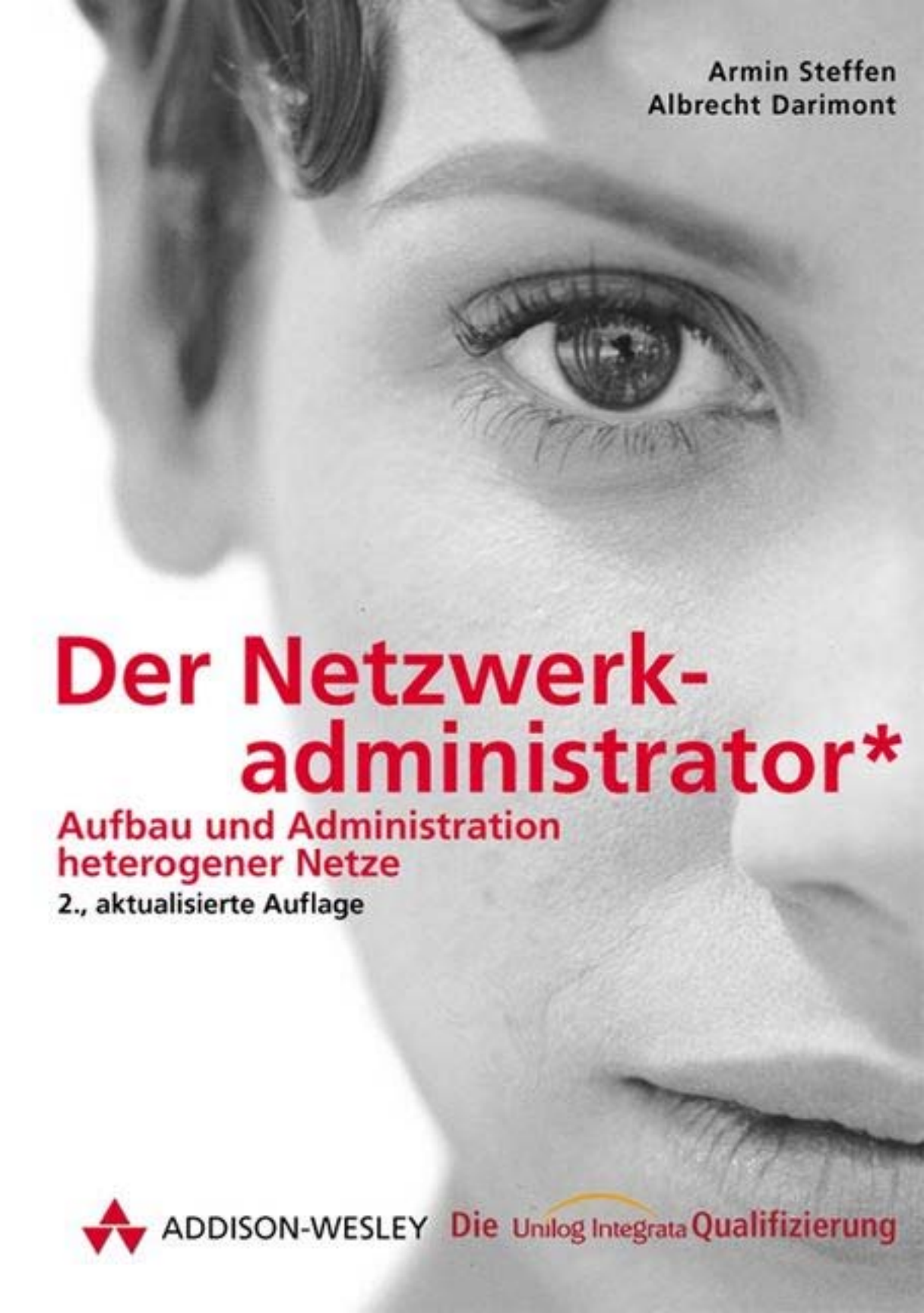


Armin Steffen
Albrecht Darimont

Der Netzwerk-administrator*

Aufbau und Administration heterogener Netze

2., aktualisierte Auflage

ADDISON-WESLEY Die Unilog Integrata Qualifizierung

Der Netzwerkadministrator

Die Unilog Integrata Qualifizierung

Herausgegeben von der Unilog Integrata Training AG und Dr. Ingrid Mikosch

In der Reihe »Die Unilog Integrata Qualifizierung« sind bisher erschienen:

Patrick E. Schärer
Der Visual FoxPro 6.0 Anwendungsentwickler
1. Auflage 1999, ISBN 3-8273-1599-9

Michael Rinke
Der IT-Trainer
1. Auflage 2000, ISBN 3-8273-1589-1

Jutta Bachmann
Der Information Broker
1. Auflage 2000, ISBN 3-8273-1703-7

Karl-Heinz Hauer
Der Oracle-Datenbankentwickler
1. Auflage 2001, ISBN 3-8273-1623-5

Albrecht Darimont, Dieter Paul Rudolph
Der Multimedia-Entwickler
1. Auflage 2001, ISBN 3-8273-1760-6

Eduard Heindl, Jens Bücking, Ulrich Emmert
Der IT-Sicherheitsexperte
1. Auflage 2001, ISBN 3-8273-1840-8

Eduard Heindl, Karin Maier
Der Webmaster
3. Auflage 2001, ISBN 3-8273-1853-X

PEARSON Education

ADDISON-WESLEY

Armin Steffen
Albrecht Darimont

Der Netzwerkadministrator

Aufbau und Administration heterogener Netzwerke

2., aktualisierte Auflage

ADDISON-WESLEY

An imprint of Pearson Education
München • Boston • San Francisco • Harlow, England
Don Mills, Ontario • Sydney • Mexico City • Madrid • Amsterdam

Die Deutsche Bibliothek – CIP-Einheitsaufnahme

Ein Titeldatensatz für diese Publikation ist bei
Der Deutschen Bibliothek erhältlich.

Umwelthinweis:
Dieses Produkt wurde auf chlorfrei gebleichtem Papier gedruckt.
Die Einschrumpffolie – zum Schutz vor Verschmutzung – ist aus
umweltverträglichem und recyclingfähigem PE-Material.

10 9 8 7 6 5 4 3 2 1
04 03 02 01

ISBN 3-8273-1836-X

ein Imprint der Pearson Education Deutschland GmbH
Martin-Kollar-Straße 10–12, D-81829 München/Germany

Einbandgestaltung: niesner & huber, Wuppertal
Lektorat: Dr. Ingrid Mikosch; Christian Schneider,
cschneider@pearson.de
Herstellung: Anna Plenk, aplenk@pearson.de
Satz: reemers publishing services gmbh, Krefeld, www.reemers.de
Gesetzt aus der Clearface 10 pt.
Druck: Bercker Graphische Betriebe, Kevelaer
Printed in Germany

Inhaltsverzeichnis

KAPITEL 1

1 Topologien und Verkabelungsstruktur

In diesem Kapitel erhalten Sie einen Überblick über die grundlegenden Themen Topologie und Verkabelung. Beide Themen beschreiben, wie ein Netzwerk räumlich strukturiert ist und auf welchen Kabeltypen und welcher Kabelinfrastruktur es aufbaut. Die praktische Relevanz dieses Kapitels ergibt sich aus der Tatsache, dass bis zu 80 Prozent aller Netzwerkprobleme auf die Topologie bzw. auf die Verkabelung zurückzuführen sind.

1.1 Topologie

Die Struktur der Verbindungen zwischen den Stationen eines Netzes wird als Topologie bezeichnet. Da die Knoten eines Netzwerkes auf sehr unterschiedliche Weise systematisch miteinander verbunden werden können, gibt es auch unterschiedliche Topologien. Die gängigen Typen sind:

- ✔ Bus
- ✔ Ring
- ✔ Stern
- ✔ Baum

Die oben beschriebenen Topologien waren in der Vergangenheit typisch für lokale Netze. Heute sollen Netzwerke nach der Empfehlung für strukturierte Verkabelung, EN 50173, als streng hierarchische Baumstruktur aufgebaut sein.

1.2 LAN-Topologien in der Schnellübersicht

Die **Bus-Topologie** besteht aus einem Informationskanal, an den alle Stationen **passiv** angeschlossen sind. Die angeschlossenen Stationen tragen nichts zur Signalverstärkung bzw. -weiterleitung bei. Das von einer Station gesendete Signal breitet sich in beide Richtungen aus. Solche Netze werden auch als Diffusionsnetze bezeichnet.

Die **Ring-Topologie** beschreibt eine geschlossene Kette von Punkt-zu-Punkt-Verbindungen, d.h. jede Station ist direkt mit einer vor ihr und einer nach ihr liegenden Station verbunden. Aufgrund dieser Anordnung müssen alle Stationen aktiv in den Ring eingebunden sein. Aktiv bedeutet, dass jede Station die ankommenden Signale regenerieren und weitergeben muss.

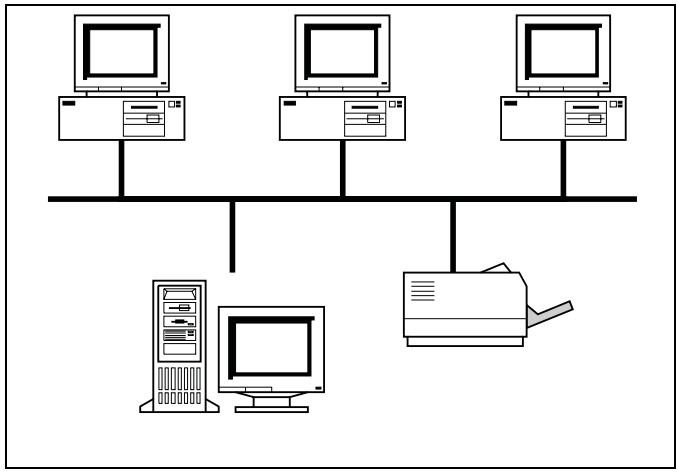


Abbildung 1.1: Bus

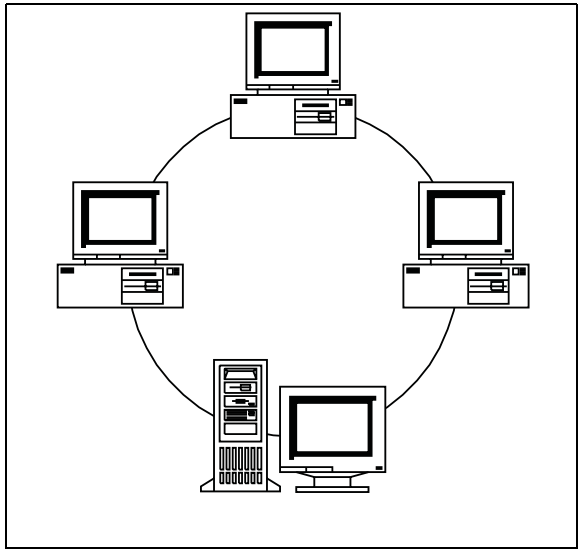


Abbildung 1.2: Ring

Die **Stern-Topologie** besitzt einen zentralen Knotenpunkt, an dem alle übrigen Stationen über genau eine Leitung miteinander verbunden sind.

