerhalb eines Einzel-Server-Systems. Zu der besseren Speicherverwaltung gehört auch eine erweiterte Version von NTFS; darauf hat man schon lange gewartet. So ist es mit dem neuen NTFS möglich, Plattenkapazitäten (Disk Quotas) pro Benutzer zu definieren. Somit kann man den Speicherplatz einfacher kontrollieren und begrenzen. Zudem soll das neue NTFS auch noch eine Dateiverschlüsselung zur Verfügung stellen.

24.1.5 Ordner »Eigene Dateien«

Der Ordner »Eigene Dateien« ist ein benutzerspezifischer Arbeitsbereich, der hinzugefügt worden ist, um Benutzer beim Verwalten und Speichern eigener Dateien zu unterstützen. Dieses Verzeichnis ist der Standardspeicherplatz für vom Benutzer erstellte Dokumente.

24.1.6 Backup-Dienstprogramm

Es ist inzwischen hinreichend bekannt, daß Server in regelmäßigen Abständen gesichert werden müssen, um unbeabsichtigten Verlust aufgrund von fehlerhafter Hardware oder defekten Speichermedien zu vermeiden. Im Gegensatz zu vorherigen Versionen von Windows NT Backup, bei denen der Benutzer Daten nur auf Bandlaufwerke sichern konnten, erlaubt die in Windows 2000 enthaltene Backup-Version das Sichern auf einer Vielzahl von Speichermedien, wie Bandlaufwerken, externen Festplattenlaufwerken, Zip-Laufwerken, beschreibbaren CD-ROMs und logischen Laufwerken.

24.1.7 Unterstützung des Distributed File System (DFS)

Das Microsoft Distributed File System (DFS) für Windows NT Server 5.0 ist eine Netzwerk-Server-Komponente, durch die es den Benutzern im Netzwerk erleichtert wird, Daten zu finden und zu verwalten. Mit Hilfe von DFS können Benutzer eine einzelne Verzeichnisstruktur erstellen, die mehrere File-Server und freigegebene Dateien einer Gruppe, Abteilung oder eines Unternehmens umfaßt. Außer-

dem stellt DFS dem Benutzer ein einzelnes Verzeichnis zur Verfügung, das sich über eine Vielzahl von File-Servern und Freigaben erstrecken kann. Auf diese Art und Weise wird die Suche nach benötigten Daten und Dateien im Netzwerk sehr stark vereinfacht. Das Durchsuchen von DFS-Verzeichnissen ist deshalb so einfach, weil den DFS-Unterverzeichnissen logische und beschreibende Namen zugeordnet werden können, wobei sie vollkommen unabhängig vom tatsächlichen Namen des File-Servers bzw. der Freigabe sind. Die einzige Schwierigkeit dürfte sein, sich zu merken, welchem DFS-Verzeichnis welche anderen Verzeichnisse von welchem Server zugewiesen worden sind. Auch dieser Verwaltungsmechanismus erfordert äußerste Disziplin, wenn man sich damit keine Nachteile einhandeln möchte.

24.1.8 **Microsoft Management Console (MMC)**

Die Microsoft Management Console stellt Systemverwaltern eine Verwaltungskonsolle zur Verfügung, mit deren Hilfe man in der Lage ist, sich Netzwerkfunktionen anzeigen zu lassen oder Tools zu nutzen, die man für die gesamte Verwaltung des Netzwerkes und seiner Umgebung benötigt. MMC zeigt Consolen an, die als Host für Programme (den sogenannten Snap-in-Modulen) fungieren, welche die Funktionen für die Verwaltung von Netzwerken bieten. Abgesehen von der Integration und gemeinsamen Nutzbarkeit der Verwaltungsprogramme können Konsolen darüber hinaus mit Hilfe von MMC benutzerdefiniert werden, so daß es dem Netzwerkverwalter möglich ist, Management Consolen zu erstellen, die nur die gewünschten und benötigten Verwaltungsprogramme enthalten. Es ist somit möglich, daß man für Subadministratoren entsprechend »abgemagerte« Verwaltungsprogramme einrichtet und definiert. Durch diese benutzerdefinierten Konfigurationen wird die Verwaltung zunehmend aufgabenbezogen, da die Verwaltungswerkzeuge dann den auszuführenden Aufgaben entsprechen.

24.1.9 **Hardware-Assistent mit Gerätemanager**

Der Hardware-Assistent umfaßt die wahrscheinlich am häufigsten verwendeten hardwarebezogenen Werkzeuge und funktioniert als einzelner Assistent. Dadurch wird der Gerätemanager nicht nur einfacher, sondern auch schneller. Die Aufgaben für den Gerätemanager bestehen unter anderem im Hinzufügen neuer Hardware, Ändern von Geräteeigenschaften, Entfernen von Geräten und in der Behebung von Hardware-Konflikten. Es bleibt einem aber nicht erspart, sich dennoch etwas mit Hardware und Hardware-Einstellungen auszukennen.

24.1.10 Windows Scripting Host (WSH)

Windows 2000 unterstützt die Ausführung von Skripten entweder direkt von der Benutzeroberfläche aus oder als Befehlszeile. Unter einem Skript versteht man dabei eine Reihe von Befehlen, die automatisch ausgeführt werden sollen. Diese hilfreichen Funktionen werden unter Windows 2000 von einem Windows Scripting Host (WSH) zur Verfügung gestellt. Auf diese Art und Weise wird es ermöglicht, daß man Aktionen, die man sonst über die Benutzeroberfläche ausführen müßte, in eine Skript-Datei überträgt. Hierzu gehören unter anderem das Erstellen von Verknüpfungen, das Verbinden und Trennen von Servern im Netzwerk oder auch das Umleiten von Druckern. Damit der WSH flexibel genug wird, stehen die folgenden Unterstützungsmerkmale zur Verfügung: integrierte Unterstützung von MS-Visual-Basic-Skripten, Unterstützung von Java-Skripten, MS ActiveX und Skriptmodule für Perl, PCL, REXX und Python.

24.1.11 Win32 Driver Model (WDM)

Es soll für Windows 2000 und Windows 98 ein neues Treibermodell verwendet werden, das sogenannte Microsoft Win32-API Driver Model, ein vereinheitlichtes Treibermodell für beide Betriebssystemwelten. Auf diese Art und Weise soll es möglich sein, daß man für ein neues »Gerät« unter Windows NT und/oder Windows 98 nur einen Treiber schreiben muß. Windows 2000 soll aber nach wie vor die vorhandenen Treiber für Windows NT unterstützen. Das Final Release wird zeigen, ob diese Aussage stimmt.

24.1.12 Plug&Play

Windows 2000 unterstützt nun auch Plug&Play, wodurch die Installation neuer Hardware-Komponenten erleichtert werden soll – hoffentlich. Man kennt die Schwächen unter Windows 95/98 zur Genüge, so daß man ab und zu gezwungen ist, die Plug&Play-Funktion der einzubauenden Hardware abzuschalten, da es andernfalls Konflikte mit anderer Plug&Play-Hardware gibt – alles das kann noch verbessert werden. Zur Plug&Play-Unterstützung von Windows 2000 gehören in diesem Zusammenhang auch der neue Hardware-Assistent, der neue Geräte-Manager und die lang erwartete, verbesserte Unterstützung für Laptops bzw. Notebooks.

24.2 Entwickeln und Verwenden von Anwendungen

Es stellt sich bei der Einführung eines neuen Betriebssystems (Workstation und Server) berechtigterweise die Frage, wie es mit der Unterstützung von Anwendungen aussieht und welche Anwendungen standardmäßig oder als Add-on von Microsoft angeboten werden. Die nächsten Ausführungen sollen zeigen, wie sich die Situation diesbezüglich bei Windows 2000 darstellt.

24.2.1 DCOM

Distributed COM (DCOM) ist eine Erweiterung der bereits bekannten COM-Umgebung (Component Object Model), welche die Datenübertragung zwischen Objekten auf unterschiedlichen Computern unterstützt, so daß Anwendungen gemäß den optimalen Anforderungen verteilt werden können. Die notwendige Datenübertragung kann damit zwischen Computern im LAN, in einem WAN oder sogar im Internet durchgeführt werden. Mit Hilfe von DCOM kann ohne größeren Aufwand eine verteilte Anwendung geschrieben werden, ganz gleich ob es sich um eine Umgebung mit einem Computer oder einen größeren Verbund mit einer Vielzahl von Netzwerk-Servern handelt. Die Bandbreite des Netzwerks wird dabei nicht zu stark beansprucht, und dennoch hat der Anwender sehr schnelle Reaktionszeiten.

24.2.2 Microsoft Transaction Server

Der Microsoft Transaction Server ist ein komponentenbasierendes Dienstprogramm, mit dem sich skalierbare und einfach zu verwaltende Transaktionsanwendungen erstellen lassen. Der Transaction Server stellt einfache Grundbausteine zur Verfügung, die komplexe Transaktionen über weit gestreute, verteilte Netzwerke zuverlässig und effizient ausführen.

24.2.3 Microsoft Message Queue Server

Der Message Queue Server ist ein Dienstprogramm, das es ermöglicht, problemlos Nachrichten zwischen Anwendungen zu übertragen, die auf mehreren Computern in einem Netzwerk ausgeführt werden. Der Message Queue Server ist deshalb eine ideale Umgebung für das Erstellen von umfangreichen verteilten Anwendungen, die mobile Systeme umfassen. Die Warteschlangen werden durch intelligentes Weiterleiten, automatisches Festlegen der Prioritäten, einfache Verwaltung und leistungsstarke Nachrichtenraten unterstützt.

24.2.4 Internet Information Server

Der Internet Information Server (IIS), der sehr eng mit dem Windows NT Server 5.0 verbunden ist, stellt transaktionsbasierende Web-Serverdienste und vollständige FTP- und Gopher-Programme zur Verfügung.

24.2.5 Index Server

Durch den Microsoft Index Server wird das Durchsuchen der Web-Server inklusive der firmeneigenen Intranet- und Internet-Seiten ermöglicht, indem ein Index des Web-Servers erzeugt wird und dieser Index dann von jedem Web-Browser aus mit Hilfe einfacher Abfrageformulare durchsucht werden kann.

24.2.6 Automatische Installation von Anwendungen

Die einfache Verwaltung von Anwendungen in einem Netzwerk wird immer wichtiger und vor allem auch immer mehr gefordert. Microsoft hat hierfür auch den Begriff ZAK (Zero Administration Kit) geprägt und eingeführt. Mit Hilfe der automatischen Installation von Anwendungen kann ein Netzwerkverwalter eine Reihe von Anwendungen definieren, die anschließend den Benutzern oder einer Gruppe von Benutzern ständig zur Verfügung gestellt werden. Ist eine festgelegte Anwendung für den Benutzer auf der Workstation nicht verfügbar, dann wird diese auf dem System ohne das Zutun des Anwenders automatisch installiert. Das neue, auf Windows NT Server 5.0 basierende Programm zur Installation von Anwendungen spielt bei dem Vorhaben von Microsoft »Zero Administration für Windows« eine zentrale Rolle:

- Es werden standardisierte Paketformate und Installationsprogramme verwendet, die für das Installieren, Reparieren, Entfernen und Suchen von abhängigen Komponenten verwendet werden.
- Die Flexibilität ist so groß, daß es ermöglicht wird, Produkte zu reparieren, einen Rollback für Transaktionen durchzuführen und redundante Installationspunkte zu verwenden, um damit Anwendungen lange erhalten zu können.
- Es werden sogenannte Just-in-Time-(JIT)-Installationen eingesetzt, bei denen die Anwendungen angewiesen werden können, Komponenten bei Bedarf zu installieren.
- Unterstützung von Mechanismen, um die Installation von Anwendungen zu ermöglichen. Auch dann, wenn der angemeldete Benutzer nicht das Recht dazu hat, die Installation auszuführen, muß man dem Benutzer deswegen noch keine Administrationsrechte geben, da die Installationsmechanismen diese Aufgaben übernehmen.

24.3 Skalierbarkeit und Verfügbarkeit

Wie aus allen bisherigen Ausführungen zu erkennen ist, wird bei den Netzwerkbetriebssystemen sehr viel Wert auf Skalierbarkeit und Verfügbarkeit gelegt. Die nachfolgenden Ausführungen sollen zeigen, welche Verbesserungen hierfür bei Windows 2000 zur Verfügung gestellt werden.

24.3.1 64-Bit-VLM

Windows NT Server 5.0 bietet Unterstützung für den Zugriff auf einen maximal 32 Gbyte großen Speicher auf 64-Bit-Prozessoren. Durch die 64-Bit-Adressierung von Prozessoren, wie diese von Digital Alpha und dem zukünftigen Intel Merced unterstützt wird, können Anwendungen, die Transaktionsvorgänge oder Entscheidungsunterstützung für große Datenmengen ausführen, mehr Daten im Speicher halten, wodurch sich eine erhöhte Leistungssteigerung ergibt. Bei der bisherigen 32-Bit-Adressierung wird lediglich ein Zugriff auf 4 Gbyte Speicher ermöglicht.

24.3.2 Microsoft Cluster Server

Mit Hilfe der Microsoft-Cluster-Server-Technologie können zwei Server zu einem Cluster zusammengefaßt werden. Auf diese Art und Weise werden eine höhere Verfügbarkeit und ein einfacheres Verwalten der Server-Ressourcen erzielt. Der Cluster Server protokolliert den Status der Standardanwendungen und -Server und kann wichtige Daten und Anwendungen bei vielen gängigen Fehlertypen in der Regel in weniger als einer Minute automatisch wiederherstellen. Der Cluster Server wird zudem dafür eingesetzt, um ein Load Balancing durchzuführen, d.h., die Aufgaben auf den beiden Cluster Servern zu verteilen. Dies kann automatisch oder auch manuell erfolgen. Durch das Load Balancing bzw. das Verschieben von Arbeitsaufgaben ist man auch in der Lage, einen Server für Wartungszwecke abzuschalten, ohne dabei Datenverluste hinnehmen oder auf die Ausführung von Aufgaben verzichten zu müssen, da der andere Server im Cluster diese Aufgaben übernehmen kann.

24.3.3 Intelligent Input/Output System

Die I/O-Architektur verwendet einen dedizierten Prozessor mit einem eigenen Speicher, um die notwendigen I/O-Vorgänge durchführen zu können. Dadurch wird die CPU von den I/O-Vorgängen entlastet, wodurch zwei Effekte erzielt werden: Die CPU ist weniger belastet, so daß andere Aufgaben noch besser erledigt werden können, und der Datendurchsatz wird wesentlich höher.

24.3.4 Kerberos-Authentifizierung

Windows NT 4.0 hat sich hinsichtlich seines Sicherheitsmechanismus nicht unbedingt von seiner besten Seite gezeigt; das zeigen nicht zuletzt die einzelnen Service Packs zur Schließung von Fehlerlücken. Deshalb hat Microsoft für den gesamten Sicherheitsmechanismus neue Verfahren eingeführt. Durch die vollständige Unterstützung des Sicherheitsprotokolls Kerberos in der Version 5 ist eine schnelle, einmalige Anmeldung für den Zugriff auf firmenweite Ressourcen möglich. Es spielt dabei keine Rolle, ob sich die Ressourcen auch tatsächlich auf dem Windows 2000 Server befinden oder in einer anderen Umgebung, in der ebenfalls das Kerberos-Protokoll unterstützt wird.

24.3.5 Certificate Server für öffentliche Schlüssel

Der auf dem X.509-Standard basierende Certificate Server für öffentliche Schlüssel sowie die Integration in die Active-Directory-Struktur ermöglichen das Verwenden von Zertifikaten mit öffentlichen Schlüsseln für die Authentifizierung.

24.4 Weitere Funktionen für Windows NT

Ohne weitschweifige Ausführungen sollen in diesem Abschnitt Funktionen von Windows NT Workstation und Windows NT Server erläutert werden, die zum größten Teil selbsterklärend sind, aber dennoch zeigen, mit welchen weiteren Änderungen man rechnen muß bzw. kann, sobald diese neue Version zur Verfügung steht.

- Auf dem Active Desktop kann eine beliebige Web-Seite oder ein HTML-Dokument als Hintergrund geladen werden.
- Es kann eine bevorzugte Web-Seite festgelegt werden, die dann automatisch und in regelmäßigen Abständen aktualisiert wird.
- Wer den Active Desktop vom Internet Explorer 4.x (IE) kennt, weiß auch, daß für fast alle Desktop-Mechanismen Funktionen eingebaut worden sind, die man vom IE bereits kennt.
- Der Active Desktop kann problemlos an die jeweiligen Bedürfnisse angepaßt werden.
- Programme können einfach über die Taskbar geöffnet werden.
- Es läßt sich einstellen, daß mit nur einem Mausklick die Anwendung geöffnet wird, d.h., der Doppelklick für den Anwendungsstart auf das Icon ist nicht mehr notwendig.
- Windows NT unterstützt notwendige ATM Services (unter Windows NT 4.0 war dies noch ein größeres Problem, vor allem ein Performance-Problem), um eine bessere Integration in ATM-Netzwerke zu ermöglichen.

24 Windows 2000

- Dateien können schneller nach bestimmten Inhalten durchsucht werden.
- Über den Task Scheduler kann auf einfache Art und Weise das Starten von Anwendungen geplant werden. Man hat hierbei zahlreiche Möglichkeiten, festzulegen, ab wann, zu welcher Zeit und in welchen Wiederholungsintervallen die Anwendung gestartet werden soll, und vor allem, mit welcher Benutzeranmeldung die Anwendung zu starten ist.
- Computer können über das Computer Management wesentlich einfacher und eleganter von jeder beliebigen anderen NT-Station aus im Netzwerk verwaltet werden. Hierzu stehen folgende Optionen zur Verfügung: System Tools (beinhaltet Event Viewer, Service Management, Device Management und Diagnostic Management), Storage zur Verwaltung der Platten sowie Server Applications und Services (DNS, DHCP, WINS, Backoffice-Anwendungen etc.). Hierbei handelt es sich wieder um ein Tool der Microsoft Management Console (MMC).
- Eine weitere Funktion für MMC ist das File Service Management, mit dem auf eine sehr einfache Art und Weise Shares (inklusive der Einrichtung neuer Shares) und aktive Sessions verwaltet werden können und von offenen Dateien eine schnelle Übersicht zu erhalten ist.
- Bei der Verwaltung von Remote-Computern ist man in der Lage, Dienste auf einem entfernten Computer anzuhalten, zu starten, in den Pausenzustand zu versetzen oder Dienste einfach neu zu starten.

Man sieht bei den letzten Beschreibungen, daß man eine Vielzahl von Funktionen, die bislang in der Systemsteuerung (Control Panel) enthalten waren, in die Microsoft Management Console übernommen worden sind. Dies war auch unbedingt notwendig, da man sich im Laufe der Zeit sehr schwer getan hat, auf Anhieb das richtige Anwendungsprogramm zu finden.

- Das System Service Management ist ebenfalls Bestandteil der MMC, so daß sich auch hier eine sehr einfache Möglichkeit ergibt, damit die Dienste auf einem Windows-NT-Rechner zu verwalten.
- Windows 2000 unterstützt zusätzlich das UDF (Universal Disk Format), ein neues Dateisystem, das entwickelt worden ist, um damit Daten auf einem DVD- und CD-ROM-System bearbeiten zu können.

Mit dieser Auflistung haben Sie bereits einen sehr guten Überblick, was bei Windows 2000 neu sein wird. Zu beachten ist dabei nur, daß sich diese Informationen auf die Beta-Version von Windows 2000 beziehen und sich deshalb bis zum endgültigen Auslieferungstermin

24.5 Active Directories

noch einiges ändern könnte. Ich hätte Ihnen auch gerne einen ähnlichen Architekturüberblick gegeben, wie dies für NT 4.0 möglich ist, jedoch habe ich bis zum Zeitpunkt der Drucklegung dieses Buchs nichts Genaues herausfinden können. Es gibt »wunderbare« Darstellungen über Active Directories, über MMC oder auch über den Replikationsaufbau der NT-Umgebung, aber nichts über die generelle Architektur.

In nächsten Abschnitt soll deshalb beschrieben werden, wie sich die Verwaltung der gesamten Ressourcen unter Windows 2000 ändern wird und was durch die Einführung von Active Directory erreicht wird.

24.5 Active Directories

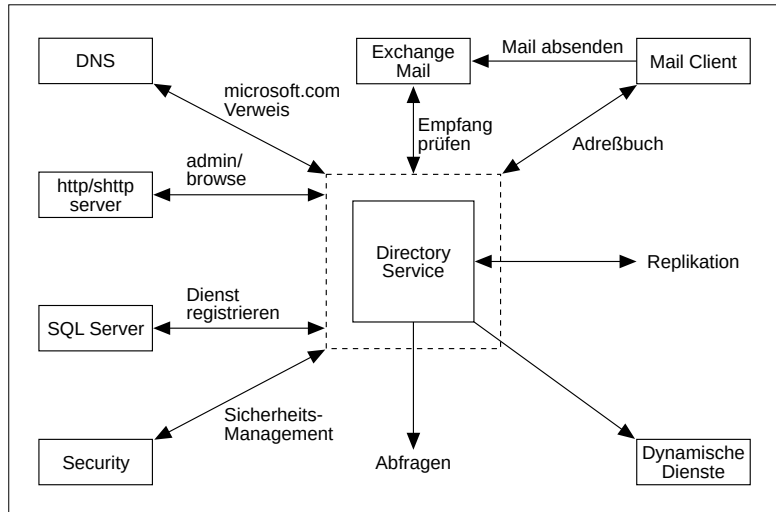
Es ist inzwischen hinreichend bekannt, daß man für die Verwaltung größerer Netzwerke mit einer Vielzahl von Servern um den Einsatz von Directory Services fast nicht mehr herum kommt, sofern man die Verwaltung des Netzwerks vereinfachen will. Novell praktiziert dies schon sehr lange mit der NDS. Mit Einführung von Windows 2000 will auch Microsoft durch die Active Directories einen Directory-Service-basierenden Dienst anbieten, der sich jedoch zum Teil grundlegend von allen bisher verfügbaren Implementierungen unterscheidet.

Entscheidend für den Einsatz der Directory Services sind neben den Möglichkeiten der Objektverwaltung auch die Protokolle, die damit verbunden sind, um den Directory Service aufzubauen. Ausschlaggebend sind auch die Application Programming Interfaces (APIs), da von diesen die zur Verfügung gestellten Tools und Anwendungen ausgehen, mit denen man die Vorteile der Directory Services direkt nutzen kann. Natürlich müssen die Directory Services nahtlos in das Betriebssystem integriert sein, und es muß eine entsprechende Unterstützung aller Applikationen zur Verfügung stehen.

Die Active Directories von Microsoft unterstützen eine Vielzahl im Einsatz befindlicher Protokolle und Formate und bieten zudem leistungsfähige, flexible und leicht einzusetzende APIs. Das Directory ist, wie alle anderen Implementierungen auch (Novell, Banyan), ein Service Provider, so wie dies in Abbildung 24.1 dargestellt ist.

Neben den herkömmlichen administrativen Aufgaben, die man von einem Directory Service erwartet, müssen von den Directory Services auch noch Aufgaben der Namensgebung, der Directory-Abfrage oder auch der Einrichtungsmechanismen in geeigneter Form gelöst werden.

Abbildung 24.1
Das Directory als
Service Provider
für alle Netzwerk-
dienste und Infor-
mationen



Mit einer solchen Architektur können sowohl kleine als auch große Netzwerke aufgebaut werden. Inwieweit Active Directory dies sinnvoll unterstützt, soll in den nächsten Ausführungen näher betrachtet werden.

Mit Active Directory stehen die folgenden Funktionen zur Verfügung:

- Unterstützung für offene Standards, um damit auch plattformübergreifende Systeme unterstützen zu können, einschließlich der Unterstützung von Domain Name System (DNS) und von Standardprotokollen wie LDAP.
- Unterstützung von Standard-Namensformaten, um eine einfache Migration und Handhabung zu gewährleisten.
- Es steht eine Vielzahl von APIs zur Verfügung, die einfach eingesetzt werden können, und dies sowohl für Script-Sprachen als auch für C/C++ Programmierer.
- Eine einfache und leicht verständliche Administration, in hierarchischer Form, so wie man dies von der Domänenstruktur kennt, und der Einsatz einer Drag&Drop-Verwaltung.
- Die Active-Directory-Objektstruktur kann durch ein erweiterbares Schema modifiziert werden, so daß nicht nur die Standardobjekte eingerichtet, sondern auch neue Objekte mit aufgenommen werden können.
- Schneller Zugriff auf Informationen durch den Einsatz eines Global Catalog (GC).
- Replizierung der Active-Directory-Informationen durch eine sogenannte Multimaster Replication.

24.5 Active Directories

- Windows 2000 Server ist immer noch kompatibel zu Windows NT 4.0 (ob dies immer von Vorteil ist?).
- Zusammenarbeit mit NetWare-4/5-Umgebungen ist möglich.

24.5.1 Überblick des Active Directory

Die Implementierung der Active-Directory-Mechanismen von Microsoft basiert auf dem Einsatz einer Vielzahl von Funktionen und Diensten, die zum Teil standardisiert sind bzw. im Bereich der IP-Mechanismen gewissen RFCs entsprechen.

Standards in Windows NT Server 5.0	RFC	Zweck
DHCP	2131	Verwaltung der IP-Adressen
Dynamic DNS	2052, 2136	Verwaltung der Host-Namen und der zugewiesenen IP-Adressen
Simple Network Time Protocol	1769	Verteilte Zeitdienste zur Synchronisation der Uhrzeiten
LDAP 3	2251	Directory-Zugriff
LDAP »C«	1777	Directory-API
LDIF Directory Information Format	Draft	Directory-Synchronisation
MIT v5 Kerberos	1510	Authentication
X.509 v3 Public Key	ISO	Directory-Schema
LDAP	2247, 2252, 2256	
TCP/IP	793, 791	Netzwerkprotokoll

Im Active Directory ist das Konzept des sogenannten Name Space verankert, so wie man dies bereits aus der Internet-Welt kennt. Zudem wird das Lightweight Directory Access Protocol (LDAP) eingesetzt, um über Betriebssystemgrenzen hinaus arbeiten zu können. Active Directory ist kein X.500 Directory und verwendet deshalb auch nicht die hierfür vorgesehenen Protokolle zur Synchronisation und zum Zugriff auf die Informationen, sondern LDAP.

Active Directory erlaubt jedoch den Single Point of Administration und verwendet den Internet Domain Name Service (DNS) als Mechanismus, um Dienste unter NT 5.0 ausfindig zu machen, etwa einen Directory Service Server zu finden. Innerhalb der Active-Directory-Struktur werden die Objekte in hierarchischer Form in Organizational Units (OU) strukturiert.

24 Windows 2000

nal Units (OUs) abgespeichert und verwaltet. Im Gegensatz zur NT-4.0-Umgebung benötigt man keinen PDC oder BDC mehr, aber man benötigt sogenannte DCs (Domain Controller). Das heißt, beim Einrichten der Active-Directory-Struktur muß immer noch eine Domäne eingerichtet werden, und innerhalb der Domäne werden die Objekte hierarchisch in OUs verwaltet. Diese Domäne ist gleichzeitig auch die Partition innerhalb des Directory Service.

Änderungen innerhalb der Domäne werden auf einem beliebigen DC durchgeführt und anschließend auf alle anderen DCs in der Domäne repliziert. Auf diese Art und Weise wird auch die Ausfallsicherheit vergrößert und verbessert, so wie man dies auch von Directory-Service-Strukturen erwarten muß.

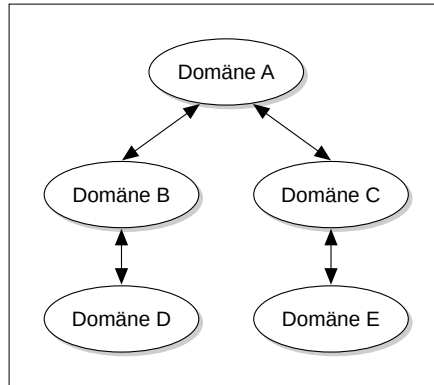
Beim Aufbau der Active-Directory-Strukturen muß deshalb vorher sehr genau bekannt sein, wie man die Hierarchie aufbauen möchte, um dann auch die Partitionen und die Verteilung der Partitionen sinnvoll festlegen zu können. Pro eigene Partition benötigt man dann auch eine eigene Domäne; Partition und Domäne müssen wiederum miteinander verbunden werden. Das heißt, zwischen den Domänen, die eine Baumstruktur bilden, existieren immer noch Vertrauensstellungen, so wie man sie aus der NT-4.0-Server-Umgebung her kennt. Der Unterschied besteht jedoch darin, daß diese Vertrauensstellungen automatisch bei der Installation der weiteren Domänen eingerichtet werden, da man bei der Installation angeben muß, unter welcher Hierarchiestufe die neu eingerichtete Domäne eingebunden werden soll. Ebenso unterstützt der Mechanismus der Vertrauensstellungen unter Windows 2000 die Transitivität für Vertrauensstellungen. Somit gilt inzwischen: Falls Domäne A der Domäne B vertraut und Domäne B wiederum der Domäne C vertraut, dann vertraut auch Domäne A der Domäne C. Wie in Abbildung 24.2 zu sehen ist, wird die Vertrauensstellung immer bidirektional eingerichtet, und das ohne Ihr Zutun.

Der einzige Nachteil an diesem gesamten Konstrukt ist, daß man für das Einrichten einer neuen Partition eine eigene Domäne einrichten muß und die Replizierung der Datenbank dieser Domäne nur auf einem Domain Controller (DC) der jeweils eigenen Domäne durchgeführt werden kann.

Nicht vergessen werden darf, daß man pro eingerichteter Domäne auch einen eigenen Server benötigt. Im Gegensatz zur NDS kann ein NetWare Server die Read Write Replicas unterschiedlicher Partitionen speichern, für den DC gilt dies für die Active-Directory-Konzeption jedoch nicht.

24.5 Active Directories

Abbildung 24.2
Automatisches
Einrichten von
Vertrauens-
stellungen



Die Active-Directory-Struktur unterstützt auch die Vererbung von Zugriffsberechtigungen innerhalb der Active-Directory-Hierarchie. So kann zu jeder Zeit auf einen Container (O oder OU) eine Zugriffsberechtigung vergeben werden, die sich nach unten vererben kann; allerdings bleibt diese Vererbung anschließend statisch, so daß ein nachträglich eingerichtetes OU bzw. »normales« Leaf-Objekt diese Berechtigung nicht besitzt. Dies liegt an folgendem Umstand: Wenn auf eine OU eine Zugriffsberechtigung vergeben wird, dann wird hierfür eine Access Control List (ACL) eingerichtet, in der die jeweiligen Berechtigungen stehen. Damit alle unterhalb des Containers befindlichen Objekte diese Berechtigungen auch erhalten, muß die ACL auf jedes Objekt unterhalb des Containers eingetragen werden. Wird ein Objekt nach dieser Berechtigungsvergabe hinzugefügt, muß die Berechtigungsvergabe wiederholt werden, da andernfalls dem Objekt die ACL-Eintragung fehlt. Es wurde bereits festgestellt, daß die Kommunikation zwischen den einzelnen Active-Directory-Komponenten über LDAP realisiert wird. Einen Active-Directory-Baum muß man sich deshalb wie in Abbildung 24.3 dargestellt vorstellen.

Aus dieser Abbildung sind die Domänengrenzen und somit auch die Partitions Grenzen sehr gut zu erkennen. Wie man sich den Aufbau innerhalb einer Active-Directory-Domäne vorstellen muß, ist in Abbildung 24.4 dargestellt.

Um den Zugriff auf die Active Directories zu verbessern, wird der Einsatz eines sogenannten Global Catalog unterstützt. Alle Objekte, die in einem Active Directory eingerichtet sind, haben gleichzeitig einen Eintrag im Global Catalog (GC), einem Dienst, der Directory-Informationen aller Domänen im Baum enthält. Konzipiert für einen schnellen Zugriff, erlaubt der GC es Benutzern, Objekte einfach und schnell zu finden, unabhängig davon, wo sich das Objekt im Baum befindet.

Abbildung 24.3
Active-Directory-
Aufbau

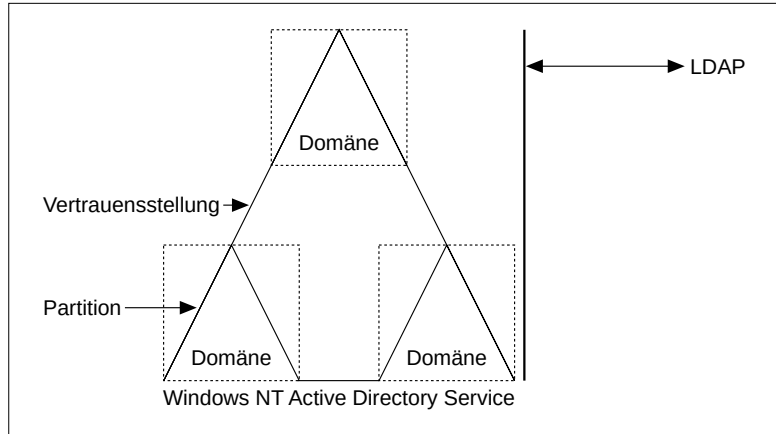
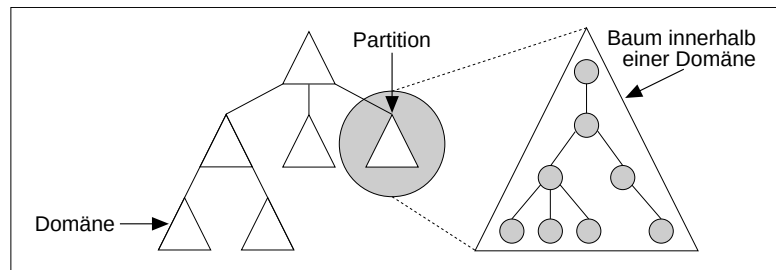


Abbildung 24.4
Container und
Objekte innerhalb
einer Partition



Die Tatsache, daß auf jedem beliebigen DC eine Änderung im Baum durchgeführt werden kann und anschließend die Replizierung auf alle anderen DCs innerhalb der Domäne durchgeführt wird, bezeichnet man auch als Multitmaster Replication.

24.5.2 Änderungen im internen Aufbau

Unter Windows NT 4.0 wird die Domänenendatenbank in Form einer verschlüsselten Datei als SAM-Datenbank (Security Account Manager) auf der Platte des Systems abgelegt. Jede Änderung, die innerhalb der Domänenendatenbank durchgeführt werden muß, erfolgt aufgrund von Zusammenhängen, so wie dies in Abbildung 24.5 dargestellt ist.

Der Zugriff erfolgt in diesem Fall über den eigenen Security Account Manager von Windows NT. Damit die Kompatibilität zu früheren NT-Versionen aufrechterhalten werden kann, findet man SAM immer noch in der neuen Architektur von Windows 2000, so wie dies in Abbildung 24.6 dargestellt ist.

24.5 Active Directories

Abbildung 24.5
Die Domänen-
struktur unter
Windows NT 4.0

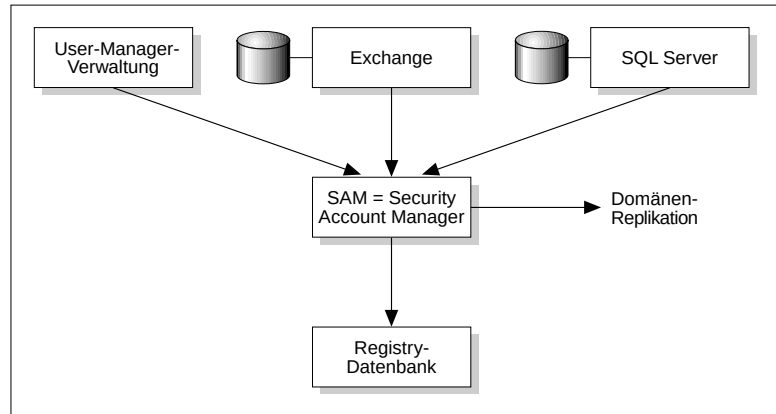
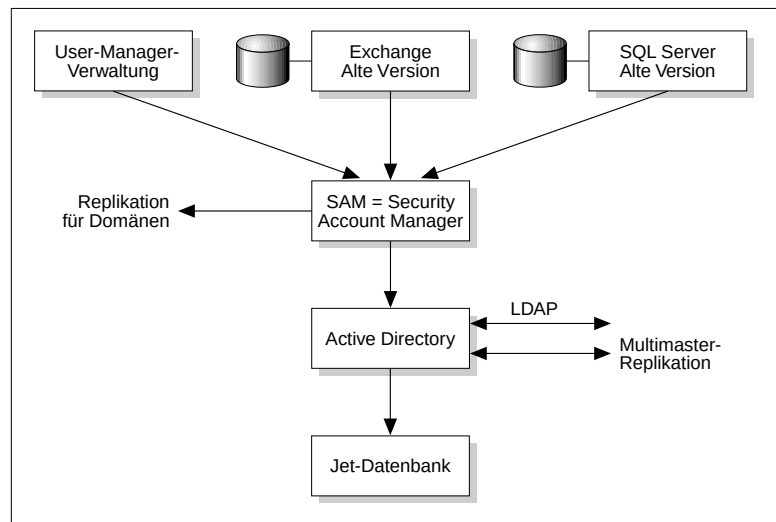


Abbildung 24.6
Active Directory,
SAM und Jet



Die Jet-Datenbank ist im Prinzip nichts Neues, da dieses Datenbanksystem bereits bei Windows NT Exchange 4.0 und 5.x verwendet worden ist. Durch die Einführung der Jet-Datenbank ist man auch in der Lage, größere Datenmengen zu verwalten, als dies mit der alten Technik der Fall war.

Windows 2000 bietet sehr wohl eine Vielzahl von Neuerungen, die sich deutlich von der Windows-NT-4.0-Version abheben. Bezüglich der Active-Directory-Strukturen kann man geteilter Meinung sein, wie gut oder wie schlecht diese Directory-Service-Implementierung gelungen ist. Schade ist es, daß es Microsoft nicht geschafft hat, sich von der Domänenstruktur zu verabschieden. Es wäre schon lange an

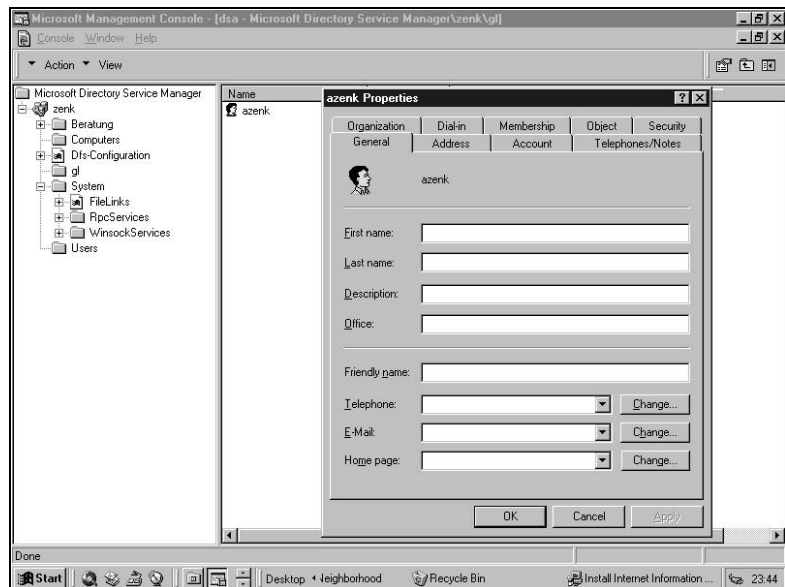
24 Windows 2000

der Zeit und gerade jetzt der richtige Zeitpunkt gewesen, einen vollkommen neuen Weg einzuschlagen. Wenn man sämtliche Mechanismen von Active Directory betrachtet, dann wundert man sich, warum auf einen der besten Flexibilitätsmechanismen – Partitions-grenzen auf jedem beliebigen Container setzen zu können – verzichtet wurde. Ebenso lassen die Mechanismen der Rechtevergabe (ACL auf jedes darunterliegende Objekt kopieren) prinzipiell zu wünschen übrig. Vielleicht ist Microsoft gerade dabei, an der einen oder anderen Stelle noch entsprechende Änderungen durchzuführen. Die nächsten Monate werden die weitere Entwicklung zeigen.

Man sollte sich jedoch bereits heute bei der Implementierung von Windows NT Server 4.0 überlegen, ab wann man auf Windows NT Server 5.0 umsteigen will. Das derzeit einfachste Modell für die Umstellung von NT 4.0 auf 2000 bietet das Single-Domänen-Modell. Alle anderen Modelle sind nur mit einem erhöhten Aufwand auf einen Windows NT Server 5.0 umzustellen. Wie bei allen Directory Services benötigt man jedoch auch noch einen entsprechenden Zeitraum, um die Planung der hierarchischen Struktur durchführen und umsetzen zu können. Dieser zeitliche Ablauf darf nicht unterschätzt werden.

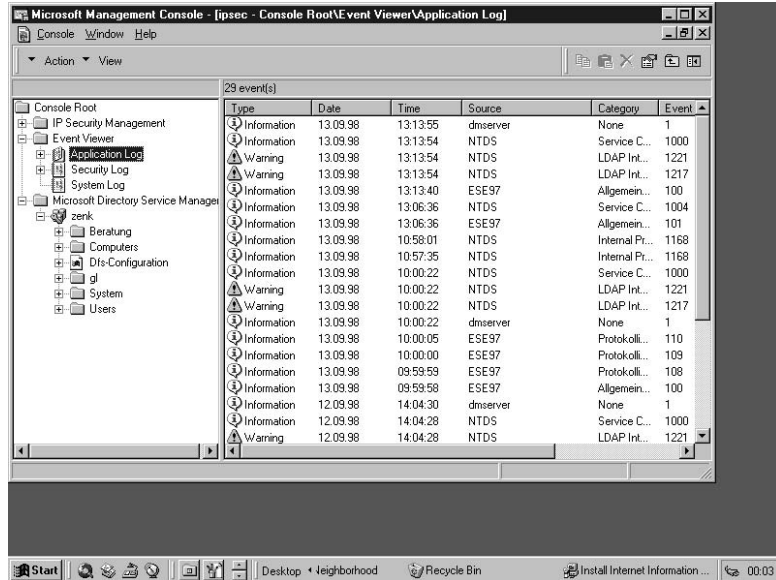
Zum Abschluß möchte ich nicht versäumen, Ihnen zumindest an einigen Bildschirminhalten zu zeigen, wie sich wahrscheinlich die Administration der Windows-NT-5.0-Serverumgebung darstellen wird.

Abbildung 24.7
Einrichten von Be-
nutzern und an-
deren Ressourcen



24.5 Active Directories

Abbildung 24.8
Mehrere Verwal-
tungsaufgaben in
einem Fenster



Diese Ausführungen sollten ausreichen, um Ihnen einen Überblick über das neue Betriebssystem Windows 2000 zu geben. Wenn im Final Release das eine oder andere Feature in der Form, wie in diesem Kapitel beschrieben, nicht enthalten ist, dann liegt es einfach daran, daß ich zum Zeitpunkt der Erstellung dieses Buchs davon abhängig war, auf die Informationen zurückzugreifen, die im Internet angeboten werden.

25

Internet/Intranet und Internet Security

Ein Thema läßt sich zur Zeit in Fachzeitschriften anscheinend nicht umgehen: Internet. Auf diesem Gebiet findet derzeit eine Entwicklung statt, deren Auswirkungen noch nicht vollständig abzusehen sind. Fest steht jedoch, daß die Art und Weise, wie zukünftig Informationen ausgetauscht, veröffentlicht und verschickt werden, neue Formen annimmt und noch annehmen wird. Das Internet bietet bis dato unvorstellbare Möglichkeiten, nicht nur an wichtige Informationen zu gelangen, sondern diese zwischen unterschiedlichen Firmen und Personen auszutauschen. Große und kleine Unternehmen aller Branchen können mit Hilfe der Internet-Technologie Informationen abfragen, auswerten und selbst zur Verfügung stellen.

Auch Privatpersonen nutzen die Vielzahl an Möglichkeiten, die durch das Internet geboten werden. Man kann auch privat ins Internet gelangen, ohne größere Ausgaben und Installationen tätigen zu müssen. So stehen günstige Übergänge in das Internet über T-Online der Telekom zur Verfügung, einem inzwischen auch bei Privatleuten sehr weit verbreiteten Dienst. In Unternehmen werden solche Übergänge, wenn kein eigener Internet-Zugang existiert, meist über CompuServe oder AOL realisiert.

Der Vorteil dieser Drittanbieter ist, daß man keine weiteren Hardware-Ausstattungen benötigt, außer einem Modem oder einer ISDN-Karte im PC. Wenn es jedoch darum geht, als Unternehmen kommerzielle Internet-Dienste nutzen und anbieten zu können, kommt man im Prinzip um einen eigenen Internet-Anschluß nicht herum. Damit Sie einen Eindruck davon erhalten, was beim Anschluß des eigenen Unternehmens an das Internet zu beachten ist und welche Voraussetzungen gegeben sein müssen, sollen in den folgenden Ausführungen die notwendigen Voraussetzungen erklärt werden.

Zunächst zu der oft gestellten Frage, wer eigentlich hinter dem Internet steckt und die Verantwortung dafür trägt:

Das Internet wird weder zentral überwacht noch verwaltet. Nur die Vergabe der IP-Adressen für den Internet-Anschluß und die Namen der DNS-Umgebung für das jeweilige Unternehmen werden zentral überwacht und verwaltet. Das Internet Network Information Center (InterNIC) übermittelt Internet-Anwendern Informationen und Registrierungsmöglichkeiten. Da der Anschluß an das Internet jedoch im-

25 Internet/Intranet und Internet Security

mer über einen Provider durchgeführt wird, der auch alle administrativen Aufgaben übernimmt, kommt man meist nicht mit dem InterNIC selbst in Kontakt.

Im Prinzip ist das Internet ein Zusammenschluß von weltweit mehreren Millionen Rechnern, die selbst Zugang zu Tausenden von Netzwerken haben und diese miteinander verbinden. Das Internet repräsentiert somit einen Daten-Highway, obwohl die Zugangsgeschwindigkeiten ab und zu noch oder wieder zu wünschen übrig lassen. Durch den immer stärker anwachsenden Datenverkehr aufgrund der ständig wachsenden Mitgliederzahl leiden derzeit auch die Übertragungsgeschwindigkeiten im gesamten Internet.

Die Geschichte des Internet beginnt während des Kalten Krieges in den späten sechziger und frühen siebziger Jahren. Der von der US-Regierung finanzierte Internet-Vorgänger war speziell darauf ausgelegt, den Informationsfluß zwischen öffentlichen Stellen auch dann noch aufrechtzuerhalten, wenn ein Teil des Netzwerks zerstört werden sollte. Durch das Kommunikationsprotokoll TCP/IP hat man die Gewißheit, daß Rechnersysteme, egal welchen Typs, Dienste gemeinsam nutzen und eine gemeinsame Kommunikation aufbauen können, so als wären sie Teil eines einzigen homogenen Systems. Das Internet ist heute so stark gewachsen, daß es weltweit viele Millionen Anwender miteinander verbindet. Das größte aller Netzwerke besteht aus Tausenden von Netzwerken an Universitäten, öffentlichen Einrichtungen und Unternehmen aller Branchen.

Das Internet ist, genau betrachtet, ein öffentliches Netzwerk, das jeder nutzen kann, der über ein Modem und ein TCP/IP-fähiges Kommunikationsprotokoll verfügt. Seit der starken Verbreitung von ISDN kann dieser Anschluß selbstverständlich auch über ISDN realisiert werden. Der Zugang zum Internet wird dann über einen Internet-Provider, über eine Standleitung oder eine Wählverbindung zur Verfügung gestellt. Man schätzt, daß derzeit ca. 60 Millionen Anwender in mehr als 84 Ländern Zugang zum Internet haben. Neben den privaten Anwendern stellen auch immer mehr Firmen fest, welches Potential im Internet steckt. Wenn man die angebotenen Dienstleistungen im Internet betrachtet, kommt die Frage auf, wie dieses enorme Potential an Informationen zur Verfügung gestellt werden kann. Das geschieht über die große Anzahl von Hosts, die am Internet angeschlossen sind. Seit 1990 ist die Anzahl der Hosts im Internet von ungefähr 500.000 auf geschätzte 6,5 bis 7 Millionen angestiegen. Unter einem Host versteht man dabei im Internet-Sprachgebrauch eine Gruppe von Rechnern, die direkt an das Internet angeschlossen sind und den Internet-Anwendern Zugriff auf die damit verbundenen Ressourcen bieten.

25 Internet/Intranet und Internet Security

Wenn man erst einmal begonnen hat, intensiver mit den Möglichkeiten des Internet zu arbeiten, stellt man fest, daß man auf eine Unmenge von Informationen stößt. Das lange Suchen und Nachfragen hat dabei sehr schnell ein Ende, da man innerhalb von wenigen Minuten entsprechende Informationen über das Internet erhalten kann. Wenn man zum Beispiel eine bestimmte Software für spezielle Anwendungen sucht, kann man im Internet einen Suchvorgang anstoßen und erhält sogleich (oder auch etwas zeitverzögert) eine Auflistung aller gefundenen Bereiche, die mit dem Suchbegriff zu tun haben. Alle renommierten Hersteller sind im Internet vertreten und stellen die Möglichkeiten zur Verfügung, neben aktuellen Informationen über Hard- und Software auch aktuelle Patches zu erhalten. Auf diese Weise kann man ohne Probleme die aktuellste Software und neue Produktinformationen erhalten.

Man kann aber auch mit dem Internet die nachfolgend aufgeführten speziellen Dienste nutzen oder als Unternehmen selbst solche anbieten, sofern man den Internet-Zugang nicht nur zum Abholen von Informationen nutzen will, sondern selbst als Anbieter fungieren möchte. In beiden Fällen ist es jedoch wichtig, das eigene Netzwerk vor unbefugten Zugängen zu schützen, sobald Sie den Zugang zum Internet freigegeben haben. Diese Schutzmechanismen werden mit Hilfe von FireWall-Systemen aufgebaut, auf deren Funktionen und Mechanismen in einem späteren Abschnitt eingegangen werden soll.

E-Mail

Eine der am meisten genutzten Funktionen des Internet ist die E-Mail-Funktion. Über diesen Mechanismus können alle über das Internet erreichbaren Personen Nachrichten und Dokumente austauschen. Da die Bedeutung des Internet-Mailing immer größer wird, haben alle Mailing-Systeme (z.B. GroupWise, MS Exchange) sogenannte SMTP Gateways, die den Übergang zur Internet-Mail ermöglichen, da es auf dem SMTP-Protokoll aufbaut. Jedem Anwender, der als Einzelperson Zugang zum Internet über T-Online, AOL oder CompuServe erhält, steht auch eine Internet-E-Mail-Adresse im Netz zur Verfügung. So lautet meine derzeitige E-Mail-Adresse über CompuServe 100010.2561@compuserve.com. Wenn Sie wollen, können Sie mich über das Internet und diese Adresse erreichen.

World Wide Web (WWW)

Neben dem E-Mail stellt das WWW die interessantesten Aufgaben im Internet und einen sehr zukunftssträchtigen Dienst zur Verfügung. Das World Wide Web bietet unbegrenzte Möglichkeiten bei der Zusammenfassung, Verbreitung und Recherche von Informationen.

25 Internet/Intranet und Internet Security

Dieses grafische, Hypertext-basierende Tool gibt Ihnen ausgefeilte Instrumente zur Darstellung und Präsentation von Informationen und Dateien an die Hand, die per Download geholt werden können.

Das World Wide Web wurde ursprünglich von Tim Berners-Lee im CERN (Europäische Organisation für Kernforschung) in Genf entwickelt, um Informationen für die Wissenschaftler im CERN besser aufbereiten zu können. Auf den Web-Servern werden die Informationen in einer Dokumentensammlung abgelegt. Jedes Dokument enthält Hypertext-Verknüpfungen, über die der Anwender verwandte Informationen in anderen Dokumenten aufrufen kann. Der Anwender kann sich dabei in alle Richtungen bewegen, indem er Wörter, Bilder oder auch Grafiken innerhalb des Texts auswählt. Aufgrund der hinterlegten Verknüpfung wird auf das entsprechende System gesprungen – für den Anwender vollkommen transparent –, um die dazugehörigen Dokumente oder auch Grafiken zu erhalten.

An dieser Stelle sei darauf hingewiesen, daß die Erstellung von Angeboten auf einem Web-Server über spezielle Mechanismen erfolgt: Man muß in der Lage sein, sogenannte Web-Seiten zu kreieren. Hierfür werden inzwischen die unterschiedlichsten Module angeboten. Zum Erstellen von Web-Seiten sollten Sie sich deshalb erkundigen, mit welchem Produkt es für Sie am besten realisierbar ist. Entsprechende Zusatzmodule gibt es unter anderem für Winword. Auf der Suche nach Informationen kann der Anwender über das Netz auf der ganzen Welt herumreisen. Da die Informationen auf einer Vielzahl von Servern verteilt sein können, wiederholt sich diese Recherche.

Um die Informationen im World Wide Web abrufen zu können, benötigt man einen sogenannten Web-Browser. Nur so ist es dem Anwender möglich, die enorme Flut und Vielzahl von Daten auf dem Web-Server abzurufen und darin zu navigieren. Ebenso ist der Anwender in der Lage, Informationen von einem FTP-Server oder einem Gopher Server abzurufen bzw. auf diesem zu »browsen«. Auf einem FTP-Server werden Informationen in Dateiform zur Verfügung gestellt, z.B. wenn es darum geht, aktuelle Patches zu erhalten. Je nach Konfiguration ermöglichen die FTP-Server den anonymen Anwendern, d.h. jedem im Internet oder auch nur bestimmten registrierten Personen mit dazugehörigen Berechtigungen, den Zugriff auf dieses System. Gopher ist ein weiteres System zur Erfassung von Daten und Informationen, das über eine menügesteuerte Schnittstelle die Informationen abrufen läßt. Gopher organisiert und verteilt die Informationen auf Internet-Servern.

Jedes Unternehmen, das Informationen im Internet zur Verfügung stellen will, wird dies mit Hilfe von Web-Servern tun. Neben diesen Begriffen werden Sie auch immer wieder auf den Ausdruck News-

25 Internet/Intranet und Internet Security

groups stoßen. Dabei handelt es sich um eine relativ alte Variante der Informationsverteilung. Bevor das World Wide Web gebildet wurde, tauschten Internet-Anwender ihre Nachrichten und Ideen über das sogenannte Usenet aus. Usenet ist ebenso unter der Bezeichnung »Network News« bekannt, es ist ein verteiltes und Internet-weites schwarzes Brett. Man kann derzeit davon ausgehen, daß weit über 5.000 dieser Newsgroups existieren.

Für das Arbeiten im Internet müssen ganz bestimmte Standards eingehalten werden, die nachfolgend näher beschrieben werden sollen. Wenn man sich nicht an diese Standards hält, ist ein Arbeiten im und über das Internet nicht möglich.

Netzwerkstandards

Über das Internet können viele unterschiedliche Computersysteme miteinander kommunizieren. Da es sich dabei um eine sehr heterogene Rechnerlandschaft handelt, kann die Kommunikationsfähigkeit nur dann erreicht werden, wenn die vorgegebenen Standards strikt eingehalten werden. Beim Zugang zum Internet wird die Datenkommunikation standardisiert und dadurch die Komplexität und die Vielfalt der unterschiedlichen Netzwerke und Rechner unterdrückt, die über das Internet miteinander verbunden sind. Das wichtigste Protokoll überhaupt ist das TCP/IP-Protokoll, das von allen am Internet angeschlossenen Rechnern verwendet werden muß. Da alle das gleiche Protokoll verwenden, spart man sich aufwendige Protokollumwandlungen und hat zudem ein leichteres Spiel beim Einrichten und Administrieren. TCP/IP ist so konzipiert, daß jeder Rechner eine eigene IP-Adresse haben muß. Über diese Adresse ist jeder Rechner bzw. jedes Endgerät im Internet identifizierbar und kann angesprochen werden. Dies wäre nicht durchführbar, wenn sich jeder Anwender im Internet die IP-Adresse des Zielrechners merken bzw. diese kennen müßte. Bei der großen Anzahl von Rechnern im Internet tut man sich da etwas schwer. Deshalb hat man sich bei der Adressierung im Internet etwas anderes ausgedacht. Zum einfachen Adressieren von Zielsystemen verwendet man Namen, die ganz bestimmten Regeln gehorchen müssen. Gesteuert und verwaltet wird das Ganze über mehrere DNS-Server im Netz bzw. in den Netzen, die an das Internet angeschlossen sind. DNS steht dabei für Domain Name System. Der DNS-Server ist in der Lage, einen vergebenen Namen für das Endgerät in die notwendige IP-Adresse umzuwandeln. Statt die IP-Adresse 137.65.1.3 zu verwenden, gibt man einfach den Namen `www.novell.com` ein, das ist der vergebene Name für die vorher aufgeführte IP-Adresse. Zum Austausch von E-Mail wurde bereits erläutert, daß hierfür das SMTP-Protokoll zum Einsatz kommt.

25 Internet/Intranet und Internet Security

Wenn man vom World Wide Web spricht, meint man damit alle Rechnersysteme im Internet, die Web-Seiten zur Verfügung stellen. Auch für das WWW sind bestimmte Protokolle definiert. Das zugrunde gelegte WWW-Protokoll ist das Hypertext Transport Protocol (HTTP). Web-Seiten und Web-Dokumente werden mit einer Hypertext Markup Language (HTML) erstellt. Über HTML kann man Dokumente mit Hypertext-Schnittstellen versehen, um damit auch Grafiken einbinden zu können. Über die URL-Angabe (Universal Resource Locator) werden die Zielrechner angegeben. So lautet die Angabe für den Zugriff auf den Web-Server von Microsoft, der im Web Browser angegeben werden muß, oder um auf den Web-Server von Novell Zugriff zu erhalten: <http://www.microsoft.com> bzw. <http://www.novell.com>. Es gibt eine Vielzahl von Web-Servern, die im Internet zur Verfügung stehen. Die Adresse jedes einzelnen Web-Servers anzugeben, würde ein eigenes Buch ergeben. Für den Fall, daß Sie eine solche Übersicht benötigen, sei auf die vorhandene Literatur hingewiesen. Sie können aber auch über den Browser selbst im Internet nach bestimmten Web-Servern suchen, um anschließend darauf zu verzweigen.

25.1 Einrichten eines Internet-Anschlusses

Wenn es darum geht, Anschluß an das Internet zu erhalten, muß man zwei Fälle unterscheiden: den Anschluß eines Einzel-PC oder den Anschluß eines Netzwerks, um allen berechtigten Personen im Netzwerk den Zugang zu ermöglichen.

Der Anschluß eines Einzel-PC kann entweder über Internet-Zugänge über CompuServe, AOL, T-Online oder andere ähnliche Anbieter erfolgen. Es ist aber auch möglich, den Einzel-PC-Anschluß über herkömmliche Internet-Provider zu erhalten. Ein bekannter Provider in Deutschland ist zum Beispiel UUNET. Bei den jeweiligen Anschlüssen muß man nur darauf achten, wie sich die monatlichen Kosten hierfür zusammensetzen. Bei T-Online ist es zum Beispiel derzeit so, daß man pro Monat einen Beitrag von DM 8,- zahlen muß. Arbeitet man mit der T-Online-Version 1.x, kostet der Zugang zum Internet pro Minute fünf Pfennige. Mit der T-Online-Version 2.x ist der Zugang zum Internet über die Zugangsnummer 0191011 kostenfrei – darin enthalten sind im Abrechnungsmonat zwei Online-Stunden (T-Online) kostenfrei. Ab der 121. Minute bezahlt man pro Minute drei Pfennige Nutzungsentgelt und drei Pfennige Verbindungsentgelt. Weitere Tarifbestimmungen können der T-Online-Preisliste entnommen werden. Je nach Dienstanbieter hat man auch noch einige Freistunden im Monat zur Verfügung. Es ist mit Sicherheit von Vorteil,

25.1 Einrichten eines Internet-Anschlusses

die einzelnen Internet-Anbieter zu vergleichen. Was Sie dann noch brauchen, ist entweder ein Modem oder ein ISDN-Anschluß für den PC. Ebenso ist es vorstellbar, den Zugang über einen RAS-Server zu realisieren, um dadurch Modem-Pools im Netzwerk verwenden zu können.

Soll hingegen ein LAN an das Internet angebunden werden, benötigen Sie nicht nur mehr Geld, sondern auch eine wesentlich größere Hardware-Ausstattung und zusätzliche Sicherheitseinrichtungen – wie FireWall-Systeme –, um den unberechtigten Zugang aus dem Internet in Ihr Netzwerk zu unterbinden. Ohne ein solches FireWall-System müssen Sie immer davon ausgehen, daß Sie mit dem Internet-Anschluß das Netzwerk für die gesamte Welt öffnen und jeder, der IP-Adressen von Endgeräten in Ihrem Netzwerk kennt, versuchen könnte, über IP auf diese zuzugreifen.

Beim Internet-Zugang müssen Sie also vor Augen haben, daß das Internet ein offenes Netzwerk ist, auf das jeder, der die technischen und logischen Voraussetzungen erfüllt, zugreifen kann. Der Zugang zum Internet erfolgt, wie gesagt, über einen Internet-Services-Provider auf Basis einer Standleitung oder einer Wählverbindung. Als Internet-Provider werden somit sowohl lokale Anbieter mit einfachen Wählverbindungen für private Anwender als auch landesweite Organisationen mit einem breiten Spektrum an Dienstleistungen und Connectivity-Optionen für Geschäftskunden verstanden.

Welche Maßnahmen müssen Sie nun ergreifen, um Ihr LAN in das Internet zu integrieren?

Vorbereitung für das LAN

Zuerst benötigen Sie eine Internet-Adresse für Ihr Netzwerk. Da die IP-Adressen für den Zugang zum Internet nicht willkürlich gewählt werden können, müssen Sie sich mit Ihrem Provider zusammensetzen, um offizielle IP-Netzadressen zu erhalten. Wenn diese Adressen vorliegen, ist es noch notwendig, daß Sie einen Domain Name Server installieren. Dafür benötigen Sie ebenfalls einen offiziell freigegebenen Namen. Auch hier hilft der Internet Provider; er verhilft Ihnen zu einem passenden Namen. So wäre es zum Beispiel denkbar, daß sich die Firma Zenk GmbH als Domain-Namen zenk.de geben läßt. Zu beachten ist, daß der Domain-Name für ein Unternehmen nicht mehrfach vergeben werden kann. Wenn Ihr Domain-Name registriert ist, besteht keine Gefahr mehr, daß jemand anderer ebenfalls diesen Namen zugeteilt bekommt.

Zu überlegen ist auch, ob die Verwaltung für den DNS im eigenem LAN oder über den Internet-Provider erfolgen soll. In der Regel wird

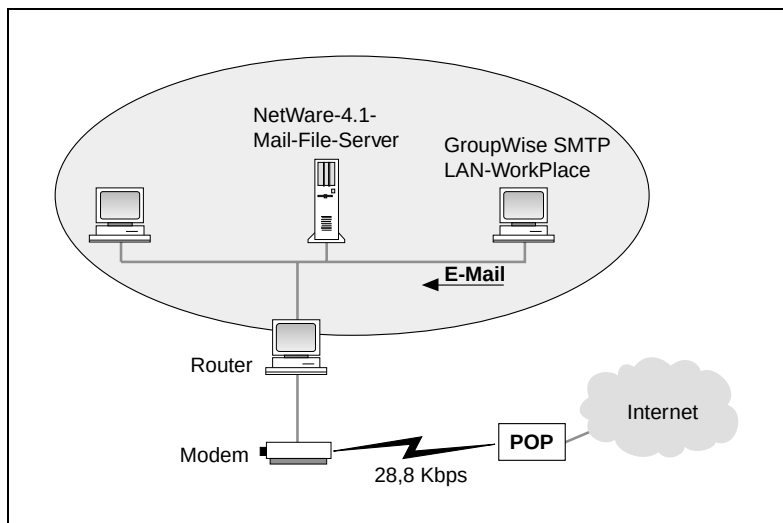
25 Internet/Intranet und Internet Security

man die Verwaltung selbst übernehmen. Bei der Betrachtung der Netzwerkbetriebssysteme fällt inzwischen auf, daß sowohl Novell als auch Microsoft Produkte zur Verfügung stellen, mit denen man auf einem Server einen DNS laufen lassen kann. Wenn diese beiden Hürden genommen sind, benötigen Sie auch noch einen Router, der Ihr LAN mit dem Internet verbindet. Man kann sagen, der Router hat das eine Bein im LAN und das andere Bein über die Remote-Verbindung zum Internet-Provider. In der Regel erfolgt der Anschluß zum Internet-Provider über eine ISDN-Verbindung, so daß entsprechende Bandbreiten verfügbar sind.

Sie sollten nicht vergessen, eine geeignete Browser-Software zur Verfügung zu stellen, damit alle Benutzer im LAN auch in der Lage sind, im Internet zu »surfen«. Neue Untersuchungen haben ergeben, daß nur noch 25 % der Internet-Surfer den Netscape Navigator nutzen. Dabei konnte festgestellt werden, daß ca. 50 % den Internet Explorer 4.x und ca. 25 % den Internet Explorer 5.x einsetzen. Der Grund hierfür kann auf alle Fälle darin gesehen werden, daß Microsoft seine Betriebssysteme standardmäßig mit den Internet Explorer ausliefert.

Für den Fall, daß auch E-Mail im Internet durchgeführt werden soll, und das aus der Mailing-Software, die bereits in Ihrem Unternehmen eingesetzt wird, benötigen Sie auch noch ein SMTP-Gateway. Über dieses Gateway können Sie problemlos Mailings erstellen und als Adressaten einen Benutzer im Internet wählen. Ebenso können Sie aus dem Internet heraus Mailings direkt, d.h. über Ihre bestehende Mailingsoftware, empfangen.

Abbildung 25.1
Mailing-Aus-
tausch im Internet

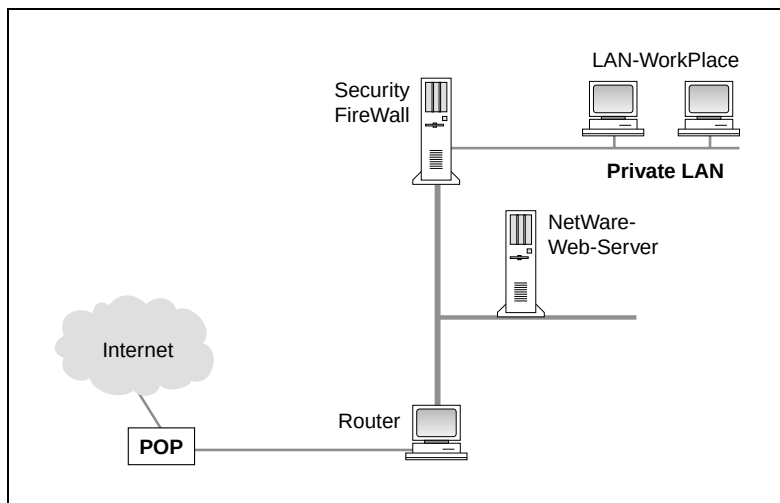


25.1 Einrichten eines Internet-Anschlusses

In Abbildung 25.1 ist dargestellt, wie Sie sich einen solchen Übergang im LAN vorstellen können.

Mit diesen Installationen im LAN sind Sie nun in der Lage, den Zugang zum Internet für Ihr Unternehmen zu realisieren. Aber vielleicht möchten Sie noch wissen, was zu tun ist, wenn Sie selbst im Internet Angebote, d.h. Web Server oder auch FTP-Server, zur Verfügung stellen wollen. In den meisten Fällen geht es darum, eigene Web-Seiten anbieten zu können. Für diesen Fall benötigen Sie »nur« einen Web-Server. Einen Web-Server können Sie auf einer Unix-Maschine installieren, oder Sie nehmen die Lösungen von Novell, um einen Web-Server auf einem NetWare 4 Server zu installieren, oder die Lösung von Microsoft, um einen Web Server auf einem NT Server zu installieren. Für das Bereitstellen von FTP-Servern stehen ebenfalls Lösungen für Unix-Maschinen oder für NetWare Server bzw. NT Server zur Verfügung.

Abbildung 25.2
Eigene Angebote
im Internet verfü-
gbar machen



Als letztes ist jetzt zu überlegen, wie das Netzwerk gegen unberechtigten Zugriff geschützt werden kann. Hierfür gibt es sehr einfache Lösungen mit weniger Sicherheit oder ausgefeilte Lösungen, die als FireWall-Systeme bezeichnet werden. Man versucht inzwischen auch, Möglichkeiten des Fire Wall auch auf herkömmliche Router zu implementieren. Um einen Überblick darüber zu geben, wie FireWall-Systeme konzipiert und aufgebaut werden können, soll im nächsten Abschnitt das generelle Prinzip erläutert werden. Wenn es dann später zu einer Implementierung für den Internet-Zugang gehen soll, muß auf alle Fälle vorher eine genaue Planung durchge-

führt werden, um die richtige Lösung für die jeweilige Umgebung zu finden. In Abbildung 25.2 ist dargestellt, wie die Implementierung von eigenen Diensten im Internet realisiert werden kann.

25.2 FireWall-Systeme

Beim Hausbau gibt es Brandschutzmauern, die das Ausbreiten eines Feuers stoppen sollen. Dieses Prinzip wird auch auf vernetzte Rechnersysteme übertragen. Die sogenannten FireWalls kontrollieren den Datenfluß und sollen unerlaubten Teilnehmern den Zugang zum Netz verweigern.

Im Internet bestehen viele Sicherheitslücken und -probleme. Ist ein Rechner an das Internet oder ein WAN angeschlossen, kann im Prinzip jeder auf der ganzen Welt auf diesen Rechner zugreifen. Mögliche Angreifer nutzen dabei zum Beispiel die Schwachstellen in Netzwerkprogrammen, um sich auf einem fremden Rechner anzumelden und Paßwörter oder andere Daten zu kopieren.

Um das Ausspionieren des eigenen Netzwerks zu verhindern (vor allem durch den Zugang zum Internet), sind die FireWall-Systeme im Einsatz. Solche Systeme bestehen in der Regel aus Hard- und Software-Komponenten und bilden eine Art Mauer zwischen den beiden Netzen (eigenes Netz und Internet), die erst überwunden werden muß, um Rechner im jeweils anderen Netz zu erreichen.

Durch technische und administrative Maßnahmen wird dafür gesorgt, daß die Kommunikation zwischen den beiden Netzen (eigenes Netzwerk und Internet) über den FireWall geführt werden muß. Auf dem FireWall hingegen sorgen Zugriffskontrolle und Audit dafür, daß nur berechtigte Benutzer Anwendungen in Anspruch nehmen dürfen und können. Somit werden potentielle Angriffe schnellstmöglich erkannt. Dies bedingt aber auch, daß das mitgeführte Audit in regelmäßigen Abständen geprüft wird.

In den meisten Fällen wird ein FireWall eingesetzt, um das eigene LAN gegen Angriffe aus dem Internet zu schützen. Ein FireWall kann aber auch an anderen Stellen eingesetzt werden, um eigene Subnetze im LAN oder firmeneigene LAN-WAN-LAN-Verbindungen abzusichern.

Beim Aufbau von FireWall-Systemen gibt es inzwischen die unterschiedlichsten Techniken und Hardware-Lösungen. Die nachfolgenden Ausführungen sollen sie näher beschreiben, damit Sie erkennen, daß es sich dabei um ein sehr komplexes Gebilde handelt, das nicht nur einfach installiert wird, sondern auch einer regelmäßigen Admi-

25.2 FireWall-Systeme

nistration und Kontrolle unterzogen werden muß. Zudem müssen Systeme eingesetzt werden, die in bestimmten Abständen per Update auf den neuesten Stand gebracht werden, da wie bei Virensystemen immer wieder neue Lücken entstehen können.

Der einzelne PC am Internet

Beim Anschluß eines LAN an das Internet ergeben sich viele Fragen bezüglich der Datensicherheit. Selbst ein temporärer und dezentraler Zugang eines PC im LAN birgt gewisse Gefahren für die Sicherheit im Netzwerk. Insbesondere das Risiko von PC-Viren, die auf diesem Weg vom Internet in das LAN gelangen, darf hier nicht vernachlässigt werden, da sich diese Viren im gesamten LAN ausbreiten können. Durch die Möglichkeit, direkten Zugang zum Internet über CompuServe, Datex-J oder MSN zu erhalten, wird dieses Problem immer größer. Geeignete Maßnahmen zu treffen ist unerlässlich, um einen unregulierten Zugang zu unterbinden.

Das LAN am Internet

Bei mehreren Internet-Nutzern im LAN stellt sich die Frage nach einer direkten Verbindung des LAN zum Internet. Ein zentraler Zugang bietet auch die Möglichkeit, die Ressourcen im LAN von außen zu nutzen. Dieser zentrale Zugang aller PCs im LAN wird oft nicht nur aus Kostengründen, sondern auch wegen möglicher Sicherheitslücken abgelehnt. Dabei kann man gerade durch eine zentrale Schnittstelle zentrale Kontrollmechanismen verwenden. Diese Kontrollmechanismen müssen jedoch zusätzlich installiert werden (z.B. durch die Verwendung eines FireWall-Systems).

■ *Lokale Sicherheit*

Bevor ein LAN einen zentralen Internet-Anschluß erhält, sollten die internen Sicherheitsmechanismen installiert und entsprechend eingesetzt werden. Dazu gehört vor allem ein strenger Umgang mit Paßwörtern, d.h. Minimallänge und regelmäßiges Ändern der Paßwörter. Weiterhin sollten die Zugriffsrechte der Benutzer auf ein zum Arbeiten notwendiges Maß beschränkt sein. Ebenso ist ein wirksamer Virenschutz in einem Netzwerk unerlässlich.

■ *Sicherheit nach außen*

Die Schutzmechanismen (FireWall-System) müssen die Zugriffsmöglichkeiten auf die LAN-Ressourcen von außen her einschränken, aber trotzdem die Nutzung von Internet-Diensten für LAN-Benutzer ermöglichen. Um dies zu realisieren und zu gewährleisten, gibt es zur Zeit drei Basistechniken, die für FireWall-Systeme zum Einsatz kommen (oder eine Kombination davon): Paketfilterung, Application-Level Gateways und Circuit-Level Gateways.

25 Internet/Intranet und Internet Security

Durch den Einsatz einer, oder besser, mehrerer Techniken in Kombination bilden FireWall-Systeme einen Schutzwall zwischen dem Internet und dem »privaten LAN«, der erst überwunden werden muß, wenn man die im LAN befindlichen Ressourcen nutzen möchte. Wird dieser Schutz legal oder illegal überwunden, kommen zusätzlich die internen Sicherheitsmechanismen wie Paßwörter oder Zugriffsrechte zum Tragen. Durch den Einsatz eines FireWall-Systems werden die bereits vorhandenen Schutzmechanismen der Netzwerkbetriebssysteme also keineswegs abgelöst. Da es die unterschiedlichsten Möglichkeiten gibt, FireWall-Systeme aufzubauen und zu realisieren, sollen die sich am meisten im Einsatz befindenden und in Frage kommenden Techniken näher betrachtet werden. Es sei jedoch darauf hingewiesen, daß die FireWall-Systeme ständig überarbeitet werden, um die Sicherheit verbessern zu können. Dies ist vergleichbar mit der Entwicklung von Virenschutzsystemen. Auch auf diesem Gebiet werden immer wieder neue Systeme und Komponenten angeboten.

25.2.1 Paketfilterung (Screening Router)

Router, die den Datenverkehr zwischen dem Internet und dem LAN nach einem bestimmten Regelwerk filtern, nennt man Screening Router. Jedes Datenpaket wird vor der Weiterleitung untersucht. Dies geschieht entweder unmittelbar nach dem Empfang (Inbound-Filter) oder vor dem Weiterleiten auf das Zielsegment (Outbound-Filter) oder zu beiden Zeiten.

Diese Filterung der TCP- und UDP-Pakete basiert auf den Informationen, die im Protokoll-Header stehen. Ausgewertet werden neben der Quell- und Zieladresse im IP-Header auch die Port-Nummern von Quell- und Zielrechner.

Grenzen der Paketfilterung

Wenn die Filterung der Pakete lediglich auf Adresse und Port ausgerichtet ist, können diejenigen Dienste, die von außen im LAN nicht erreichbar sein sollen, auch nicht im Internet vom LAN aus genutzt werden. Dies hängt damit zusammen, daß sowohl die Request- als auch die Reply-Pakete dieselben Adressen und Ports benutzen.