Strukturen, die ausgehend von einem zentralen Rechner unterschiedliche Topologien wie Bus und Ring integrieren, bilden eine Baum-Topologie, die auch als **nichthierarchische Baumstruktur** bezeichnet wird.

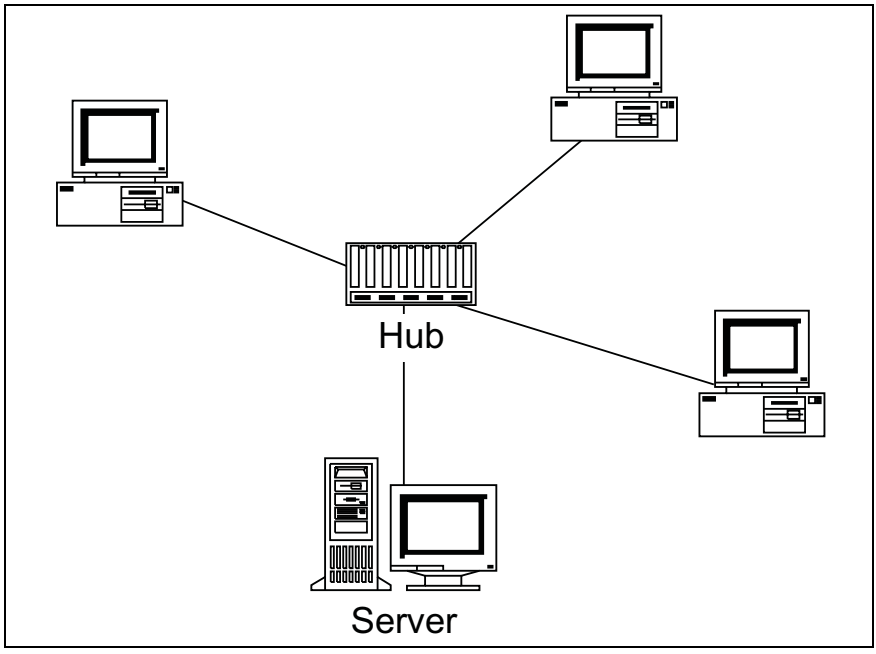


Abbildung 1.3: Stern

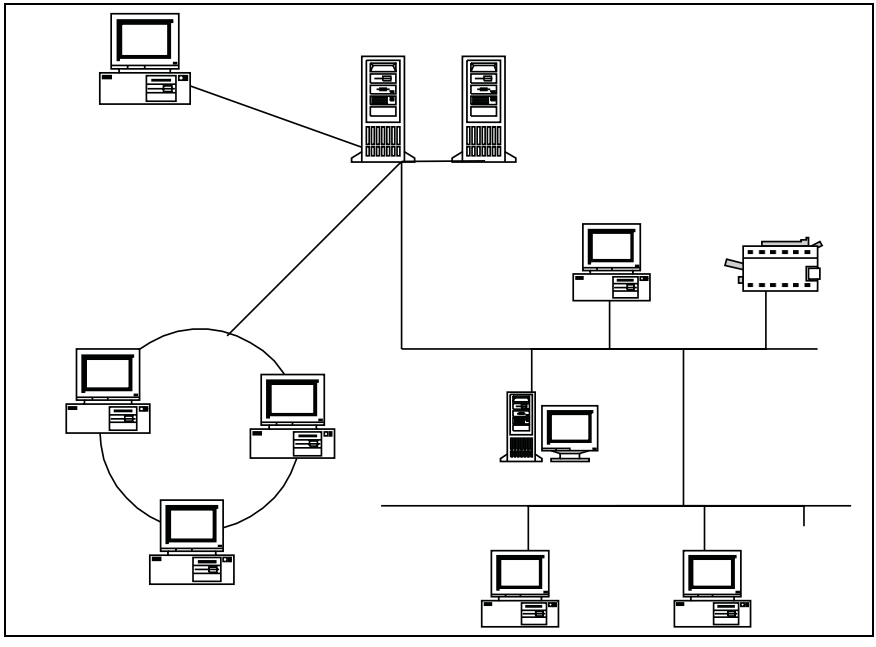


Abbildung 1.4: Nichthierarchischer Baum

Für die Entstehung von nichthierarchischen Baumstrukturen gibt es drei wesentliche Ursachen:

- ✔ Isoliert entstandene Netze, Insellösungen, werden im Zuge einer unternehmensweiten Infrastruktur miteinander zu einem Netz verbunden.
- ✔ Die Baumstruktur bildet die tatsächlichen organisatorischen und räumlichen Randbedingungen des Unternehmens ab.
- ✔ Die Baumstruktur entwickelt sich aus der Integration abteilungsweiter, lokaler Netzwerke in die unternehmensweite, zentrale Datenverarbeitung.

Die Vergangenheit hat gezeigt, dass lokale Netze immer größer werden. Die bisher beschriebenen Topologien können nur mit erheblichem Aufwand erweitert werden. Die strukturierte Verkabelung beschreibt eine hierarchische Baumstruktur. Diese kann sehr leicht erweitert werden und gilt deshalb als einzig zukunftssichere Topologie.

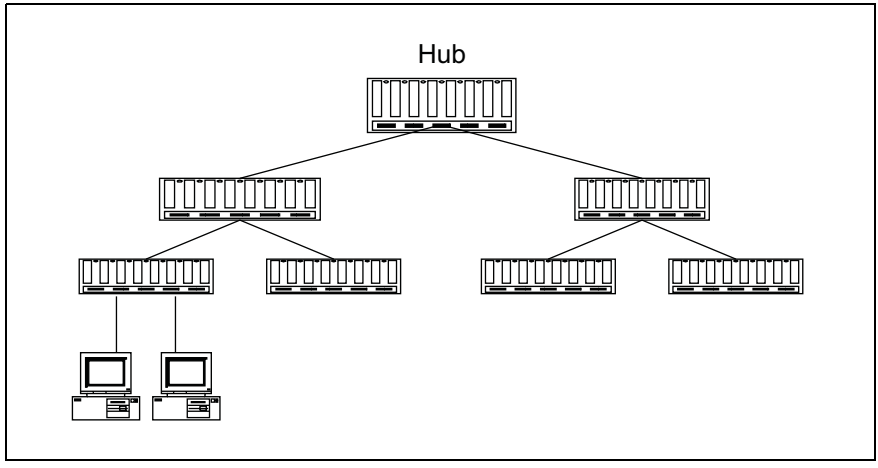


Abbildung 1.5: Hierarchische Baumtopologie

Weitere Details zur strukturierten Verkabelung finden Sie im Kapitel 1.5 Strukturierte Verkabelung.

1.3 Datenkabel – Technik und Leistungsmerkmale im Überblick

Netzwerke werden immer größer und schneller. Durch Client/Server-Konzepte und die zukünftige Integration von Sprach- und Datendiensten steigen die Anforderungen bezüglich Geschwindigkeit und Verfügbarkeit. Daraus ergibt sich zwangsläufig die Notwendigkeit zukunftsorientiert zu planen. Als Faustregel gilt: Die Verkabelung muss eine Lebensdauer von mindestens zehn Jahren besitzen. Diese Vorgabe wird nur erreicht, wenn die Verkabelung hochwertig ist und strukturiert erfolgt.

In lokalen Netzwerken kommen standardisierte Kupfer- oder Glasfaserkabel zum Einsatz. Diese unterscheiden sich in der Regel in den folgenden Merkmalen:

- ✔ Übertragungsrate
- ✔ Material, Dicke und Gewicht
- ✔ Verkabelungselemente
- ✔ Abschirmung
- ✔ Preis

Als Kupferkabel kommen symmetrische Kabel in Frage, bei Glasfaser sind es Multimode- oder Monomodekabel.

Entscheidende Einsatzkriterien für Kupfer sind:

- ✔ Übertragungsbandbreite
- ✔ Teilebelegung/Vollbelegung

Für Glasfaser gelten folgende Entscheidungsgrundlagen:

- ✔ Bündelfaser (aufwendige Anschlusstechnik)
- ✔ Breakout (einfacher zu installieren, aber höherer Kabelpreis)

1.3.1 Verdrillte Kabel

Es handelt sich hier um ein dünnes Kupferkabel mit 0,4 bis 0,6 mm Aderndurchmesser, das zur besseren Abschirmung als Doppelader verdrillt wird. Verdrillte Kabel werden auch als symmetrische Kabel bezeichnet und sind aus zwei Gründen verdrillt:

1. Verminderung restelektromagnetischer Felder.
2. Minimierung des Übersprecheffekts.

Es können zwei Schirme unterschieden werden:

Der Screen ist der Kabelschirm. Grundsätzlich sind wegen Störeinflüssen und Abstrahlungen nur Kabel mit Schirm zu verwenden. Dieser Kabelschirm sollte wegen der besseren Schirmwirkung immer aus einer Folie und einem Geflecht bestehen.

Das Shield ist die Schirmung einer Doppelader (Twisted Pair). Diese Aderabschirmung reduziert wesentlich das Übersprechen (Nahnebensprechen) zwischen den Adernpaaren und verbessert die Übertragung. In der Kabelbezeichnung wird hierfür der Begriff PiMf verwendet, Paar in Metallfolie.

In der Praxis finden Sie mehrere Ausführungen und auch Bezeichnungen für **verdrillte Kabel**.

Mit **UTP**, Unshielded Twisted Pair, werden Kabel ohne Paarschirm und ohne Gesamtschirm bezeichnet. Nach den Vorgaben der strukturierten Verkabelung dürfen UTP-Kabel nicht mit mehr als 30 MHz betrieben werden. Damit bieten angesichts der Entwicklung im Bereich der Hochgeschwindigkeitsnetze nur noch geschirmte Kabeltypen Investitionssicherheit. Zu beachten ist, dass die Bezeichnung UTP-Kabel oft eine Vereinfachung ist und im Bereich der Klasse D in der Regel S/UTP-Kabel gemeint sind, also Kabel mit einem Gesamtschirm.

S/UTP, Screened Unshielded Twisted Pair, wiederum steht für einen Kabeltyp mit Abschirmung des Gesamtkabels, ohne dass hierbei das Kabelpaar selbst abgeschirmt ist. Dies Kabel gibt es in den Variationen einfach, eine Folie, zweifach, Folie und Geflecht, geschirmt.

S/STP-Kabel sind etwas teurer als S/UTP-Kabel, bieten jedoch erhebliche Leistungsreserven. Mit einer geeigneten Anschlusstechnik können über ein Kabel gleichzeitig mehrere Signale parallel übertragen werden. Sie bieten auch größere Reserven für Verluste der Kabelqualität durch Alterung oder mechanische Beanspruchung.

Am Markt werden auch Kabel mit der Bezeichnung S/FTP oder FTP angeboten. Bei diesen Kabeln handelt es sich um UTP-Kabel, bei denen anstelle eines PiMf eine Kunststofffolie um jede Doppelader gewickelt wird. Hierdurch können die mechanischen Eigenschaften eines Kabels verbessert werden, so dass Änderung der Kabelgeometrie bei der Leitungsverlegung mit den Auswirkungen auf die Übertragungseigenschaften verringert werden.

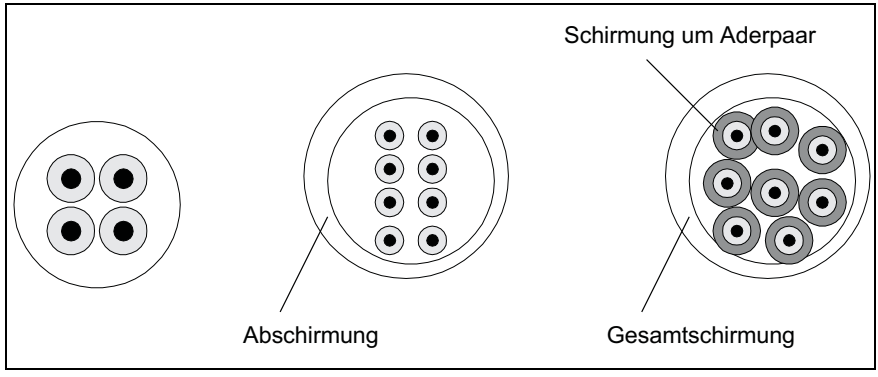


Abbildung 1.6: Verdrillte Kabel

Zurzeit werden bevorzugt STP-Kabel eingesetzt.

Nach **EIA/TIA**, Electronic Industries Association, werden Kabel in Kategorien eingeteilt. Anhand dieser Kategorien ist die Leistungsfähigkeit eines Kabels erkennbar.

Kat.3-Kabel bieten eine Übertragungsfrequenz bis 16 MHz. Damit werden 10 Mbit/s Übertragungsrate erreicht.

Kat.5-Kabel bieten Frequenzen bis 100 MHz. Damit ist die technische Grundlage für den Einsatz in Hochgeschwindigkeitsnetzen mit mehr als 10 Mbit/s gelegt. Aus diesem Grund werden bereits für die meisten Neuinstallationen Kat.5-Kabel oder bessere verwendet bzw. der Einsatz muss dringend empfohlen werden.

Die neuesten Kabelkategorien sind Kat.6 und Kat.7 mit bis zu 600 MHz Übertragungsfrequenz. Da hier noch kein einheitlicher Standard vorliegt, werden zurzeit noch überwiegend Kat.5-Kabel eingesetzt.

Die Einteilung der einzelnen Kabeltypen nach **EIA/TIA** ist sehr stark durch den US-amerikanischen Markt geprägt. Aus diesem Grunde wurden ab dem 01.01.1996 europäische Normen nach dem Gesetz über die elektromagnetische Verträglichkeit, EMV, definiert. Verschiedene Übertragungsverfahren werden nach EN50173 in Leistungs- oder Link-Klassen aufgeteilt. Die folgende Tabelle gibt zunächst einen Überblick.

Link-Klasse	Übertragungsrate
Klasse A	bis 100 kHz
Klasse B	bis 1 MHz
Klasse C	bis 16 MHz
Klasse D	bis 100 MHz
Klasse E	bis 200 MHz
Klasse F	bis 600 oder 1000 MHz

Tabelle 1.1: Link-Klassen nach EN50173

Wie die oben aufgeführten Klassen zu interpretieren sind, zeigt das folgende Beispiel für **Klasse D**. Danach sind folgende Zuordnungen, für die eine Schirmung der Kabel notwendig ist, vorgesehen:

ATM 51,84 Mbps	2 Paare
ATM 100 Mbps	2 Paare
ATM 152,52 Mbps	2 Paare
ATM 622,08 Mbps	4 Paare
TP-DDI (CDDI) 100 Mbps	2 Paare
100 Base TX 100 Mbps	2 Paare
1000 Base TX 1000 Mbps	4 Paare

Tabelle 1.2: Zuordnungen für Kabeltypen der Link-Klasse D

Den Zusammenhang zwischen der Einteilung in Kategorien und den Link-Klassen zeigt beispielhaft die nachfolgende Tabelle.

	Klasse A	Klasse B	Klasse C	Klasse D
Kat.3	2 km	500 m	100 m	-
Kat.4	3 km	600 m	150 m	-
Kat.5	3 km	700 m	160 m	90 m

Tabelle 1.3: Kabelkategorien und Link-Klassen

Welches Kabel soll verwendet werden?

Aktuell wird die Standardisierung eines Twisted Pair Kabels mit einer Übertragungsrate von bis zu einem GHz diskutiert. Diese soll dann als Kat.7 oder als Klasse-F-Kabel auf den Markt kommen. Damit wird der Entwicklung von Netzwerken, die Übertragungsbandbreiten > 1 Gbit/s bieten, Rechnung getragen. Die gegenwärtige Diskussion zeigt aber auch, dass die Meinungen zu Kat.6 und Kat.7 sehr kontrovers sind. So gibt es Stimmen, die Kat.7 keine Chance geben und auf Kat.6 setzen bzw. Kat.5 für ausreichend halten. Hauptargument hierfür ist, dass das zukünftige Gigabit Ethernet selbst mit einem Kat.5-Kabel zu realisieren sei und Kat.6 genügend Reserven für zukünftige Entwicklungen biete.

Schirmung ja oder nein?

Für abgeschirmte Kabel spricht die Entwicklung hin zu Highspeednetzen. Die hohen Frequenzen in einem Hochgeschwindigkeitsnetz führen dazu, dass die Kabel zur abhörbaren Informationsquelle werden. Es entstehen Gleichtaktwellen, die sich mit entsprechender Ausrüstung noch im Kilometerbereich abhören lassen. Dadurch ist eine Rekonstruktion der gesendeten Daten möglich. Nur durch Abschirmung kann diesem Effekt vorgebeugt werden.

1.3.2 Glasfaser

Eine andere Bezeichnungen für diesen Kabeltyp ist **LWL** für Lichtwellenleiter. Es handelt sich hierbei um eine sehr feine zylindrische Faser aus Quarzglas, die aus einem Kern und einem Mantel mit etwas geringerer optischer Dichte besteht. Als Informationsträger dient Licht mit den Wellenlängen 850, 1300 und 1550 Nanometer. In diesem Bereich, auch »optische Fenster« genannt, ist die Dämpfung minimal.

Wichtige Leistungsmerkmale der Glasfaser sind die Dämpfung, gemessen in db/km und das Bandbreitenlängenprodukt. Hier ein Beispiel:

Ein Lichtwellenleiter mit dem Bandbreitenprodukt von 600 MHz*km ermöglicht folgende Übertragungsraten:

Entfernung	Übertragungsrate
500 Meter	1200 MHz
1000 Meter	600 MHz
6 km	100 MHz

Tabelle 1.4: Anwendungsbeispiel Bandbreitenprodukt eines Glasfaserkabels

Man unterscheidet die leistungsfähigeren Monomode- und Gradientenfasern, die weniger Leistung, d.h. Übertragungsrate, ermöglichen. Gradientenfasern sind aber in der Anschlusstechnik kostengünstiger.

Als Moden bezeichnet man Lichtstrahlen, die unter verschiedenen Winkeln in den Kern des LWL eintreten. Der Eintrittswinkel einer Mode bestimmt die unterschiedlich langen Übertragungsstrecken.

In einer **Monomodefaser,** auch **Singlemode Faser SMF,** ist der Kerndurchmesser und damit der Eintrittswinkel so klein, 3-15 micron, dass sich das Licht entlang der Faserachse ausbreitet. Es entstehen keine »Wellen«, die sich dann am Mantel brechen. Dies bringt eine Reihe übertragungstechnischer Vorteile mit sich.

Der wichtigste Vorteil besteht darin, dass eine höhere Übertragungsrate über eine weitere Strecke ohne Verstärkung realisiert werden kann. Monomodefasern weisen aber auch Nachteile auf. Aufgrund des geringen Kerndurchmessers müssen z.B. anstelle der problemloseren und billigeren LEDs Laserdioden verwendet werden.

Die beiden Arten von **Gradientenfasern,** auch **Multiomode Faser MMF,** besitzen einen größeren Kerndurchmesser, 50/125 µm bzw. 62,5/125 µm, micron, als Monomodefasern. Damit ist die mögliche Übertragungsrate über eine definierte Strecke aufgrund der Brechung des Lichts im Faserkern geringer. Demgegenüber steht aber der Vorteil einer problemloseren Handhabung sowie kostengünstigerer Anschlusstechnik.

In der DIN EN 50 173 werden beide Fasertypen zugelassen. Es sprechen somit der günstigere Preis und die bessere Verfügbarkeit in Europa für den Einsatz der 50/125-µm-Faser.

Für Multimodefasern gibt es noch eine weitere Klassifizierung, das so genannte Profil. Unterschieden werden das Stufenindex-Profil und das Gradientenindex-Profil.

Beim **Stufenindex-Profil** ändert sich die optische Dichte (der Brechungsindex) vom Kern zum Mantel schlagartig. Dadurch ergeben sich große Laufzeitunterschiede und Signalverfälschungen. Aus diesem Grund hat das Stufenindex-Profil in der Datenübertragung keine Bedeutung, mit Ausnahme der Monomodefaser, die eine Sonderform des Stufenindex-Profils mit sehr kleinem Kerndurchmesser ist.