Um Dienste von LAN-Seite her zuzulassen, aber von der Internet-Seite aus zu sperren, muß der Router wissen, wer für die Initiierung der Verbindung verantwortlich ist. Zusammenhänge aus den Paketen können dafür nicht ausgewertet werden. Es bleibt nur die Möglichkeit, die Paketfolgen zu protokollieren.

25.2 FireWall-Systeme

Filter bei TCP-basierten Anwendungen

Bei Diensten, die auf dem TCP-Protokoll aufsetzen (FTP, Telnet, SMTP, Gopher und HTTP), kann der Router aufgrund von Status-Flags feststellen, von welchem Host aus die Verbindung initiiert wurde. Damit liegt auch fest, von welcher Router-Seite, LAN oder Internet, eine Verbindung angefordert wurde.

Filter bei UDP-basierten Anwendungen

Für Anwendungen, die das verbindungslose Protokoll UDP verwenden (Archie, WAIS, NFS, DNS, SNMP etc.), stehen solche Status-Informationen nicht zur Verfügung.

Zusätzliche Anforderungen an Screening Router

Anwendungen wie FTP oder X-Windows stellen zusätzliche Anforderungen an die Filtermechanismen der Router. Bei diesen Verbindungen vom Client zum Server wird der Verbindungsaufbau über fest definierte Ports erledigt. Für den Datenaustausch werden aber zusätzlich dynamisch gewählte Ports verwendet.

Das stellt besonders beim oft gewünschten FTP ein Problem dar. Der Router muß, um FTP-Verbindungen nicht zu filtern, Pakete mit Portnummern größer 1024 ohne weitere Prüfung passieren lassen. Dies stellt natürlich eine potentielle Sicherheitslücke dar, insbesondere für X-Windows-Anwendungen, die mit diesem Port-Bereich arbeiten.

Zur Vermeidung solcher Probleme müssen entweder die Protokolle eingeschränkt werden oder der Router muß auf höheren Protokollebenen filtern können.

Filterstrategien

Die genannten Probleme zeigen, daß der Aufbau und die Verwaltung der benötigten Filtertabellen keine leichte Aufgabe ist. Sie setzt genaue Kenntnisse über die Funktionsweise aller TCP/IP-Protokolle voraus. Zusätzlich sind eventuelle Nebeneffekte zwischen einzelnen Filterregeln zu beachten.

Für höchste Sicherheitsanforderungen sollte man nach der Regel vorgehen: Was nicht erlaubt ist, ist verboten. Dies gewährleistet auch einen Schutz vor der Nutzung von ausgeschlossenen Diensten über alternative Port-Nummern.

Nachteile der Paketfilterung

In komplexen Netzwerken können die Filter schnell zu einem kaum zu verwaltenden Regelwerk werden, da jeder Dienst und jeder einzelne Server in das Regelwerk einbezogen werden muß. Sicherheitslücken sind daher kaum vermeidbar. Da der Router für die Hosts transparent arbeitet, bietet er keine zusätzlichen Authentisierungen. Neben reinen Paketstatistiken bietet er keine Möglichkeit, Zugriffsinformationen auszuwerten. Der Router bleibt zudem potentieller Angriffspunkt. Gelingt es einem Eindringling, die Filterbedingungen im Router abzuschalten, ist das LAN ungeschützt. Aus all diesen Gründen ist ein FireWall in dieser Form nur als »Erste Hilfe« zu sehen. Der echte Schutz muß über weit mehr Mechanismen und Möglichkeiten verfügen, wie auf den nächsten Seiten zu sehen ist.

25.2.2 Application-Level Gateway

Im Gegensatz zum Screening Router kontrollieren die Application-Level Gateways den Paketfluß auf höchster Ebene des Anwendungsprotokolls. Das bedeutet, sie benötigen eine Unterstützung durch die Client-Anwendungen wie FTP, Gopher oder HTTP.

Ein FireWall auf Basis eines Gateway bietet sich für lokale Netze an, die einen Unix-Rechner als Verbindung zum Internet nutzen. Ohne Schutzmaßnahmen wären alle Rechner und Dienste innerhalb des LAN von außen erreichbar und somit auch angreifbar. Die Idee beim Gateway-FireWall ist, das Routing zu unterbinden und alle direkten Verbindungen zwischen LAN und Internet zu verhindern. Der einzige vom LAN aus erreichbare Rechner im Internet ist der FireWall-Rechner, und umgekehrt ist der Gateway-Rechner der einzige Host vom lokalen Netz, der vom Internet aus erreichbar ist. Eine direkte Verbindung zwischen LAN und Internet ist nur noch über spezielle Anwendungen auf dem FireWall möglich. Bei Diensten, die keine Interaktion erfordern, werden die entsprechenden Server einfach auf dem Gateway-Rechner installiert. Meist werden hierzu die sogenannten Proxy-Server auf dem Gateway-Rechner verwendet.

Ein Proxy-Server ist ein Daemon-Prozeß auf dem Bastion-(Gateway-) Rechner. Er nimmt eine Verbindung vom Quellrechner an, baut nach der Überprüfung der Quell- und Zieladresse eine Verbindung zum Zielrechner auf und kopiert danach die Daten zwischen diesen beiden Verbindungen. Für den Server auf dem Ziel-Host scheint die Verbindung von einem Client auf dem Gateway-Rechner zu kommen. Aus der Sicht des Clients verhält sich dagegen der Gateway-Rechner wie der gewünschte Ziel-Server. Proxy-Server können für beliebige Protokolle eingesetzt werden.

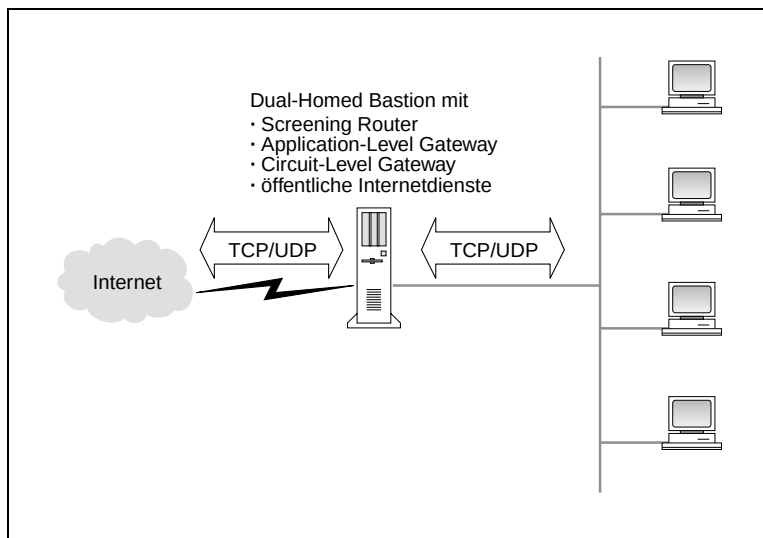
25.2.3 FireWall-Architekturen

FireWall-Installationen bestehen in der Regel aus einer Kombination der vorgestellten Basistechniken. Im wesentlichen existieren dabei zwei Architekturen: die Dual-Homed Bastion und das Screened Subnet.

Dual-Homed Bastion

Bei der Dual-Homed Bastion sind alle Mechanismen auf einem Computer integriert. Zusätzlich zu den schützenden Komponenten wie Screening Router und den entsprechenden Gateways werden auch die Internet-Services, die öffentlich erreichbar sein sollen, installiert. Die Bastion stellt den einzigen Schutz des LAN dar. Wird er überwunden, liegt das Netzwerk schutzlos offen. In Abbildung 25.3 ist der Aufbau eines Internet-Anschlusses gezeigt, wenn eine Dual-Homed Bastion verwendet wird.

Abbildung 25.3
Der Einsatz einer
Dual-Homed-
Bastion



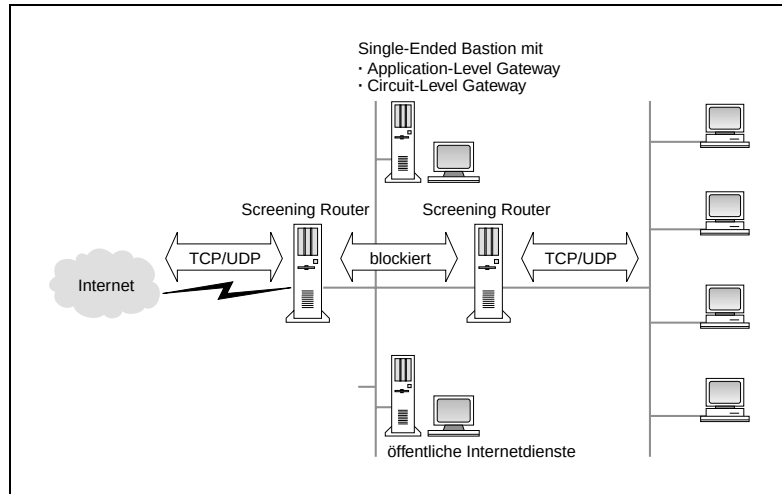
Screened Subnet

Das Screened Subnet besteht aus einem durch Screening Router isolierten Teilnetz zwischen LAN und Internet. In diesem Teilnetz werden sowohl die Application-Level und Circuit-Level Gateways als auch die Internet-Server mit den öffentlich zugänglichen Diensten platziert. Der direkte Paketfluß zwischen den Routern wird unterbunden. Auf diese Weise überwachen die Gateways den Datenaustausch, und das interne Netzwerk bleibt nach außen weitgehend unsichtbar.

25 Internet/Intranet und Internet Security

Selbst wenn die Filter des äußeren Routers überwunden werden, existiert zum internen Netzwerk eine weitere Hürde. Durch die Verteilung der Aufgaben auf mehrere Rechner läßt sich dieses System besser skalieren. In Abbildung 25.4 ist dargestellt, wie ein Screened-Subnet-System aufgebaut werden kann.

Abbildung 25.4
Der Screened-Subnet-Aufbau



Bei der Auswahl eines FireWall-Systems sollten diese Mechanismen und technischen Feinheiten beachtet werden, um nicht nur irgend ein FireWall-System zu haben, sondern das richtige. Da es auf dem Markt unterschiedliche Anbieter gibt, die auch unterschiedliche Mechanismen (wie oben beschrieben) realisiert haben, ist vor dem Einsatz eines solchen Systems genau zu untersuchen, ob die gestellten Anforderungen erfüllt werden und ob vor allem die Erweiterbarkeit für die Zukunft gegeben ist.

Ein FireWall-System ist in etwa so beständig wie ein Virenschutzprogramm, d.h., es muß immer wieder auf den aktuellen Stand gebracht werden. Der Hersteller ist dafür verantwortlich, auf neue Probleme mit seinem Produkt zu reagieren.

Seit kurzem wird nicht nur über Internet geschrieben und diskutiert, sondern es wird immer mehr über eine vollständig neue Technik und logische Netzwerkstruktur gesprochen: Es geht um das sogenannte Intranet. Da es sich anscheinend um eine zukunftssträchtige Netzwerkphilosophie handelt, soll im nächsten Abschnitt näher erläutert werden, was man sich unter einem Intranet vorstellen muß und welche Möglichkeiten damit verbunden sein werden.

25.3 Der Einsatz eines Intranet

Unter einem Intranet ist die Implementierung der Internet-Technologie im eigenen Unternehmen zu verstehen, wobei in diesem Fall die externe Kommunikation zum externen Internet zwar in Frage kommen kann, aber nicht das primäre Ziel ist. Für den Aufbau der Intranet-Technologie auf Basis der Internet-Technik sprechen mehrere Gründe:

- *Universelle Kommunikation*

Jeder Mitarbeiter und jede Abteilung kann durch den Einsatz einer einheitlichen Technologie mit jedem anderen Mitarbeiter und jeder anderen Abteilung kommunizieren.

- *Performance*

Auf Basis eines schnellen Netzwerks werden über die Intranet-Techniken nicht nur herkömmliche Daten transportiert, sondern auch Videos, Sprache etc. Durch die Internet-Technik hat man Erfahrungen damit, effektiv Grafiken und/oder Bilder etc. zu transportieren. Wenn man vergleicht, welche »geringen« Datenmengen im Internet für solche Datenbestände benötigt werden, kann man nur Vorteile daraus ziehen.

- *Zuverlässigkeit*

Durch den Aufbau des großen Internet hat man schon die entsprechende Erfahrung, ausgereifte und sichere Techniken einzusetzen.

- *Kosten*

Im Vergleich zu anderen Techniken erhält man die Internet-Techniken zum Aufbau unternehmensweiter Intranets zu sehr günstigen Preisen.

- *Standards*

Durch die Anpassung der Standardprotokolle und APIs wie MIME, Windows Sockets, TCP/IP, FTP und HTML steht eine Vielzahl von Werkzeugen und Anwendungen zur Verfügung, die auch beim Aufbau von Intranets erfolgreich genutzt werden können. Mit den oben aufgeführten Techniken lassen sich die nachfolgend aufgezeigten typischen Einsatzgebiete realisieren. Es sei darauf hingewiesen, daß es sich dabei erst um den Anfang der Entwicklung handelt, da im Prinzip täglich neue Komponenten und Anwendungen angeboten werden.

- *Veröffentlichung gemeinsamer Dokumente*

Wenn es darum geht, schnell und zuverlässig notwendige Informationen im Netz zu verbreiten bzw. bekanntzugeben, eignen sich die Techniken des Intranet besonders gut. Es kann sich dabei um Newsletter, Jahresberichte, Preislisten, Produktinformationen o.ä. handeln.

25 Internet/Intranet und Internet Security

■ *Zugriff auf »verknüpfte« Directories*

Aufgrund der Techniken, die mit der Web-Server-Technologie verbunden sind, hat jeder Anwender Zugang und Zugriff auf Informationen, Anwendungen oder auch aktuelle Dateien. Der Einsatz eines Web-Browsers erleichtert dabei die gesamte Handhabung zum Durchsuchen, Auffinden und auch Herunterladen der benötigten Daten. Bei genauer Betrachtung ist es durchaus denkbar, daß durch den Einsatz von HTML vollkommen neue Groupware-Produkte und -Umgebungen geschaffen werden.

■ *Software-Distribution*

Die Administratoren in einem Intranet können mit diesem System bei Bedarf auch Software-Produkte und Updates über das Netzwerk verteilen. Wenn sich die Entwickler mehr in Richtung Java orientieren, kann noch mehr Flexibilität auf diesem Gebiet erreicht werden. Auch hier ist davon auszugehen, daß die bislang bekannten Systeme zur Software-Distribution ein neues Gesicht erhalten werden. Hierfür sind jedoch die zukünftigen Entwicklungen abzuwarten.

■ *Mailing*

Wenn Mailing bereits für das Internet einer der essentiellen Mechanismen ist, so gilt dies natürlich auch für den Aufbau von Intranets. Fast alle guten Mailing-Systeme sind in der Lage, Übergänge für das Internet zu realisieren, das gilt natürlich auch für Intranets. Es gibt aber auch Mailing-Systeme, die standardmäßig auf SMTP aufsetzen und deshalb besonders gut in eine Intranet-Umgebung passen.

■ *Benutzerschnittstelle*

Wer bereits mit einem Web-Browser gearbeitet hat, der wird feststellen, daß man sich damit sehr schnell und einfach zurechtfindet. Die gesamte grafische Oberfläche und die hinterlegten Verknüpfungen führen dazu, daß man überhaupt nicht mehr wissen muß, wo sich die Informationen im Netzwerk befinden. Durch die hinterlegten Links in der HTML-Page muß nur noch auf den Link-Button geklickt werden, und im Hintergrund wird, für den Anwender vollkommen transparent, die Verbindung zur hinterlegten Information aufgebaut. Ebenso wie im Internet können die Links auf die unterschiedlichsten Server verweisen. Der einzige, der davon Kenntnis haben muß, ist derjenige, der die Web-Seite erstellt.

In den beiden folgenden Abbildungen ist beispielhaft dargestellt, wie die Web-Seite von Novell Deutschland und die von Microsoft aussieht. Die einzelnen Buttons und Icons dienen dazu, auf eine andere Web-Seite zu verzweigen. In den oberen Bildschirmleisten

25.3 Der Einsatz eines Intranet

kann einfach und bequem durch das Intranet (bzw. Internet) gewandert werden; im allgemeinen Sprachgebrauch ist dabei auch die Rede vom Surfen im Intranet bzw. Internet.

Abbildung 25.5
Die Web-Seite von
Novell Deutsch-
land

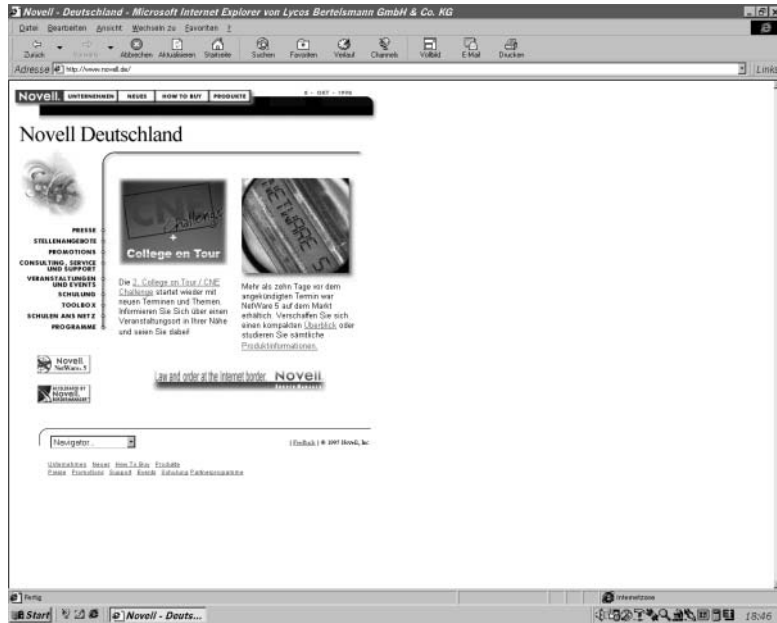
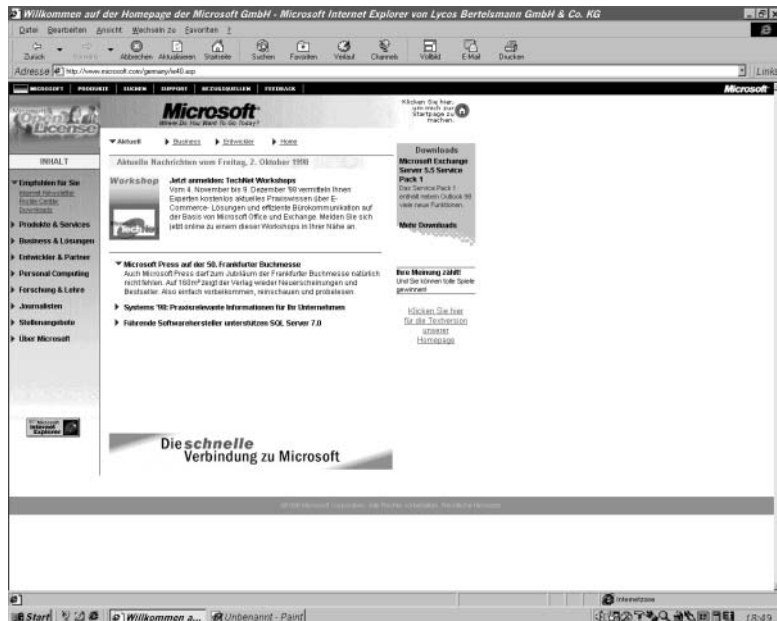


Abbildung 25.6
Die Web-Seite von
Microsoft



Die Implementierung von Intranets wird aber auch dadurch vorangetrieben, daß eine Vielzahl renommierter Hersteller Web-Server-Produkte anbieten. Wenn Sie die letzten beiden Bilder genau betrachten, nimmt sowohl bei Novell als auch bei Microsoft das Angebot des jeweiligen Web-Servers eine zentrale Stellung ein. Jeder versucht, passende Web-Server zu entwickeln, die nicht nur als Anwendung auf dem jeweiligen Netzwerkbetriebssystem laufen, sondern auch die Erstellung von Web-Seiten wesentlich vereinfachen. Bereits diese beiden Web-Seiten lassen eindeutig erkennen, wo derzeitige Schwerpunkte zu setzen sind bzw. von den jeweiligen Herstellern gesetzt werden.

Die bereits zuvor angesprochenen Schutzmechanismen auf der Basis eines FireWall-Systems können auch für ein Intranet von Bedeutung sein, um die Intranets einzelner Abteilungen vor anderen in einem Unternehmen zu schützen. Auch in einer Unternehmenskultur kann die Notwendigkeit bestehen, Sicherheit in gleicher Art und Weise zu implementieren, wie sie für das Internet benötigt wird. Die Ausführungen dieses Kapitels lassen erkennen, welche Bedeutung das Internet bzw. das Intranet erlangen wird bzw. teilweise schon erlangt hat. Auffallend an der gesamten Thematik ist, daß die Entwicklung sehr schnell voranschreitet. Kaum hat man sich an eine neue Technik gewöhnt, sind auch schon wieder neue Entwicklungen erkennbar. Es stellt sich da die Frage, ob man wirklich jede neue Entwicklung sofort mitmachen muß. Oft sind es aber Zwänge von außen, die dafür verantwortlich sind, daß die eine oder andere technologische Neuerung eingeführt werden muß.

In der letzten Zeit liest man immer mehr über den Einsatz von VPN und die Vorteile, die damit verbunden seien. Es stellt sich deshalb die Frage, was sich hinter VPNs verbirgt, was man damit erreichen kann und was dabei beachtet werden muß. VPN ist die Abkürzung für Virtual Private Network. Damit sollen LANs über öffentliche Netze gekoppelt werden können, ohne daß man Sicherheit für das eigene private Netzwerk einbüßt.

25.4 Der Einsatz von VPN

Unter einem VPN versteht man ein privates »Datennetzwerk«, das zum Aufbau öffentliche Netzwerke dient, aber durch den Einsatz spezieller VPN-Komponenten ein privates Netzwerk betreibt. In den meisten Fällen verwendet man das Internet, um darüber VPNs zwischen Unternehmen aufbauen zu können. In einem herkömmlichen LAN-LAN-Verbund eines privaten Netzwerks werden die beiden Netzwerke über Router (Bridges) und Point-to-Point-WANs miteinander verbun-

25.4 Der Einsatz von VPN

den. Diese Point-to-Point-Verbindungen werden für den Kunden durch entsprechende Service Provider (Telekom, Arcor, Viag etc.) angeboten. Hierbei unterscheidet man in der Regel den Einsatz von Mietleitungen oder Festverbindungen. Die Verbindungen werden deshalb als private Verbindungen bezeichnet, weil die verfügbare Bandbreite ausschließlich für den Kunden bestimmt ist. Die notwendigen Hard- und Software-Komponenten und die gemietete Datenleitung, das WAN-Protokoll inklusive der notwendigen Managementfunktionen bilden die private WAN-Infrastruktur.

Bei einem VPN werden alle privaten WAN-Infrastrukturen – mit einer Vielzahl von TCP/IP-basierten Dienstumgebungen – oder Teile davon vom Netzwerk-Service-Provider angeboten. In einer minimalen VPN-Umgebung wird das Unternehmen die Point-to-Point-Verbindungen gegen gemeinsam genutzte IP-Backbone-Verbindungen des Netzwerk-Service-Providers austauschen.

Die Komponenten zum Aufbau der WAN-Infrastruktur werden somit ausschließlich vom Netzwerk-Service-Provider zur Verfügung gestellt. Die installierten Komponenten im LAN, wie LAN Switches, Shared Hubs, Netzwerk-Server und Router, werden von der Arbeitsweise des VPN nicht beeinflusst. VPNs sind deshalb Endgeräte bzw. Endgeräte-Anwendungen, die unabhängig vom internen Campus-Netzwerk arbeiten.

Der am weitesten verbreitete Einsatz von VPN-Verbindungen dient der Kopplung von LANs zweier Unternehmensstandorte über das Internet. Wenn man sich mit der Tatsache abfinden kann, keine garantierte Bandbreite zur Verfügung zu haben (das ist derzeit über das Internet etwas schwierig), dann hat man hiermit eine sehr gute Möglichkeit, kostengünstig eine LAN-Kopplung durchzuführen. Da die getrennten Unternehmensstandorte zumeist einen eigenen Internet-Zugang besitzen, stellt sich berechtigterweise die Frage, warum man diesen nicht gleich auch noch für andere Zwecke, wie eben LAN-LAN-Kopplung über VPN, nutzen soll. Dies spart Kosten, weil man keine zusätzlichen Leitungen für die LAN-LAN-Verbindung anmieten muß. Andererseits kann es dann aber auch passieren, daß es schlechte Antwortzeiten gibt oder Verbindungen unter Umständen nicht sofort zustande kommen können.

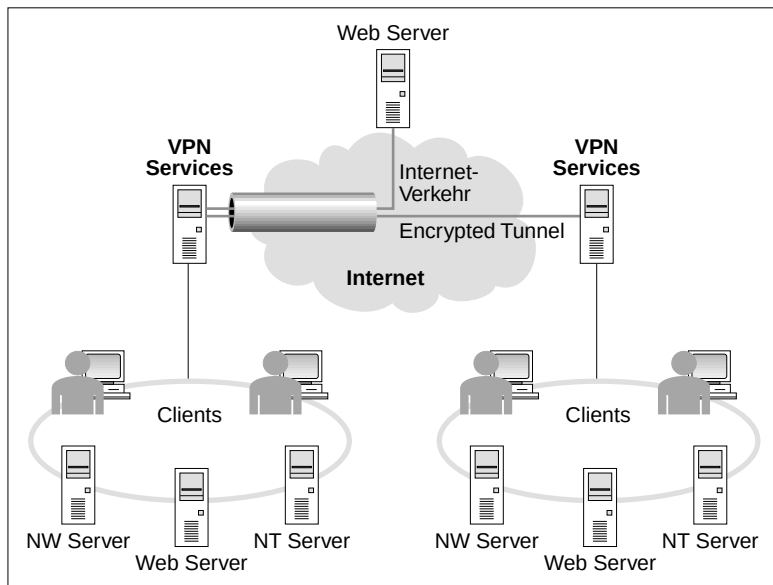
Damit die Kopplung von LANs über öffentliche Netze sicherer wird – gerade das Internet erweckt in diesem Zusammenhang nicht unbedingt das größte Vertrauen –, werden bei der VPN-Technik Lösungen eingebaut, bei denen eine Datenkommunikation über einen »Encrypted Tunnel« realisiert wird, d.h., VPN basiert auf Tunneling-Mechanismen, welche die Verbindungen zwischen zwei oder mehreren verteilten LANs herstellen.

25 Internet/Intranet und Internet Security

In Abbildung 25.7 ist der prinzipielle Aufbau eines VPN-Netzwerkes mit Hilfe des Internet dargestellt.

Die VPN-Sicherheit wird dabei in der Regel im Router eingebaut, mit der die Anbindung an das Internet durchgeführt wird; es ist aber auch möglich, daß der VPN-Mechanismus im FireWall-System implementiert wird.

Abbildung 25.7
Tunneling-Verfahren
beim Einsatz
von VPN



Das Tunneling-Verfahren unterstützt dabei für die meisten Implementierungen das IP- und das IPX-Protokoll als Point-to-Point-WAN-Verbindung. Abhängig von den angebotenen VPN-Mechanismen wird bei diesem Tunneling-Verfahren die Datenübertragungsrate verbessert, da zusätzlich Kompressionsverfahren und effiziente WAN-Routing-Verfahren eingesetzt werden, um hohe Übertragungsraten über VPN erzielen zu können.

Somit ist es auch problemlos möglich, daß bei einer IP-/IPX-Tunneling-Unterstützung NetWare-Netzwerke oder Windows-NT-Netzwerke über das IPX-Protokoll miteinander kommunizieren, obwohl als Datenübertragungsmedium das IP-basierende Internet verwendet wird – Tunneling ermöglicht dies.

Um nun die Sicherheit zu erhöhen, kann man nicht einfach ein VPN-System mit einem anderen VPN-System koppeln. Das entsprechende Verfahren, um Sicherheit für die Einbindung in einen solchen Verbund zu gewähren und eine Verschlüsselung beim »Encrypted Tun-

25.4 Der Einsatz von VPN

nel« zu erreichen, kann von Hersteller zu Hersteller etwas anders funktionieren. Ein mögliches Verfahren ist beispielsweise nach dem sogenannten Master/Slave-Prinzip aufgebaut. In diesem Falle wird das erste VPN-System als Master-VPN installiert und erzeugt dabei einen Master-Schlüssel. Dieser Master-Schlüssel wird verwendet, um die Einbindung der weiteren VPN-Systeme, die dann als Slave-System bezeichnet werden, durchzuführen. Das heißt, bei der Installation eines VPN-Slave-Systems benötigt man den Master-Schlüssel, und nach der Integration bzw. Installation wird daraus ein Slave-Schlüssel erzeugt. Dieser Slave-Schlüssel wird anschließend verwendet, um auf dem Master-System diesen Slave-Schlüssel einzubinden. Ab diesem Zeitpunkt weiß der Master, welche Slaves existieren, und die Slaves wissen, wer der jeweilige Master ist. Nur durch den Austausch dieser generierten Informationen ist man in der Lage, eine VPN-Verbindung zwischen diesen Systemen herzustellen. Zu beachten ist, daß die derzeit angebotenen VPN-Lösungen meist proprietär sind und es nicht unbedingt erforderlich ist, daß die Lösung A und die Lösung B zusammenarbeiten können. Außerdem ist es möglich, daß die eingesetzten Sicherheitsmechanismen stark variieren. Es laufen auch bereits Entwicklungen und Implementierungen, die es ermöglichen, über einen VPN-Client auf der Workstation das Internet zu nutzen, um sich im Netzwerk eines Unternehmens anmelden zu können. In diesem Falle benötigt man nur ein entsprechendes VPN-System im Unternehmensnetzwerk, einen VPN-Client auf der Workstation und einen Zugang der Workstation (und des Unternehmens-LAN) zum Internet. Wenn dies dann entsprechend konfiguriert ist, kann der Client einen herkömmlichen Login durchführen und so arbeiten, als wäre er direkt im Netzwerk des Unternehmens eingebunden. Das heißt, es fallen in diesem Falle alle Remote-Access-Mechanismen, die man hierfür zusätzlich installieren müßte, weg. Der Home-Arbeitsplatz kann somit immer eleganter eingerichtet und abgesichert werden.

Zum Schluß sei noch angemerkt, daß man die VPN-Technologie zum Teil auch als Extranet bezeichnet. Wir haben somit Internet, Intranet und Extranet.

26

Electronic-Mail-Systeme

Es wurde schon darauf verwiesen, welche Bedeutung den E-Mail-Systemen im Zuge einer LAN-Installation und eines LAN-Verbundes beizumessen ist. Da für die E-Mail-Systeme auch Aspekte und Funktionen von Groupware zu berücksichtigen sind, sollen in diesem Kapitel deren Grundlagen behandelt werden. Anschließend sollen hierfür zwei weitverbreitete Produkte dargestellt werden: GroupWise von Novell und Microsoft Exchange Server.

Das OSI-Referenzmodell wurde von der ISO mit dem Ziel definiert, die Kommunikation in einem offenen System zwischen heterogenen realen Systemen zu standardisieren. Unter realen Systemen werden beispielsweise Rechner bzw. Anwendungsprozesse verstanden, die einen Informationsaustausch mit anderen realen Systemen durchführen. Der Austausch von Informationen wurde inzwischen auch für menschliche Anwender und deren Nachrichten erweitert. Die Anwender verwenden dazu die Dienste des Mitteilungs-Übermittlungs-Systems.

Das Mitteilungs-Übermittlungs-System (Message Handling System, MHS) stellt Anwendungen und Dienste bereit, mit denen man – ähnlich wie bei der gewohnten Post – Briefe oder Nachrichten elektronisch erstellen und versenden kann.

Zur Unterstützung bzw. Förderung der Kompatibilität sowie zum Erreichen einer weltweiten Standardisierung der elektronischen Nachrichtenübermittlung wurde die sogenannte X.400-Empfehlung veröffentlicht.

26.1 Der CCITT-X.400-Standard

Der X.400-Standard ist eine CCITT-Empfehlung (Comité Consultatif International Téléphonique et Télégraphique) der X-Serie für Datenübermittlungsnetze und der Oberbegriff für Mitteilungsübermittlungsnetze.

Die CCITT, eine Vereinigung internationaler Postorganisationen und Telekommunikationsfirmen, veranstaltete 1984 ihre VIII. Vollversammlung; deren Ergebnisse wurden in den *Rotbüchern* festgehalten, die folgende Empfehlungen beinhalten:

26 Electronic-Mail-Systeme

- *X.400-Mitteilungs-Übermittlungs-Systeme*
Systemmodell dienstelemente der Schichten
- *X.401-Mitteilungs-Übermittlungs-Systeme*
Basisdienstelemente und wahlfreie Leistungsmerkmale
- *X.408-Mitteilungs-Übermittlungs-Systeme*
Kodierte Informationsregeln der Umsetzung
- *X.409-Mitteilungs-Übermittlungs-Systeme*
Syntax der Darstellung und der Notation
- *X.410-Mitteilungs-Übermittlungs-Systeme*
Zusammenwirken zwischen den Schichten
- *X.411-Mitteilungs-Übermittlungs-Systeme*
Schicht für den Transfer von Mitteilungen
- *X.420-Mitteilungs-Übermittlungs-Systeme*
Schicht für die interpersonelle Mitteilungsübermittlung
- *X.430-Mitteilungs-Übermittlungs-Systeme*
Zugangsprotokoll für Teletex-Terminals

Diese Empfehlungen, in der Literatur als X.400(84)-Standard bezeichnet, wurden aufgrund einiger Schwächen im Jahr 1988 von der IX. Vollversammlung der CCITT in Kooperation mit der ISO in ihren Funktionen erweitert. Die Erweiterung wurde in den *Blaubüchern* publiziert und ergab die nachstehende Umorganisation der Normendokumente:

- *X.400-Mitteilungs-Übermittlungs-Systeme*
Systemmodell und Überblick über Dienste (ISO 10021-1)
- *X.402-Mitteilungs-Übermittlungs-Systeme*
Gesamte Architektur (ISO 10021-2)
- *X.403-Mitteilungs-Übermittlungs-Systeme*
Conformance Testing
- *X.407-Mitteilungs-Übermittlungs-Systeme*
Konventionen der abstrakten Dienstedinitionen (ISO 10021-3)
- *X.408-Mitteilungs-Übermittlungs-Systeme*
Konvertierungsregeln für kodierte Informationen
- *X.411-Mitteilungs-Übermittlungs-Systeme*
Definition der abstrakten Dienste und Prozeduren (ISO 10021-4)
- *X.413-Mitteilungs-Übermittlungs-Systeme*
Meldungsspeicher: Definition der abstrakten Dienste (ISO 10021-5)
- *X.419-Mitteilungs-Übermittlungs-Systeme*
Protokollspezifikationen (ISO 10021-6)
- *X.420-Mitteilungs-Übermittlungs-Systeme*
System der interpersonellen Mitteilungsübermittlung (ISO 10021-7)

26.1 Der CCITT-X.400-Standard

Die folgenden Abschnitte geben Ihnen einen Überblick über den grundsätzlichen Aufbau und die Funktionen des CCITT-X.400-Standard-MHS bzw. des ISO MOTIS (Message Oriented Text Interchange System), wie das ISO-Pendant bezeichnet wird.

26.1.1 Das funktionale X.400-Modell

In einem X.400-System wird die grafische Schnittstelle zum Benutzer (User) mit einem sogenannten User Agent (UA) realisiert. Der UA, ein Anwendungsprozeß, liefert die Funktionen zum Erstellen, Versenden, Empfangen oder Archivieren von Nachrichten und wird auf der Arbeitsstation des Benutzers implementiert. Dieser User Agent gibt die erstellte Nachricht über einen Message Transfer Agent (MTA) an das Nachrichtenübermittlungssystem (Message Transfer System, MTS) weiter. Das MTS bezeichnet dabei die Gesamtheit aller in einem System verbundenen MTAs, die Transportdienste für den Benutzer zur Verfügung stellen. Der MTA agiert als Schnittstelle zum MTS, übernimmt die Nachrichten vom UA und leitet sie entweder direkt an den lokalen Ziel-UA oder über einen, unter Umständen auch mehrere MTAs, an den entfernten MTA des Empfängers weiter. Der Ziel-MTA übermittelt die Nachricht seinerseits mit Hilfe des UA an den Briefkasten (Mailbox, Inbox) des Empfängers.

Die MTA-Funktionen werden meist auf einem Server eines LAN, auf einem Gateway oder auch auf Host-Systemen implementiert. Zu den Funktionen zählt der Store-and-Forward-Mechanismus, der eine Nachricht so lange zwischenspeichert, bis sie weitergeleitet oder als unzustellbar (nondeliverable, NDR) deklariert wird, wovon der Sender in Kenntnis gesetzt wird.

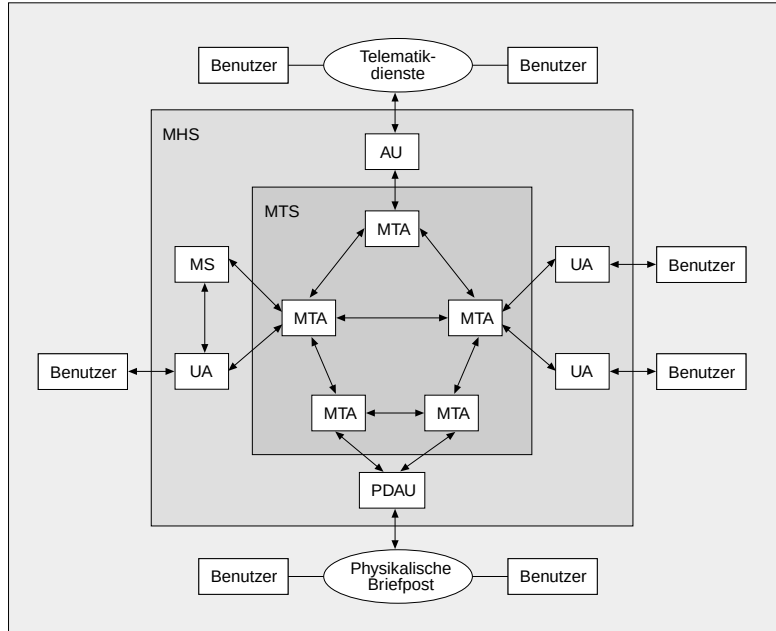
Das funktionale Modell des X.400(84)-MHS wurde, wie bereits angesprochen, in der X.400(88)-Empfehlung modifiziert und um einige Objekte erweitert. Dazu zählen die Access Unit (AU), die Physical Delivery Access Unit (PDAU) und das Message Store (MS). Das funktionale Modell dieses X.400(88)-MHS wird in der nachfolgenden Abbildung dargestellt.