Das **Gradientenindex-Profil** wird bevorzugt im Inhousebereich eingesetzt. Der Übergang vom Kern zum Mantel erfolgt nicht schlagartig, wie bei der Stufenindexfaser, sondern kontinuierlich. Dies wird erreicht, indem vom Kern nach außen unterschiedlich dichtes Glas verwendet wird. Aufgrund der unterschiedlichen Brechungsindizes dieser Gläser haben alle Moden immer den gleichen Nulldurchgang. Signalverzerrungen sind dadurch gering. Die Laufzeitschwankungen liegen im Bereich von 60 bis 0,5 ns/km.

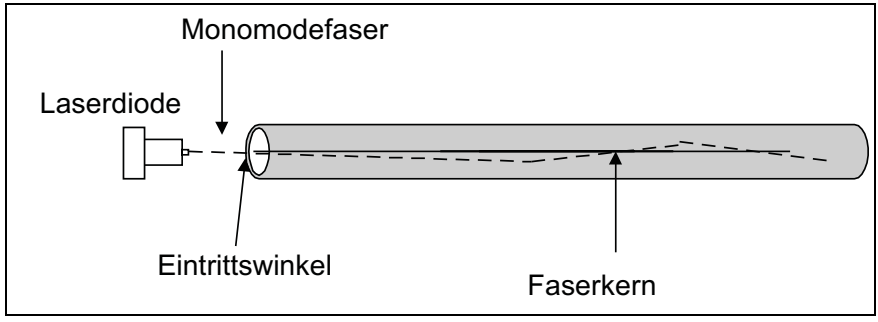


Abbildung 1.7: Monomodefaser

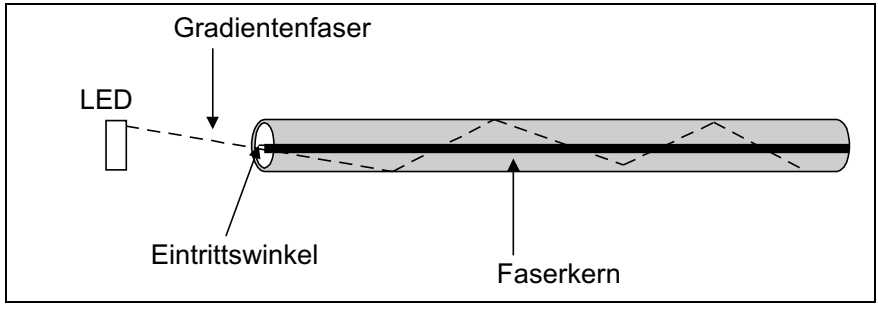


Abbildung 1.8: Gradientenfaser

In den USA werden in der Regel Gradientenfasern mit einem Kern/Manteldurchmesser von 62,5/125 µm eingesetzt. In Europa bevorzugt man die 50/125-µm-Variante. Diese bietet mit 1200 MHz*km das bessere Bandbreitenlängenprodukt. Glasfaser bis an den Arbeitsplatz hat folgende Vorteile:

- ✔ Unempfindlich gegenüber elektrischen und magnetischen Störungen
- ✔ Geringes Gewicht
- ✔ Größere Reichweiten
- ✔ Sehr hohe Übertragungsraten über 1000 Mbps

Nachteile:

- ✔ Etwa 30 Prozent teuerer als Kupfer
- ✔ Aktive Komponenten sind zwischen 100 und 200 Prozent teurer als mit Kupferanschluss.

1.4 Drahtloses Netz (Wireless LAN)

Bei drahtlosen Netzen wird für die Signalübertragung das Übertragungsmedium Raum verwendet. Die Übertragung erfolgt entweder mit Radiowellen in den Frequenzbereichen von 100 kHz bis 10 GHz oder mit Infrarotwellen im Frequenzbereich von 300 THz.

Die drahtlose Signalübertragung, insbesondere im IR-Bereich, setzt direkten oder, über eine reflektierende Fläche, indirekten Sichtkontakt zwischen Sender und Empfänger voraus und ist daher sehr stark von den örtlichen Gegebenheiten abhängig. Aus diesem Grund wird jedes drahtlose Netz in so genannte Zellen unterteilt. In jeder Zelle befindet sich mindestens ein Sender/Empfängerpaar. Alle Sender/Empfängerpaare innerhalb einer Zelle benutzen eine gemeinsame Frequenz bzw. denselben Code. Die einzelnen Zellen, die sich räumlich überlappen können, sind miteinander zu einem Gesamtnetzwerk gekoppelt.

Für die Verbindung zwischen Sender und Empfänger können zwei Arten unterschieden werden.

Bei der gerichteten Verbindung muss zwischen Sender und Empfänger Sichtkontakt bestehen. Dies gilt für viele Laptops und Drucker, die mit IR-Schnittstellen ausgestattet sind.

Diffuse Verbindungen nutzen die Reflexionen an Wänden, Decken usw. Die meisten für den LAN-Bereich angebotenen Funknetze arbeiten auf diese Weise. Der Ersatz der Tertiärverkabelung durch drahtlose Netze hat neben erheblichen Einschränkungen in der Bandbreite (< 2 Mbit/s) eine Reihe weiterer Nachteile.

Für den Übergang zum Gebäudenetz sind Kabel zu den zentralen Access-Points jeder Zelle zu verlegen. In der Regel beschränkt sich die Zellgröße auf einen Raum, so dass jeder Raum mit einem Kabel angefahren werden muss und zusätzlich teure Funkmodule zu beschaffen sind. Die konventionelle Verkabelung ist daher in den meisten Fällen wirtschaftlicher. Ausnahmen können sich durch Sonderanwendungen oder besondere Gebäudestrukturen ergeben. Dies sind:

- ✔ Netze mit hohem Mobilitätsgrad (Laptops in Lager oder Werkstattbereichen, Hallen, Messen etc.)
- ✔ Bauliche Restriktionen
- ✔ Bauliche Probleme bei der Errichtung von Trassensystemen

1.5 Strukturierte Verkabelung nach EN 50173

Weltweit existieren seit Ende der 80er Jahre Normungsansätze für den Aufbau von strukturierten, systemneutralen Verkabelungssystemen. Die derzeit gültigen Normen und Gremien sind:

- ✔ EN 50173 in Europa
- ✔ EIA/TIA 568 in den USA
- ✔ ISO/IEC 11801 international

Das Modell der strukturierten Verkabelung unterteilt die Kabelinfrastruktur in drei Bereiche:

- ✔ Primärbereich
- ✔ Sekundärbereich
- ✔ Tertiärbereich

Die Unterscheidungskriterien für diese Aufteilung ergeben sich aus den unterschiedlichen Längen zwischen den entsprechenden Verteilern bzw. Endgeräten und durch die benötigten Anforderungen an die Übertragungsgeschwindigkeit.

Wird die Verkabelung nach den Normen der EN 50173 aufgebaut, dann spricht man auch von einem anwendungsneutralen Verkabelungssystem, das sowohl für Sprache als auch für Bild und Daten geeignet ist.

Die Komponenten sind:

- ✔ Standortverteiler **SV**
- ✔ Gebäudeverteiler **GV**
- ✔ Etagenverteiler **EV**

Primärbereich

Der Primärbereich umfasst alle gebäudeübergreifenden Kabelwege. Der Haupt- oder Standortverteiler verzweigt in den Sekundärbereich zu Gebäudeverteilern.

Leistungskriterien in diesem Bereich sind:

- ✔ Hohe Übertragungsraten
- ✔ Ausfallsicherheit

Im Normalfall erfolgt die Verkabelung mit Monomode Glasfaser. Als maximale Länge ist in der Norm eine Strecke von 1500 Metern vorgesehen.

Sekundärbereich

Der Sekundärbereich verbindet die verschiedenen Stockwerke eines Gebäudes. Damit definiert dieser Bereich die Strecke zwischen Gebäude- und Etagenverteilern. Die Leistungskriterien entsprechen dem Primärbereich. Auch hier kommen normalerweise Glasfaserkabel zum Einsatz. Die normgerechte Entfernung beträgt maximal 500 Meter.

Tertiärbereich

Der Tertiärbereich verbindet in einer Etage die Datendosen mit dem Etagenverteiler. In der Regel ist die Anzahl der Anschlussdosen höher als die tatsächliche Anzahl von Arbeitsstationen und Netzgeräten, etwa im Verhältnis 2:1. Auch hier gelten natürlich Längenbeschränkungen. Die maximale Entfernung zwischen Endgerät und Verteiler ist 100 Meter, die nochmals in folgende Bereiche aufgeteilt werden:

- ✔ 90 Meter zwischen Verteiler und Endgeräteanschluss
- ✔ Je 5 Meter Rangier- und Anschlusskabel

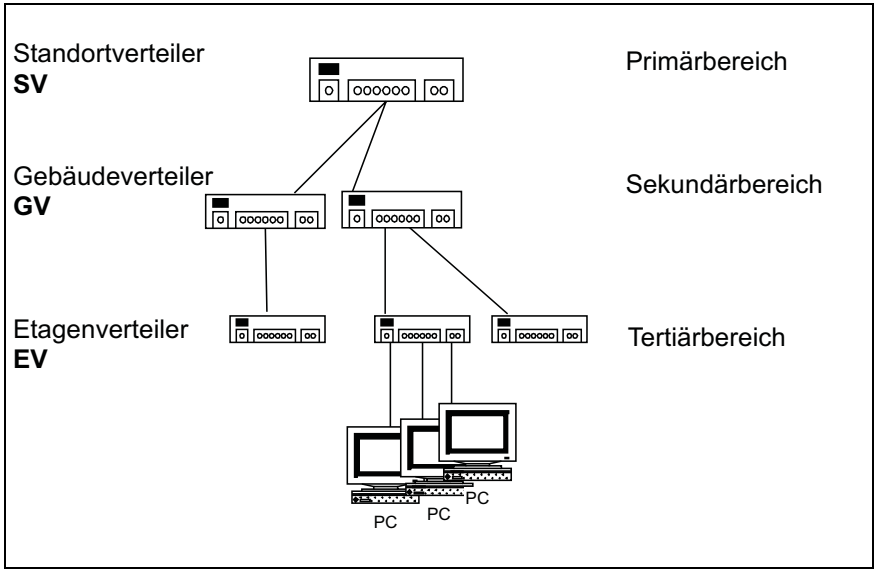


Abbildung 1.9: Strukturierte Verkabelung

Dimensionierung

Die Norm EN 50173 sieht folgende maximale Längen vor:

- ✔ SV nach GV: 1500 Meter
- ✔ GV nach EV: 500 Meter
- ✔ EV nach Anschlussdose: 90 Meter

KAPITEL 2

2 Standards und Protokolle

Standards, oft auch als Normen bezeichnet, definieren technische, funktionale und materielle Vorgaben, die von Hard- und Softwareherstellern als Richtlinien eingehalten werden. Dabei kann man zwischen folgenden Standards unterscheiden:

- ✔ International anerkannte Normungsgremien, de jure
- ✔ Industriestandards, de facto

Internationale Standardisierungsgremien sind solche, die aufgrund von Verträgen zwischen Länderregierungen entstanden sind oder freiwillige Organisationen. Im Folgenden erhalten Sie eine Übersicht.