Die Objekte AU und PDAU sind die Anschlußerweiterung zu anderen externen Telematik-Diensten. Die PDAU ermöglicht beispielsweise die Anbindung an die physikalische Briefpost, indem die Nachricht ausgedruckt wird. Die AU kann hingegen als Gateway zu anderen Mailing-Systemen, wie dem Internet, sowie weiteren Telematik-Diensten, wie Faximile (Fax) oder Teletex, gesehen werden.

Der ebenso neu spezifizierte Meldungsspeicher bietet wichtige Erweiterungen des X.400(84)-Systems zur Archivierung bzw. zur Zwischenspeicherung von Mitteilungen.

26 Electronic-Mail-Systeme

Abbildung 26.1
Das funktionale
X.400-Modell



26.1.2 Meldungsspeicher (Message Store, MS)

Der Meldungsspeicher (Message Store, MS), auch als Nachrichtenspeicher bezeichnet, löst das große Problem des Archivierens und der ständigen Verfügbarkeit eines UA. Viele UAs sind auf Single-User-Systemen implementiert, z. B. einem PC oder einer Workstation, die meist nicht rund um die Uhr betriebsbereit sind. Aus diesem Grund wurde in der X.400(88)-Spezifikation eine Lösung definiert, die zwischen einem MTA und einem UA liegt und die Nachrichten so lange zwischenspeichert, bis sie vom Benutzer über den UA abgerufen werden. Der Nachrichtenspeicher kann aber auch als Zwischenspeicher für die Nachrichtenübermittlung von einem UA zu einem MTA eingesetzt werden.

Der Message Store bietet datenbankähnliche Funktionen, indem es erhaltene oder zu versendende Nachrichten in unterschiedliche Informationsbasen ablegt. Die Nachrichten werden in den Informationsbasen als Einträge (Entries, Items) gehalten, die durch mehrere Attribute und deren Werte näher spezifiziert werden.

Obwohl dieser MS, der UA und auch der MTA völlig unterschiedliche Anwendungen darstellen, können sie physikalisch gemeinsam auf einem Rechner realisiert werden. Das hängt jedoch im wesentlichen davon ab, wie vom Hersteller die Implementierung durchgeführt

26.1 Der CCITT-X.400-Standard

worden ist. Zusätzlich muß bei produktiven Systemen geprüft werden, ob es aus Performance-Gründen sinnvoll ist, eine vollständige Implementierung auf nur einem System durchzuführen.

Das eben beschriebene Modell des X.400-MHS wurde hauptsächlich für die verbindungslose Übermittlung von Informationen wie Text, Sprache oder Grafiken zwischen Anwendungen ausgelegt. Für die spezielle Informationsübermittlung zwischen Personen (Benutzern) wurden die Dienste dieses Systems funktional erweitert. Es entstand das Interpersonal Messaging System (IPMS), das in der Empfehlung X.420 näher beschrieben wird.

Zu den erweiterten Diensten wurden dem System auch weitere Objekte hinzugefügt. Zu diesen Objekten zählen beispielsweise der IPMS-User Agent (IPMS-UA), das IPMS-Message Store (IPMS-MS), der Telematic Agent (TLMA) und die Telex Access Unit (TLXAU).

26.1.3 X.400-Nachrichtenstruktur

Die Struktur einer elektronisch zu versendenden Nachricht hat sehr viel Ähnlichkeit mit der eines herkömmlichen Briefs. Die Nachricht (Message) besteht aus einem Umschlag (Envelope), der mit der Adresse des Absenders (Originator) und des Empfängers (Recipient) versehen wird. Der Umschlag liefert mit der Empfängeradresse die vom MTS benötigten Adressierungs- und Routing-Informationen. In diesem Umschlag steckt die eigentliche Mitteilung, deren Daten vom MTS transparent behandelt werden, da sie für das MTS nicht relevant sind. Der wesentliche Vorteil des IPMS spiegelt sich in der erweiterten Grundstruktur dieser Mitteilung wider. Die interpersonelle Mitteilung (Interpersonal Message, IPM), oft auch als P2-Inhaltstyp bezeichnet, setzt sich im Gegensatz zur früher eingesetzten Nachrichtenstruktur aus dem Nachrichtenkopf (Header, Heading) und dem Nachrichtenkörper (Body) sowie dessen Inhalt (Content) zusammen.

Abbildung 26.2 zeigt den prinzipiellen Aufbau einer IPM und die Analogie zur Briefpost.

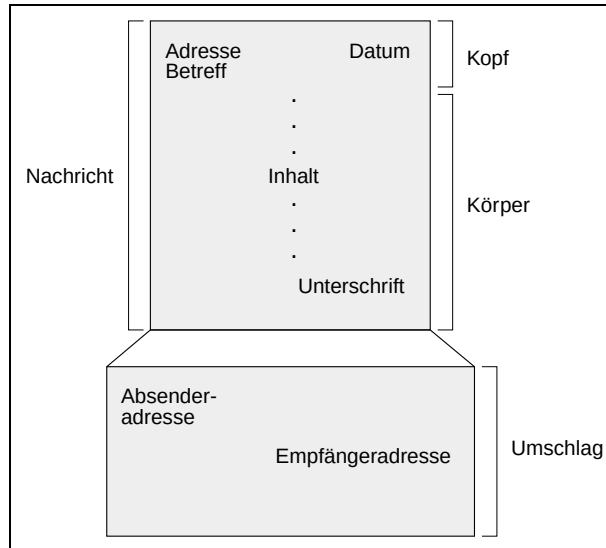
Der Header enthält Informationen über den Absender der Nachricht und besteht aus mehreren Header-Feldern. Diese Header-Felder, die der Absender ausfüllen muß bzw. zum Teil optional ausfüllen kann, werden durch Schlüsselwörter spezifiziert. Die Schlüsselwörter und deren Bedeutungen werden im folgenden erklärt.

This IPM

Jeder Nachricht wird durch das Transportsystem eine eindeutige Identifikation zugeteilt, die in diesem Feld gespeichert wird.

26 Electronic-Mail-Systeme

Abbildung 26.2
Die Struktur einer
X.400-IPM-
Nachricht



- Originator** Im Feld Originator wird automatisch die Adresse des Absenders eingetragen. In den User Agents der meisten Mailing-Systeme wird dieses Feld mit From bezeichnet. Damit weiß man immer, von wem die Post kommt.
- Authorizing Users** Dieses Header-Feld beinhaltet den Namen der Person, die das Senden der Nachricht autorisiert hat.
- Primary Recipients** In dieses Feld, in dem ein Eintrag zwingend erforderlich ist, werden alle Empfänger eingetragen, die als Empfänger der Nachricht dienen sollen. Die Adressen werden durch ein Komma oder durch einen Strichpunkt getrennt. Dem Benutzer eines User Agent zeigt sich dieses Feld meist mit dem Schaltknopf (Button) To.
- Copy Recipients** Den im Copy-Feld eingetragenen Adressen wird eine Kopie der Nachricht zur Kenntnisnahme übertragen. Dieses Feld wird meist mit Carbon Copy (CC) betitelt. Der Empfänger kann auch feststellen, wer die Nachricht zur Kopie erhalten hat.
- Blind Copy Recipients** Die Empfänger der Adressen, die in diesem Feld hinzugefügt werden, erhalten ebenfalls eine Kopie der Nachricht. Allerdings sind die Adressen dieser Empfänger für die To- und CC-Empfänger nicht ersichtlich. Dieses Feld wird meist Blind Carbon Copy (BCC) genannt.
- Replied to IPM** Bezieht sich eine Nachricht auf eine bereits früher erhaltene Nachricht, wird diese in dem Replied-to-IPM-Feld dargestellt. In diesem Fall kann davon ausgegangen werden, daß es sich um die Antwort auf eine zuvor erhaltene Nachricht handelt.

26.1 Der CCITT-X.400-Standard

Obsoleted IPMs	In diesem Feld werden Nachrichten aufgezeigt, die durch die neu erhaltene Nachricht obsolet werden.
Related IPMs	Stehen bestimmte Nachrichten in einem Zusammenhang mit der eben erhaltenen Nachricht, können sie über dieses Feld spezifiziert werden.
Subject	Dieses Feld gleicht der Betreffzeile in einem herkömmlichen Brief und sollte den Inhalt der Nachricht kurz beschreiben. Dem Benutzer wird mit jeder eingehenden Nachricht der Inhalt dieses Felds angezeigt, um bereits vor Öffnen der Post zu wissen, um was es sich handelt. Man kann somit die Entscheidung treffen, ob man die Post gleich oder erst später lesen will.
Expire Time	Expire Time gibt den Zeitpunkt an, ab dem eine Nachricht als ungültig bzw. gegenstandslos betrachtet werden kann.
Reply Time	Mit der Reply Time wird dem Empfänger eine bestimmte Zeitspanne für das Absenden einer erwünschten Antwort vorgeschlagen.
Reply Recipients	Wird auf die gesendete Nachricht eine Antwort erwartet, kann der Sender in dieses Feld die Empfängeradressen eintragen, die eine Antwort erhalten sollen. Die Antwort wird normalerweise dem Sender der Nachricht zugesandt. Im Subject-Feld der Antwort wird dabei die Betreffzeile mit dem vorangestellten RE: (Reply) gekennzeichnet.
Importance	Die Wichtigkeit einer Nachricht kann dem Empfänger mit unterschiedlichen Abstufungen (hoch, normal oder niedrig) verdeutlicht werden.
Sensitivity	Unterliegt eine versendete Nachricht einer bestimmten Vertraulichkeitsstufe, kann diese hier eingestellt und dem Empfänger mitgeteilt werden.
Auto Forwarded	Dieses Feld zeigt dem Empfänger, daß die Nachricht von einem UA automatisch weitergeleitet wurde. Im Subject-Feld der weitergeleiteten Nachricht wird hier die Betreffzeile mit dem vorangestellten FW: für Forward gekennzeichnet.
Extensions	Sollen zusätzliche Informationen an den Empfänger übermittelt werden, können sie optional in das Extensions-Feld eingefügt werden. Der Body einer IPM-Nachricht beinhaltet den eigentlichen Nachrichtentext und teilt sich in mehrere Bodyparts auf. Diese Bodyparts können verschiedene Mitteilungstypen zum Inhalt haben. Zu diesen zählen zum Beispiel Text, Grafiken, Voice oder auch OLE-Objekte (Object Linking and Embedding). Es sei an dieser Stelle angemerkt, daß nicht in jedem Mailing-System all diese Felder implementiert sind bzw. nicht jedes diese implementiert haben muß. Die Bedeutungen der einzelnen Felder sind aber immer die genannten, was die Oberflächenbedienung der Mailing-Systeme sehr einfach macht.

26.1.4 Namen und Adressen

Voraussetzung für eine weltweite Kommunikation mit Hilfe von E-Mail-Systemen ist die Verfügbarkeit eindeutig identifizierbarer Namen bzw. Adressen, so wie dies bei den Postdiensten auch der Fall ist.

Ein Name spezifiziert in einem MHS ein bestimmtes Objekt. Eine Adresse hingegen spezifiziert ein Objekt und gibt zugleich an, an welchem Ort dieses Objekt lokalisiert ist. Eine Adresse ist also auch ein Name; das Umgekehrte gilt dagegen nicht.

Diese präzise Unterscheidung ist erforderlich, da im X.400-Standard die Adressen der Objekte irreführenderweise als Originator/Recipient-Namen (O/R) bezeichnet werden, obwohl sie die Lokalität des Objekts repräsentieren. Neben diesen O/R-Namen könnten aber auch Directory-Namen verwendet werden. Das Verzeichnis und die damit zusammenhängende Namenskonvention werden zu einem späteren Zeitpunkt genauer erläutert.

Zum Erstellen dieser Adressen und für die unterschiedlichen Arten von MHS-Benutzern werden im X.400-Standard mehrere Adreßformate unterschieden.

- *Mnemonic O/R Address*

Mit der mnemonischen O/R-Adresse kann auf einfache Weise ein Benutzer oder eine Verteilerliste identifiziert werden. Die Art der Adressierung bezeichnet die von X.400 verwendete Standardadresse und ähnelt einem Directory-Namen (s. spätere Ausführungen über Directory Services).

- *Terminal O/R Address*

Die Terminal-O/R-Adresse definiert eine Adresse, die entsprechend der Netzwerkadresse des Endsystems generiert wird.

- *Numeric O/R Address*

Über diese O/R-Adresse kann ein Benutzer auf Basis einer numerischen Kombination adressiert werden.

- *Postal O/R Address*

Die Post-O/R-Adresse identifiziert einen Benutzer mit Hilfe der üblichen Postadresse. Dieses Adreßformat ermöglicht also auch die Zustellung einer Nachricht über den gewohnten Postweg.

Die X.400-O/R-Adressen bestehen aus einem Satz von Attributen, die das Objekt näher spezifizieren. Mit der Adresse wird versucht, die Lokalität des Objekts und die logische Struktur bzw. die Abbildung einer Organisation zu ermöglichen. Die folgende Tabelle gibt einen umfassenden Überblick über die von der CCITT definierten Attributstypen, ihre Beschreibung und die dafür verwendeten Schlüsselwörter.

26.1 Der CCITT-X.400-Standard

Schlüsselwort	Attributstyp	Beschreibung
C	Country Code	Länderkennung
A	Administration Domain	Öffentlicher Verwaltungsbereich
P	Private Domain	Privater Verwaltungsbereich
O	Organization	Organisation
OU	Organizational Unit	Organisationseinheiten
I	Initials	Initialen
G	Given Name	Vorname
S	Surname	Nachname

Die X.400-Originator/Recipient-Namen werden nach einer definierten Schreibweise bzw. Syntax konstruiert. Das folgende Beispiel soll zeigen, wie ein solches Konstrukt aussehen kann:

```
C=de;a=dbp;p=zenk;o=zenk_gmbh;ou=gl;g=andreas;s=zenk
```

Dieses Beispiel verdeutlicht die X.400-Adresse für den Geschäftsführer Andreas Zenk der Zenk GmbH. Die Organisation Zenk GmbH ist dabei im Land Deutschland lokalisiert und kann über die Verwaltungsbereiche Deutsche Bundespost und Zenk adressiert werden.

Einen wesentlichen Dienst, der ebenfalls mit dem Adressieren eines Objekts bzw. eines Benutzers zusammenhängt, stellt die Verteilerliste dar. Die Verteilerliste, die durch das MHS der X.400(88)-Spezifikation zur Verfügung gestellt wird, soll jetzt erläutert werden.

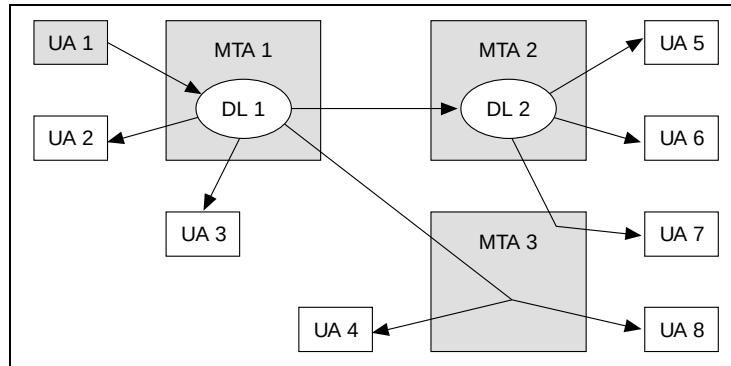
Verteilerliste (Distribution List, DL)

Die Verteilerliste (Distribution List, DL), manchmal auch als Gruppe bezeichnet, erlaubt einem MHS-Benutzer das gleichzeitige und einfache Adressieren mehrerer Empfänger. Die Verteilerliste beinhaltet die Adressen dieser Empfänger oder weiterer Verteilerlisten und wird lediglich mit einer eindeutigen Adresse (O/R-Name) identifiziert. Die Empfängeradressen der Verteilerliste werden von dem zuständigen MTA expandiert und an die entsprechenden UAs oder auch die MTAs entfernter UAs weitergeleitet. Das Prinzip der Verteilerliste ist in Abbildung 26.3 dargestellt.

Der UA 1 des oben dargestellten Beispiels übergibt eine Nachricht an den MTA 1. Dieser MTA 1 expandiert die Adresse der Verteilerliste DL 1 und leitet die Nachricht an den UA 2, UA 3, MTA 2 und auch an den MTA 3 weiter.

26 Electronic-Mail-Systeme

Abbildung 26.3
Die Anwendung
von Verteilerlisten



Der MTA 2 expandiert hingegen die DL 2 und sendet die Nachricht an die User Agents 5, 6 und 7. Die UAs 4 und 8 erhalten ihre Nachricht über den MTA 3.

Dieses Beispiel zeigt, daß eine Verteilerliste durchaus ihrerseits Verteilerlisten beinhalten kann (in einem System kann es darüber hinaus mehrere Verteilerlisten geben). Damit aber keine Schleife beim Adressieren einer Verteilerliste entstehen kann, wird am Ende einer Nachricht eine Verteilerlisten-Expansionsgeschichte angehängt. Mit dieser Expansionsgeschichte kann ein MTA eine bereits ausgeführte Expansion erkennen und den erneuten Expansionsprozeß verhindern.

26.1.5 Verfügbare Dienste

Die Dienste, die ein Mitteilungs-Übermittlungs-System einem Benutzer zur Verfügung stellt, werden über fest definierte Schnittstellen realisiert. Diese Schnittstellen, meist als Ports bezeichnet, können die Übertragung einer Nachricht erst nach dem Ausführen einer grundlegenden Operation beginnen. Diese Operation nennt sich MTS-Binde-Operation. Die Binde-Operation identifiziert einen UA und ermöglicht dessen Zugang zum MTS sowie die Bereitstellung der Dienste, die durch die nachfolgend erklärten Schnittstellen ermöglicht werden.

Mit der Loslöse-Operation kann dagegen der Zugang zum MTS über einen MTA unterbrochen oder unterbunden werden.

26.1 Der CCITT-X.400-Standard

- *Übertragungsschnittstelle*
Für das Weiterleiten (Relaying) einer Nachricht von einem MTA zu einem weiteren MTA des MTS wird die Übertragungsschnittstelle verwendet. Für diesen Dienst nutzt man das Nachrichtenübertragungsdienstelement (Message Transfer Service Element, MTSE) des Protokolls P1. Eine Erklärung dieser Protokolle erfolgt an anderer Stelle.
- *Übermittlungsschnittstelle (Submission Port)*
Über den Submission Port kann ein UA bzw. ein MS eine zu sendende Nachricht an einen Message Transfer Agent zum Weitertransport übergeben.
- *Belieferungsschnittstelle (Delivery Port)*
Mit Hilfe des Delivery Port wird eine Nachricht von einem MTA an den MS eines Empfängers übergeben.
- *Verwaltungsschnittstelle (Administration Port)*
Über diese Schnittstelle können benutzerspezifische Parameter wie der Name, die Adresse oder auch das Paßwort modifiziert werden.
- *Holschnittstelle*
Die Holschnittstelle stellt unterschiedliche Dienste zwischen einem UA und dessen MS zur Verfügung. Zu diesen Schnittstellen zählt beispielsweise ein Auswahlverfahren, mit dem nur bestimmte Nachrichten angezeigt und ausgegeben werden können.

26.1.6

Zeichensätze

Der Inhalt einer Mitteilung kann über unterschiedliche Zeichensätze kodiert werden. Eine wesentliche Aufgabe dabei ist, die Zeichensätze auch für den Empfänger lesbar und verständlich zu übermitteln. Im X.400-Standard sind für die korrekte Übertragung verschiedene Zeichensätze bzw. Nachrichtenformate relevant.

International Alphabet No.5 (IA5)

Beim internationalen Alphabet Nr. 5 (IA5) handelt es sich um einen 7-Bit-Code, der die wichtigsten Ziffern, Buchstaben, Steuerzeichen und auch Sonderzeichen enthält.

Für die internationale Angleichung wurde eine weitere Version dieses Zeichensatzes definiert. Diese internationale Referenzversion (IRV) entspricht dem US-ASCII-Zeichensatz.

Teletex (T.61)

Der Teletex-Zeichensatz (T.61) ist weit besser als der IA5-Zeichensatz für die Nachrichtenübermittlung geeignet, da dieser 8-Bit-Zeichensatz die Darstellung von 256 Zeichen ermöglicht.

Neben den oben erwähnten Zeichensätzen werden auch zahlreiche Nachrichtenformate unterschieden:

- Group 3 Fax (Dokumente der Gruppe 3)
- Group 4 Fax (Dokumente der Gruppe 4)
- Class 1 Fax
- Telex
- Videotext
- Voice
- Mixed Mode

Damit die Kooperation und die offene Kommunikation zwischen den realen Systemen ermöglicht werden konnten, wurde eine einheitliche Sprachgrundlage definiert, die in der CCITT-Empfehlung X.208 verabschiedet wurde. Diese Sprache (Syntax) bezeichnet man als Abstract Syntax-Notation One (ASN.1); sie ist für die Umwandlung der verschiedenen Datentypen sowie für ihre Kodierung zuständig. Bei der Beschreibung der Netzwerkmanagementsysteme wurde diese Sprache ebenfalls erwähnt, da die MIB-Definitionen die ASN.1 Notation ebenfalls nutzen.

26.1.7

Verwaltungsbereiche (Management Domains)

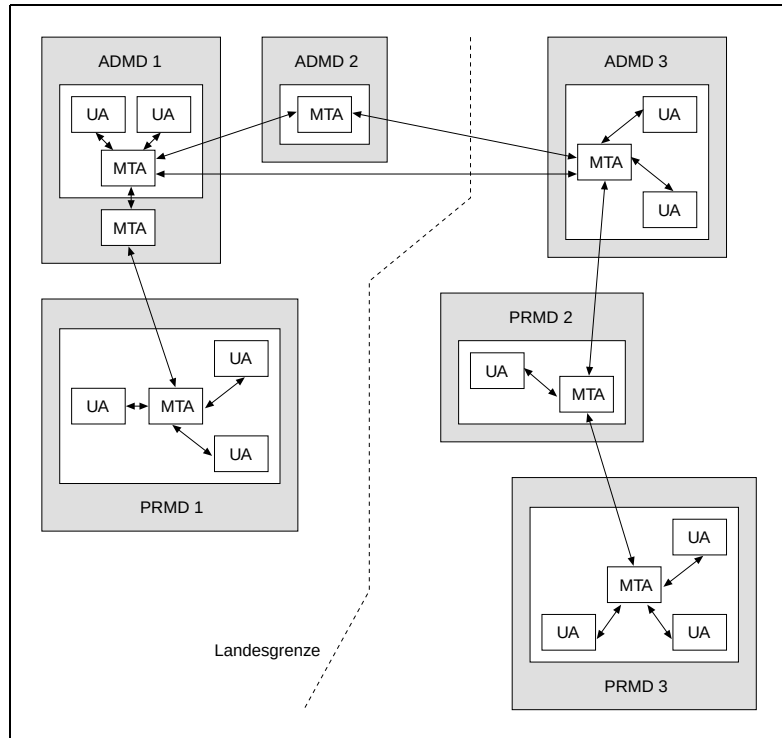
Die Verantwortung für die Organisation und die Verwaltung eines international verteilten Message Transfer System wird in sogenannte Verwaltungsbereiche (Management Domains, MDs) aufgeteilt, die auch als Versorgungsbereiche oder Führungsdomänen bezeichnet werden. Diese Domains beinhalten eine beliebige Anzahl von UAs sowie mindestens einen MTA. Zur internen Verantwortung einer Domain zählen dabei die zuverlässige Nachrichtenübermittlung sowie die optimale Wegwahl (Routing).

Die Aufteilung der Management Domains wurde anhand privater und öffentlicher Anbieter jeweils innerhalb eines Landes vorgenommen, das auch über die nationalen Abgrenzungen hinweg tätig werden kann.

Abbildung 26.4 zeigt ein organisatorisches MTS-Modell mit der Aufteilung in die zwei verschiedenen Verwaltungsbereiche Administration Management Domain (ADMD) und Private Management Domain (PRMD).

26.1 Der CCITT-X.400-Standard

Abbildung 26.4
Das Zusammen-
spiel von Admini-
stration Manage-
ment Domain und
Private Manage-
ment Domain



■ Öffentlicher Verwaltungsbereich (Administration Management Domain)

Der öffentliche Verwaltungsbereich (Administration Management Domain, ADMD) wird durch die nationalen Postgesellschaften (Postal, Telephone and Telegraphy, PTT) zur Verfügung gestellt. Eine ADMD ist verantwortlich für das Erbringen und Einhalten der zur Nachrichtenübermittlung benötigten Dienste sowie für die Vereinheitlichung und Normierung dieser Telekommunikationsdienste und -schnittstellen.

Zum Erbringen der Transferdienste verfügt die ADMD über Routing-Informationen zu anderen ADMDs oder PRMDs.

■ Privater Verwaltungsbereich (Private Management Domain)

Der private Verwaltungsbereich (Private Management Domain, PRMD) wird von Hochschulen und privaten Einrichtungen wie Firmen oder Unternehmen bereitgestellt. Diese nationalen Einrichtungen können als untergeordnete Einheit einer ADMD angesehen werden, da deren internationale Kommunikation vorerst nur über eine ADMD durchgeführt werden kann. In der ISO-Normierung 10021 ist allerdings die direkte Kommunikation zweier PRMDs über eine Landesgrenze bereits möglich.

26.1.8 Protokolle

Die Dienste des Message Handling System werden durch drei Protokolle zur Verfügung gestellt. Diese Protokolle sind vollständig in die Anwendungsschicht des OSI-Referenzmodells implementiert und integrieren darüber hinaus anwendungsspezifische Dienstelemente dieser Schicht.

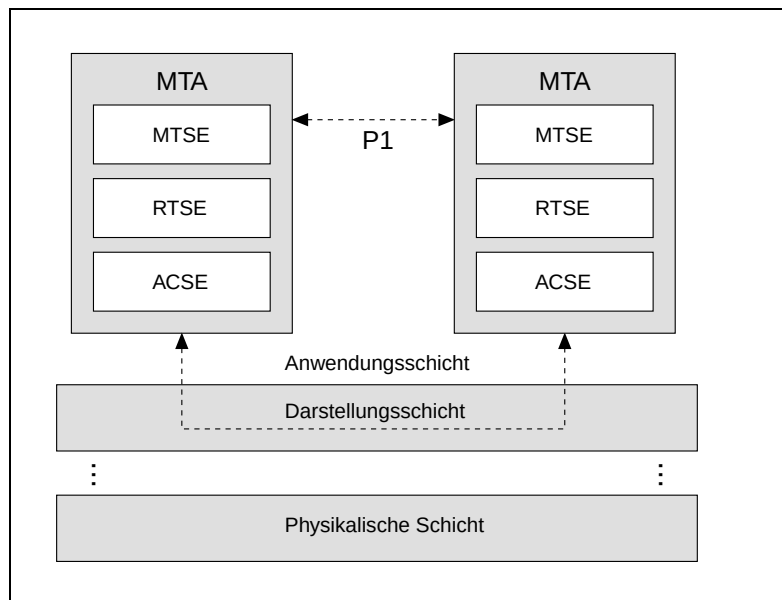
Solche allgemeinen Dienstelemente sind einzelne Unterteilungen der Anwendungsschicht, die für die offene Kommunikation sowie für die Bereitstellung der geforderten Dienste zuständig sind.

MTS-Übertragungsprotokoll (MTS Transfer Protocol, P1)

Das MTS-Übertragungsprotokoll (MTS Transfer Protocol, P1) wird für die interne Kommunikation zwischen den MTAs und den symmetrischen Store-and-Forward-Verbindungen eingesetzt.

Die Implementierung des MTS-Protokolls in die Schicht 7 des OSI-Referenzmodells wird durch Abbildung 26.5 veranschaulicht.

Abbildung 26.5
Das Protokollmodell für das MHS



Die Dienste des Nachrichtentransports, realisiert durch das Message Transfer Service Element (MTSE), werden für die Übertragung von Nachrichten im Message Transfer System eingesetzt. Das MTSE setzt dabei auf dem Reliable Transfer Service Element (RTSE) auf, das sich für die sichere Datenübertragung auf diesem Protokoll verantwort-

26.1 Der CCITT-X.400-Standard

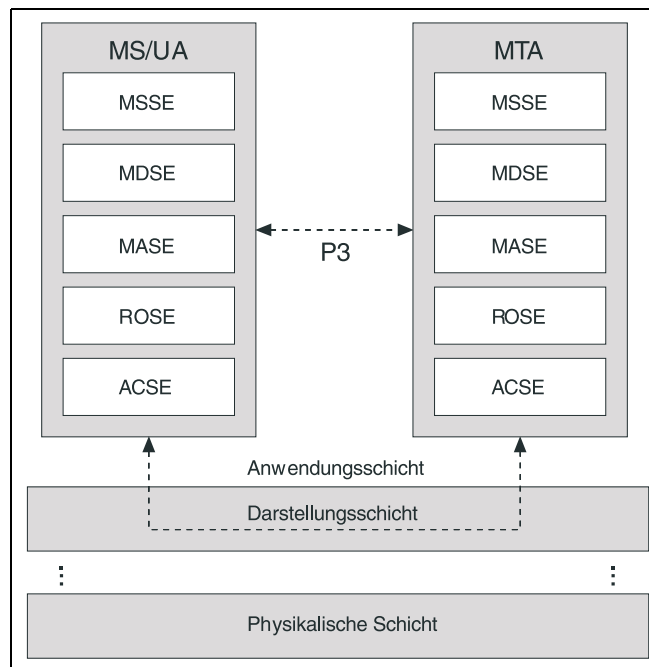
lich zeigt. Für die Steuerung des Auf- und Abbaus eines Anwendungsprozesses wird vom RTSE das Association Control Service Element (ACSE) verwendet.

MTS-Zugangsprotokoll (Message Transfer System Access Protocol, P3)

Die Kommunikation für den Zugang eines User Agent oder eines Message Store zum Message Transfer System wird über das MTS-Zugangsprotokoll (Message Transfer System Access Protocol, P3) durchgeführt. Über dieses Protokoll werden Nachrichten versendet bzw. empfangen sowie benutzerspezifische Parameter wie beispielsweise der Name oder auch das Paßwort modifiziert.

Das Protokoll P3 integriert anwendungsspezifische Dienstelemente (Service Elements, SEs), die durch die Übermittlungs-, Belieferungs- und Verwaltungsschnittstelle beschrieben werden.

Abbildung 26.6
Das Protokollmodell für den MTS-Zugang



Das in dem obigen Protokollmodell dargestellte Message Submission Service Element (MSSE) unterstützt die Dienste des bereits beschriebenen Submission Port. Die Dienste des Delivery Port werden durch das darunterliegende Message Delivery Service Element (MDSE) zur Verfügung gestellt. Für allgemeine Verwaltungsaufgaben werden die

26 Electronic-Mail-Systeme

Dienste des Administration Port über das Message Administration Service Element (MASE) angeboten.

Zusätzlich zu diesen Dienstelementen sind weitere Dienstelemente der Anwendungsschicht implementiert. Zu diesen zählen das Remote Operation Service Element (ROSE) und das Association Control Service Element (ACSE). ROSE dient für entfernte asymmetrische Tätigkeiten. ACSE wird dagegen für den Auf- und Abbau einer Anwendungs-Association benutzt. Für die detaillierte Erklärung dieser Dienstelemente verweise ich allerdings auf weiterführende Literatur.

MS-Zugangsprotokoll (Message Store Access Protocol, MSAP, P7)

Das MS-Zugangsprotokoll (Message Store Access Protocol, MSAP, P7), das im grundsätzlichen Aufbau dem Protokoll P3 ähnelt, dient der Kommunikation zwischen einem User Agent und dem für ihn zuständigen Message Store.

Auch in diesem Protokoll sind Dienste des Submission Ports implementiert. Umgesetzt werden die Dienste des Protokolls P7 auch durch das Message Submission Service Element (MSSE). Neben den Diensten des Retrieval Port, die durch das Message Retrieval Service Element (MRSE) angeboten werden, sind ebenfalls die Dienste des Administration Port mit Hilfe des Message Administration Service Element (MASE) realisiert.

Die Ähnlichkeit zum MTS Access Protocol zeigt sich auch durch die zusätzlich integrierten Dienstelemente für entfernte asymmetrische Tätigkeiten (ROSE) sowie für die Steuerung des Aufbaus und Abbaus (ACSE) eines Anfrageprozesses.

26.1.9

Sicherheitsmodell

Für die Kommunikation zwischen zwei oder mehreren UAs, die über Verbindungen im Message Handling System durchgeführt wird, werden unterschiedliche Sicherheitsvorkehrungen benötigt. Ähnlich wie in der Gelben Post, in der das Briefgeheimnis gebrochen werden kann, besteht auch in der elektronischen Post die Möglichkeit zur Spionage oder Manipulation. Damit diese Eingriffe verhindert werden können, sind unterschiedliche Sicherheitsdienstelemente implementiert, die nun kurz erläutert werden.

■ *Message Origin Authentication*

Mit diesem Dienstelement wird die Identität eines Senders sowie die Herkunft der Nachricht sichergestellt. Für dieses Dienstelement existiert auch eine strengere Form namens Nonrepudiation of Origin, die sowohl die Identität des Senders als auch die Herkunft der Nachricht gegenüber Dritten belegt.

26.1 Der CCITT-X.400-Standard

- *Data Integrity*
Die sichere Übermittlung einer Nachricht wird mit dem Dienst Data Integrity unterstützt. Damit kann der Empfänger überprüfen, ob die Nachricht während des Transports manipuliert wurde.
- *Data Confidentiality*
Soll wirklich nur der autorisierte Empfänger eine Nachricht lesen können, wird das mit Hilfe von Data Confidentiality ermöglicht.
- *Message Security Labeling*
Mit diesem Sicherheitselement kann eine Mitteilung mit einer bestimmten Klassifizierung bzw. einer definierten Sicherheitsmarke versehen werden.
- *Message Sequence Integrity*
Mit Message Sequence Integrity wird ermöglicht, daß die Sendereihenfolge von Nachrichten ersichtlich bleibt. Zudem ist sichergestellt, daß weder Nachrichten bzw. Nachrichtenteile fehlen noch dupliziert worden sind.
- *Proof of Delivery*
Ähnlich dem Einschreiben der Gelben Post wird mit Proof of Delivery bestätigt, daß eine Nachricht ordnungsgemäß an einen UA ausgeliefert wurde. Soll der Empfang auch gegenüber Dritten bestätigt werden, wird das Dienstelement Nonrepudiation of Delivery eingesetzt.
- *Proof of Submission*
Neben Proof of Delivery, bei dem der Empfang einer Nachricht bestätigt wird, existiert auch das Dienstelement Proof of Submission. Mit diesem Element wird die vorschriftsgemäße Übermittlung einer Nachricht von einem UA zu einem MTA bestätigt. Ebenso wie bei Message Origin Authentication und bei Proof of Delivery existiert auch für das Sicherheitselement Proof of Submission eine strengere Art des Dienstelements, das als Beweis gegenüber Dritten eingesetzt wird. Dieses Sicherheitsdienstelement nennt sich Nonrepudiation of Submission.
- *Message Flow Confidentiality*
Nicht nur die Nachrichten selbst, auch die Häufigkeit von versendeten Nachrichten zu einem bestimmten Empfänger könnte für die Spionage von erheblicher Bedeutung sein. Aus diesem Grund werden zum Beispiel leere Nachrichten oder über mehrere Zwischenempfänger weitergeleitete Nachrichten versendet.

Zur Realisierung dieser eben beschriebenen Sicherheitsdienstelemente werden symmetrische und asymmetrische Chiffriersysteme verwendet. Letztere finden in elektronischen Mitteilungs-Übermittlungssystemen vor allem in Form des RSA-Chiffriersystems (Rivest, Shamir and Adleman) Verwendung. Dieses asymmetrische Kryptosy-

stem basiert auf zwei unterschiedlichen Schlüsseln – Public Key und Private Key –, die für die Chiffrierung sowie für die elektronische Unterschrift benötigt werden.

Der X.400-Standard wurde in der Theorie für einen relativ breiten Anwendungsbereich ausgelegt. Die Funktionen sind deshalb in der Praxis nur mit einem extremen Aufwand zu implementieren. Zudem setzt der X.400-Standard für den Nachrichtentransport die in lokalen Netzwerken eher selten eingesetzten OSI-Protokolle voraus. Aus diesem Grund ist X.400 vornehmlich in Telekommunikationsnetzen (WANs) realisiert. In der Praxis gibt es aber bereits Installationen, bei denen im gesamten Unternehmen die Mailing-Systeme auf Basis von X.400 aufgebaut werden.

Die privaten Organisationen sparen jedoch in der Regel die hohen Kosten für X.400-konforme Systeme, indem ein X.400-Gateway zum Übergang auf ein X.400-System bereitgestellt wird.

26.2 Das Simple Mail Transfer Protocol (SMTP)

Das Simple Mail Transfer Protocol (SMTP) ist ein Protokoll, das in die TCP/IP-Anwendungsprotokollfamilie implementiert wurde und sich für die einfache elektronische Nachrichtenübermittlung innerhalb eines TCP/IP-Netzwerks zuständig zeigt. Die Kommunikation erfolgt dabei über den dafür reservierten TCP-Port 25.

Die Integration von SMTP und TCP/IP in das OSI-Referenzmodell wird zur Verdeutlichung in Abbildung 26.7 dargestellt. Auf die Darstellung der zusätzlich in TCP/IP standardmäßig implementierten Protokolle habe ich an dieser Stelle jedoch verzichtet.

SMTP wurde in den Standards RFC 821 (Request for Comment) und RFC 822 definiert. Als Request for Comment bezeichnet man einen nummerierten Standardisierungsvorschlag für das Internet, dessen Spezifikationen in offener Form diskutiert werden können.

RFC 821 beschreibt das Transportprotokoll, die Interaktion zwischen zwei kommunizierenden Stationen sowie den Nachrichtenumschlag, der lediglich die Senderadresse und die Empfängeradressen beinhaltet. Der Standard RFC 822 dagegen spezifiziert den Nachrichteninhalt, der ähnlich dem X.400-Standard aus einem Header und einem Text-Body besteht. Dieser Header setzt sich aus dem Datum (Date), dem Absendernamen (From), dem Empfängernamen (To), dem Betreff (Subject) und den Namen für Kopieempfänger (CC) zusammen.

26.2 Das Simple Mail Transfer Protocol (SMTP)

Der Text im Body einer SMTP-Nachricht kann im Gegensatz zum X.400-Standard allerdings nur den 7-Bit-US-ASCII-Zeichensatz verarbeiten. Soll nun trotz dieser Einschränkung eine andere Datei als die im ASCII-Format erstellte Datei versendet werden, wird ein sogenannter Binary-to-ASCII-Kodierer benötigt. Dieser Kodierer wandelt die Binärdateien in zu bearbeitende ASCII-Dateien um. Diese Aufgabe übernehmen zum Beispiel Programme wie UUENCODE, XXENCODE, BASE64 oder auch BTOA (Binary to ASCII), die in der Regel kostenlos über das Internet zu beziehen sind. Der Empfänger der Nachricht muß zum Dekodieren lediglich einen ASCII-to-Binary-Kodierer wie das UUDECODE-Programm einsetzen.

Abbildung 26.7
Die Protokolle
SMTP und TCP/IP
im OSI-Referenz-
modell

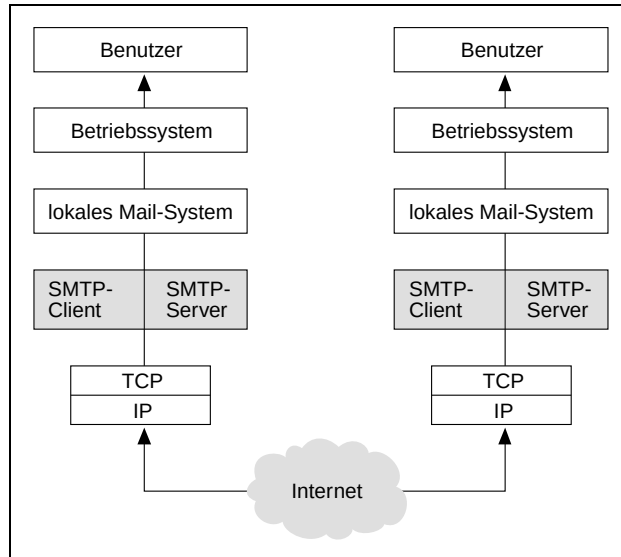
OSI	TCP/IP
Anwendungsschicht	Anwendung
Darstellungsschicht	Simple Mail Transfer Protocol (SMTP)
Sitzungsschicht	
Transportschicht	Transmission Control Protocol (TCP)
Vermittlungsschicht	Internet Protocol (IP)
Sicherungsschicht	Übertragungsmedium
Physikalische Schicht	

26.2.1 Das SMTP-Modell

Das SMTP-System ist ein einfaches Store-and-Forward-Mailing-System, das sich aus einem SMTP-Client und einem SMTP-Server zusammensetzt, deren Kombination sich analog zu einem X.400-User-Agent verhält. Ein Client-Prozeß, die aktive Komponente des Systems, sendet Kommandos über Nachrichtenvermittler (MTAs) zu einem Server-Prozeß, der diese akzeptieren oder ablehnen kann. Bei diesen Kommandos handelt es sich um Protokolldateneinheiten, die aus einer dreistelligen Zahlenkombination bzw. aus einer Textpassage bestehen.

26 Electronic-Mail-Systeme

Abbildung 26.8
Der Aufbau eines
SMTP-Systems



In Abbildung 26.8 ist der mögliche Aufbau eines SMTP-Systems dargestellt. Das in der Abbildung integrierte lokale Mailing-System ist für die Übergabe der gesendeten Nachricht an den SMTP-Client-Prozeß bzw. für die Entgegennahme der ankommenden Nachricht durch den SMTP-Server-Prozeß zuständig.

In dieser Abbildung wird auch gezeigt, daß SMTP als Übergang zum Internet konzipiert ist, um darüber Mailings austauschen zu können. Es ist aber auch möglich, einheitlich in einem Unternehmen dieses Protokoll zu verwenden, ohne daß dafür ein Internet-Anschluß notwendig ist. Es soll nur verdeutlicht werden, daß SMTP das Standardprotokoll für Mailing im Internet ist.

26.2.2 Adressierungsschema

Das Adressierungsschema bei RFC 822 benutzt nicht die von X.400 verwendete O/R-Adressierung, sondern beruht auf dem Domain Name System (DNS) und dessen local-part@domain-part-Adressierung. Diese Adressierung gründet auf einer hierarchischen Namensstruktur, die sich in sogenannte Toplevel Domains, deren Subdomains und die lokalen Ressourcennamen unterteilt. Die Teilung wird durch den Klammeraffen durchgeführt, der hier als At-Sign bezeichnet wird. Die nachfolgende Tabelle zeigt einige der im DNS verwendeten Toplevel-Domänen.

26.3 Multipurpose Internet Mail Extension (MIME)

Domänenname	Bedeutung
COM	Commercial Organizations
DE	Germany
EDU	Educational Institutions
GOV	Government Institutions
INT	International Organizations
MIL	Military Group
NET	Internet Support Centres
ORG	Nonprofit Organizations
UK	United Kingdom
US	United States

Eine mögliche Adresse für die Mailbox des Geschäftsführers Andreas Zenk der Zenk GmbH könnte zum Beispiel so aussehen:

azenk@zenk-gmbh.de

Solange Sie keine Internet-Integration vorhaben, können Sie den Namen der Domain zenk-gmbh.de selbst wählen. Mit einem offiziellen Internet-Anschluß ist es jedoch notwendig, sich einen offiziellen Domain-Namen zuweisen zu lassen, damit dieser auch registriert und nicht doppelt vergeben wird. In der Regel hilft der Internet-Provider bei der Beantragung des Domain-Namens.

26.3 Multipurpose Internet Mail Extension (MIME)

Eine SMTP-Nachricht hat eine wesentliche Einschränkung – sie kann lediglich im 7-Bit-US-ASCII-Zeichensatz und ohne Anlagen wie Grafiken, Audio- oder Video-Dateien versendet werden. Doch im Rahmen der ständigen Erweiterung und der fortschreitenden Standardisierung der Mitteilungs-Übermittlungs-Systeme durch CCITT und ISO wurde sowohl eine Lösung zur Anpassung an ein X.400-konformes System als auch eine kompatible Erweiterung des alten RFC-822-Standards gesucht.

Die Lösung war MIME (Multipurpose Internet Mail Extension), die in den RFCs 1341, 1342 und 1521 spezifiziert wurde. MIME erweitert die Header-Funktion des RFC 822 und bietet somit die Möglichkeit, sogenannte Multipart Messages einzusetzen. Bei den Multipart Mes-

sages wird der Body einer Nachricht in eigenständige Bodyparts unterteilt, die Inhalte (Attribute) wie Text, Multipart, Message, Image, Audio, Video, Application oder auch benutzerdefinierte Typen (X-Private) enthalten können. Zudem wurden die Header-Felder der RFC-822-Spezifikation um die Felder Content Type, Content Transfer Encoding, MIME Version, Optional Content ID und Optional Content Description ergänzt. Diese Ergänzungen beschreiben die Attribute der Bodyparts, die Kodierungsmaßnahmen, die aktuell benutzte MIME-Version sowie die im Body der Nachricht verwendeten Daten.

26.4 Application Programming Interfaces (APIs)

Die Anwendungsschnittstellen (Application Programming Interfaces, APIs) sind definierte und zum Teil normierte Software-Schnittstellen für Front-End-Applikationen. Sie ermöglichen nicht nur das Versenden von Nachrichten durch einen User Agent, sondern auch Mailing-Funktionsaufrufe in Applikationen der Textverarbeitung oder Tabellenkalkulation. Diese Anwendungen werden in drei grundlegende Kategorien unterteilt: Messaging-enabled, Messaging-aware und Messaging-based Workgroup Applications.

■ *Messaging-enabled Application*

Unter einer Messaging-enabled Application versteht man zum Beispiel Anwendungen wie Microsoft Word oder Microsoft Excel, die mit einem Menüpunkt *Nachricht senden* erweitert werden, mit dem aus der Anwendung heraus ein Dokument oder Spreadsheet verschickt werden kann. Diese Funktion kann für Applikationen inzwischen fast als zwingend bezeichnet werden.

■ *Messaging-aware Application*

Eine Messaging-aware Application bezeichnet eine Anwendung, die speziell für das Versenden von Nachrichten entwickelt worden ist. Solche Applikationen sind zum Beispiel der Microsoft-Exchange-Client, der Novell-GroupWise-Client oder auch der Lotus cc:Mail-Client.

■ *Messaging-based Workgroup Application*

Die Messaging-based Workgroup Applications sind komplexere, auf der Basis der elektronischen Nachrichtenverarbeitung aufsetzende Anwendungen, die um Funktionen wie z.B. Terminplanung, Workflow und ähnliche Workgroup-Funktionen erweitert werden. Als Beispiele für diese Applikationen kann Lotus Notes oder auch das bald verfügbare Novell GroupWise XTD aufgeführt werden.

26.4 Application Programming Interfaces (APIs)

Ein großes Problem bei der Umsetzung dieser Anwendungen stellt allerdings auch hier die Uneinigkeit zahlreicher Software-Hersteller dar.

26.4.1 Common Messaging Calls (CMC)

Verschiedene Herstellergruppierungen wie zum Beispiel die X.400 API Association (XAPIA) versuchten im Bereich der Mitteilungs-Übermittlungs-Systeme Anwendungsschnittstellen zu definieren. Dabei entstanden das X.400 Gateway API und das X.400 Application API. 1992 reichte allerdings die Microsoft Corporation ihre eigene Entwicklung einer API bei der XAPIA als Diskussionsgrundlage für einen neuen Standard ein. In Zusammenarbeit wurde daraus die protokollunabhängige Schnittstelle namens Common Messaging Calls (CMCs), die funktional der im nachfolgenden Kapitel besprochenen Simple-MAPI-Schnittstelle entspricht.

Die CMCs arbeiten mit zehn wesentlichen Funktionsaufrufen für den Auf- und Abbau eines Nachrichtendienstes sowie für das Senden und Lesen von Nachrichten.

26.4.2 Messaging Application Programming Interface (MAPI)

Microsoft veröffentlichte 1992 ihre Windows Open Services Architecture (WOSA), um sowohl für Anwender als auch für Entwickler offene Schnittstellen für Verbindungen von Front-End-Applikationen mit Back-End-Services zu liefern. Die WOSA setzt sich, wie in der folgenden Abbildung zu sehen ist, aus den Application Programming Interfaces (APIs) und den Service Provider Interfaces (SPIs) zusammen.

Mittlerweile besteht die WOSA aus neun Komponenten, im einzelnen: Database Access (Open Database Connectivity, ODBC), Messaging (Messaging API, MAPI), File Sharing, Printing, Software Licensing (Licensing Software API, LAPI), Communication Services (Telephony API, TAPI), Distributed Security, Systems Management und den Directory Services.

Speziell für die Mailing-Funktionen wurden dabei die Messaging Application Programming Interfaces (MAPI) spezifiziert, die sich in zwei Gruppen – Simple MAPI und Extended MAPI – aufteilen.

■ *Simple MAPI*

Die Simple MAPI (SMAPI) entspricht bis auf kleine Erweiterungen den CMCs der XAPIA. Sie beinhaltet die zwölf grundlegenden Schnittstellenaufrufe zum Senden, Adressieren und Empfangen

26 Electronic-Mail-Systeme

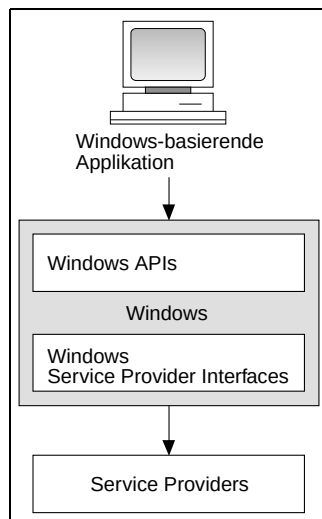
von Nachrichten. Diese Nachrichten können in verschiedenen Anwendungen unterschiedlicher Plattformen wie Windows, Macintosh oder Unix bearbeitet und um Anlagedateien oder OLE-Objekte (Object Linking and Embedding) erweitert werden.

■ *Extended MAPI*

Die Extended MAPI ist eine Erweiterung des Simple MAPI-Schnittstellensatzes. Sie wurde für Applikationen wie Groupware-Anwendungen entworfen, die komplexere Nachrichten bzw. kompliziertere Adressierungsmechanismen fordern.

Die Erweiterungen der Extended MAPI liefern umfangreiche Möglichkeiten für die Nachrichtenorganisation in Ordnern (Folder) sowie die Benutzeradressenverwaltung in definierten Listen. Die Ansammlung dieser Listen wird als Adreßbuch (Address Book) bezeichnet.

Abbildung 26.9
Die Microsoft-
WOSA-Architektur



■ *MAPI-Messaging-Subsystem*

Die besprochenen Schnittstellen wie CMC, Simple MAPI und Extended MAPI arbeiten über Schnittstellenaufrufe mit dem MAPI-Messaging-Subsystem zusammen.

Dieses Subsystem ist ähnlich dem Druck-Subsystem unter Windows aufgebaut. Es gibt für die notwendigen Dienste entsprechende Treiber, die als DLLs realisiert und gemeinsam mit einem Spooler für das Senden und Empfangen von Nachrichten zuständig sind. Der Spooler, als MAPI.DLL abgespeichert, liefert auch die wichtige Store-and-Forward-Funktion, bei der eine Nachricht so lange zwischengespeichert wird, bis sie an den erforderlichen Dienst übergeben werden kann.

26.4 Application Programming Interfaces (APIs)

Abbildung 26.10
Die MAPI-
Architektur

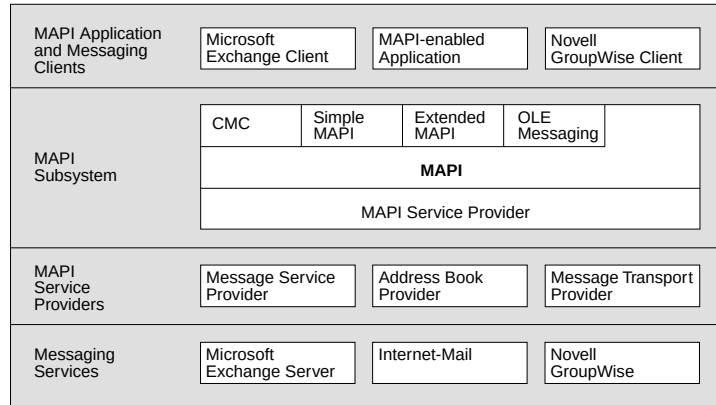


Abbildung 26.10 zeigt den grundsätzlichen Aufbau der Microsoft-MAPI-Architektur, in die sich unterschiedlichste Mailing-Lösungen wie Microsoft Exchange Server oder auch Novells GroupWise integrieren lassen.

26.4.3 Vendor Independent Messaging (VIM)

Die Vendor-Independent-Messaging-Schnittstelle (VIM) wurde von Apple Computer, Lotus Development, Borland, WordPerfect und Novell entwickelt. Sie wird hauptsächlich in den Lotus-Mailing-Produkten cc:Mail und Notes genutzt und bietet Dienste zum Bearbeiten, Senden, Empfangen und Lesen von Nachrichten sowie zum Verwalten von Adreßbucheinträgen.

Die VIM-Schnittstelle wurde mit ca. 60 Funktionsaufrufen realisiert und entspricht in seiner Komplexität der Extended MAPI von Microsoft.

26.4.4 Novell Standard Message Format (SMF)

Die von Novell entwickelte dateibasierende API-Schnittstelle bezeichnet man als Standard Message Format (SMF). Diese in der aktuellen Version SMF 71 verfügbare Schnittstelle unterstützt die hierarchische Adressierung, den nachrichtenbasierenden Verzeichniszugriff und den Austausch von Verzeichnisinformationen.

26.5 Sonstige Mailing-Systeme

Die folgenden Abschnitte sollen lediglich einen kleinen Einblick in die neben Microsoft Exchange und Novell GroupWise wichtigsten Mailing-Systeme geben. Auf die Host-basierenden Systeme wie Banyan IM (Intelligent Messaging), Office Vision, Verimation MEMO, VMS Mail (Virtual Memory System) oder auch dem IBM Mail Exchange wurde verzichtet. Die Bedeutung dieser Host-basierenden Mailing-Systeme sinkt parallel zu der Bedeutung der Großrechner in den heutigen Netzwerken. Trotzdem sollte nicht außer acht gelassen werden, daß diese Systeme auch weiterhin im Einsatz sind, weshalb dafür immer noch Gateways angeboten und benötigt werden.

Systems Network Architecture Distribution Services (SNADS)

IBM entwickelte in den siebziger Jahren für Mainframes eine Netzwerkarchitektur, die unter dem Namen Systems Network Architecture (SNA) vorgestellt wurde. In dieser ähnlich dem heutigen OSI-Schichtenmodell aufgeteilten Architektur wurde das Nachrichtentransportprotokoll SNA Distribution Services (SNADS) implementiert. SNADS liefert asynchrone Peer-to-Peer-Verbindungen und arbeitet nach dem Store-and-Forward-Mechanismus.

Professional Office System (PROFS)

Professional Office System, kurz PROFS genannt, bezeichnet ebenfalls eine IBM-Entwicklung, die in der Mainframe-Umgebung eingesetzt wird. Die Büro-Automations-Software PROFS, die auf VM/CMS-Mainframe-Systeme (Virtual Machine/Conventional Monitor System) aufsetzt, liefert neben Messaging-Funktionalitäten für Text oder Grafiken auch die Möglichkeiten für Terminplanung und elektronische Kalender. Ebenso unterstützt diese Automationssoftware das Dokumentenmanagement sowie den Dokumentenaustausch mit DISOSS (Distributed Office Support System).

NetWare Message Handling Services (MHS)

Die von Novell angebotenen Message Handling Services (MHS), nicht zu verwechseln mit dem Message Handling System (MHS) des X.400-Standards, bezeichnen ein Nachrichtentransportsystem, das in verschiedenen Varianten unter Novell NetWare implementiert werden kann. Dazu zählen NetWare MHS, NetWare Basic MHS oder auch NetWare Global MHS. Bei NetWare MHS handelt es sich allerdings, wie schon angedeutet, um kein vollständiges Mailing-System.

26.5 Sonstige Mailing-Systeme

Dieses als reine Back-End-Anwendung realisierte Store-and-Forward-System stellt lediglich die Funktionalitäten für den Transport der Nachrichten vom Sender zum Empfänger zur Verfügung. Als Front-End-Applikationen, mit denen der Anwender die Nachrichten erstellt oder liest, kann zum Beispiel DaVinci EMail oder auch das standardmäßig mitgelieferte FirstMail for DOS bzw. FirstMail for MS Windows eingesetzt werden. Inzwischen wurde jedoch ein Windows-DLL-Treiber entwickelt, der auch die Microsoft-Mail-Anwendung als Front-End erlaubt. Dieses Produkt namens MS Mail Driver for MHS unterstützt allerdings nicht das von Novell entwickelte Standard-Message-Format-71, sondern basiert auf der von Microsoft definierten MAPI-Schnittstelle.

Ein wesentlicher Vorteil dieses Systems ist die vollständige Integration in die NetWare Directory Services und andere NetWare-4-Komponenten. Zu diesen Komponenten zählt z.B. das NWADMIN-Administrations-Tool, das zur Verwaltung und zum Einrichten von Benutzern (inklusive der GroupWise-Mailing-Komponente) eingesetzt wird. Es zeichnet sich jedoch ab, daß MHS von Novell immer weniger Bedeutung haben wird, da Novell durch GroupWise ein wesentlich leistungsfähigeres System anbieten kann.

Lotus Notes

Lotus Notes, ein Produkt der Lotus Development Corporation, ist eine Groupware-Lösung, die neben einer dokumentenorientierten Datenbank und deren Replication-Technologie auch E-Mail-Funktionen zur Verfügung stellt. Ebenso bietet diese Client/Server-Plattform sowohl die Möglichkeit der Workflow-Automatisierung als auch eine flexible Umgebung für die Anwendungsentwicklung. Als Front-End-Applikationen können neben den Lotus-Notes- und Lotus-cc:Mail-Clients auch Anwendungen implementiert werden, die auf der VIM-Schnittstelle aufsetzen.

Microsoft Mail

Microsoft Mail bietet Funktionen für den Nachrichtenversand sowohl für kleine Arbeitsgruppen als auch für größere Unternehmen. In letzterem Fall wird diese mit dem BackOffice-Produkt Microsoft Mail Server realisiert. Dieses Produkt unterstützt die MAPI-Schnittstelle, unterschiedliche Client-Plattformen, Remote Access mittels Modem und eine Vielzahl von Gateways zu anderen Messaging-Umgebungen.

26 Electronic-Mail-Systeme

Microsoft Mail verwendet ein geteiltes Dateisystem, das als Postoffice bezeichnet wird. Dieses Postoffice ist lediglich eine Verzeichnisstruktur, in der die Nachrichten abgelegt werden können. Diese Verzeichnisstruktur wird auf der lokalen Festplatte des Mail-Servers von Microsoft bzw. auf einer in der Arbeitsgruppe definierten Workstation verwaltet.

Der Client für diese Mailing-Lösung wird standardmäßig mit den Betriebssystemen Windows for Workgroups oder auch Windows NT ausgeliefert. Beim Kauf eines MS-Office-Pakets ist ebenfalls ein MS Mail Client enthalten.

Auch hier gilt, daß MS-Mail immer mehr durch den Mail Exchange Server in den Hintergrund gedrängt wird.

27

Die Grundlagen der Directory Services (Verzeichnisdienste)

Wie bereits in Kapitel 9 besprochen, wird versucht, die Kommunikation gemäß OSI in einem offenen System zwischen verschiedenen realen Systemen zu standardisieren. Kommunizieren nun in einem offenen System eine große Menge an realen Systemen miteinander, muß jedes dieser realen Systeme eindeutig identifiziert werden können. Diese Menge von eindeutig identifizierbaren realen Systemen wird im Sinne von OSI als Verzeichnissystem spezifiziert.

Das Verzeichnis (Directory), auch als Adreßbuch bezeichnet, enthält Informationen über die realen Systeme und kann von einem Anwender oder einem Anwendungsprozeß genutzt werden, um Informationen über einen anderen Benutzer oder Prozeß anzufordern. Diese Anfragen werden ähnlich der Suche im Telefonbuch oder den Gelben Seiten durchgeführt – lediglich elektronisch.

Zur Vereinfachung und Normierung dieses komplexen Verzeichnissystems wurde von der CCITT der X.500-Standard verabschiedet. Man wird beim Lesen dieses Kapitels auch feststellen, wie groß die Übereinstimmung mit NetWare 4 ist. Daraus ist zu erkennen, daß bei der Entwicklung der NDS auf die X.500-Standards zurückgegriffen worden ist. Langfristig gesehen werden wahrscheinlich alle modernen Netzwerkbetriebssysteme auf der Basis der Directory Services aufgebaut sein, da damit eine Menge Vorteile verbunden sind.

27.1 Der CCITT-X.500-Standard

Ebenso wie der X.400-Standard ist auch der X.500-Standard eine CCITT-Empfehlung der X-Serie für Datenübermittlungsnetze und der Oberbegriff für den Verzeichnisdienst (Directory Service, DS).

Die CCITT hat 1988 in Zusammenarbeit mit der ISO folgende äquivalente Normen definiert:

- *X.500*
Das Verzeichnis – Übersicht über Konzepte, Modelle und Dienste (ISO 9594-1)
- *X.501*
Das Verzeichnis – Modelle (ISO 9594-2)

27 Die Grundlagen der Directory Services (Verzeichnisdienste)

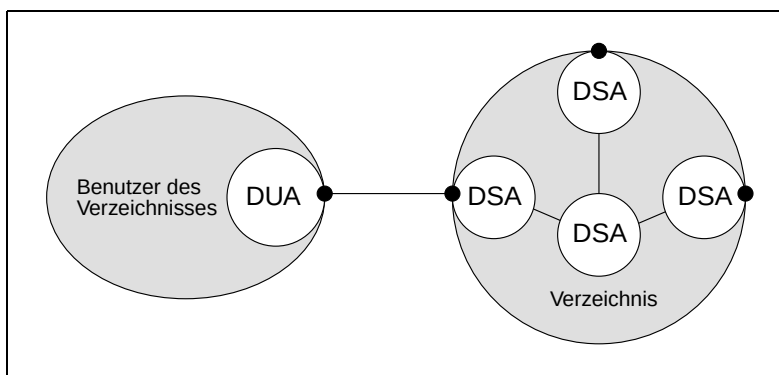
- X.509
Das Verzeichnis – Rahmen für Authentifizierungen (ISO 9594-8)
- X.511
Das Verzeichnis – Definition eines abstrakten Dienstes (ISO 9594-3)
- X.518
Das Verzeichnis – Verfahren für verteilte Operationen (ISO 9594-4)
- X.519
Das Verzeichnis – Protokoll-Spezifikation (ISO 9594-5)
- X.520
Das Verzeichnis – Ausgewählte Attributtypen (ISO 9594-6)
- X.521
Das Verzeichnis – Ausgewählte Objekttypen (ISO 9594-7)

Die folgenden Abschnitte geben einen allgemeinen Überblick über die Verzeichnisdienste und vertiefen damit das Verständnis für die in der elektronischen Nachrichtenübermittlung gebräuchlichen Namenskonventionen.

27.1.1 Das funktionale Modell

Jeder Benutzer oder Anwendungsprozeß, der Informationen von einem Verzeichnissystem anfordert, kooperiert mit den Diensten eines Verzeichnisbenutzeragenten (Directory User Agent, DUA). Der DUA baut über die Zugriffspunkte (Access Points) des Verzeichnissystems eine verbindungsorientierte Kommunikation auf, die mit dem Verzeichnisdienstagenten (Directory Service Agent, DSA) und dessen Diensten durchgeführt wird.

Abbildung 27.1
Der Zugang zum
Verzeichnissystem



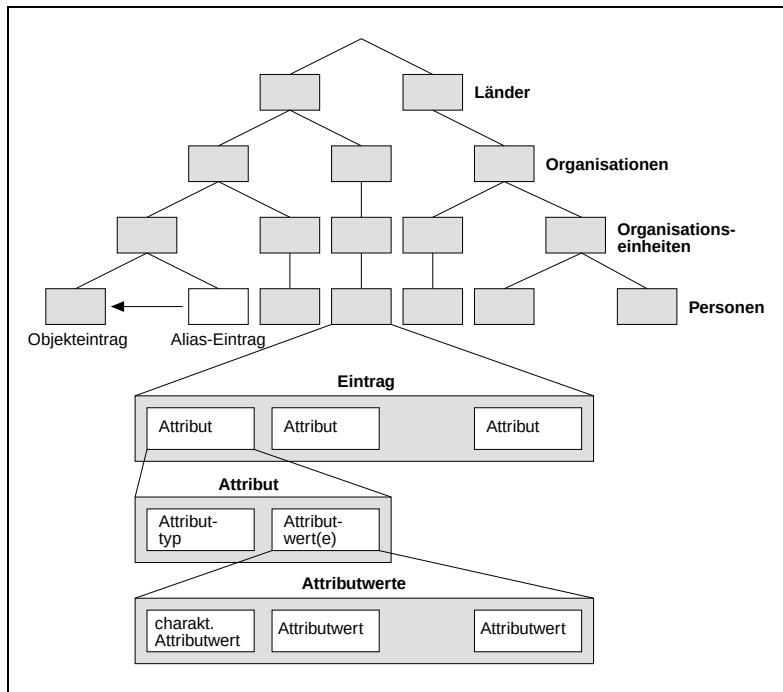
27.1 Der CCITT-X.500-Standard

Das in Abbildung 27.1 gezeigte Verzeichnissystem beinhaltet mehrere DSAs, da in der Realität ein Verzeichnis eine sehr große, geografisch verteilte Datenmenge verwalten muß.

27.1.2 Das Informationsmodell

Die Hauptaufgabe des DS ist die Verwaltung und Pflege von Objektinformationen, um diese einem Anwender oder Anwendungsprozeß zugänglich zu machen. Die vollständige Menge dieser Informationen wird in der Verzeichnisinformationsbasis (Directory Information Base, DIB) gespeichert, die ähnlich einer verteilten Datenbank arbeitet und als hierarchische Baumstruktur aufgebaut ist. Diese Baumstruktur wird als Verzeichnisinformationsbaum (Directory Information Tree, DIT) bezeichnet und ist in Abbildung 27.2 dargestellt.

Abbildung 27.2
Der Directory
Information Tree
(DIT)



Der Directory Information Tree verwaltet alle Verzeichnisobjekte, die als Einträge bzw. Knoten realisiert werden. Diese Objekte, deren Klassifizierung in der folgenden Tabelle aufgezeigt wird, können dabei als Container- oder Leaf-Objekte angelegt werden. Ein Container-Objekt kann Leaf-Objekte oder wiederum Container-Objekte beinhalten. Das Leaf-Objekt bildet hingegen den Abschluß und kann keine weiteren Objekte zum Inhalt haben.

27 Die Grundlagen der Directory Services (Verzeichnisdienste)

Schlüsselwort	Objektklasse	Beschreibung
C	Country	Land
O	Organization	Organisation
OU	Organizational Unit	Organisationseinheit
CN	Common Name	Personenname

Mit diesen Objektklassen ermöglicht der DIT die logische Abbildung eines Organisationsaufbaus sowie schnellere Zugriffszeiten bei Verzeichnisabfragen.

Namen

Genau wie im Telefonbuch ist auch im Verzeichnis die eindeutige Benennung einer Person, einer Organisation etc. von erheblicher Bedeutung. Jedem Objekt ist durch seine Anordnung im DIT ein eindeutiger Name zugeordnet, der sich aus der Zusammenstellung aller DIT-Objektnamen ergibt. Eine Person Herbert Weiß, die in dem Land Deutschland, in der Fachhochschule München und dem Fachbereich Elektrotechnik eingetragen ist, kann somit eindeutig und benutzerfreundlich identifiziert werden. Ein X.500-Verzeichnisname könnte wie im folgenden Beispiel aussehen:

C=DE; O=Zenk-GmbH;OU=Systemberatung; CN=Herbert_Weiss

Der Objektname Herbert_Weiss unter dem Knoten Systemberatung heißt relativer charakteristischer Name (Relative Distinguished Name, RDN), da er die Person relativ zu dem übergeordneten Objekteintrag Systemberatung charakterisiert. Der komplette Name vom Country-Objektnamen bis zum Objektnamen Herbert_Weiss wird dagegen als charakteristischer Name (Distinguished Name, DN) ausgegeben, da er die Person weltweit eindeutig, aber nicht einmalig charakterisiert. Es existiert neben dem Systemberater Herbert_Weiss auch der Referent Herbert_Weiss, der ebenfalls bei der Organisation Zenk-GmbH arbeitet, aber aus bestimmten Gründen andere Bezüge benötigt. Diese Eintragung bezieht sich auf den Objekteintrag Herbert_Weiss und wird Alias-Eintrag genannt. Der Alias-Eintrag kann nur als Eintrag im DIT definiert werden. Ob diese mehrfachen Bezüge implementiert werden, hängt von der jeweiligen Umgebung ab. Eine endgültige Entscheidung darüber hängt von einer ausführlichen Planung und Untersuchung der Unternehmensstruktur ab.

27.1 Der CCITT-X.500-Standard

Eintrag

Der Objekteintrag `Herbert_Weiss` enthält bestimmte Informationen, die dieses Objekt durch eine Ansammlung von Attributen näher spezifizieren.

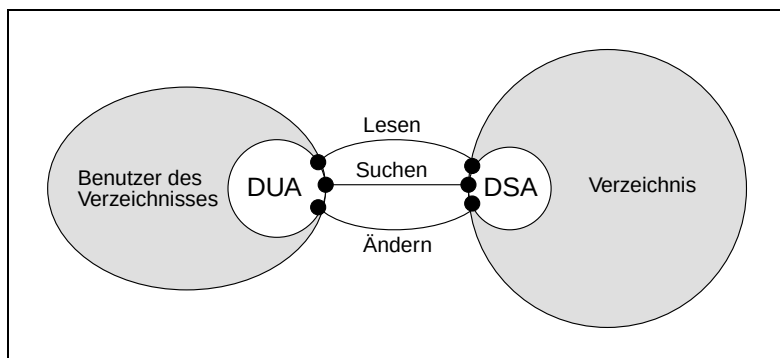
Für die interne Verwaltung des Verzeichnisses werden dabei zwei grundlegende Attribute verwendet. Zu diesen zählt man das Attribut Alias-Objektname sowie das Attribut Objektklasse. Das Aliasattribut existiert lediglich bei einer Alias-Eintragung und enthält den Objektnamen, auf den sich die Alias-Eintragung bezieht. Das Attribut Objektklasse wird hingegen bei jeder Eintragung benötigt und definiert neben der Objektklasse, die in der vorherigen Auflistung bereits dargestellt wurde, auch bestimmte Regeln. Diese Regeln spezifizieren für die entsprechende Objektklasse vorgeschriebene und optional einzutragende Attribute. Der Aufbau eines Verzeichniseintrags mit Attributstypen und -werten wird in der Abbildung 27.2 des DIT veranschaulicht.

Der Objekteintrag `Herbert_Weiss` enthält zum Beispiel neben dem Attribut Objektklasse auch zusätzliche Attribute, die diesen Eintrag näher spezifizieren. Dazu fügt man dem Eintrag des Systemberaters `Herbert_Weiss` zusätzliche Attribute wie dessen Personalnummer, Eintrittsdatum, Geburtsdatum oder Adresse hinzu.

27.1.3 Dienste bzw. Operationen

Um die Dienste, die ein Verzeichnissystem bietet, nutzen zu können, wurde in X.500 der Zugang von einem DUA über einen Zugangspunkt zu einem DSA mittels fest definierter Schnittstellen realisiert. Diese Schnittstellen, die auch Ports genannt werden, ermöglichen die interaktive Kommunikation zum Lesen, Suchen oder Verändern von Verzeichnisinformationen.

Abbildung 27.3
Das Modell für
den Verzeichnis-
zugang



27 Die Grundlagen der Directory Services (Verzeichnisdienste)

Für den Auf- und Abbau eines Verzeichniszugangs, dessen Schnittstellen im Modell Abbildung 27.3 dargestellt sind, müssen grundlegende Operationen des Verzeichnissystems ausgeführt werden. Dies sind die Verzeichnis-Binde-Operation und die Verzeichnis-Loslöse-Operation. Die Binde-Operation identifiziert die Verbindung des DUA mit einem DSA und erlaubt dessen Zugang zum Verzeichnis. Die Loslöse-Operation unterbindet hingegen nach Ablauf der Zugangszeit die zuvor aufgebaute Kommunikation.

Das Zustandekommen einer Verbindung ermöglicht die Ausführung der nachfolgenden Abfrage- und Änderungsoperationen.

Leseschnittstelle (Read Port)

Der Read Port, auch als Leseschnittstelle bezeichnet, stellt drei Operationen für die Informationsabfrage in einem Verzeichnis zur Verfügung.

- *Lesen (Read)*

Die Leseoperation erlaubt es, bestimmte Informationen abzufragen und zu lesen, wie z.B. den Attributwert eines ausgewählten Verzeichniseintrags.

- *Vergleichen (Compare)*

Zur Überprüfung von Attributwerten eines Objekts kann das Verzeichnissystem den Inhalt eines Attributwerts mit einem spezifizierten Wert vergleichen. Diese Operation kann möglicherweise für die Eingabe eines Paßworts genutzt werden.

- *Abbrechen (Abandon)*

Soll eine Lese- oder Suchabfrage aufgrund einer vermuteten Fehleingabe oder einer Zeitüberschreitung beendet werden, obwohl die relevanten Informationen vom Verzeichnissystem noch nicht geliefert wurden, kann mit der Operation Abbrechen diese Abfrage vorzeitig abgebrochen werden. Für die Änderungsschnittstelle existiert diese Funktion allerdings nicht.

Leseschnittstelle (Search Port)

Für Suchabfragen innerhalb des Verzeichnisses werden der Search Port und die mit ihm verbundenen Operationen verwendet.

- *Auflisten (List)*

Diese Operation listet alle Einträge des DIT auf, die einem ausgewählten Objekteintrag unmittelbar unterliegen.

- *Suchen (Search)*

Die Suchoperation gibt Attributwerte aus, die durch einen bestimmten Parameter gefiltert werden.

27.1 Der CCITT-X.500-Standard

Änderungsschnittstelle (Modify Port)

Die Änderungsschnittstelle bietet vier Operationen an, um Einträge im DIT zu erstellen, zu ändern oder zu löschen.

- *Einfügen (Add Entry)*
Mit dieser Operation besteht die Möglichkeit, einen neuen Leaf-Eintrag zum DIT hinzuzufügen. Das kann sowohl ein Objekteintrag als auch ein Alias-Eintrag sein.
- *Entfernen (Remove Entry)*
Mit Entfernen wird ein Leaf-Eintrag aus dem DIT gelöscht. Die Möglichkeit, einen Knoten innerhalb des DIT zu entfernen, ist bei X.500 nicht gegeben.
- *Ändern (Modify Entry)*
Haben sich im Lauf der Zeit Änderungen in einem Eintrag ergeben, können deren Attributwerte mittels Ändern modifiziert werden. Eine Änderung, die den Eintrag und dessen RDN umorganisieren würde, kann allerdings nur mit dem nachfolgenden Befehl ausgeübt werden.
- *RDN ändern (Modify Relative Distinguished Name)*
Soll der RDN eines Eintrags geändert werden, stellt die Änderungsschnittstelle eine Operation bereit, mit der charakteristische Attributwerte eines Leaf-Eintrags geändert werden können.

27.1.4 Verteiltes Verzeichnis

Die heutige Kommunikation bedeutet in vielen Fällen eine weltweit verteilte Anwendung mit einer riesigen Anzahl von Systemen und einer daraus resultierenden großen Datenmenge. Eine große Anzahl von Einträgen in einem Verzeichnis kann nicht allein von einem DSA verwaltet werden. Ein Verzeichnissystem besteht aus diesem Grund in der Praxis aus mehreren untereinander kommunizierenden DSAs. Stellt ein Anwender über den DUA und dessen Schnittstellen eine Anfrage an das Verzeichnissystem, wird die Anfrage, falls sie der lokale DSA nicht beantworten kann, an entfernte DSAs des Systems weitergeleitet und bearbeitet. Das geschieht über die verketteten bzw. verteilten Lese-, Such- und Änderungsschnittstellen des verteilten Verzeichnisses.