- ✔ **ISO**, International Standards Organization

  Mitglieder sind die nationalen Normungsinstitute der 89 beteiligten Staaten.

- ✔ **ITU**, International Telecommunication Union

  Ehemals CCITT, hier sind die nationalen Telekom-Gesellschaften beteiligt.

Zu den freiwilligen Organisationen zählen:

- ✔ **ANSI**, American National Standards Institute

  ANSI ist eine, trotz ihres offiziellen Namens, private und gemeinnützige Organisation, deren Mitglieder Hersteller, Telekom-Gesellschaften und andere Interressensgruppen in den USA sind.

- ✔ **IEEE**, Institute of Electrical and Electronic Engineers

  Diese Organisation repräsentiert den international größten Fachverband von Elektro- und Elektronikingenieuren und ist das entscheidende Gremium bei der Standardisierung von LAN-Standards.

- ✔ **ECMA**, European Computer Manufacturers Association

  Die Mitglieder der ECMA waren ursprünglich europäische Computerhersteller. Heute genügt es, wenn das Mitgliedsunternehmen eine europäische Produktionsstätte besitzt.

- ✔ **EIA**, Electronic Industries Association

  Eine Vereinigung amerikanischer Hersteller elektronischer Geräte. Dieses Gremium hat großen Einfluss im Bereich der Verkabelungstechnik.

- ✔ **IETF**, Internet Engineering Task Force

  Die Koordination der Entwicklung neuer Internetprotokolle wird von der IETF geleistet. Hier sind Entwickler, Anwender, Hersteller und Wissenschaftler zusammengeschlossen, die mit dem Internet und Internetprotokollen zu tun haben. Die IETF umfasst insgesamt acht Arbeitsgruppen, die sich mit Themen wie Applikationen, Host- und Benutzerservice, Internet-Services, Routing, Network Management, OSI-Integration, Operations und Sicherheit befassen.

- ✔ **ATM** Forum

  Das ATM-Forum, ein Zusammenschluss ATM-Technologie produzierender Unternehmen, ist federführend bei der Integration der ATM-Technologie in den LAN-Bereich.

Häufig übernehmen die offiziellen Normungsgremien de facto Standards.

Warum Standards?

Zu Beginn der »Netzwerkerei« entwickelte jeder Hersteller seine eigenen Normen. Die IBM besaß allein ein Dutzend. Das Ergebnis war, dass Rechner unterschiedlicher Hersteller nicht miteinander kommunizieren konnten. Diese Situation entspricht heute nicht mehr den Anforderungen der Anwender, die auf den Dialog von Endgeräten unterschiedlichster Herkunft drängen und die Abhängigkeit von einem Hersteller vermeiden möchten.

Standards führen zu erhöhter Wirtschaftlichkeit bei der Herstellung von Netzwerkprodukten und damit zu niedrigeren Preisen. Sie bieten eine größere Akzeptanz und Konnektivität zwischen Endgeräten verschiedener Hersteller.

Was sind Protokolle?

Protokolle sind das Ergebnis von Normen. Protokolle regeln den Austausch von Informationen zwischen den an der Kommunikation beteiligten Instanzen. Geregelt werden

- ✔ die Darstellung der Information, Syntax und die Bedeutung der Information, Semantik
- ✔ die zeitliche Abfolge der Übertragung
- ✔ der Zugriff auf das Übertragungsmedium

Die Datenkommunikation, und damit auch der Informationsaustausch in einem lokalen Netz, ist viel zu komplex, um mit einem einzigen Protokoll beschrieben zu werden. Deshalb wurden schon früh hierarchische Modelle entwickelt, die die Kommunikation in Teilschichten aufteilen. Die für die heutige Diskussion maßgeblichen Modelle sind das OSI-Modell der ISO und das Internetschichtenmodell.

2.1 Das OSI-Modell im Überblick

OSI, Open System Interconnection, unterteilt die Kommunikation in sieben Schichten. Für jede Schicht können Protokolle entwickelt werden, die die Offenheit des Gesamtsystems gewährleisten.

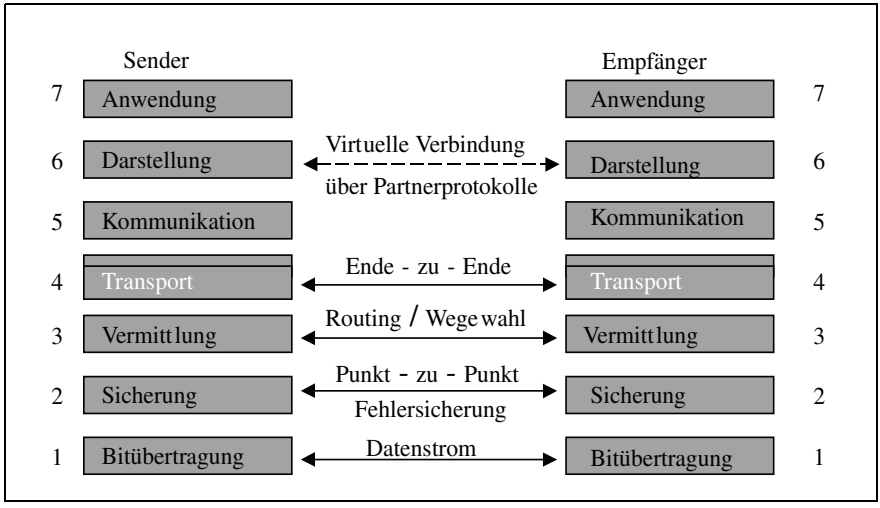


Abbildung 2.1: OSI-Modell

Die Protokolle der Schicht 1, **Bitübertragungsschicht**, legen im Sinne des Modells die physikalischen Eigenschaften der Übertragungsmedien fest. Die Dienstleistung für die nächsthöheren Schichten besteht in der Übertragung von Daten. Die Schicht 1 ist die einzige Schicht, in der auch eine physikalische Verbindung aufgebaut wird. Die Verbindungen der nachfolgenden Schichten sind logischer Art und werden deshalb auch als virtuelle Verbindungen bezeichnet. Technische Details der Sicherungsschicht fallen in den Zuständigkeitsbereich von Fachleuten, so dass mancher davon ausgeht, diesen Bereich »mit ruhigem Gewissen als Aufgabe eines Elektroingenieurs (zu) bezeichnen.« Dennoch ist zu bedenken, dass nach Schätzungen über 50 Prozent aller auftretenden Fehler in einem LAN der Bitübertragungsschicht zuzuordnen sind.

Die **Sicherungsschicht** dient dazu, in der Schicht 1 aufgetretene Übertragungsfehler zu erkennen und zu korrigieren. Wichtig ist in diesem Zusammenhang, dass die Sicherungsschicht immer eine Punkt-zu-Punkt-Sicherung darstellt. D.h. diese Schicht stellt sicher, dass keine Bitfehler zwischen zwei Vermittlungsstellen auftreten. Es wird nicht geprüft, ob es z.B. logische Fehler gibt.

Die Hauptfunktion der Schicht 3, der **Vermittlungsschicht**, besteht darin, für Datenpakete im Netz den richtigen Weg zu finden. Diese Funktion wird auch als Routing bezeichnet.

In der Schicht 4, **Transportschicht**, werden auf der Basis der von den unteren Schichten bereitgestellten Dienste Transportverbindungen aufgebaut, gesteuert und beendet. D. h. auf dieser Schicht spielen Vermittlung und Übertragungsnetz keine Rolle. Die Schicht 4 muss also beim Sender und Empfänger einer Nachricht implementiert sein. Auf der Transportschicht werden Ende-zu-Ende-Verbindungen aufgebaut. Damit stellt diese Schicht sicher, dass die Daten auch den Empfänger erreichen, für den sie auf dem Host-System bestimmt sind.

Die Einhaltung der in den Schichten 1 bis 4 verankerten Protokolle führt dazu, dass Informationen in einem Netzwerk fehlerfrei übertragen werden. Deshalb werden alle Protokolle dieser Schichten auch als Transportsystem bezeichnet. Die Schicht 4 hat dabei die Funktion einer Schnittstelle zwischen dem eigentlichen Netzwerk und den anwendungsorientierten Schichten 5 bis 7.

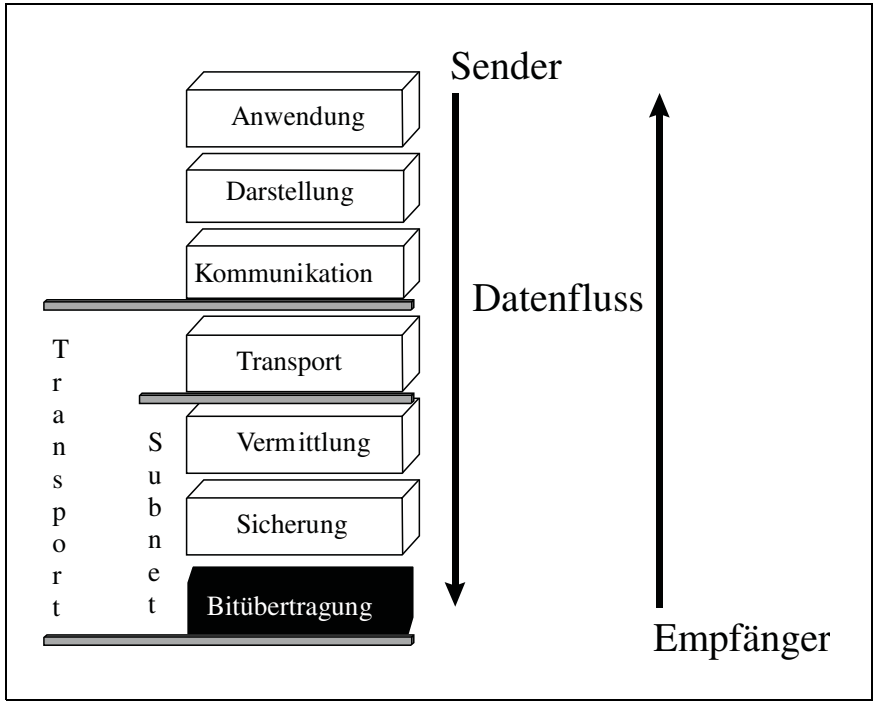


Abbildung 2.2: Struktur des OSI-Modell und Datenfluss

In der Schicht 5, **Sitzungsschicht**, wird eine Kommunikation, auch Session genannt, eröffnet, durchgeführt und beendet. Auf dieser etwas »dünnen« Schicht können zum Beispiel Synchronisationstechniken implementiert werden.