Die verteilten Schnittstellen stellen unterschiedliche Mechanismen zur Verfügung, mit denen eine Anfrage an das Verzeichnis weitergeleitet und die gewünschte Verzeichnisinformation angefordert werden kann. Diese Mechanismen werden als Verkettung (Chaining), Multicasting oder auch als Verweis (Referral) bezeichnet.

27 Die Grundlagen der Directory Services (Verzeichnisdienste)■ *Verkettung (Chaining)*

Kann ein DSA eine Anfrage nicht befriedigen, verfügt aber über die Wissensinformation, welcher DSA des Verzeichnisses diese Anfrage beantworten könnte, so leitet dieser die Anfrage mittels Chaining zu dem gewünschten DSA des Verzeichnisses weiter.

■ *Multicasting*

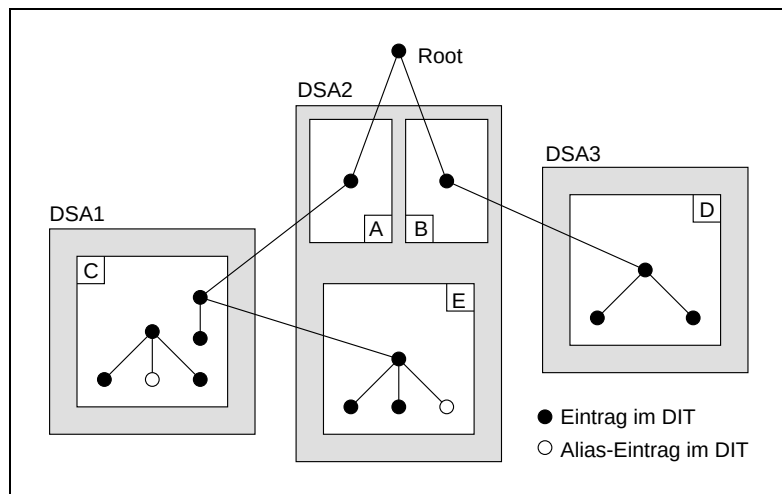
Anders als beim Chaining, bei dem eine Anfrage aufgrund der Wissensinformation an einen konkreten DSA weitergeleitet werden kann, wird bei diesem Mechanismus das Verzeichnis auf die gewünschte Information mittels sequentieller oder auch paralleler Anfragen durchsucht.

■ *Verweis (Referral)*

Bei dieser Anfrage wird nicht sofort die gewünschte Information ausgegeben, sondern lediglich der DSA mitgeteilt, der diese Information bereithält. Anschließend kann die Anfrage mittels Chaining oder Multicasting bearbeitet werden.

Die Informationsanfrage mittels Chaining basiert wie bereits angesprochen auf der Wissensinformation (Knowledge Information) der DSAs über den Informationsgehalt der entfernten DSAs. Jeder DSA besitzt bei einer Anfrage an das Verzeichnis Kenntnis von der Aufteilung der Verzeichniseinträge. Dazu wird der DIT in sogenannte Kontexte oder Partitionen aufgeteilt, von denen ein DSA eine oder mehrere verwalten kann. Das Wissen dieser Partitionen steht über verschiedene Referenzklassen wie zum Beispiel Aufwärts-, Abwärts- oder Querreferenz in einer hierarchischen Relation, die den Zugang zu allen DSAs über einen DUA ermöglicht.

Abbildung 27.4
Der hypothetische
DIT



27.1 Der CCITT-X.500-Standard

Der hypothetische DIT, wie in Abbildung 27.4 veranschaulicht, entspricht mit der Kontextaufteilung einer verteilten Datenbank. Diese Datenbank ist zum Beispiel über drei DSAs verteilt, die die Kontexte A bis E verwalten. Diese Aufteilung fördert schnellere Zugriffszeiten und eine hohe Verfügbarkeit der Verzeichnisinformationen.

27.1.5 Verwaltungsbereiche (Management Domains)

Ähnlich dem X.400-Standard werden auch beim X.500-Standard unterschiedliche Verwaltungsbereiche (Directory Management Domains, DMDs) für die Organisation und die Verwaltung des Verzeichnisses unterschieden.

- *Öffentlicher Verzeichnisverwaltungsbereich*
(Administration Directory Management Domain)
Der öffentliche Verzeichnisverwaltungsbereich (Administration Directory Management Domain, ADDMD) wird von einer PTT oder einer öffentlichen Fernmeldeverwaltung betrieben.
- *Privater Verzeichnisverwaltungsbereich*
(Private Directory Management Domain)
Der private Verzeichnisverwaltungsbereich (Private Directory Management Domain, PRDMD) wird hingegen von Hochschulen, Unternehmen oder privaten Organisation bereitgestellt.

27.1.6 Protokolle

Für die Kommunikation zwischen einem DUA und einem DSA bzw. zwischen zwei DSAs wurden speziell für den Verzeichnisdienst eigene Protokolle definiert. Diese Protokolle sind in der Anwendungsschicht des OSI-Referenzmodells implementiert und integrieren auch anwendungsspezifische Dienstelemente dieser Schicht.

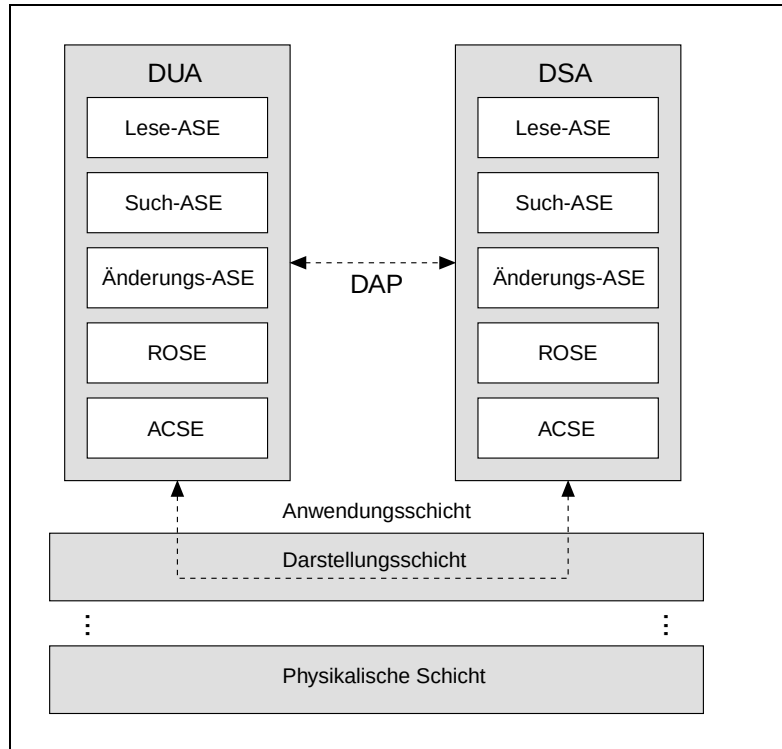
Als Dienstelement versteht man hier einen Teil der Anwendungsschicht, der sich für die Bereitstellung und Realisierung der angebotenen Dienste zuständig zeigt.

Verzeichniszugangsprotokoll (Directory Access Protocol, DAP)

Das Verzeichniszugangsprotokoll (Directory Access Protocol, DAP) wird für die Kommunikation eines DUA und eines DSA genutzt. Auf diesem Protokoll sind die anwendungsspezifischen Dienstelemente (ASEs) implementiert, die durch die Lese-, Such- und Änderungsschnittstellen beschrieben werden.

27 Die Grundlagen der Directory Services (Verzeichnisdienste)

Abbildung 27.5
Das Protokoll-
modell für den
Verzeichniszu-
gang



Zusätzlich zu den Dienstelementen des Verzeichnissystems sind weitere Dienstelemente für entfernte asymmetrische Tätigkeiten (Remote Operation Service Element, ROSE) sowie für die Steuerung des Aufbaus und Abbaus (Association Control Service Element, ACSE) eines Anfrageprozesses integriert. Für die präzise Erklärung dieser Dienstelemente verweise ich auf die weiterführende Literatur, da die genaue Beschreibung dieser Elemente hier zuviel Raum beanspruchen würde.

Verzeichnissystemprotokoll (Directory System Protocol, DSP)

Die Verbindung für interne Verzeichnisanfragen oder das Weiterleiten von Anfragen wird auf dem Verzeichnisprotokoll (Directory System Protocol, DSP) ausgeführt. Die Kommunikation für diese Anfragen erfolgt zwischen zwei oder mehreren DSAs, bis die erwartete Information gefunden und ausgegeben werden kann. Dies geschieht mit den bereits besprochenen verteilten Lese-, Such- und Änderungschnittstellen.

27.1 Der CCITT-X.500-Standard

Zusätzlich zu den verteilten Dienstelementen des Verzeichnissystems sind auch hier weitere Dienstelemente der Anwendungsschicht für die entfernten Verbindungen (ROSE) sowie für die Steuerung des Auf- und Abbaus (ACSE) eines Anfrageprozesses hinzugefügt.

27.1.7

Sicherheitsmechanismen

Die Informationen des Verzeichnisses über Objekte wie Länder, Organisationen, Abteilungen oder Personen sollten im Grunde für jeden zugänglich sein. Die Verfügbarkeit dieser Daten bietet allerdings einen möglichen Angriffspunkt für Mißbrauch.

Im Verzeichnissystem muß deshalb für die Sicherheit der gespeicherten Daten gesorgt werden, indem die Identität eines Benutzers vor dem Zugriff verifiziert und die sichere Übermittlung dieser Daten gewährleistet wird. Der X.500-Standard stellt einige Mechanismen für die Sicherheit der Informationen zur Verfügung:

Zugriffskontrolle (Access Control)

Über die Zugriffskontrolle (Access Control) wird festgelegt, welche Personen Berechtigungen für das Lesen, Suchen oder Ändern von Verzeichnisinformationen erhalten. Dies wird durch sogenannte Zugriffsrechte auf Einträge bzw. auf Attribute oder Attributwerte eines Eintrags verwirklicht. Die Zugriffskontrolle kann allerdings nur realisiert werden, wenn die Identität dieser Person überprüft wird. Das geschieht mittels der Authentifizierung.

Authentifizierung (Authentication)

Als Authentifizierung beschreibt man einen Vorgang, bei dem ein System die Echtheit und Glaubwürdigkeit einer Person oder einer Information bestätigt. Die Authentifizierung wird beim Verzeichnissystem in zwei Sicherheitsstufen unterschieden:

- *Einfache Authentifizierung (Simple Authentication)*
Die einfache Authentifizierung wird hauptsächlich für die lokale Beglaubigung eines DUA gegenüber einem DSA benutzt. Hier handelt es sich um eine unverschlüsselte Kombination des charakteristischen Namens eines Benutzers in Verbindung mit einem zusätzlichen generierten Paßwort.
- *Starke Authentifizierung (Strong Authentication)*
Die starke Authentifizierung bietet neben der Benutzerauthentifizierung auch eine sichere Übermittlung der Informationen sowie die Möglichkeit der digitalen Unterschrift. Die Strong Authentication verwendet dafür ein asymmetrisches Chiffrierverfahren mit einem Public und einem Private Key (Public Key Crypto System, PKCS).

28

Die Jahr-2000-Problematik

Je näher der Jahrtausendwechsel kommt, desto mehr Gedanken muß man sich machen, ob die eigene Systemlandschaft diesen Jahrtausendwechsel überstehen wird. Man sollte schleunigst damit beginnen – sofern man nicht bereits damit angefangen hat –, sich mit diesem Problem intensiver zu beschäftigen, damit man nicht am 1.1.2000 vor einem »Scherbenhaufen« steht.

Im Jahr 1997 wurde von Dave Barry (Getting the Bugs out) die folgende Aussage für das Jahr-2000-Problem gemacht:

»Experts tell us that if the Millennium Bug is not fixed, when the year 2000 arrives, our financial records will be inaccurate, our telephone system will be unreliable, our government will be paralyzed and airline flights will be cancelled without warning. In other words, things will be pretty much the same as they are now.«

In den letzten Wochen ist festzustellen, daß selbst Versicherungen nervös werden und Unternehmen Fragebögen versenden. Diese Situation dürfte sich in den nächsten Monaten noch mehr verschärfen. Es ist aber nicht damit getan, sich nur um die Einhaltung der Jahr-2000-Fähigkeit bei den Anwendungen zu kümmern, auch die eingesetzte Hardware muß dieses Problem lösen können. Die beginnt ganz einfach beim BIOS des Rechners, der in der Lage sein muß, alle relevanten Informationen und Umstellungsmechanismen auf das Jahr 2000 zu bieten, und endet bei den Steuerungsanlagen. Das Jahr-2000-Problem entsteht vor allem dadurch, daß Software-Programme die Jahreszahl in den meisten Fällen zweistellig verwenden; zudem fallen weitere Aspekte ins Gewicht, die eine Jahr-2000-Fähigkeit unmöglich machen. Problematisch ist die Situation deshalb, weil bei Verwendung der letzten zwei Stellen für die Jahreszahl interne Berechnungen ganz andere Ergebnisse bringen können. So ist es nicht selten, daß bei der Jahresdifferenzberechnung in alten Programmen wie folgt vorgegangen worden ist: 98 minus 80 ergibt 18 Jahre Unterschied. Sofort nach dem Jahrtausendwechsel ergibt dies 00 minus 80 und somit eine Jahresdifferenz von -80. So könnte es z.B. sehr seltsame Nebeneffekte bei der Rentenberechnung, bei den Krankenkassen und einer Vielzahl anderer Institute geben, wenn die Programme nicht dementsprechend angepaßt werden. Es reicht aber auch nicht aus, ein System zu nehmen, auf das Jahr 2000 umzustellen und abzuwarten, ob sich das Programm noch starten läßt. Der Start alleine ist kein Beweis dafür, daß es Jahr-2000-fähig ist. Für die gesamten Systemeinheiten, Anwendungen und alle anderen Komponenten, die

28 Die Jahr-2000-Problematik

auf eine Jahr-2000-Fähigkeit hin überprüft werden müssen, ist ein entsprechender Projektplan notwendig, der genau festlegt, wie ein Testszenario aussehen muß und in welcher Form die Tests durchgeführt werden sollen.

Man kann für das Jahr-2000-Problem die folgenden Regeln aufstellen, die erfüllt werden müssen, um ein Produkt Year-2000-Ready zu nennen:

1. Das Datum muß bis in das Jahr 2035 korrekt angezeigt werden.
Hierzu gehören alle Debugging-, Logging- und Diagnose-Informationen.
2. Das Jahr 2000 ist definitiv ein Schaltjahr, eine Tatsache, die von vielen nicht erkannt wird, da für die Schaltjahrregel im Jahr 2000 eine weitere Sonderregel zutrifft.
3. Der Wochentag muß bis in das Jahr 2035 korrekt berechnet werden.
4. Die Kalenderberechnung muß auch für Sonderfälle korrekt durchgeführt werden, da es sonst zu ungewollten Nebeneffekten kommt, die sich bereits vor dem und nach dem Jahrtausendwechsel ergeben. Über die folgenden Sonderfälle sollte man sich speziell Gedanken machen:
 - 31. Dezember 1999
Hier hat das BIOS eventuell Probleme, den Wechsel auf das Jahr 2000 durchzuführen.
 - 1. Januar 2000
 - 28. Februar 2000
 - 29. Februar 2000
Hier muß als Tag Dienstag ausgegeben werden.
 - 1. März 2000
Hier muß als Tag Mittwoch ausgegeben werden.
 - 31. Dezember 2034
Auch hier kann es bei Hard- und Software-Systemen zu Problemen beim Jahreswechsel kommen
 - 1. Januar 2035
5. Alle Produkte und Anwendungen müssen in der Lage sein, die Sortierung nach Datum in allen Fällen korrekt auszuführen (mindestens bis zum Jahr 2035).
6. Es muß genau überprüft werden, ob die Datumseingaben auch alle akzeptiert werden.
7. Wenn intern mit Zeitstempeln gearbeitet wird, müssen auch diese in jeder Konstellation korrekt berechnet werden.
8. Wenn bei der Kommunikation zwischen zwei Systemen das Kommunikationsprotokoll mit Zeit- bzw. Datumsabgleich arbeitet, muß gewährleistet sein, daß die Systeme bei den Übergängen die Datumsangaben im alten und im neuen Format akzeptieren.

9. Bei herkömmlichen Anwendungen ist darauf zu achten, daß auch nach der Umstellung auf das neue Datumsformat die Anwendung immer noch korrekt läuft.

Von allen führenden Herstellern werden in regelmäßigen Abständen aktuelle Informationen im Internet zur Verfügung gestellt, die den aktuellen Status der Jahr-2000-Fähigkeit widerspiegeln. Besonders wichtig sind in diesem Zusammenhang die beiden Hersteller Novell und Microsoft. Beide dokumentieren, welche Updates durchzuführen sind bzw. welche Patches eingespielt werden müssen, um alle Anwendungen Jahr-2000-fähig zu machen.

Es sei nochmals darauf hingewiesen, daß auch die Hardware in einem Netzwerk auf die Jahr-2000-Fähigkeit überprüft werden muß: Server, Workstations, Hub-Systeme und dergleichen mehr – d.h., alles was Datumsangaben verwendet. Für die Überprüfung der Hardware-Komponenten im PC-Bereich gibt es entsprechende Programme, die einen Jahr-2000-Wechsel im BIOS simulieren und die oben aufgeführten Datumsangaben (die meisten zumindest) prüfen und dann als Ergebnis ausgeben, ob die Hardware das Jahr 2000 und auch die Zeit danach übersteht oder nicht. Die entsprechende Software kann von den unterschiedlichsten Web-Servern im Internet geholt werden. Sie wird aber auch zum Teil von Hardware-Herstellern zur Verfügung gestellt. Ein mögliches Testergebnis könnte wie folgt aussehen:

(C) Copyright 1997-1998, Novell Inc. All Rights Reserved \			
Testing set and report of:	Test Results	Reported by -	
01-01-2035	Critical Rollover Dates: RTC BIOS		
Set: 01-01-2035 23:59:57	12-31-1998 to 01-01-1999	Pass	Pass
RTC: 01-01-2035 23:59:57	12-31-1999 to 01-01-2000	N/A	Pass
BIOS: 01-01-2035 23:59:58	02-28-2000 to 02-29-2000	Pass	Pass
	02-29-2000 to 03-01-2000	Pass	Pass
	12-31-2034 to 01-01-2035	Pass	Pass
	Critical Reporting Dates: RTC BIOS		
	09-09-1999	Pass	Pass
	12-31-1999	Pass	Pass
	01-01-2000	Pass	Pass
	02-29-2000	Pass	Pass
	01-01-2035	Pass	Pass

28 Die Jahr-2000-Problematik

Es gibt eine Vielzahl interessanter Web-Adressen, die sich mit der Jahr-2000-Problematik auseinandersetzen. Da man auf diesen Web-Seiten sehr viele interessante Informationen findet, möchte ich es nicht versäumen, Ihnen diese Adressen mitzuteilen, damit Sie sich selbst bei Bedarf mit weiteren Informationen versorgen können. Die Adressen hierfür lauten wie folgt:

Greenwich Mean Time	http://www.gmt-2000.com
Das Year-2000-Information-Center	http://www.year2000.com
IBM Year 2000	http://www.ibm.com/IBM/year2000
Sun Microsystems Year 2000 Program	http://www.sun.com/y2000
ITAA	http://www.itaa.org
Die Institution of Electrical Engineers (IEE) 2000 Dangers for Engineers	http://www.iee.org.uk/2000risk/
GTBecker	http://207.182.213.132
Other Sites for Year 2000	http://www.mitre.org/research/y2k/docs/Y2K_LINKS.html

Neben diesen Informationen bieten alle renommierten Hersteller im Internet Informationen über den aktuellen Stand der Testergebnisse. Da es sehr interessant ist, zu erfahren, wie sich die Hersteller bis zum Zeitpunkt der Erstellung dieses Buchs bezüglich der Jahr-2000-Problematik verhalten, sind nachfolgend die entsprechenden Statusinformationen von Microsoft und Novell aufgeführt.

28.1 Jahr-2000-Fähigkeit bei Microsoft

Beim Testen der Microsoft-Produkte ist Microsoft wie folgt vorgegangen:

- Das Produkt speichert und berechnet das Datum einheitlich in einem 4-Ziffern-Format, und das für die ganze Operation.
- Wenn das Produkt eine 2-Zeichen-Eingabe für die Jahreszahl erlaubt, dann setzt das Produkt das Format einheitlich auf vier Ziffern um.
- Das Produkt hat keine Probleme bei der Schaltjahrberechnung (siehe auch die Angaben in den vorherigen Ausführungen).
- Die Produkte verwenden keine speziellen Werte für das Datum innerhalb der internen Bearbeitung.
- Die Produkte laufen im 21. Jahrhundert bis zum Ende des Jahres 2035.

28.1 Jahr-2000-Fähigkeit bei Microsoft

Wenn man die im Internet veröffentlichte Liste betrachtet, stößt man auf einige Angaben, die es gilt, richtig zu interpretieren; dies soll nachfolgend getan werden.

- *Compliant*

Das Produkt entspricht im vollen Umfang den Microsoft-Standards für Verträglichkeit. Es kann durchaus sein, daß zum Erreichen dieses Zustands Patches bzw. Service Packs eingespielt werden müssen.

- *Compliant with Minor Issues*

Das Produkt entspricht den Microsoft-Standards für Verträglichkeit mit leichten Einschränkungen.

- *Not Compliant*

Das Produkt erfüllt die Microsoft-Standards für Verträglichkeit nicht.

- *Testing yet to be completed*

Das Produkt wurde noch nicht getestet oder der Test hat noch nicht begonnen; es wird jedoch einen Test geben.

- *Will not test*

Das Produkt wird nicht getestet.

Sie haben über nachfolgende Webseite Zugang zu dieser Liste, die einen Überblick über den aktuellen Stand gibt:

<http://www.microsoft.com/technet/topics/year2k/default.htm>

Auf dieser Webseite können Sie einsehen, mit welchen Produkten derzeit der Wechsel in das Jahr 2000 problemlos möglich ist und mit welchen Produkten dies zum abgefragten Zeitpunkt noch nicht oder nur mit Einschränkungen möglich ist.

Auch die Liste der noch nicht getesteten Produkte sollte eingesehen werden. Microsoft führt laufend notwendige Tests durch, und es ist deshalb ratsam, von Zeit zu Zeit den aktuellen Stand im Internet abzufragen.

Für alle getesteten Produkte gibt es zusätzliche ausführliche Informationen im Internet, um die Compliance-Informationen für Microsoft-Produkte im Detail nachlesen zu können. Alle hier von Microsoft aufgeführten Informationen können im Internet unter der folgenden Adresse eingesehen werden:

<http://www.microsoft.com/technet/topics/year2k/product/product.htm>

28.1.1

Windows 2000

Inzwischen ist bekannt und von Microsoft offiziell bestätigt, daß der Windows-NT-5.0-Familiename umbenannt wird in Windows 2000.

28 Die Jahr-2000-Problematik

Die Windows-2000-Produktlinie, die nach Angaben von Microsoft 1999 ausgeliefert werden soll, wird vier Produkte umfassen:

- *Windows 2000 Professional*
Workstation-Betriebssystem für Unternehmen beliebiger Größe.
- *Windows 2000 Server*
Eine Server-Lösung für kleine und mittlere Unternehmen. Windows NT 4.0 Server mit bis zu vier Prozessoren können auf dieses Produkt umgestellt werden.
- *Windows 2000 Advanced Server*
Die High-End-Server-Lösung mit integrierter Clustering- und Load-Balancing-Lösung.
- *Windows 2000 Datacenter Server*
Dies ist die High-High-End-Lösung, die ebenfalls Clustering- und Load-Balancing unterstützt. So unterstützt diese Variante noch mehr Prozessoren und kann mit bis zu 64 Gbyte Hauptspeicher ausgestattet werden.

Im Web von Microsoft ist hierzu folgende Aussage zu lesen:

„The new name also serves our goal making it simpler for customers to choose the right Windows products for their needs. The new naming system eliminates customer confusion about whether NT refers to client or server technology. Also, with our across-the-board improvements in ease of use, mobile support and total cost of ownership that provide benefits to so many users, NT technology is no longer just for high-end-workstations.“

(Brad Chase, Vice President at Microsoft)

Microsoft will mit der neuen Namensgebung auch zum Ausdruck bringen, daß diese Version für den Jahr-2000-Wechsel tauglich ist. Dies liest sich auf der Webseite folgendermaßen: *„Windows 2000 is ready for the next millenium.“*

28.2 Jahr-2000-Fähigkeit bei Novell

Die Testkriterien von Novell stimmen zum größten Teil mit den oben angeführten Punkten 1 bis 9 überein, so daß hierzu keine weiteren Ausführungen notwendig sind. Die Ergebnisse der aktuellen Tests zeigen die nachfolgenden Tabellen; aufgrund des Umfangs der Informationen habe ich mich auf das Wesentliche konzentriert. Detaillierte Informationen finden Sie unter der Internet-Adresse:

<http://www.novell.com/year2000>

Auf dieser Webseite gelangt man über die Option »Product Status« an eine Tabelle, die einen Überblick über den aktuellen Stand der Jahr-2000-Fähigkeit der Produkte bei Novell wiedergibt. Nachfolgend se-

28.2 Jahr-2000-Fähigkeit bei Novell

hen Sie einen Auszug aus der Tabelle die im August 1999 vom Internet geholt wurde. Besuchen Sie regelmäßig die Webseite, um sich über Neuerungen zu informieren. Sie können aber auch, wenn Sie das wünschen, Ihre E-Mail-Adresse durch Ausfüllen des entsprechenden Feldes auf der Webseite eintragen lassen, um automatisch über aktuelle Änderungen informiert zu werden. So spart man sich ein regelmäßiges Nachsehen, ob sich Neuerungen bezüglich der Jahr-2000-Verträglichkeit ergeben haben.

NetWare/intraNetWare Platform

Product	Status	Date Y2K Update oder Upgrade verfügbar
NetWare v5	Year 2000 Ready	JVM update to be provided in NW5 SP3. See Third party product list
NetWare v4.2 Language Versions (includes Year 2000 Ready English version)	Year 2000 Ready	No update necessary
NetWare v4.2 English Only Version	Year 2000 Ready	Optional update available
intraNetWare (including SMP and SFTIII support)	Year 2000 Ready	Optionaler Update erhältlich
NetWare v4.11 (including SMP and SFTIII support)	Year 2000 Ready	Optionaler Update erhältlich
NetWare v4.11 for OS/2	Year 2000 Ready with update	Optionaler Update erhältlich
NetWare v4.10 (not being supported for OS/2, SMP or SFTIII)	Currently Testing	Q4 1998
SMP for NetWare v4.10 (and prior versions)	Not being tested – Upgrade to NetWare 4.11 or NetWare 5	
SFTIII for NetWare v4.10 (and prior versions)	Not being tested – Upgrade to NetWare 4.11 SFT III	
NetWare 4.10 (and prior versions) for OS/2	Not being tested – Upgrade to NetWare 4.11 for OS/2	

28 Die Jahr-2000-Problematik

Product	Status	Date Y2K Update oder Upgrade verfügbar
NetWare 4.x versions prior to v4.10	Not being tested – Upgrade to NetWare 4.11 / intraNetWare oder NetWare 5	Update verfügbar
NetWare v3.2	Year 2000 Ready	
NetWare v3.12 *	Year 2000 Ready with update – Upgrade to NetWare 3.2, NetWare 4.11/intraNetWare, NetWare 5	
NetWare v3.11 and prior versions *	Not being tested – Upgrade to NetWare 3.2, NetWare 4.11/intraNetWare oder NetWare 5	

* Siehe auch Informationen über Upgrade Wizard von Novell

Product	Status	Date Y2K Update oder Upgrade verfügbar
NetWare for Macintosh v4.11	Year 2000 Ready	No update necessary
NetWare for Macintosh v3.12	Year 2000 Ready with update – Upgrade to NetWare 3.2, NetWare 4.11/intraNetWare oder NetWare 5	Update verfügbar
NetWare for Macintosh – versions prior to v3.12	Not being tested – Upgrade to NetWare 3.2 or NetWare 4.11 (includes Macintosh)	
NEW Novell Small Business Suite (NSBS) v5	Year 2000 Ready	No update necessary
NetWare for Small Business v4.11, v4.2	Year 2000 Ready	No update necessary
intraNetWare for Small Business (INSB) v1.1	Year 2000 Ready	Optional Update verfügbar
Personal NetWare v1.0 (English)	Year 2000 Ready	
NetWare Lite v1.1 (English)	Year 2000 Ready	

28.2 Jahr-2000-Fähigkeit bei Novell

High Availability & Clustering Products

Product	Status	Date Y2K Update oder Upgrade verfügbar
Novell High Availability Server for NetWare/intra-NetWare	Year 2000 Ready	Product Available
Novell StandbyServer for NetWare/intraNetWare	Year 2000 Ready	Product Available
Novell StandbyServer Many-to-One for NetWare/intraNetWare	Year 2000 Ready	Product Available
Novell SnapShotServer for NetWare/intraNetWare	Year 2000 Ready	Product Available

NetWare/intraNetWare Clients

Product	Status	Date Y2K Update oder Upgrade verfügbar
Novell Client v4.6 for Windows NT	Year 2000 Ready	No update necessary
Novell Client v4.51 for Windows NT	Year 2000 Ready	No update necessary
Novell Client v4.5 for Windows NT	Year 2000 Ready	No update necessary
Novell Client v4.3 for Windows NT	Year 2000 Ready	No update necessary
NetWare/intraNetWare Client for NT v4.11b for Windows NT	Year 2000 Ready	No update necessary
Novell Client v3.1 for Windows 95/98	Year 2000 Ready	No update necessary
Novell Client v3.02 for Windows 95/98	Year 2000 Ready	No update necessary
Novell Client v3.01 for Windows 95/98	Year 2000 Ready	No update necessary
Novell Client v3.0 for Windows 95/98	Year 2000 Ready	No update necessary
Novell Client v2.5 for Windows 95/98	Year 2000 Ready	No update necessary

28 Die Jahr-2000-Problematik

Product	Status	Date Y2K Update oder Upgrade verfügbar
Novell Client v2.71 for DOS/Win 3.x	Year 2000 Ready	No update necessary
Novell Client v2.7 for DOS/Win 3.x	Year 2000 Ready	No update necessary
Novell Client v2.6 for DOS/Win 3.x	Year 2000 Ready	No update necessary
Novell Client v2.5 for DOS/Win 3.x	Year 2000 Ready	No update necessary
NetWare/intraNetWare Client v2.20 for Win95 (Client 32)	Year 2000 Ready	Optional Update verfügbar
NetWare Client v2.12 for Win95 and prior versions	Not supported – Upgrade to latest client version	
NetWare/intraNetWare Client v2.20 for DOS/Win 3.1	Year 2000 Ready	Optional Update verfügbar
NetWare Client v2.12 for DOS/Win 3.1 and prior versions	Not being tested – Upgrade to intraNetWare Client 2.2 für DOS/Win 3.1	
NetWare/intraNetWare Client for NT v4.11a (Supports NT OS versions v3.51 and v4.0)(incl. WSMgr)	Year 2000 Ready	Optional Update verfügbar
NetWare/intraNetWare Client for NT v4.10 and prior versions	Not supported – Upgrade to latest client version	
intraNetWare Client v5.11 for Mac	Year 2000 Ready	No update necessary
NetWare/intraNetWare Client v2.12 for OS/2	Year 2000 Ready	No update necessary
NetWare/intraNetWare Client for OS/2 – v2.11 and prior versions	Not supported – Upgrade to latest client version	
NETX Client (NETX.EXE)	Not supported – Upgrade to latest client version	
NetWare Client VLM v1.21	Year 2000 Ready (Recommend Upgrade to intraNetWare Client 2.2 für DOS/Win 3.1	No update necessary

28.2 Jahr-2000-Fähigkeit bei Novell

Product	Status	Date Y2K Update oder Upgrade verfügbar
NetWare Client VLM v1.20 and prior versions	Not supported – Upgrade to NetWare Client VLM v1.21 (Recommend Upgrade to latest version)	
NetWare Client VLMIP	Not supported – Upgrade to latest client version	
NetWare Mobile Client v1.0	Not being tested – no upgrade path	
NetWare Mobile Client v1.0 all languages	Not being tested – no upgrade path	

Year 2000 Ready NetWare/intraNetWare Products

Product	Status	Date Y2K Update oder Upgrade verfügbar
Z.E.N.works (Includes Novell Client v4.3 for Windows NT, Novell Client v2.5 for Windows 95/98, and Novell Client v2.5 for DOS/Win 3.x)	Year 2000 Ready	No update necessary
Novell Web Server v3.1A	Year 2000 Ready	No update necessary
Novell Web Server 2.5 and prior versions	Not being tested – Upgrade to Novell Web Server v3.1A	
NetWare/IP v2.2 (for NetWare 4.11)	Year 2000 Ready	No update necessary
NetWare/IP v2.1	Not being tested – Upgrade to NetWare/IP v2.2 (for NetWare 4.11)	
Novell Application Launcher (NAL) v2.01	Year 2000 Ready	No update necessary
Novell Application Launcher (NAL) v1.1 and prior versions	Not being tested – Upgrade to NAL 2.01	
NDPS	Year 2000 Ready	No update necessary

28 Die Jahr-2000-Problematik

Product	Status	Date Y2K Update oder Upgrade verfügbar
Novell Replication Services 1.2 (NRS)	Year 2000 Ready	No update necessary
NDS for NT 1.0	Year 2000 Ready	No update necessary
Novell Administrator for Windows NT v2.0c	Year 2000 Ready	Optional Update verfügbar
Novell Administrator for Windows NT v2.0 and prior versions	Not being tested – Upgrade to Novell Administrator für Windows NT 2.0c	
Novell Cross-Platform Services (NCPS) v4.10b	Year 2000 Ready	Optional source code available to authorized partners
LDAP 1.0	Year 2000 Ready	No update necessary
NetWare Telephony Services (NTS) v2.11 and prior versions	Not being tested – Upgrade to NTS 2.21	
DHCP v2.1	Year 2000 Ready	No update necessary
DHCP v2.0b and prior versions	Not being tested – Upgrade to DHCP v2.1	
ODI LAN Driver (dev kit)	Year 2000 Ready	No update necessary
NetWare for DEC Access	Not being tested – no upgrade path	

Collaboration Products

Product	Status	Date Y2K Update or Upgrade Available
GroupWise 5.2	Year 2000 Ready	No update necessary
GroupWise 5.2 Administration	Year 2000 Ready	No update necessary
GroupWise 5.2 Client for Mac, Unix, Win 3.1, Win 95/NT	Year 2000 Ready	No update necessary
GroupWise 5.2 Manage-Wise Agent (NLM, NT, UNIX)	Year 2000 Ready	No update necessary
GroupWise 5.2 Monitor	Year 2000 Ready	No update necessary

28.2 Jahr-2000-Fähigkeit bei Novell

Product	Status	Date Y2K Update or Upgrade Available
GroupWise 5.2 Language Versions	Year 2000 Ready	No update necessary
GroupWise WebAccess 5.2(NLM, NT)	Year 2000 Ready	No update necessary
GroupWise WebAccess 4.1	Not being tested. Upgrade to WebAccess 5.2	
GroupWise Internet Agent (NLM, NT)	Year 2000 Ready	No update necessary
GroupWise 5.0 & 5.1 – All components	Not being tested – Up- grade to GW 5.2	
GroupWise v4.1	Year 2000 Ready	No update necessary
GroupWise v4.1 Administration	Year 2000 Ready	No update necessary
GroupWise v4.1a Client for Win 3.1	Year 2000 Ready	No update necessary
GroupWise v4.1 Admin & Post Office Servers for NLM and OS/2	Year 2000 Ready	No update necessary
GroupWise v4.1 Client for Macintosh	Not being tested – Up- grade to GW 5.2	
GroupWise v4.1 Clients for DOS and Unix	Not being tested – Up- grade to GW 5.2	
GroupWise v4.1 Servers for DOS and Unix	Not being tested – Up- grade to GroupWise 4.1 NLM or GW 5.2	
GroupWise v4.1 PhoneAccess (OS/2)	Not being tested – Up- grade to GW 5.2	
GroupWise Async Gateway (NLM, OS/2)	Year 2000 Ready	No update necessary
GroupWise API Gateway v4.1(NLM, OS/2)	Year 2000 Ready	No update necessary
GroupWise Async Gateway (DOS) v4.1	Not being tested – Up- grade to Async Gateway (NLM) oder GW 5.2	

28 Die Jahr-2000-Problematik

Product	Status	Date Y2K Update or Upgrade Available
GroupWise Fax/Print Gateway (DOS) v2.0	Not being tested – No Upgrade Path	
GroupWise cc:Mail Gateway (OS/2)	Year 2000 Ready	No update necessary
GroupWise MS Mail Gateway (OS/2)	Year 2000 Ready	No update necessary
GroupWise Notes Gateway (OS/2)	Year 2000 Ready	No update necessary
GroupWise Pager Gateway v4.1 NLM (not OS/2)	Year 2000 Ready	No update necessary
GroupWise SMTP/MIME Gateway v4.1 NLM	Year 2000 Ready	No update necessary
GroupWise X.25 Gateway (OS/2)	Year 2000 Ready	No update necessary
GroupWise X.400 Gateway (NLM, OS/2)	Year 2000 Ready	No update necessary
GroupWise v4.1 SNADS Gateway (NLM, OS/2)	Gateway Supported but not Y2K tested. Applications that use gateway should be user/developer tested for Y2K issues.	
GroupWise v4.1 Office-Vision/VM&PROFS Gateway(NLM, OS/2)	Gateway Supported but not Y2K tested. Applications that use gateway should be user/developer tested for Y2K issues.	
GroupWise v4.1 MHS Gateway (DOS)	Not being tested – No Upgrade Path	

28.2 Jahr-2000-Fähigkeit bei Novell

Border Manager

Product	Status	Date Y2K Update oder Upgrade verfügbar
Border Manager Authentication Services 1.0 (BMAS 1.0)	Year 2000 Ready	No update necessary
Border Manager v2.1	Year 2000 Ready with update	Update verfügbar
FastCache 1.0	Year 2000 Ready	No update necessary

Network Management

Product	Status	Date Y2K Update oder Upgrade verfügbar
ManageWise 2.6	Year 2000 Ready	NEW PRODUCT – Is Shipping
ManageWise v2.5	Year 2000 Ready with update	Update verfügbar
ManageWise v2.1 and prior versions	Not being tested – Upgrade to ManageWise 2.6	
NetWare Management Agent (NMA) v2.1	Year 2000 Ready	No update necessary
NetWare Services Manager (all versions)	Not being tested – No upgrade path available	
NetWare Management System v2.1 and prior versions	Not being tested – Upgrade to ManageWise 2.6	
LANalyzer for Windows v2.2	Year 2000 Ready	No update necessary
NetWare LANalyzer Agent v1.21	Year 2000 Ready	No update necessary
NetWare LANalyzer Agent v1.1 and prior versions	Not being tested – Upgrade to LANalyzer Agent 1.21	

28 Die Jahr-2000-Problematik

Product	Status	Date Y2K Update oder Upgrade verfügbar
LANtern Network Monitor for Ethernet (all versions)	Not being tested – no upgrade path	
LANtern Services Manager (all versions)	Not being tested – no upgrade path	

MultiProtocol Router Products

Product	Status	Date Y2K Update oder Upgrade verfügbar
MultiProtocol Router v3.1 (NetWare Enterprise Router 16 WAN Port configuration)	Year 2000 Ready	No update necessary
MultiProtocol Router v3.1 (NetWare BranchLink Router 2 WAN Port configuration)	Year 2000 Ready	No update necessary
MultiProtocol Router v3.0 (NetWare Enterprise Router configuration)	Not being tested – Upgrade to MPR 3.1 (NetWare Enterprise Router 16 WAN Port) or Border Manager 2.1	
MultiProtocol Router v3.0 (NetWare BranchLink Router configuration)	Not being tested – Upgrade to MPR 3.1 (NetWare BranchLink Router 2 WAN Port v3.1) or Border Manager 2.1	
MultiProtocol Router v2.2 and prior versions	Not being tested – Upgrade to Border Manager 2.1	
WAN Extensions v3.1	Year 2000 Ready	No update necessary
WAN Extensions v3.0	Not being tested – Upgrade to WAN Extensions v3.1 or Border Manager 2.1	

28.2 Jahr-2000-Fähigkeit bei Novell

Product	Status	Date Y2K Update oder Upgrade verfügbar
SNA Extensions v3.1	Not being tested – No Upgrade Path	
SNA Extensions v3.0	Not being tested – No Upgrade Path	

Host Connectivity

Product	Status	Date Y2K Update oder Upgrade verfügbar
NetWare for SAA v3.0 (intraNetWare for SAA v3.0)	Year 2000 Ready	No update necessary
NetWare for SAA v2.0	Year 2000 Ready	No update necessary
NetWare for SAA v2.2 (incl. Services Manager)	Year 2000 Ready	No update necessary
NetWare for SAA: AS/400 Edition	Year 2000 Ready	No update necessary
intraNetWare for SAA: AS/400 Edition 2 (mistaken as SAA 2.3 also)	Year 2000 Ready	No update necessary
NetWare HostPrint 2	Year 2000 Ready	No update necessary
NetWare HostPrint/400	Year 2000 Ready	No update necessary
NetWare Hostprint 1.11	Year 2000 ready with update	Update verfügbar
NetWare Hostprint 1.1 and prior versions	Not being tested – Upgrade to HostPrint 1.11	No update necessary
intraNetWare Host Publisher	Year 2000 Ready	
NetWare for SAA 1.3b	Not being tested – Upgrade to SAA 2.2 or SAA:AS/400 Edition 2	

28 Die Jahr-2000-Problematik

Dial-in/Dial-Out Connectivity

Product	Status	Date Y2K Update oder Upgrade verfügbar
NetWare Connect v2.0	Year 2000 Ready	No update necessary
NetWare Connect v1.0	Not being tested – Upgrade to NetWare Connect 2.0 or Border Manager 2.1	
NetWare Connect View v2.0	Year 2000 Ready with update	Update verfügbar

NFS/UNIX Products

Product	Status	Date Y2K Update oder Upgrade verfügbar
intraNetWare NFS Services v2.3 (NetWare/intraNetWare 4 Edition)	Year 2000 Ready	No update necessary
intraNetWare NFS Services v2.12	Year 2000 Ready	No update necessary
intraNetWare NFS Services v2.1	Year 2000 Ready	No update necessary
intraNetWare NFS Services v1.2c	Year 2000 Ready	No update necessary
intraNetWare Print Services for UNIX (UPS) v2.12	Year 2000 Ready	No update necessary
NetWare NFS v1.2c/NFS Gateway v1.2 Bundle	Year 2000 Ready	No update necessary
FLEx/IP v1.2c	Year 2000 Ready	No update necessary

Man sieht am Beispiel dieser beiden Firmen, daß es ein nicht unerheblicher Aufwand ist, bis man alle Produkte vollständig auf Jahr-2000-Verträglichkeit überprüft hat. Es sollte deshalb nicht vergessen werden, daß man sehr frühzeitig beginnt, sich mit diesem Problem auseinanderzusetzen, je früher, desto besser. Der 1.1.2000 und die darauffolgenden Monate werden zeigen, mit welchen Schwierigkeiten man unter Umständen noch rechnen muß bzw. bei welchen Komponenten vergessen worden ist, diese auf Jahr-2000-Verträglich-

28.2 Jahr-2000-Fähigkeit bei Novell

keit zu prüfen. Es ist bereits heute eine Fluggesellschaft bekannt, die am 1.1.2000 keine Starts und Landungen durchführen will, weil das Risiko hierfür zu groß ist.

Wenn Sie beim Lesen bis hierher gekommen sind, dann haben Sie (und auch ich) es geschafft: Das Buch ist zu Ende. Ich hoffe, es ist mir gelungen, auch komplizierte Sachverhalte einfach und verständlich darzustellen, so daß das breite Spektrum der Netzwerktechnik durchschaubarer und vor allem handhabbar für Sie geworden ist. Es ist nicht immer ganz einfach, einen zum Teil trockenen Stoff leicht lesbar und trotzdem anschaulich zu formulieren. Meine langjährige Erfahrung auf dem Gebiet der Netzwerktechnik und meine Erfahrungen im Bereich Schulung helfen jedoch dabei, in den meisten Fällen die richtigen Worte zu finden.

Sollten an der einen oder anderen Stelle Verbesserungsvorschläge angebracht sein, dann scheuen Sie sich nicht, mich davon in Kenntnis zu setzen. Für Anregungen bin ich immer dankbar. Sie können mir helfen, dieses Buch für die nächsten Überarbeitungen noch besser zu machen.

Stichwortverzeichnis

!

10/100 Auto-Negotiation 137
 100Base-T-Regeln 138
 100VG-AnyLAN Hub 151
 100VG-AnyLAN Network Link 152
 100VG-AnyLAN Nodes 152
 100VG-AnyLAN von HP 150
 100VG-AnyLAN-Komponenten 151
 100VG-AnyLAN-Netzwerken 152
 10Base2 92
 10Base5 92
 10Base-F 92
 10Base-T 92, 103, 107
 10BASE-T-Concentrator 105
 10BASE-T-Standard 106
 10Broad5 92
 1-persistent 78
 2-Zeichen-Eingabe 1056
 3270-Wel 111
 32-Bit API 865
 32-Bit-Adreßraum 854
 32-Bit-Architektur 909
 3C503 668
 3C505 668
 3C523 668
 3CO 96
 4-Zahlen-Format 1056
 64-Bit-Prozessor 976
 64-Bit-VLM 976
 802.2-LLC-Interface-Spezifikationen 172
 802.6 411
 80286-Protected-Mode-Betriebssystem 497
 9/9/99 1054

A

AAL 165
 Abakus 31
 Abend-Recovery-Optionen 701
 Ablaufdatum des User-Account 608, 927
 Abort Remirror 772
 Abschlußwiderstand 94
 Access Control 614, 1051
 Access Control List 723, 744, 874

Access Token 871
 AccessLink 382
 Accessories and Applications 896
 Account Disabled 928
 Account Operator 931, 967
 Account-Balance 608
 Accounting 596, 661, 717, 892
 Accounting-Dienste 603
 Accounting-System 603, 608
 Account-Management 608
 ACL 723, 874
 ACL-Liste 744
 ACL-Property 744
 ACS 317
 Active Directory 969, 970, 979
 Adaptionsschicht 165
 Adaptive Routing-Methode 314
 ADD NAME SPACE (Befehl) 670
 Add-On 876
 Address Translation 789
 Administration Directory Management
 Domain 1049
 Administration Management Domain 1025
 Administration, zentrale 514
 Administrationsoberfläche 792
 Administratoren 930, 967
 Advanced-Server 907, 923
 Ändern RWXD 944
 Änderungsschnittstelle 1047
 Äquivalenzdefinitionen 601
 AHA1520 668
 AHA1540 668
 AHA1640 668
 AHA1740 668
 AIC7770 668
 Aktuelle Normen 224
 Allied Telesyn 284
 Alloc Pool 570
 ALLOW 656
 American Power Conversion 284
 Anpassung der Paketgröße 347
 Anschlußeinheiten 454
 ANSI X3T9.5 140

Stichwortverzeichnis

- Anwendungsschicht 317
- Anwendungs-Software 483
- Anwendungs-Standards 536
- Anzeigen 943
- APC 284
- APIs 1034
- APPC 482
- Apple 626
- Apple Filing Protocols 506
- Apple-Computer 506
- Apple-Macintosh 543
- AppleTalk 559, 620, 621, 626, 882
- AppleTalk Filing Protocol 628
- Appletalk Transaction Protocol 554
- Application Layer 317
- Application Programming Interfaces 859, 1034
- Application Services 730
- Application-Level Gateway 1002
- Applications 896
- Arbeitsplatzrechner 461, 474, 478
- Archive Needed 617
- Archive-Server 52
- Archivierungs-Server 553
- ARCNET 65, 88, 442
- Arcor 429
- Arithmetische Einheit 32
- ASCII-Zeichen 296
- ASMP 863
- Asymmetrisches Multiprocessing 863
- Asynchrone Datenübertragung 295
- Asynchrone Service-Schnittstelle 557
- Asynchroner Datenverkehr 414
- Asynchronous Transfer Mode 159
- ATM 159, 426
- ATM LAN-Emulation 167
- ATM Services 977
- ATM-Netzwerke 160, 162
- ATM-Zellen 161
- ATOTAL 657
- ATP 554
- ATTACH 653
- Attachment Unit Interface 108
- Attributes 861
- Attribut-Sicherheit 601
- Auditcon 768
- Auditing 705, 933
- Auditing-System 933
- Aufbau von Hubs 215
- AUI 108
- Ausdehnung von LANs 43
- Ausgabe 32
- Auswahlkriterien für LANs 436
- Ausweichzeichen 297
- Authentication 891, 1051
- Authentifizierung 977
- Authentisierung 1051
- AUTOEXEC.BAT 576, 607
- Automatische Fehlersignalisierung 364
- AVM 285
- B**
- Babbage 32
- Backbone 126
- Backbone-Verkabelung 199
- backoff 77
- Backup Domain-Controller 919
- Backup Operators 931
- Backup Server 459
- Backup-Dienstprogramm 971
- Bandbreite 72
- Bandwith/ATM-Service 429
- Banyan Vines 884
- BASIC 758
- Basisband 71, 72
- Basis-I/O-System 875
- Basis-Mode-Protokolle 302
- Bay Networks 285
- Beginning of Message 414
- Benutzer-Equivalence 599
- Benutzername 871, 926
- Benutzerprofil 911
- Benutzerverwaltung 910
- Berechtigungsmarke 78
- Beteiligte Stationen 46
- Betriebsarten 301
- Betriebssystemkern 563
- Betriebssystem-Kernel 781, 859
- Bewegtbild 74, 402
- BIGFON 408
- Bildfernsprechen 408
- BIND (Befehl) 670
- Bindery 596, 601, 757, 910
- Bindery-Dateien 596
- Bindery-Eintrag 757
- Bindery-Emulation 739

Stichwortverzeichnis

Bindery-Kompatibilität 739
 Bindery-Komponenten 596, 597
 Bindery-Objekt 598
 Bindery-Sicherheit 596, 597
 Bindery-Überprüfung 639
 BINDFIX 657
 Binding 886
 BINDREST 657
 BIOS 1053
 bit stuffing 298
 Bitserielle Informationsübertragung 42
 Bit-Synchronisation 296, 298
 B-Kanal 388, 399
 Blockbildung 301
 Blocknumerierung 301
 Blocks Read 605
 Blocks Written 605
 Blockungsgröße 579
 BNC-Stecker 111
 BNC-T-Stecker 102
 BOM 414
 Boole 31
 Bottom-Up-Angabe 734
 Breitband 71, 72
 Breitband-ISDN 407, 426
 Breitbandkommunikation 419
 Breitband-Netz 73
 Breitband-System 74
 Breitbandtechnologie 72
 Bridge 200, 329, 331, 461
 Bridging Router 342
 Broad-Cas 319
 BROADCAST (Befehl) 672
 Brouter 200, 329, 342
 Browse 745
 Bürokommunikation 486
 Burst Mode Protocol 709
 Bus A 412
 Bus B 412
 Bus-Struktur 83
 Bussysteme 64, 75
 Bustopologie 43, 63
 Busverkabelung 64
 Byte-(Oktett-)Synchronisation 296
 Byte-Synchronisation 296

C
 C (NLM-Technik) 522
 Cabletron 285
 Cache-Manager 868
 Cache-Puffer 567
 Caching 586, 785
 Caching-Mechanismus 781
 Caching-Verfahren 584
 CAPTURE 655
 Capture 768
 Carrier Sens 95
 CASTOFF 654
 CASTON 654
 CAT-4-RJ45 235
 CAT-5-Kabel 234
 CAT-5-Spezifikationen 235
 Catalog Services 795
 Catalog Services Manager 795
 CCITT 386
 CCITT-X.400-Standard 1013
 CCITT-X.500-Standard 1041
 C-Concentrator 141
 CDFS 855
 CD-ROM 632
 CD-ROM-Laufwerk 766
 CD-ROM-Schutz 281
 CD-ROM-Server 457
 CD-ROM-Unterstützung 633
 Certificate Server 977
 Chaining 1048
 Charge Rates 605
 Chat 278
 Cheapernet 91, 101
 CHKDIR 654
 CHKVOL 655
 City-Netz 363
 Class-A 140
 Class-B 140
 CLEAR STATION (Befehl) 672
 CLIB 762
 CLIB (NLM) 673
 CLIB-Erweiterung 762
 Client für Windows NT 525
 Client/Server-Modell 857
 Client32 525
 Client-Dienste 708
 Client-Server 500

Stichwortverzeichnis

- Client-Server-Modell 545
- Client-Server-Prinzip 539
- Client-Server-Protokoll NCP 558
- Client-Server-Protokolle 538
- CLS (Befehl) 672
- Cluster-Technologie 494, 815
- CMC 1035
- Code-Konvertierung 460
- Codierung 301
- COGEN 96
- Collapsed Backbone 206
- Colorpal 666, 770
- COM 414
- Commandline-Utilities, 653
- Common Gateway Interface (CGI) 815
- Common Messaging Calls 1035
- Common-Name 733
- Communication Protocols 559
- Communication-Server 460, 481, 488
- Complete Trust-Modell 922
- Compliance-Informationen für Microsoft-Produkte 1057
- Component Object Model 974
- Compu-Shac 96
- CONFIG (Befehl) 670
- Config Reader 636
- Connect Time 605
- Connections-Lizenz 546
- Connectivity 698, 750
- Console 619
- Consolen-Befehle 653, 772
- ConsoleOne 791, 812
- Container-Objekt 724, 725, 739
- Context 732, 733
- Context des Objekts 733
- Continuation of Message 414
- Control Panel 896
- Controlled Cryptography Service (CCS) 810
- Copy Inhibit 617
- Corporate Networks 405
- Country 726
- Create 613, 614, 745
- CREATOR OWNER 946
- CSMA 75
- CSMA/CA 75
- CSMA/CD 75, 172
- CSMA/CD-Netz 101
- CSMA/CD-Verfahren 78
- CSMA/CD-Zugriffsverfahren 75
- CSMA/CE 75
- Customer Access System 416
- Customer Gateway 416, 417
- Customer Network Interface Unit 418
- Cut-Through-Switches 349
- C-Worthy Menüs 677
- Cx 768
- D**
- DAP 1049
- Data Confidentiality 1029
- Data Integrity 1029
- Data Link Protocol 909
- Data Migration 703
- Data Set 600
- Datagramm 313, 323
- Datagramm Delivery Protocol 554
- Datagrammschnittstelle 555
- Datagrammtechnik 314
- Datapoint 83
- Dateiattribute 612, 774, 902
- Datei-Besitzrecht 947
- Datei-Einträge 590
- Dateien sehen 960
- Dateiname, globaler 516
- Dateinamenskonventionen 557
- Datei-Rechte 612
- Datei-Sharing 39
- Dateisystem 597, 702
- Datei-Trustee-Einträge 590
- Datei-Trustee-Liste 591
- Datenbank-Server 482, 553
- Datenfernübertragung 37, 294
- Datenformat 45, 59, 301
- Datenkabel 218
- Datenkommunikation 306
- Datenmanipulation 564
- Datenpaket 45, 296
- Datensammelstation 486
- Datenschutz 477, 502
- Datensicherheit 477, 502, 595
- Datentransferphase 299, 300
- Datentransfer-Rate 448
- Datenübertragung 75, 294, 301, 476
- Datenverbund 355

Stichwortverzeichnis

- Datex-M 422
- Datex-P 379
- Datex-P Business 380
- Datex-P ISDN Access 381
- Datex-P Remote Access 380
- Datumsabgleich 1054
- Datumsangaben 1054
- Datumseingabe 1054
- Datumsformat 1055
- DCB 668
- DDN-Network Information Center 323
- DDP 554
- De Morgan 31
- DEC 451
- DEC VAX 478
- DEC-Alpha 854
- DECnet 543, 626
- dedicated 553, 883
- Default Accounts 894
- Default-Partition 736
- Delete 745
- Delete Inhibit 617, 618
- DELETED.SAV – Directory 594
- DEModulator 74
- Department of Defense 322
- Desktop Access 278
- Desktop Remote 278
- Desktop-Access-Funktionen 282
- DHCP Server 759
- DI 91
- Dialog-Terminals 37
- Dienste 1022, 1045
- Dienstintegration 360
- Digital Equipment 39, 91, 96
- Digital Network 386
- Digital Service Unit 425
- DIN 44312-5 240
- Directory Access Protocol 1049
- Directory Cache Buffer 785
- Directory Entry Tabellen (DET) 785
- Directory Service Security 706
- Directory Services 318, 969, 1041
- Directory System Protocol 1050
- Directory-Attribute 612, 774
- Directory-Block 590
- Directory-Caching 447, 567, 584, 586
- Directory-Eintrag 590, 597
- Directory-Hashing 567, 584
- Directory-Pfad 616
- Directory-Rechte 612
- Directory-Replication 914
- Directory-Services-
Sicherheitsmechanismen 743
- Directory-Tabellen 589
- Directory-Trustee-Einträge 590
- Directory-Überprüfung 639
- DISABLE LOGIN (Befehl) 672
- DISABLE TTS (Befehl) 672
- Disk Allocation Block 579
- Disk Allocation Block Size 576, 579, 583, 605
- Disk Caching 648, 806
- Disk Duplexing 781
- Disk Mirroring 642, 781
- Disk Storage 605
- Disk-Driver 629, 668
- Disk-Duplexing 642, 643
- Disk-I/O 575, 577
- Diskless-Workstation 488
- DISMOUNT (Befehl) 672
- DISPLAY NETWORKS (Befehl) 670
- DISPLAY SERVERS (Befehl) 671
- Distributed Applications 539, 543
- Distributed COM (DCOM) 974
- Distributed File System (DFS) 971
- Distributed Networks 883
- Distributed Queue Dual Bus 411
- Distributed Run Queue 783
- Distribution List 1021
- D-Kanal 388, 399
- DL 1021
- DLC-Protokoll 302
- DLP 909
- DNS Server 760
- DNS/DHCP-Dienste 803
- DNS-Clients 970
- DNS-Datenbank 970
- DoD 322
- Dokument, integriertes 515
- Dokumentation 720
- Domain 884, 913
- Domain Network 884, 885
- Domain Users 932
- Domain-Administrator 885
- Domain-Controller 919

Stichwortverzeichnis

- Domain-Konzept 915
 - Domain-Network-Konzept 882
 - Domänen-Konzept 967
 - DOS 503, 560
 - DOS Client Software 708
 - DOS Requestor 708
 - DOS-Dateiservice 556
 - DOS-Funktionsaufrufe 565
 - DOS-Interrupt 21H 565
 - DOS-Umgebung 565, 872
 - DOWN (Befehl) 672
 - DOWN LOAD 486
 - DQDB 411
 - DQDB-Standard 412
 - DQDB-Technik 411
 - Driversoftware 876
 - Druckdienste 718
 - Drucken 948
 - Druckerverwaltung 911
 - Druck-Server 553
 - DS 318
 - DS Migrate 763
 - DSDIAG (DS Diagnostics) 797
 - DSP 1050
 - Dspace 660
 - Dsrepair 768
 - DSU 425
 - Dual Attachment Concentrator 147
 - Dual Attachment Station 147
 - Dual MAC-Option 140
 - Duplex-Betrieb 294
 - Durchsatz 78
 - Durchschaltvermittlung 411
 - Dynamic DNS 970
 - Dynamic DNS (DDNS) 970
 - Dynamic Host Configuration Protocol (DHCP) 802, 970
 - Dynamic Resource Configuration 569
 - Dynamisches Load Balancing 819
- E**
- Early Token Release 125, 128
 - ECB 622
 - ECMA 319
 - Edge Gateway 418
 - EDIT (NLM) 670
 - EDV-Konzept 502
 - Effective Rights 724
 - Effektives Recht 616
 - Eigenschaften von Windows NT 870
 - Eigentümer 960
 - Eingabe 32
 - Einprotokoll-Router 341
 - Einrichten eines Internet-Anschlusses 994
 - Eintrag 1045
 - Electronic Mail 39, 54, 288, 876, 887
 - Electronic-Mail-Systeme 1013
 - Elektromagnetische Verträglichkeit 221, 228
 - Elevator-Seeking 587
 - Elevator-Seeking-Algorithmus 588
 - E-Mail 991
 - Empfänger 294
 - Empfängeradresse 299
 - Empfangseinheit 293, 294
 - EN 50 173 225
 - EN 50173 240
 - EN 55022 224
 - ENABLE LOGIN (Befehl) 672
 - ENABLE TTS (Befehl) 672
 - Encrypted Password 598, 601
 - Encrypted Tunnel 1010
 - End of Bus 413
 - End of Message 414
 - End of Text 296
 - End of Transmission 296
 - ENDCAP 656
 - end-to-end-Protokoll 324
 - ENIAC 33
 - Enterprise JavaBeans 522
 - Entwicklungsgeschichte 489
 - Environment Subsystems 872
 - EOB 413
 - Erase 613, 614
 - Erkennung von Eindringlingen 611
 - Error-Log-File 641
 - Ersatzwegeschaltung 364
 - Erweiterbarkeit 852
 - ETHERNET 39, 91
 - Ethernet 87, 170, 325, 442, 500
 - Ethernet Frame 634
 - Ethernet Standard 172
 - Ethernet_802.3 Frame 634
 - Ethernet-Cross-Point-Switch-Netzwerken 156

Stichwortverzeichnis

- Ethernet-LAN-Driver 634
- Ethernet-Switching, klassisch 156
- Event Control Block 622, 623
- Everyone 946
- Execute Only 617
- Executive 866
- Executive Driver 868
- EXIT (Befehl) 671
- Export-Server 914, 938
- Extended MAPI 1036
- Extended Partitions 904
- Extranet 1011

- F**
- Fast Ethernet 134, 171
- Fast Ethernet LANs 131
- FastTrack Server 815
- FAT 569, 579, 580, 641, 875, 890, 939
- FAT-Dateisystem 940
- FAT-Eintrag 580, 583
- FAT-Index 582
- FAT-Tabellen 785
- Fault Tolerance 737
- Faults 856
- Fax-Server 49, 458
- Fconsole 666
- FDDI 88, 140
- FDDI Physical Layer Protocol 145
- FDDI Physical Medium Dependent 146
- FDDI-LAN 140
- FDDI-Protokoll 141
- FDDI-Ring 140
- FDDI-Station-Management 147
- FDDI-Stationstypen 147
- FDDI-Topologie 140
- Fehlererkennung 301, 639
- Fehler-Tolerante-NetWare 476
- Fehlertoleranz 476, 952
- Fernnetze 38, 45
- Fernskizzen 402
- Fernsprechen 378, 382
- Fernsprechnet 359
- Festbilder 74
- Festplattenverwaltung 476, 575
- Festverbindung 363
- Fibre Distributed Data Interface 88
- Fibre Optic 123
- File Allocation Table 579, 580, 639, 875, 939
- File Caching 806
- File Manager 896
- File Scan 614
- File Services 704
- File System Recovery 875
- File System Security 706
- File Systems 868
- File Transfer 278
- File Transfer Protocol (FTP) 325
- File-by-File Compression 702
- File-Caching 447, 567, 586
- File-Manager 886
- Filer 659, 770
- File-Server 47, 62, 446, 450, 454, 481
- File-Server-Sicherheit 601, 618
- File-Server-System 587
- File-Service 495
- File-Service Core Protocol (NCP) 552
- File-Sharing 39, 539, 540
- File-System-Performance 547
- File-Transfer 288, 325
- Filterstrategien 1001
- FireWall-Architekturen 1003
- FireWall-System 468, 998
- Firmengelände 43
- FLAG 655
- Flag 767
- FLAGDIR 655
- Floppy-Laufwerk-Schutz 280
- Flußkontrolle 301
- Flußsteuerung 45, 313
- Folgenummer 324
- Formelle Methode 554
- Frame 46
- Frame Relay 378
- Frame-Größe 172
- Frame-Relay-Service 429, 430
- Frame-Relay-Technik 411
- Free Space 904
- Frei-Token 84
- Frequenzspektrum 74
- FTAM 317
- FTP 325, 627, 888
- FTP Server 758
- Full Name 927
- Full-Duplex-Mechanismus 175

Stichwortverzeichnis

Funktionsverbund 355

G

Gateway 126, 329, 343, 460
 Gateway-Rechner 460
 Gateway-Server 483
 Gebührensatz 605
 General Motors 84
 Geschirmte Kabel 219
 Gigabit Ethernet 171
 Gigabit Ethernet Migration 185
 Glasfaser 446
 Glasfaserkabel 45, 72, 140, 214
 Gleichlaufverfahren 301
 Global Queue 783
 Globale Gruppe 288
 Globalen Catalogs (GC) 980
 Global-Network-Strategie 511
 Grace Logins 609, 610
 GRANT 656
 Graphical User Interface 714, 749
 graphisches SYSCON 676
 Greenwich Mean Time 1056
 Großrechner 481
 Group Scheduling 887
 GroupWare Messaging AntiVirus 281
 Gruppe 606
 Gruppenzugehörigkeit 928
 GTBecker 1056
 Guests 930
 GUI 767, 865
 GUI-Programm 795
 GUI-Systeme 771

H

HAL 853, 859, 869
 HAL Dynamic Link Library 860
 Half-Duplex-Betrieb 294
 Half-Duplex-Flußkontrolle 176
 Half-Duplex-Modus 176
 Hardware Abstraction Layer 853, 859, 869
 Hardware Assistent 972
 Hardwarekonfiguration 472
 Hardware-Sicherheit 595
 Hash-Algorithmus 584
 Hauptspeicher 447
 HDLC 298

HDLC/SDLC-Protokolle 302
 Head of Bus 413
 Help 772
 Hermaphroditischer Stecker 112, 114
 Heterogener Workstation Support 695
 Hewlett Packard 96
 Hidden 617, 618
 High Level Data Link Control 298
 High Performance File System 875, 939
 High- und Low-Trigger-Last 784
 High-Speed-Token-Ring (HSTR) 186
 Hinzufügen & Lesen -RWX 944
 Hinzufügen WX 944
 HOB 413
 Hollerith 32
 Home-Directory 928
 Hostbasierende Server 531
 Host-Gateway 461
 Host-Rechner 481
 Hot Fix II 646
 Hot Fix Redirection Area 576
 Hot Plug PCI 793
 Hot-Fix-Mechanismus 640
 Hot-Spare 646
 HPFS 875, 890, 939
 HPFS Dateisystem 940
 Hub-Management 215, 217, 270

I

I/O Manager Device Driver 876
 I/O- und Datei-Systeme 875
 I/O-Belastung 443
 I/O-Manager 868
 I/O-Operation 875
 I/O-Request-Paket 877
 I/O-System 859, 868
 I2O 794
 I2O Architektur 976
 IAE 391
 IB 96
 IBM 33, 40, 550
 IBM 3600/4700 111
 IBM 4300 111
 IBM 525 111
 IBM 8100 111
 IBM 821 121, 122
 IBM 8228 120

Stichwortverzeichnis

- IBM PC 40
- IBM Year 2000 1056
- IBM-Gateway-Schnittstelle 557
- IBM-Kabeltyp 120
- IBM-MVS-Großrechner 543
- IBM-Token-Ring 116
- IBM-Token-Ring-Kabel 446
- IBM-Verkabelungssystem 111
- ICAN 425
- IDE 668
- IDN 386
- IDN Plus 419, 421
- IEEE 319
- IEEE 1003.1 855
- IEEE 802. 111, 319
- IEEE 802.1 319, 320
- IEEE 802.3 320
- IEEE 802.3x-Standard 176
- IEEE 802.4 83
- IEEE 802.5 116, 125
- IEEE 802.6 412
- IEEE 802.x-Full-Duplex/Flow-Control-Standard 175
- IEEE-802-High-Speed-Token-Ring-Standards 195
- IETF Service Location Protocol (RFC 2165) 801
- Import-Computer 914
- Import-Server 938
- Indexed 582, 617
- Individual Customer Access Network 425
- Individuelle Datenverarbeitung 475
- Informations-technischer Anschluß 228
- Informelle Methode 553
- Inherited Rights Filter 724, 745
- Inherited Rights Mask 612, 613, 616, 660
- Initial Profile 896
- Initial User Account 895
- Initialisierung 301
- InocuLAN 280
- In-Place Upgrade Utilities 632
- INSTALL (NLM) 669
- Institution of Electrical Engineers (IEE) 1056
- Integral Subsystem 866
- Integrated Services 386
- Integrated Services Digital Network 74
- Integration von LANs 484
- Integrity Checking 280
- Intel 39, 91
- Intel 8088 Prozessor 40
- Intelligent Input Output System 976
- Intelligenz, periphere 516
- INTERAKTIV 946
- Interconnection 217
- interframe gap 77
- Inter-MSS Router 418
- International Alphabet No.5 1023
- International Standard Organisation 42
- Internes Routing 621
- Internet Access Service 429
- Internet Domain Name Service (DNS) 981
- Internet Information Server (IIS) 975
- Internet Packet Exchange 554
- Internet Protocol (IP) 323
- Internet Security 989
- Internet Services 519
- Internet/Intranet 967, 989
- Internet-Access-Service 432
- Internet-Web/Database-Development-Umgebung 522
- Internetwork Packet Exchange Protocol 626
- Internetworking 329
- Internetwork-Konzept 563
- Internet-Zugang 374
- Interprocess Communication 859, 864
- Interrupt Monitoring 280
- Intranets 1005
- intraNetWare for Small Business 494, 678
- intraNetWare for Small Business 4.11 776
- Intruder 611
- Inventory Manager 278
- IOEngine 684
- IP 323, 798
- IP-/IPX-Tunneling-Unterstützung 1010
- IP-basierendes Drucken 806
- IPC 627
- IPTUNNEL 669
- IPX 538, 554, 619, 621, 798
- IPX/IP Gateway 761
- IPX/SPX 321, 559, 620, 627, 781, 882
- IPX-basierendes Drucken 806
- IPX-Endgeräte 271
- IPX-Protokoll 1010
- IPXS (NLM) 674

Stichwortverzeichnis

IRF 747
ISADISK 668
ISDN 74, 360, 386, 387, 403
ISDN-Anschluß-Einheit 391
ISDN-Backup 364
ISDN-Basisanschluß 388
ISDN-Bilddienste 402
ISDN-Datenübermittlung 398
ISDN-Fernsprechen 394
ISDN-Fernwirken 402
ISDN-IDN für Datex-P 400
ISDN-Netz 385
ISDN-Telefax 398
ISDN-Teletex 397
ISDN-Textfax 403
ISO 42, 304, 356
ISO/OSI-Modell 553
ISO/OSI-Referenzmodell 95, 322
isochronen Datenverkehr 414
ISO-OSI-Modell 323, 452, 461, 565
ISO-Referenzmodell 307
ISO-Schichtenmodell 303
ITAA 1056
ITEM Properties 597

J

Jahr-2000-Fähigkeit 494, 793, 1053, 1056, 1058
Jahr-2000-Problematik 1053
Jahr-2000-Umstellung 494
Jahr-2000-Wechsel im BIOS 1055
Jahresdifferenzberechnung 1053
Jahreswechsel 1054
Jahrtausendwechsel 1053
jam signal 77
Java 520
Java Class Libraries 522
Java Naming Directory Interface (JNDI) 813
Java/CORBA-Runtime-Umgebung 522
Java-Anwendung 788
Java-Application-Server-Umgebung 522
JavaBeans 522
Java-Plattform 782, 811
Java-Script 973
JavaScript 522, 758, 814
JavaSoft 814
Java-Technik 545

Java-Technologie 814
Java-Unterstützung 791, 813
Jitte 117
JTM 317

K

Kabel, geschirmt 219
Kabel, ungeschirmt 218
Kabelbruch 64
Kabeltypen 68
Kalenderberechnung 1054
Kanalteilung 364
Kapazität 696
Kapazität, große 516
Kategorie-6-Kabel 238
Kategorie-7-Kabel 240
Kein Zugriff 943
Kerberos-Authentifizierung 977
Kerberos-Protokoll 977
Kernel 868
Kernel Mode 852, 858, 864, 873
Kernel-Adreßbereich 786
KEYB (NLM) 670
Keyb Ländercode 772
Klassifikationen Lokaler Netzwerke 59
Klassisches Ethernet-Switching 156
Knotenrechner 45
Koaxialkabel 45, 68, 71, 446
Koaxialkabelsegment 99
Koax-Kabel 73
Kommunikation 303
Kommunikation, bidirektionale 516
Kommunikationsdienst 298
Kommunikationsprotokolle 301
Kommunikations-Server 49, 52
Kommunikationssoftware 529, 531
Kommunikationssteuerungs-
Schnittstelle 555
Kommunikationssystem 293
Komponenten eines PC-Netzwerkes 452
Kontrollen 640
Kryptographische Dienste 810

L

Ladbare Driver 853
Längenausdehnung 64
LAN 290, 356, 449, 474

Stichwortverzeichnis

- LAN am Internet 999
- LAN Manager 876
- LAN Manager Domain 884
- LAN Switches 209
- LANalyzer Agent 269
- LANalyzer-Console 268
- LAN-Anwender 478
- LAN-ATM-Umgebung 197
- LAN-Concentrator 216
- LAN-Connect-Service 429, 431
- LANDeskManagement 261
- LAN-Driver 495, 557, 621, 629, 668
- LANE-Prozesse 168
- Language 772
- LAN-Host-Verbindung 487
- LAN-Kopplung 57
- LAN-Manager 500, 503
- LAN-Manager-Philosophie 908
- LAN-Manager-Redirector 866
- LAN-Manager-SMB-Protokollen 879
- LAN-Manager-Software 879
- LAN-Server 500
- LAN-Support-Module 547
- LAN-Technik 170
- LAN-WAN-LAN-Kopplung 428
- Large IPX 750
- Lastverbund 39, 355
- Layer-2-Switch 348
- Layer-3-Switch 351
- LDAP 796, 815, 981
- Leaf-Objekte 724, 725
- LeasedLink 363, 364
- LeasedLink International 367
- LeasedLink-Digital 368
- Leibniz 31
- Leistungsfähigkeit 533, 855
- Leistungsmeßverfahren 446
- Leistungsverbund 355
- Leitungsdurchschaltung 313
- Leitungssignal 296, 298
- Leistungsverstärker IBM 821 122
- Leitwerk 32
- Lesekopf 588
- Lesen RX 943
- Leseschnittstelle 1046
- Lichtleiter-Umsetzer 122
- Lichtwellenleiter 68, 72
- Lightweight Directory Access Protocol (LDAP) 796
- Link State 109
- Link Support Layer 621, 622
- Link-Segmente 92, 100
- LIPX 750
- List Devices 772
- LISTDIR 655
- listen while talking 77
- LLC-Layer 306
- LOAD (Befehl) 668
- Load Balancing 782, 976
- Load-Balancing-Algorithmus 783
- Load-Balancing-Mechanismus 783
- Local Area Network 39, 42, 356
- Local Procedure Call 856, 867
- Local Repeaters 97
- Locational-Map-Funktion 265
- Logical Link Control 306
- LOGIN 653
- Login 769
- Login Authentication 705
- Login SDK 525
- Login-Restriktionen 608
- Login-Sicherheit 601, 606
- Logische Speicheradressierung 790
- Logische Verbindung 298
- Logischer Ring 117
- Logisches Laufwerk 659
- Logon From 927
- Logon-Prozeß 870
- Logon-Script 928, 934, 937
- Logon-Stunden 927
- Logon-Zeit 932
- LOGOUT 653
- Logout 769
- Lokale DOS-Partition 805
- Lokale Gruppen 929
- Lokale Netze 41
- Lokale Netzwerke 435
- Lokale Run Queue 783
- Looped Bus 415
- Lotus Notes 1039
- LPC 856, 867
- LRU Sitting Time 786
- LSL 621, 622, 623
- LSL-Layer 622