Die **Darstellungsschicht** legt fest, wie Daten dargestellt werden. Dies umfasst die Beschreibung von Daten-, Druck- und Bildschirmformaten. Beispiele sind hier Zeichensätze wie ASCI oder EBSIDIC.

In der **Anwendungsschicht** werden Dienste für die Anwendungsprogramme der Netzteilnehmer zur Verfügung gestellt.

Für die Übertragung im so genannten Transportnetz müssen auf den Vermittlungsrechnern allerdings nur die Schichten 1 bis 3 vorhanden sein. Erst im Endsystem sind die darüber liegenden Schichten von Bedeutung.

Der in Kapitel 7 vorgestellte Samba-Server ist ein Beispiel für die Implementierung der Schichten 5 bis 7 auf einem Host-System.

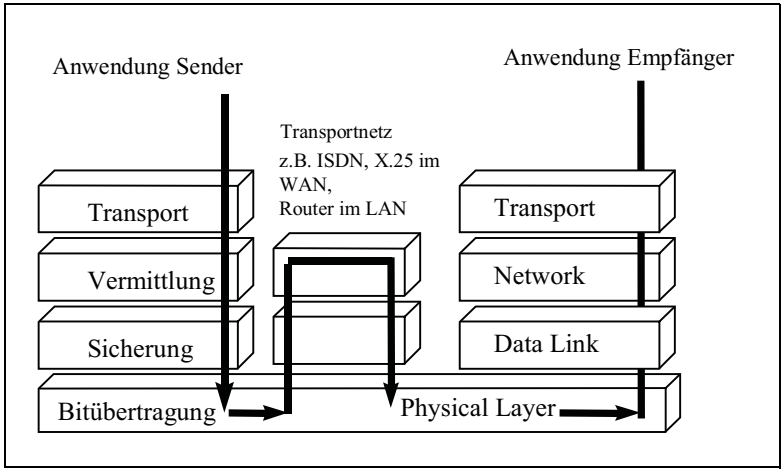


Abbildung 2.3: OSI-Transport

2.2 Lokale Netze im OSI-Modell

Für lokale Netzwerke werden die unteren drei Schichten des Modells diskutiert. D.h. nur die Transportmechanismen auf der physikalischen, der Sicherungs- und der Vermittlungsebene sind für die Standardisierung eines LAN relevant.

Diese drei Ebenen bestimmen:

- ✔ Die Austauschbarkeit der Netzwerkhardware, Kompatibilität
- ✔ Die LAN-Verbindungsmöglichkeiten, Konnektivität
- ✔ Die Möglichkeit, heterogene Netze aufzubauen, indem mehrere bisher unabhängige LAN-Segmente zu einem einzigen Netz miteinander verbunden werden.

Aus der Sicht des OSI-Modells sind Netzwerke dann heterogen, wenn unterschiedliche Protokolle auf der Schicht 2 zum Einsatz kommen.

2.2.1 LAN in Schicht 2 des OSI-Modells

Ein Merkmal, das lokale Netzwerke von öffentlichen Netzwerken unterscheidet, ist die Tatsache, dass in einem LAN immer mehrere Stationen um den Zugriff auf das Übertragungsmedium konkurrieren.

Ein LAN-Protokoll muss deshalb die Mechanismen des Zugriffs auf den Übertragungskanal regeln. Aus diesem Grunde wird die Schicht 2 des OSI-Modells, die Sicherungsschicht, in zwei Sublayer unterteilt, die **LLC**, Logical Link Control, und die **MAC**-Schicht, Medium Access Control.

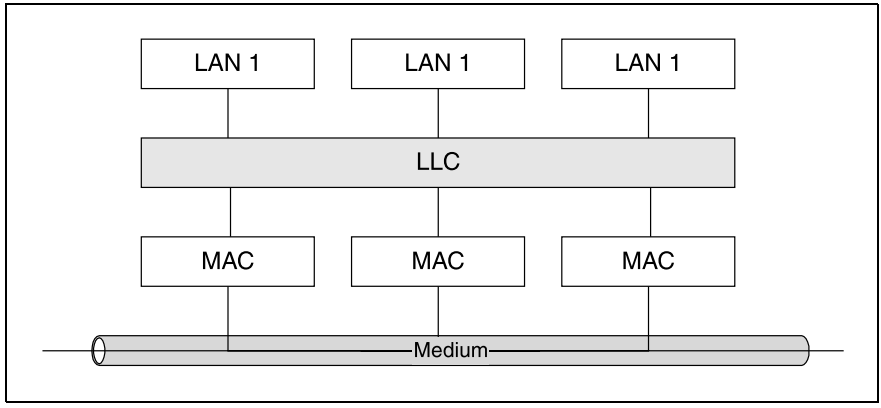


Abbildung 2.4: Die Sublayer der OSI-Schicht 2

Die LLC ist für den gesicherten Informationsaustausch zuständig und für alle standardisierten LANs gleich. Die MAC-Teilschicht regelt die Art und Weise, wie in einem LAN auf das Übertragungsmedium zugegriffen wird. Hier gibt es erhebliche Unterschiede, die in den folgenden Kapiteln detailliert besprochen werden.

2.2.2 MAC (Medium Access Control)

Aus der Sicht des Netzadministrators sind die Protokolle der MAC-Schicht relevant. Diese Protokolle sind es, die den Unterschied zwischen den auf dem Markt konkurrierenden Netzwerken ausmachen. MAC-Protokolle wurden von der IEEE normiert und sind inzwischen auch als ISO-Normen dokumentiert. Eine Ausnahme bildet **FDDI**, Fiber Distributed Data Interface, eine Erweiterung des Token Ring-Verfahrens. FDDI wurde von ANSI standardisiert, ist aber als IEEE-Standard dokumentiert und implementiert.

Auch wenn zwei Endsysteme jeweils das OSI-Modell verwenden, dann bedeutet dies nicht zwangsläufig, dass sie auch tatsächlich miteinander kommunizieren können. Ein offensichtliches Beispiel ist die MAC-Schicht, in der mehrere Standardprotokolle miteinander konkurrieren. Abbildung 2.6 macht nochmals das Zusammenspiel der unteren OSI-Schichten in einem lokalen Netzwerk deutlich.

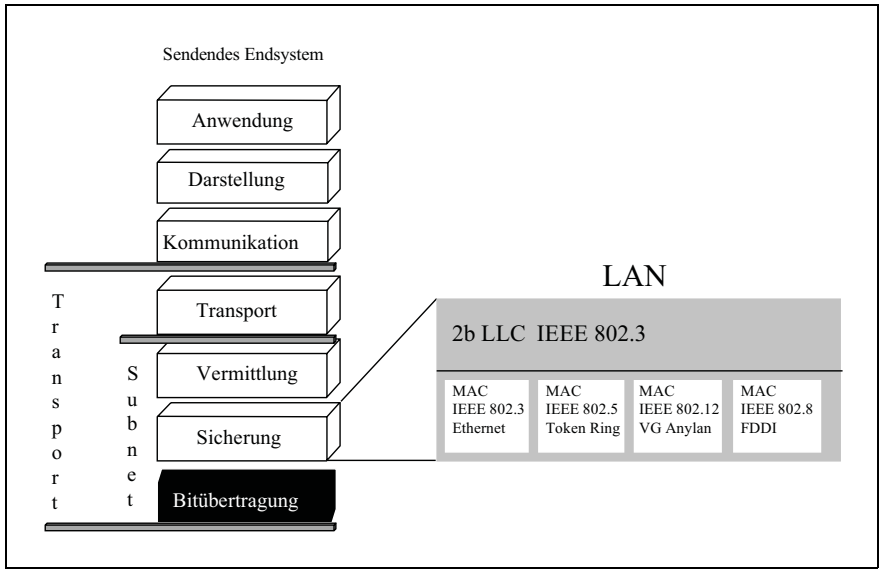


Abbildung 2.5: MAC-Layer

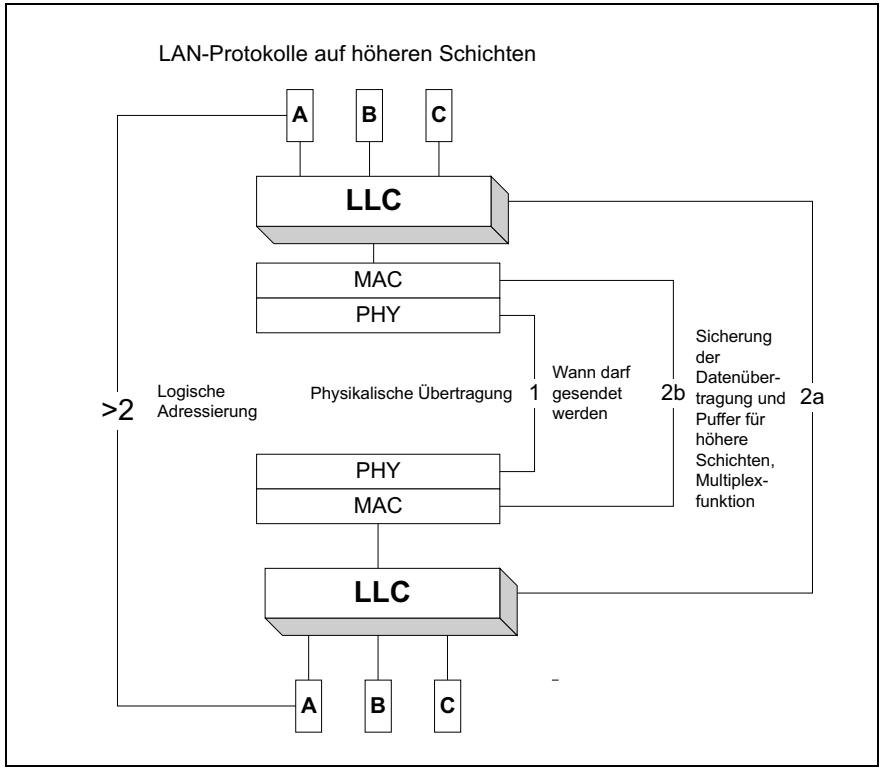


Abbildung 2.6: OSI-Schichten im LAN.

2.3 Netzwerkstandards nach IEEE802.xx

Im Februar 1980 startete die IEEE das Projekt 802, 80 für die Jahreszahl und 2 für den Monat, mit dem Ziel, allgemein gültige Standards für lokale Netzwerke zu definieren. Dazu wurden Arbeitsgruppen gebildet, deren Ergebnisse dann als 802.xx Standard veröffentlicht sind bzw. wurden. Die Platzhalter xx stehen für die jeweilige Arbeitsgruppe. Eine Norm nach 802.1 ist also das Ergebnis der Arbeitsgruppe 1 des Projektes 802 der IEEE. Die vom IEEE 802-Gremium verabschiedeten Standards werden als internationale Standards ISO 8802 übernommen.

Das 802.x Komitee mit der offiziellen Bezeichnung IEEE 802 Local and Metropolitan Area Networks Standards Committee besteht aus 13 Arbeitsgruppen: Diese beschäftigen sich mit folgenden Bereichen, die als Standardkategorien bezeichnet werden:

- ✔ Internetworking
- ✔ LLC
- ✔ MAC in LAN und WAN

Die unten abgebildete Tabelle gibt einen ersten Überblick. Details finden Sie dann in den anschließenden Kapiteln.

802 Arbeitsgruppe	Thema
802.1	Internetworking
802.2	Logical Link Control
802.3	Bustopologie mit CSMA/CD, Ethernet
802.4	Token Bus Topologie
802.5	Token Ring Topologie
802.6	Metropolitan Area Networks, MAN
802.7	Beratergruppe Breitband
802.8	Beratergruppe Glasfasertechnik, LAN mit Glasfasertechnik
802.9	Integrierte Voice/Daten-Netze
802.10	Sicherheit
802.11	Drahtlose Netzwerke
802.12	Demand Priority Access LAN
802.14	Kabelfernsehen, Kabelmodems

Tabelle 2.1: Arbeitsgruppen des IEEE 802 Komitees

2.4 IEEE 802.3 – Ethernet

Basis eines Ethernet-LAN ist der Bus, auch trunk oder ether genannt. An den Bus werden die Teilnehmerstationen angeschlossen. Der Anschluss erfolgt über einen Transceiver. Das ist eine Basisband-Sende-/Empfangseinheit, die über das Transceiverkabel mit der Netzwerkkarte der Teilnehmerstation verbunden ist. Auf der Netzwerkkarte, dem Ethernet-Controller, sind mehrere Chips integriert, die das gesamte Ethernet-Protokoll abarbeiten. Damit bestehen die Komponenten eines Ethernet-Anschlusses aus

- ✔ Transceiver
- ✔ Transceiverkabel
- ✔ Ethernet Controller

Der klassische Ethernet-Standard sieht für 10 Base 5, das sind 10 Mbp/s über ein Basisband mit 500 Metern Länge, folgende Spezifikationen vor:

Kategorie	Wert
Länge des Busses	500 Meter
Kabel	Koaxialkabel mit 50 Ohm Impendanz, wegen der Farbe der Außenhaut auch Gelbes Kabel, Yellow Cabel, genannt.
Bandbreite	10 Mbps
Abstand Transceiver	2,5 Meter (mindestens)
Länge Transceiverkabel	50 Meter
Anzahl der Stationen	100

Tabelle 2.2: 10 Base 5 Spezifikation

Neben dem »klassischen« Ethernet sind weitere Varianten standardisiert, deren Details Sie in den folgenden Kapiteln erfahren. Alle Ethernetvarianten besitzen allerdings gleiche Merkmale. Diese sind:

- ✔ Standardisierung nach 802.3
- ✔ Broadcast
- ✔ Basisbandnetze
- ✔ Gleiches Paketformat, maximal 1518 Byte und minimal 64 Byte

Die verschiedenen Implementierungen der Ethernettechnik unterscheiden sich in folgenden Punkten:

- ✔ Geschwindigkeit, 10, 100 oder 1000 Mbit/s
- ✔ Medium, Kupfer- oder Glasfaser sowie Varianten der jeweiligen Technik
- ✔ Internetworking, Komponenten wie Hubs und Switches

Zurzeit sind die in der folgenden Tabelle aufgeführten Ethernetarbeitsgruppen aktiv:

Arbeits-gruppe	Arbeitsgebiet
IEEE 802.3z	Arbeitsgruppe für die Übertragung von Gigabit Ethernet über Glasfaser
IEEE 802.3ab	Arbeitsgruppe für die Übertragung von Gigabit Ethernet über Twisted Pair Kat. 5 über 100 Meter
IEEE 802.3x	Erweiterung von IEEE 802.3 in Richtung Full-Duplex-Betrieb und Datenflusssteuerung, Flow Control
IEEE 802.1p	Erweiterung der Schicht 2 Pakete um Prioritätsinformationen, Stichwort Quality of Services für die Übertragung von Multimediadaten, d.h. Sprache, Sound und Video
IEEE 802.1Q	Erweiterungen in Richtung VLAN

Tabelle 2.3: Übersicht Arbeitsgruppen für IEEE 802.3

In der Praxis hat sich ein Klassifizierungsschema für die verschiedenen Ethernetnetze eingebürgert. Dieses informiert über die Übertragungsrate, das Übertragungsverfahren, den verwendeten Kabeltyp und über die maximale Länge eines Segmentes.

Beispiele:

10 BASE 5 Ein Ethernet mit 10 Mbps, Basisbandverfahren und einer maximalen Segmentlänge von 500 Metern.

10 BASE T Ein Ethernet mit 10 Mbps, Basisband mit Twisted Pair Kabel. Hier entfällt wegen der standardmäßigen Begrenzung auf 100 Meter die Längenangabe.

10 BASE FL Ein Ethernet mit 10 Mbps, Basisband mit Glasfaserkabel 50/125 µm. Hier entfällt wegen der standardmäßigen Begrenzung auf 2000 Meter die Längenangabe.

Die folgende Tabelle gibt einen Überblick über die »klassischen« Ethernetstandards, die alle eine Übertragungsrate von 10 Mbit/s liefern. Im Kapitel 2.6 finden Sie eine Übersicht über die Standards für die schnelleren Fast Ethernet Varianten.

	10 Base 5	10 Base 2	10 Base T	10 BaseFL
Segmentlänge	500 Meter	185 Meter	100 Meter	2 km
Medium	Dickes Koax 50Ω	Dünnes Koax 50Ω	Kat. 5 TP	Monomode
Stationen pro Segment	100	30	1	1
Topologie	Bus	Bus	Stern	Stern

Tabelle 2.4: Klassische Ethernetstandards

Für den Einsatz von Repeatern, die als Verstärker Ethernetsegmente miteinander verbinden, gilt die 5-4-3 Repeaterregel:

	10 Base 5/2	10 Base FL
5	X	X
4	X	X
3	X	

Zwischen zwei Stationen liegen maximal fünf Segmente mit maximal vier Repeatern oder maximal drei Bussegmente mit angeschlossenen Stationen, populated.

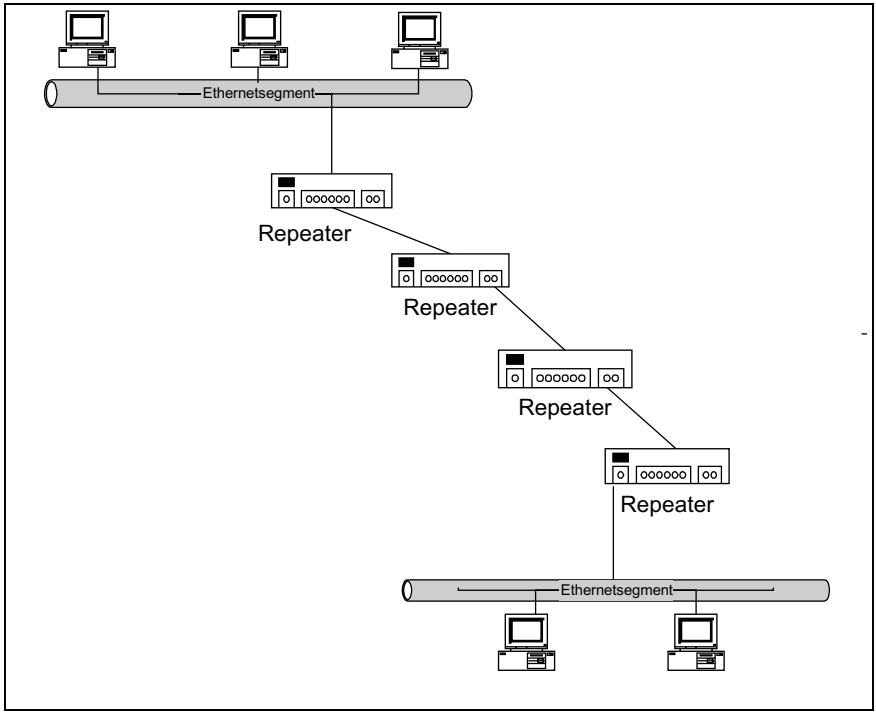


Abbildung 2.7: Ethernet-Segmente miteinander verbinden

2.4.1 CSMA/CD – MAC-Protokoll im Ethernet

Das Ethernet verwendet für den Zugriff auf den Bus ein **CSMA/CD**, Carrier Sense Multiple Access with Collision Detection, genanntes Verfahren. Nach diesem Verfahren kann prinzipiell jede Station zu jedem beliebigen Zeitpunkt Daten senden, Multiple Access. Bedingung ist lediglich, dass das Übertragungsmedium, der Bus, frei ist.

Dazu hört jede Station den Bus permanent ab, Carrier Sense.

Während der Übertragung hört die Station auch weiterhin den Bus ab und kann Kollisionen erkennen, Collision Detection. Eine Kollision ist dann aufgetreten, wenn eine positive Spannung auf dem Kabel liegt.

Eine Kollision veranlasst die erkennende Station, ein JAM genanntes Signal zu erzeugen. Das Signal informiert alle angeschlossenen Stationen über eine aufgetretene Kollision und besteht aus vier Byte mit dem Bitmuster 10101010 10101010 10101010 10101010.