Stichwortverzeichnis

- LU 6.2 482
- LWL 407, 408
- LWL-Verkabelung 227

- M**
- MAC (NLM) 670
- MACintosh-OS 560
- MAC-Layer 306
- MAC-Protokoll 101
- MAC-Spezifikation 175
- MADGEODI3 668
- Magazine 772
- Mail Server 458
- Mail Transfer 325
- Mail Transfer (SMTP) 326
- Mail-Gateway 461
- Mail-Server 51
- Mailslots API 878
- Mainframe 60
- MAN Switching System 416
- Management 56
- Management Domains 1024, 1049
- Management Tools 170
- Management von Workstations 278
- Management-Aufgaben 706
- Managementbarkeit 698
- ManageWise 260, 266
- Manufacturing Automation Protocol 84
- MAP 84, 654
- Map 767
- MAPI 1035
- MAPI-Messaging-Subsystem 1036
- Mark I 33
- Master 738
- Master Domain-Modell 921
- Master/Slave-Prinzip 1011
- MATHLIB (NLM) 674
- MATHLIBC (NLM) 674
- MAU 107
- Maximale Gesamtausdehnung 441
- MDI 107
- MDT 449, 474
- MDT-Anlage 451, 476, 480, 483
- Media 772
- Media Access Control 306, 320
- Media Access Unit 107
- Media-Management 215

- Medium 113
- Mehrwertnetz 421
- Meilensteine von Novell 505
- Meldungsspeicher 1016
- MEMORY (Befehl) 674
- Memory Management 530, 700
- Memory Protection 700
- Menüprogramm 666
- Menü-Utilities, 653
- Merced-Prozessor-Unterstützung 793
- Message Flow Confidentiality 1029
- Message Origin Authentication 1028
- Message Security Labeling 1029
- Message Sequence Integrity 1029
- Message Store 1016
- Message Store Access Protocol, MSAP 1028
- Message Transfer System Access Protocol 1027
- Messaging Application Programming Interface 1035
- Messaging Services 731
- Messaging-aware Application 1034
- Messaging-based Workgroup Application 1034
- Messaging-enabled Application 1034
- Metropolitan Area Network 409
- MHS 55, 317, 1038
- MIB-Browser 264, 266
- MIB-Compiler 266
- Microkernel 859
- Microsoft 550
- Microsoft Cluster Server 976
- Microsoft Domain Name Server (DNS) 970
- Microsoft Index Server 975
- Microsoft Mail 1039
- Microsoft Management Console (MMC) 972, 978
- Microsoft Message Queue Server 974
- Microsoft Transaction Server 974
- Microsoft Windows Internet Naming Service (WINS) 970
- Microsoft-Standards für Verträglichkeit 1057
- Mietleitung
 - analog 363
 - digital 363
- Mietleitungsnetze 359
- Migration 632

Stichwortverzeichnis

- Migration Agent 800
 - Migration Agent Server 794
 - MIME 1033
 - Minicomputer 481
 - MIPS 854
 - Mirror Status 772
 - MIRROR STATUS (NLM) 673
 - Mirrored Server Links 681
 - Mittlere Datentechnik 469, 473
 - MLID 621, 622
 - MLID Layer 622
 - Mnemonic O/R Address 1020
 - Moab 494
 - MODEM 74
 - Modem 361
 - Modify 614
 - Modulare Struktur 852
 - Modularisierung 469
 - Modulator 74
 - MODULES (Befehl) 671
 - Monitor 769
 - MONITOR (NLM) 672
 - Monitorstation 80
 - Moreland 31
 - MOUNT (Befehl) 672
 - Moveable Memory 572
 - MPK-Fähigkeit 782
 - MPR 751
 - MS 1016
 - MS ActiveX 973
 - MS-DOS 550, 874
 - MSEngine 684
 - MS-Mail 55
 - MS-NET 550
 - MS-Visual-Basic-Skript 973
 - MS-Zugangsprotokoll 1028
 - MTS Transfer Protocol 1026
 - MTS-Übertragungsprotokoll 1026
 - MTS-Zugangsprotokoll 1027
 - Multi Protocol Router 751
 - Multi Station Access Uni 117
 - Multi-Cas 319
 - Multicasting 1048
 - Multifunktionaler Arbeitsplatz 74, 485
 - Multi-Link 189, 191
 - Multi-Link-Interface-Driver 621
 - Multiple 313
 - multiple access 77
 - Multiple Master Domain-Modell 922
 - Multiple Name Space Support 589, 590, 591
 - Multi-Port-Repeater 102
 - Multi-Port-Transceiver 98
 - Multiprocessing-Kernel 782
 - Multiprocessor-System 863
 - Multiprocessor-Unterstützung 857
 - Multiprotocol Router 3.1 (MPR) 761
 - Multiprotokoll-Router 341
 - Multiprozessorfähigkeit 546
 - Multiprozessor-Synchronisation 860
 - Multipurpose Internet Mail Extension 1033
 - Multi-User-Fähigkeit 290
- ## N
- Nachfolger 83
 - Nachrichtenaustausch 38, 288
 - Nachrichtenquelle 293
 - Nachrichtensenke 293, 294
 - NAFS 515
 - NAL-Utility 730
 - NAME (Befehl) 673
 - Name Space 591
 - Name Space Modul 591
 - Named Pipes 627
 - Namen 1044
 - Namen und Adressen 1020
 - Name-Server 326
 - Name-Space-Module 806
 - Name-Space-Unterstützung 806
 - Naming-Service-Dienst 507
 - National Language Support 719
 - Nationale Tastaturunterstützung 633
 - Native IP 781, 798
 - Native Mode 591
 - Native Server 531
 - Native Service 873
 - N-Barrel-Steckern 93
 - NCOPY 655
 - Ncopy 769
 - NCP 619
 - NCP Packet Signature 631
 - NCP-Protokoll 525
 - NDIR 655
 - Ndir 768
 - NDIS 909

Stichwortverzeichnis

- NDPS 516
- NDS 721, 724, 815, 916
- NDS Manager 715, 796
- NDS4NT 494
- NDS-Baum 798
- NDS-Datenbank 734
- NDS-Objekt 722
- NE1000 668
- NE2 668
- NE2000 668
- NE-32 668
- NE3200 668
- Nebensprechen 71
- NET\$OBJ.SYS 596
- NET\$PROP.SYS 596
- NET\$VAL.SYS 596
- Net2000 521
- Net2000 Support 515, 516, 517
- NETAdmin 714
- Netadmin 769, 770
- NetBasic 522, 815
- NetBasic 6.0 814
- NetBasic 7.0 814
- NetBEUI 321, 881, 882
- NetBEUI/DLC 538, 626, 627
- NetBIOS 482, 543, 556
- NetBIOS API 878
- NetBIOS-Unterstützung 496
- Netexplorer-Discovery-System 267
- Netexplorer-NLM-Software 265
- Netscape FastTrack Servers 758
- Netuser 769, 770
- NetWare 286 499
- NetWare 3 Source Bindery 812
- NetWare 3.12 530, 549, 552, 557
- NetWare 3.12 Leistungskomponenten 561
- NetWare 3.12 Loadable Modules 558
- NetWare 3.12 Neuerungen 630
- NetWare 3.12 Streams Interface 625
- NetWare 3.12 Systemarchitektur 557
- NetWare 3.12 Überblick 552
- NetWare 3.12
 - Übertragungseinrichtungen 553
- NetWare 3.12 Volumes 576
- NetWare 3.2 549
- NetWare 3.2 Enhancement Packs 635
- NetWare 3.2 Streams Interface 625
- NetWare 4 499
- NetWare 4.11 781
- NetWare 4.x 574, 693, 910
- NetWare 5 494, 781
- NetWare 5 Kernel 782
- NetWare 86 41
- NetWare Administrator 714
- NetWare Advanced File Services (NAFS) 515
- NetWare Ankündigungen 499
- NetWare Backup und Storage Services 518
- NetWare Client 32 712
- NetWare Client 32 für DOS und
 - Windows 713
- NetWare Client 32 für Windows_95 713
- NetWare Communication Services 517
- NetWare Connect Server (8 Port) 777
- NetWare Core Protocol 627
- NetWare Database Services 517
- NetWare Directory Service 514
- NetWare Directory Services 721, 729
- NetWare Directory Services Rights 723
- NetWare Distributed Print Services
 - (NDPS) 516
- NetWare DOS Requester 631
- NetWare Easy Administration Tool 777
- NetWare Einbindung 965
- NetWare File Migration 764
- NetWare for VMS 478
- NetWare Host Connectivity Services 519
- NetWare LANalyzer Agent 268
- NetWare Licensing Services (NLS) 518, 732
- NetWare Link Protokoll 909
- NetWare Loadable Module 629, 800
- NetWare Management Agent 267
- NetWare Message Handling Services 1038
- NetWare Mobile Services 518
- NetWare Open System 498, 508, 509
- NetWare Partition 574, 575, 576, 804
- NetWare Patches 635
- NetWare Security Services 517
- NetWare SFT III 689
- NetWare Symmetric Multiprocessing 761
- NetWare Telephony Services 519
- NetWare v3.11 508
- NetWare v3.11 SFT III 679
- NetWare v3.11/4.0 506
- NetWare Volume 576

Stichwortverzeichnis

- NetWare Web Server 758
 - NetWare/IP 752
 - NetWare-3-Bindery-Kompatibilität 800
 - NetWare-5-TCP/IP-Implementierung 801
 - NetWare-Datenbereich 576
 - NetWare-Dienste 507, 508, 557
 - NetWare-DOS-Requester 711
 - NetWare-Hub-Services 270
 - Netwise 543
 - NETWORK 946
 - Network Auditing 717
 - Network Computing 498, 502, 503, 507, 508, 545, 558, 590
 - Network Driver Interface Specification 909
 - Network File System (NFS) 326, 628
 - Network-Computing 506
 - Netz, virtuelles 350
 - Netzabschluß 390
 - Netzwerk 474
 - Netzwerkadapter-Driver 885
 - Netzwerkadapterkarte 452, 460, 572
 - Netzwerkanalyse 268
 - Netzwerkbetriebssystem 59
 - Netzwerk-Dienste 529
 - Netzwerkdrucker 464
 - Netzwerkkarten 271
 - Netzwerkkomponenten 879
 - Netzwerkmanagement 248, 265
 - Netzwerk-Redirector 868
 - Netzwerkressourcen-Sharing 54
 - Netzwerk-Server 868
 - Netzwerksicherheit 959
 - Netzwerkstatistiken 269
 - Newhall-Verfahren 78
 - Nlist 768
 - NLM 568, 618, 629
 - NLM-Konzept 630
 - NLMs 558, 629
 - NLS 518
 - NLSP 751
 - NMAGENT (NLM) 674
 - NMS Agents 267
 - NMS-Console 264, 266
 - NMS-Console-Software 264
 - NMS-Discovery-Architektur 281
 - Node-Address 611
 - non-dedicated 553
 - Nonmoveable Memory 571
 - Non-persistent 78
 - Nonreturnable Memory 570
 - Not-Logged-In Clear 634
 - Novell 476
 - Novell Application Launcher (NAL) 807
 - Novell Cluster 641
 - Novell Directory Services (NDS) 794
 - Novell Distributed Print Services (NDPS) 806
 - Novell International Cryptographic Infrastructure (NICI) 810
 - Novell JVM 813
 - Novell NetWare 90, 445, 505
 - Novell NetWare 3.2 552
 - Novell NetWare 4 693
 - Novell Object Request Broker (ORB) 813
 - Novell SnapshotServer für NetWare 641
 - Novell Standard Message Format 1037
 - Novell StandbyServer für NetWare 641
 - Novell StandbyServer Many-to-One für NetWare 641
 - Novell Storage Service (NSS) 804
 - NPRINT 656
 - Nprint 768
 - Nprinter 769
 - NSS 787
 - NSS-Installationsprogramm 804
 - NSS-Partition 804
 - NT Executive 864
 - NT File System 875
 - NT-Basisdienst 873
 - NTFS 855, 875, 889, 938, 939
 - NTFS-Dateisystem 886, 910
 - NTMS (Windows NT Media Service) 971
 - NT-Objekt 873
 - Nukleus 563
 - Numeric O/R Address 1020
 - Nutzsignal 74
 - NVER 656
 - Nver 769
 - NWAdmin 796
 - Nwadmin 770
 - NWLINK 909
 - NWLink (IPX/SPX) 321
- O**
- Object Manager 867

Stichwortverzeichnis

Objekt 597, 722, 852, 857, 873
 Objekt-ID 597, 600
 Objektmodell 861
 Objektnamen 733
 Objektnummer 862
 Objekt-Properties 722
 Objekt-Trustees 744
 ODI 626
 ODI-Treiber 626
 Öffentliche
 Datenkommunikationseinrichtungen 35
 7
 Öffentlicher Verwaltungsbereich 1025
 Öffentlicher
 Verzeichnisverwaltungsbereich 1049
 OFF (Befehl) 673
 Offene Architektur 491, 507, 552, 563
 Offene Netzwerkarchitektur 909
 Offene Protokolltechnologie 507
 Offene Systemarchitektur 851
 Offline-USV 456, 955
 Oktett 323
 Oktett-Sequenz 298
 Onboard-Processor 447
 One-way Interaction 316
 Online-USV 456, 954
 Open Data Link Interface 559, 619, 626
 Open Protocol Technology 498, 506
 Open Solution Architecture 494, 521
 Open Systems Interconnection 304, 322
 Open-Bus 415
 Operationen 1045
 OPT 506
 Ordner sehen 960
 Organization 726
 Organizational Unit 726
 Original-Logon-Script 938
 Orion 816
 Orion I 816
 Orion I und II 494
 Orion II 816, 817
 Orion-Phasen 641
 OS/2 500, 503, 560, 714, 874
 OS/2 Presentation Manager 771
 OS/2-Subsystem 872
 OS/2-Unterstützung 498
 OS-Adreßbereich 786

OSI 304, 627
 OSI-Modell 306

P

P1 1026
 P3 1027
 P7 1028
 Packet Burst Mode 750
 Packet Exchange Protocol 554
 Page 856
 Page Directory Table 790, 791
 Page Entry Table 790, 791
 Page Translation Table 787, 791
 paged Pool 874
 Paging 874
 Paketfilterung 1000
 Paketübertragung 621
 Partition 576, 736, 904, 984
 Partition Manager Utility 739
 Partition-Baum 736
 Partitions Grenzen 986
 Partmgr 770
 Pascal 31
 Paßwort 893, 926
 Paßwort-Änderungsintervall 609
 Paßwort-Eindeutigkeit 610
 Paßwort-Länge 609
 Paßwort-Schutz 596
 Paßwort-Vergabe 609
 Paßwort-Verschlüsselung 610
 Patch-Kabel 236
 Patch-Level-Stände 636
 Patchpanel 234
 PAUDIT 657
 PC am Internet 999
 PC-Host-Kopplung 487
 PCL 973
 PC-LAN 39, 451, 550
 PCN2L 669
 Pconsole 663, 771
 Peer-to-Peer 62, 503, 876
 Peer-to-Peer-Protokoll 482, 496
 PEP 554
 Performance 491, 696, 850
 Performanceüberwachung 912
 Peripherie am File-Server 455
 PERL 815

Stichwortverzeichnis

- Perl 522, 973
- Perl5 814
- PERL-Script-Interpreter 758
- Permanent Memory Alloc Pool 571
- Permanent Returnable 571
- Permanent Virtual Circuit 430
- Per-Prozessor Run 783
- Personalcomputer 38
- Pflichtenheft 469
- Phasen der Netzwerkinstallation 468
- PHY 142
- Physical Layer Medium Dependent 142
- Physical Layer Protocol 142
- PING (NLM) 670
- Plattenkanal 574
- Plattenkanalausnutzung 574
- Plattenkapazität 875
- Plattenplatzbeschränkung 610
- Plattenverwaltung 903
- Plattform Support Modul (PSM) 785
- Plug-and-Play-Funktion 973
- Plug-and-Play-Unterstützung von Windows NT 5.0 973
- Plug-and-Print 517
- PMA 107
- PMD 142
- Point-to-Point-WAN-Verbindung 1010
- Polling-Verfahren 62
- Polymorphe Analyse-Erkennung 280
- Portable NetWare 506, 508, 509
- Portierbarkeit 853
- POSIX 861, 865, 874, 875
- Postal O/R Address 1020
- Power User 897
- p-persistent 78
- Präsentationsschicht 316
- Preemptiver Modus 784
- Pre-Insertion Prüfungen 187
- Presentation Layer 316
- Primäre Time-Server 743
- Primäres LAN 199
- Primärmultiplexanschluß 389
- Primärverkabelung 227
- Primary Partition 904
- Print Manager 896
- Print Operators 931
- Print Services 719, 757
- Printcon 664, 771
- Printdef 665, 771
- Printer Sharing 886
- Print-Manager 886
- Print-Queue 757
- Print-Server 48, 481, 757
- Print-Spooler 950
- Prioritäten 950
- Private Directory Management Domain 1049
- Private Management Domain 1025
- Privater Verwaltungsbereich 1025
- Privileg 598
- Process Manager 867
- Processor-Sharing 539, 540
- Professional Office System 1038
- Profil 928
- Profile Editor 934
- Profile-Login-Script 711
- Profile-Typen 936
- PROFS 1038
- Programm-Manager 896, 934
- Programm-Server 47
- ProNET10 128
- ProNET80 128
- Proof of Delivery 1029
- Proof of Submission 1029
- Properties 597, 861
- Property 597, 722
- Property ACCOUNT_BALANCE 604
- Property ACCOUNT_HOLDS 604
- Property ACCOUNT_SERVERS 604
- Property SET 597
- Property Set 599
- Property Set OBJ_SUPERVISOR 600
- Property-Rechte 745
- Property-Sicherheit 598
- Property-Wert 597
- Protected Subsystems 855, 864
- Proteon 112
- Protocol ID 623
- Protocol Stack 621
- Protocol-ID-Information 623
- Protokoll 59, 301, 1026, 1049
- Protokollabhängigkeit, 627
- Protokollanpassung 346
- Protokollaufbau 487
- Protokoll-Standards 537

Stichwortverzeichnis

Protokolltechnologie 508
 Protokollunabhängigkeit 506
 Provider 881
 Prozeßsteuerung 46
 Prozessorleistung 480
 Prüfbedingungen 220
 PS2ESDI 668
 PS2MFM 668
 PS2SCSI 668
 PSC 656, 769
 PSERVER (NLM) 674
 Public Key Infrastructure Services (PKIS) 810
 Puffer-Speicher 447
 Punkt-zu-Mehrpunkt-Konfiguration 391
 Punkt-zu-Punkt-Konfiguration 391
 PURGE 594, 655
 Purge 617, 618
 Python 973

Q

Quasi-Parallelität 857
 Queue Monitor 279
 Queued Packet Switch Exchange 411

R

räumliche Ausdehnung 59
 Rahmen 294
 Rahmenaufbau 296
 RAID Level 0 953
 RAID Level 1 913, 953
 RAID Level 2 953
 RAID Level 3 953
 RAID Level 4 953
 RAID Level 5 913, 953
 Raid-0 645
 Raid-1 645
 Raid-2 645
 Raid-3 645
 Raid-4 645
 Raid-5 646
 Raid-Level-Stufen 644
 RAID-Level-Systeme 952
 Raid-Technologien 644
 RAS 459, 956
 RAS-Client 956
 RAS-Dienste 956
 RAS-Server 956

RCONSOLE 670
 Rconsole 769
 Read 613, 614
 Read after Write Verification 639
 Read Audit 617
 Read-Only 617, 738
 Read-Write 738
 Realtime Scanning Mode 280
 Real-Time-Betriebssystem 561
 Realzeit-Steuerung 78
 Receiver 94
 Rechnernetze 355
 Rechte-Sicherheit 601, 612
 Rechtesystem 773
 Rechtevergabe 986
 Record-Locking 540
 Redirection Software 529
 Redirector 524, 877, 879, 881
 Redundant Arrays of Inexpensive Disks 644
 Redundante Dateisystemkomponenten 641
 Redundanz 295
 Reference Time-Server 741
 Referral 1048
 REGISTER MEMORY (Befehl) 674
 Remirror Partition 772
 REMOTE (NLM) 670
 Remote Access Services (RAS) 459, 915, 956
 REMOTE CONSOLE 676
 remote Directories 886
 Remote Execution 326
 remote I/O-Request 877
 Remote Job Entry 37, 317
 Remote Management Facility 658
 Remote Method Invocation 526
 Remote Procedure Call 542, 853, 878
 remote Repeat 97, 100
 REMOVE 656
 REMOVE DOS (Befehl) 671
 Rename 745
 Rename Inhibit 617, 618
 RENDIR 656
 Rendir 769
 Repeater 96, 329, 330
 Replicas 737
 Replicator 931
 Replies 531
 Replizierung, globale 515

Stichwortverzeichnis

- Reproduktion 914
- Requests 531
- RESET ROUTER (Befehl) 671
- Ressourcen-Sharing 39, 288, 289
- Returnable Memory 571
- REVOKE 656
- REXX 973
- RFC 822 1032
- RG58-A/U-Koaxialkabel 102
- RIGHTS 655
- Rights 768
- Ring-Input-Anschluß 118
- Ringleitungsverteiler 117
- Ring-Output-Anschluß 118
- Ringstruktur 64
- Ringtopologie 43, 64, 75
- RIP 750
- RJ45-Anschlußdosen 234
- RJ45-Stecker 109
- RJ45-Steckerbelegung 236
- RJE-Stationen 37
- RLV 117
- Root 725
- Root-Directory 649, 659
- Round-Robin Verfahren 784
- Round-Robin-Methode 80
- ROUTE (NLM) 674
- Router 200, 329, 338
- Router-Management 271
- Routing 313, 563, 800
- Routing Information Protocol 750
- Routing-Algorithmen 314
- Routing-Funktionen 215
- Routing-Service 496
- RPC 853, 878
- RPC-Modul 542
- RPC-Tools 543
- RSPX (NLM) 670
- Run Queue 782
- r-Utilities 888

- S**
- s 241
- Salvage 661
- Salvageable Dateien 589, 593
- SAM-Datenbank (Security Account Manager) 984
- SAP 308
- SAS 317
- Satellitenübertragung 446
- SBACKUP (NLM) 670
- Scan For New Devices 773
- Schaltjahr 1054
- Schaltjahrberechnung 1056
- Schedule+ 887
- Scheduling 530
- Schichtenstruktur 858
- Schmalband-ISDN 411
- Schneider & Koc 96
- Schnittstelle 294
- Schnittstellenvervielfachung 364
- Schreibkopf 588
- Screened Subnet 1003
- Screening Router 1000
- Script-Sprachen 522
- SCSI Controller 577
- SCSI Disconnect 578
- SCSI-Driver-Prozeß 577
- SDK 525
- SDLC-Protokoll 302
- SEARCH (Befehl) 671
- Secure Authentication Services (SAS) 810
- SECURE CONSOLE 619
- SECURE CONSOLE (Befehl) 673
- Secure-Socket-Layer-3.0-Funktion 758
- SECURITY 657
- Security Access 598
- Security Equivalence 602, 607, 747, 748
- Security Reference Monitor 867
- Security Services 707
- Security Subsystem 865, 870
- Security-Equivalence-Funktion 599
- Security-Equivalence-Rechte 599
- Security-Management 749
- Sekundäre Time-Server 743
- Sekundäres LAN 199
- Sekundärverkabelung 227
- SEND 654
- Send 768
- Sendeeinheit 293, 294
- Sender 294
- Sequence Number 324
- Sequenced Packet Protocol 554
- Server 471, 856, 858, 879
- Server Operators 931
- SERVER.EXE 558, 576, 629

Stichwortverzeichnis

- Server/Host 474
- Server-Based 541
- Server-Message-Block- 628
- Server-Peripherie 470, 471
- Serverplattform 507, 529
- Server-Strategie 544
- Service Access Point 308
- Service Advertising Protocol 751
- Service Provider 979, 1009
- Service Requests 605
- Service-Protokoll 619
- Services for Macintosh 957
- Session 659
- Session Layer 316
- SET (Befehl) 671
- Set Filer Options 660
- SET Properties 597
- SET TIME (Befehl) 673
- SETPASS 654
- Setpass 769
- SETTTS 656
- Settts 770
- SFT I 639, 643
- SFT II 639, 640, 643
- SFT III 560, 639, 643, 647, 679, 816
- SFT Level I 576, 640
- SFT Level II 642
- SFT Level III 651
- SFV Analog 370
- SFV Digital 371
- Shareable 617
- Shared Memory 864
- Shared Ressources 886
- Shell 565
- Sicherheit 56, 491, 534, 696
- Sicherheitsgruppen 601
- Sicherheitsmechanismen 495
- Sicherheitsstufen 598
- Sicherheitssystem 705
- Sicherungsverfahren 301
- Siemens 451
- Signalreflexionen 93
- Signalsenke 99
- Signalverzerrungen 295
- Signatur Scanning 280
- Simple Mail Transfer Protocol 326, 1030
- Simple MAPI 1035
- Simplex-Betrieb 294
- Single Attachment Concentrator 147
- Single Attachment Station 147
- Single Domain-Modell 920
- Single Reference Time-Server 741
- Single System Image (SSI) 817
- Single-User-Anwendungen 539
- Sitzungsschicht 316
- Skalierbarkeit 756
- SLIST 654
- Small Computer Systems Interface 577
- SMDS 421
- SMF 1037
- SMODE 654
- SMP 857, 863
- SMP-Lizenz 546
- SMP-Prozessor-Lizenz 546
- SMT 142
- SMTP 325, 326, 627, 1030
- SNA 627
- SNA/APPC 543
- SNADS 1038
- Snap-In-Module 284
- SNMP-Objekt-Management 277
- Software Development Kit 525
- Source Routing Bridges 188
- Sourcecodekompatibilität 855
- Source-Routing-Verfahren 337
- Spanned Files 592
- Sparse Files 589, 592
- Special-Access-Rechte 900, 901
- Speicher 32
- Speicheradressierungsschema 790
- Speicherfragmentierung 790
- Speicherschutz 785
- Speicherverwaltung 856
- Split Seeks 646
- Split-Pair 235
- SPP 554
- SPX 543
- SPXS (NLM) 674
- SQL-Server 530
- SSM 414
- S-STP 230
- Standardfestverbindung 363
- Standard-Rechte 898, 901
- Standards 535

Stichwortverzeichnis

- Standard-Topologien 72
 - Stapeljobs 289
 - Start of Header 296
 - Start of Text 296
 - Startbit 295
 - Station Management 142
 - Stationen-Restriktion 611
 - Stationsadresse 611
 - Stations-Shell-Schnittstelle 555
 - Stecker 114
 - Sternnetz 63, 117
 - Sterntopologie 43, 60, 109
 - Steuerung 45
 - Steuerung der Datenverbindung 301
 - Stopbit 295
 - Store-and-Forward 313
 - Store-and-Forward-Switches 349
 - STP 230
 - Stream End 625
 - Stream Head 625
 - Streamer 466
 - STREAMS (NLM) 674
 - Streams Interface 559
 - StreetTalk 916
 - StreetTalk-Konzept 913
 - Stripe Sets 904
 - Stromversorgung, unterbrechungsfreie 456
 - Strukturierte Verkabelung 231, 235
 - Sub-Admin-Bereich 967
 - Subadministratoren 967
 - Suballocation 703, 704
 - Suballocation-Tabellen 785
 - Subnetwork Router 418
 - Sun Microsystems Year 2000 Program 1056
 - Supervisor 599, 609, 610, 745
 - Supervisor-Equivalence 602
 - Supervisor-Utilities, 653
 - Supervisory 613, 614
 - S-UTP 230
 - Swap-Datei 790
 - Switch 348, 351
 - SwitchedLink 372
 - Switching-Hubs 211
 - Switching-Technik 215
 - symmetric multiprocessing 857
 - Symmetrisches Medium 113
 - Symmetrisches Multiprocessing 863
 - Synchrone Datenübertragung 295, 296
 - Synchronisation 294, 296, 301
 - Synchronisationsverfahren 294
 - Syscon 661
 - SYSTEM 946
 - System 617, 618
 - System Administrator Account 894
 - System Fault Tolerant 506
 - System Fault Tolerant Stufe II 560
 - System Guest Account 895
 - System Management 689
 - Systemcode 874
 - System-Dienst 858
 - System-Executive 568
 - System-Login-Script 607, 711
 - Systems Network Architecture Distribution Services 1038
 - Systemübersicht 856
 - SYSTIME 654
 - Systime 770
- T**
- TA 94
 - Task 675
 - Tastaturunterstützung national 633
 - TCP 324, 554
 - TCP/IP 321, 325, 538, 543, 559, 620, 621, 626, 627, 882, 888, 961
 - TCP/IP-Anwendung 325
 - TCP/IP-Protokoll 290, 322
 - TCP/IP-Protokoll-Umgebungen 681
 - TCPCON (NLM) 670
 - TCPIP (NLM) 670
 - TDI 909
 - Technische Eigenschaften 436, 438
 - Telefax 382
 - Telefonnetz 385
 - Teletex (T.61) 1024
 - Telex 361, 363
 - Telexnetz 359
 - Telnet 325, 627
 - Terminal O/R Address 1020
 - Terminaladapter a/b 400
 - Terminalemulation 325, 460
 - Terminalemulation (TELNET) 325
 - Terminals 37
 - Terminierung 301

Stichwortverzeichnis

- Tertiäres LAN 199
- Tertiärverkabelung 227
- Text- und Datennetz (IDN) 385, 398
- TFTP 325
- Thin-Wire-Verkabelung 91
- Third-Party Add-Ons 815
- Thread 857, 867, 870
- TIME (Befehl) 673
- Time-Server 741
- Time-Synchronization 741
- T-InterConnect 372
- TLI (NLM) 674
- TLIST 654
- T-Net-ATM 376
- TOKEN 669
- Token 78
- Token-Bus 75, 84
- Token-Bus-Zugriffsverfahren 83
- TOKENDMA 669
- Token-Passing 75
- Token-Passing-Methode 83
- Token-Passing-Zugriffsverfahren (IEEE 802.5) 78
- TokenPipe 189, 191
- Token-Ring 65, 87, 124, 325, 442, 500
- Token-Ring-Netzwerkunterstützung 497
- Token-Ring-Verfahren 78
- TOKENRPL (NLM) 674
- Token-Verfahren 75
- Tokenzyklus 83
- Topologie 43, 45, 59, 64, 438
- Topologieaufbau 138
- TOPS Filing Protocol 628
- Trägerfrequenz 74
- Traile 128
- Transaction Tracking System 805
- Transactional 618
- Transaktions-Backout 648
- Transaktionsfortschreibung 563
- Transceiver 94
- Transceiververkabel 95
- Transitive Synchronisation 794
- Translation Table 789
- Transmission Control Protocol 324, 554
- Transmission Control Protocol/Internet Protocol 322
- Transmitter 94
- Transparenz 297, 301
- Transport Driver 877
- Transport Driver Interface 881, 909
- Transport Layer 315
- Transport Layer Interface 627
- Transport Level Interface 625
- Transport/Client-Server-Protokoll 557
- Transportmedium 74
- Transportnetz 420
- Transportprotokoll 627, 881
- Transportprotokoll IPX 558
- Transportschicht 315
- Transportsystem 299, 452
- Trivial File Transfer Protocol 325
- Trusted Domain 917
- Trusted-Domain-Konzept 913
- Trustee 613
- Trustee Assignments 606, 748
- Trustee-Recht-Definition 613, 616
- Trustee-Rechte 596, 612, 636
- Trustee-Recht-Zuweisung 616
- Trusting Domain 921
- TRXNET 668
- TTS 647
- TTS-System 647
- Tunneling-Mechanismen 1009
- Turbo-FAT 581
- Turbo-File Allocation Table 581
- Twisted-Pair-Ethernet 103
- Twisted-Pair-Kabel 213, 234
- Twisted-Pair-Kupferkabel 241
- Two-way Alternate Interaction 316
- Typ 1 Kabel 112
- Typ 2 Kabel 112
- Typ 3 Kabel 112
- Typ 5 Kabel 113
- Typ 6 Kabel 113
- Typ 8 Kabel 113
- Typ 9 Kabel 113
- U**
- UDP 324, 554
- UDP-basierten Anwendungen 1001
- Übertragungseigenschaften 221
- Übertragungsgeschwindigkeit 59, 301, 439, 447
- Übertragungskanal 293, 294

Stichwortverzeichnis

Übertragungsmedium 45, 59, 67, 293, 438, 454
 Übertragungsnetz 42
 Übertragungsraten 68
 Übertragungstechnik 59
 Übertragungsverfahren 159, 440
 Uimport 769
 Unabhängigkeit 491
 Unabhängigkeit des Mediums 495
 UNBIND (Befehl) 671
 Ungeschirmte Kabel 218
 Unicode-Dateinamen 875
 Uninterruptable Power Supply 650, 890
 Universal Disk Format 978
 Unix Print Services 760
 Unix V 625
 Unix-Partition 574
 Unix-Rechner 560
 Unix-Systeme 451
 UnixWare 499
 UNLOAD (Befehl) 671
 UP LOAD 486
 UPS 641, 761
 UPS (NLM) 674
 UPS Monitoring 639, 641, 650
 UPS-Unterstützung an der seriellen Schnittstelle 761
 User Datagram Protocol 324, 554
 User Identifikation 891
 User Interface 866
 User Mode 852, 858, 864
 User Policy Package Objekt 808
 User Template 729
 User-Account 608, 892
 User-Account-Manager 601, 608, 609, 610
 User-Account-Typ 928
 USERLIST 654
 User-Login-Script 607, 711
 User-Memory-Bereich 874
 User-Mode-Proze 866
 Username 606
 User-Objekt Admin 735
 User-Objekt-ID 598
 Users 930
 UTP 230
 UTP-Kabel 70
 UTP-Verkabelungstechnik 69

V

VDM 872
 Vendor Independent Messaging 1037
 Verarbeitungskapazität 289
 Verbindungsabbauphase 299
 Verbindungslos 298
 Verbindungslose Kommunikation 299
 Verbindungsorientiert 298
 Verbindungsorientierte Kommunikation 299
 Verbindungsphase 299
 Verdrillte Vierdrahtleiter 68, 71
 Verdrillte Zweidrahtleiter 68, 71
 Verfügbarkeitsverbund 355
 Verkabelung 136
 Verkabelungslänge 64
 Verkettung 1048
 Verteilerliste 1021
 Verteilerrahmen 115
 Verteilte Datenbank, 721
 Verteilte Datenverarbeitung 481
 Verteilte Verarbeitung 474
 Verteiltes Verzeichnis 1047
 Verwaltungsbereiche 1024
 Verweis 1048
 Verzeichnissystemprotokoll 1050
 Verzeichniszugangsprotokoll 1049
 VHS-Funktion 480
 VIM 1037
 Vinca 815
 Virtual DOS Machine 872
 Virtual Loadable Modules 709
 Virtual Memory Manager 868
 Virtual Memory System 864
 Virtuelle Kanäle 313, 314
 Virtuelle Netze 350
 Virtuelle Verbindung 314, 555
 Virtueller Speicher 789, 874
 Virus Protect 279
 Virus Quarantine 280
 Virus Wall 280
 VLM-Manager 709
 VLM-Umgebung 711
 VM 868
 VM-Manager 874
 VMS-Unterstützung 498
 Volinfo 661
 Vollständiger Pfad 733

Stichwortverzeichnis

Vollzugriff 944
 Volume 574, 575, 904
 VOLUMES (Befehl) 673
 Volume-Segment 576
 Volume-Verwaltung 575
 Vorgänger 83
 Vorverarbeitung von Daten 486
 VPN 1008
 VPN-Komponenten 1008
 VPN-Sicherheit 1010
 VREPAIR (NLM) 674
 VT 317
 VT100 326
 VT220 326

W

Wählnetze 359
 WAN 43, 290, 356, 557
 WAN Traffic Manager (WTM) 797
 WAN-Konzept 405
 Web-Server 51
 Wegsteuerung 314
 Wegsteuerung (Routing) 314
 WG_MANAGER 599
 WHOAMI 654
 Whoami 770
 Wide Area Network 39, 43, 356, 557
 Wiederherstellbare Dateien 589, 593
 Wiederherstellungsverfahren 302
 Win32 873
 WIN32 API 855
 Win32 Driver Model (WDM) 973
 Win32 I/O API 877
 Win32 Named Pipe 878
 Win32 Network API 878
 Win32 Protected Subsystem 860
 Win32 Subsystem 870
 Win32-Programm-Manager 871
 Win32-Subsystem 872
 Win32-WNet 880
 Windows 874
 Windows 2000 1057
 Windows NT 849
 Windows NT 5.0 967
 Windows NT 5.0 Management 968
 Windows NT Advanced-Server 907
 Windows NT Command Prompt 896

Windows NT Features 850
 Windows NT File-System 939
 Windows NT Help 896
 Windows NT-Dateisystem 940
 Windows Scripting Host (WSH) 973
 Windows Socket API 878
 Windows-Desktop 934
 Windows-NT-Environment-Subsystem 874
 WINS-Dienst 970
 Wire-Center 117
 WNet 878
 WNet API 881
 WNet Provider 881
 Workgroup 920
 Workgroup Computing 501, 504, 508, 851
 Workgroup-Manager 599, 606, 609, 610
 Workgroup-Manager-Status 599
 Workgroups 55
 Workgroup-Segmentierung 189
 Workstation 62, 471
 Workstation Manager 807
 Workstation-Based 541
 Workstation-Betriebssystem 504
 Workstation-Unterstützung 534
 World Wide Web 991
 WOSA 1035
 Write 613, 614
 Write Audit 618
 Wsupdate 770

X

X.25-Service 429, 430
 X.400 55, 317
 X.400-Modell 1015
 X.400-Nachrichtenstruktur 1017
 X.500 318
 X.500 Directory 981
 X.500 Interoperabilität 514
 X.509-Standard 977
 Xerox 39, 91
 Xerox Network System 626
 X-Windows-Umgebung 791

Y

Year 2000 Ready 1054
 Year-2000-Information-Center 1056
 Yellow-Cable 91, 102

Stichwortverzeichnis

Z

- Z.E.N.works 494
- Z.E.N.works Starter Pack 807
- Zeichensätze 1023
- Zeitabgleich 1054
- Zeitrestriktion 611
- Zeitstempel 1054
- Zeitsynchronisation 741
- Zentrale Administration 514
- Zentrale Betriebsmittel 288
- Zentrale Datenbestände 288, 289
- Zentrale Datenverarbeitung 37, 481
- Zentraler Knotenrechner 61
- Zero Administration Kit 975
- Zero Effort Networking 807
- Zugangskontrolle 302
- Zugangsverfahren 45
- Zugriffsberechtigung 502
- Zugriffskontrolle 1051
- Zugriffsmethode 83
- Zugriffsrechte 898
- Zugriffsregelung 61
- Zugriffsschutz 564
- Zugriffssynchronisation 564
- Zugriffsverfahren 59, 74, 439, 487
- Zukunftssichere Verkabelung 230
- Zuse 33
- Zuverlässigkeit 491, 533, 696, 851, 854
- Zweidrahtleitung 45