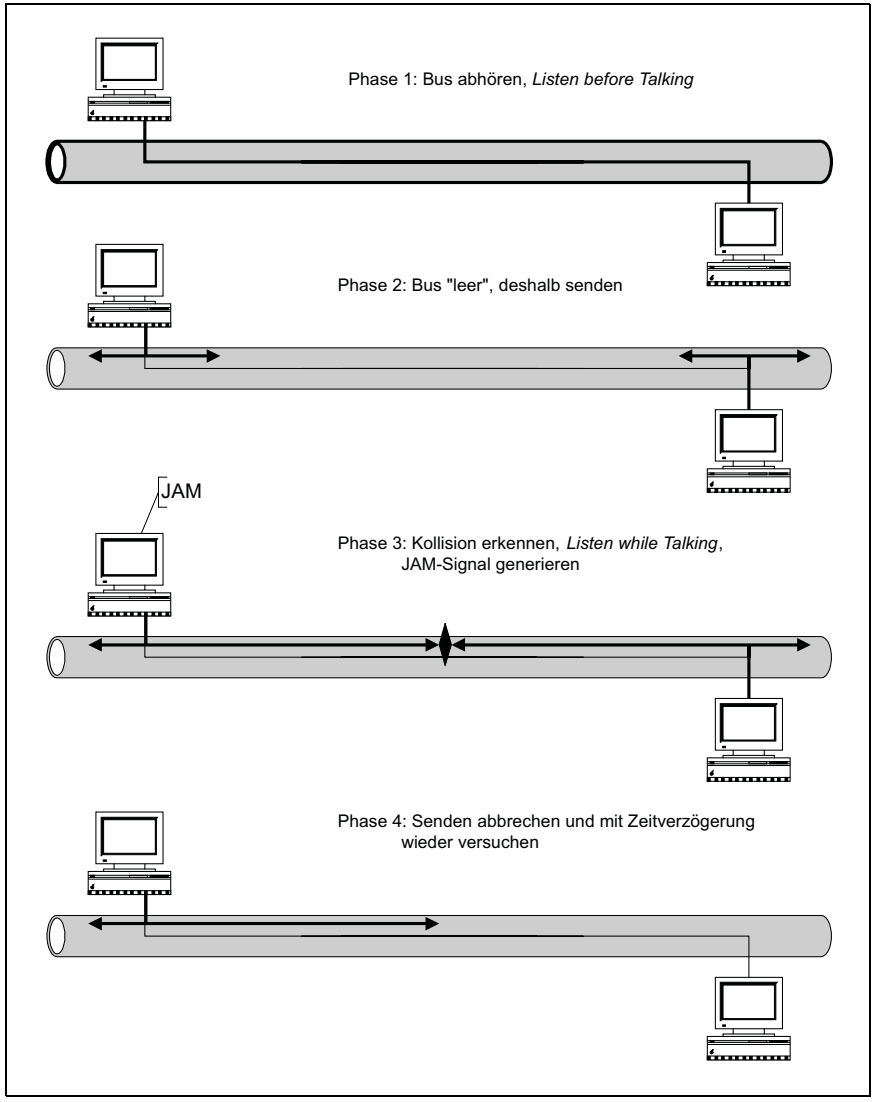


Abbildung 2.8: CSMA/CD – Zugriffsverfahren

Nachdem eine Kollision erkannt wurde, versuchen alle beteiligten Stationen erst nach einer zufällig kalkulierten Zeit wieder zu senden. Das verwendete Verfahren wird Backoff-Verfahren genannt. Der Backoff-Algorithmus ist so ausgelegt, dass eine Sendung 16-mal durch eine Kollision verhindert werden kann, bevor durch den LAN-Coprozessor der Netzwerkkarte eine Fehlermeldung erzeugt wird.

Die maximale Slottime von 51,2 µs legt fest, wie lange eine Station warten muss, bis sie erkennen kann, dass keine andere Station sendet. Sie entspricht damit der längstmöglichen Verbreitungsdauer im Übertragungsmedium. Bei der Festlegung der maximalen Slottime wurde von einer 2,5 km langen Kabelstrecke mit vier Repeatern ausgegangen. Die maximale Slottime wird auch als Collision Window bezeichnet.

2.4.2 Datenformat im Ethernet – Paketübertragung

Im Ethernet wie auch in anderen LAN-Standards nach IEEE 802.xx werden die Daten als Rahmen oder Frame übertragen. Diese Technik hat gegenüber einer seriellen Übertragung als Datenstrom den wesentlichen Vorteil, dass die Daten transparent übertragen werden können, d.h. für die Übertragung der Daten ist ihre Bedeutung unerheblich. Abbildung 2.9 zeigt den Aufbau zweier Ethernet-Rahmen.

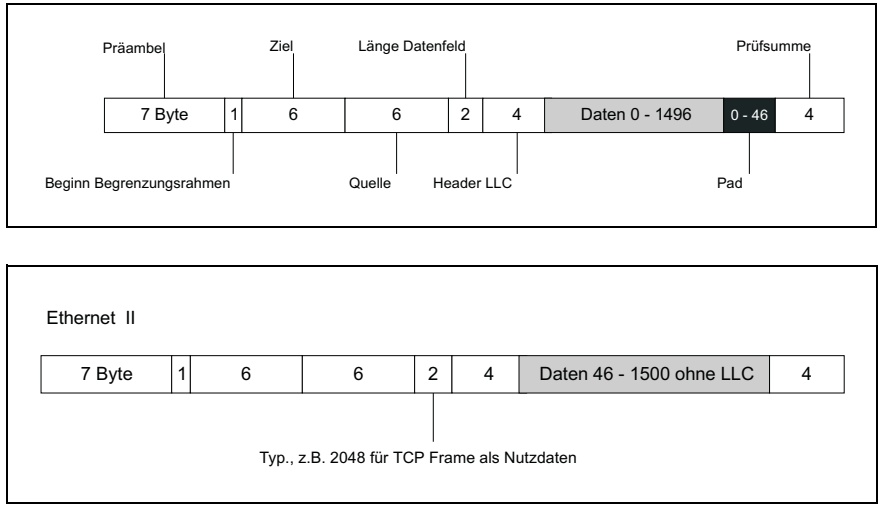


Abbildung 2.9: Ethernet – Frameaufbau

Jeder Rahmen beginnt mit einer sieben Byte langen Präambel, deren Byte jeweils das Bitmuster 10101010 enthalten. Diese Kodierung dient zur Synchronisation von Sender und Empfänger. Das folgende Byte, der Beginn des Rahmenbegrenzers, enthält das Bitmuster 10101011.

Der Rahmen enthält zwei Adressen, die des Empfängers, Ziel oder Destination, und die des Senders, der Quelle Sender. Der Standard sieht hier zwar Längen zwischen zwei und sechs Byte vor, in der Praxis wird jedoch immer eine sechs Byte lange Adresse verwendet. Das höherwertige Bit, Bit 47, der Zieladresse kann zweifach kodiert werden. Die Null bedeutet, dass genau ein Empfänger angesprochen werden soll, »normale« Adresse. Die Eins bedeutet, dass es sich um eine Gruppenadresse handelt. Die Gruppenadressierung ermöglicht es, dass eine Sendung auch an mehrere Stationen erfolgen kann, Multicast. Besteht die Zieladresse nur aus Einsen, dann empfangen alle Stationen, Broadcast oder Rundsenden.

Auch dem Bit 46 kommt eine besondere Bedeutung zu. Mit dessen Hilfe kann zwischen einer lokalen und einer globalen Adresse unterschieden werden. Lokale Adressen werden vom Netzadministrator vergeben und haben außerhalb des Netzes keine Bedeutung. Globale Adressen vergibt die IEEE.

Die Länge des Adressraumes, 48-2 gleich 46 Bit, gewährleistet, dass es weltweit nie zwei Ethernet-Stationen mit gleicher Adresse geben kann. Die Länge des Datenfeldes, das die Informationen für den Empfänger enthält, wird nach den Adressen in ein zwei Byte langes Feld eingetragen. Die Länge von null Byte für das nachfolgende Datenfeld ist zulässig, führt aber aufgrund physikalischer Gegebenheiten zu Problemen im Netz. Diese werden durch das Pad-Feld verhindert. Diese Feld ist immer so lang, dass Datenfeld und Pad immer mindestens 46 Byte umfassen. Dadurch wird eine Mindestlänge von 64 Byte für jeden Ethernet-Rahmen garantiert.

Frames, die kleiner als 64 Byte sind, werden Short Frames oder Runts genannt. Sie entstehen bei Kollisionen.

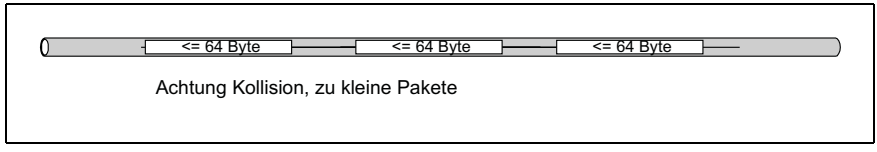


Abbildung 2.10: Runts oder Short Frames – Datenpakete nach einer Kollision

Die vier Byte lange Prüfsumme schließt den Rahmen ab. Es handelt sich hier um ein Prüfsummenverfahren, das mit nahezu hundertprozentiger Sicherheit das Nichtentdecken eines Übertragungsfehlers ausschließt.

Das Ethernet Format Version 2, Ethernet II, benutzt ein Typenfeld, um damit auf Kommunikationsprotokolle der Schicht 3 zu verweisen. Netzwerke, die die TCP/IP Protokolle einsetzen, verwenden Ethernet II Frames. Der Wert 2048 im Typenfeld signalisiert, dass TCP-Frames als Nutzdaten transportiert werden. Sie sehen, dass die Typenkennung größer ist als die MTU, Maximum Transfer Unit, der 802.3 Rahmen. Damit ist gewährleistet, dass Clients, die nur IEEE 802.3 verwenden, entsprechende Rahmen als fehlerhaft interpretieren und gar nicht erst an den Protokollstack weiterreichen.

2.4.3 Aufbau der MAC-Adresse einer Ethernet-Karte

Das Ethernet arbeitet mit so genannten kanonischen Adressen. Technisch bedeutet dies, dass das niederwertigste Bit eines jeden Byte als erstes übertragen wird.

Für nichtkanonische Adresse gilt, dass zuerst das höchstwertige Bit übertragen wird. Dies ist bei Token Ring und FDDI der Fall. Insgesamt ist eine MAC-Adresse sechs Byte lang, wobei drei Byte auf die Hersteller ID und drei Byte auf die Station-ID entfallen. Anhand der ersten beiden Bit werden universelle oder lokale Adresse sowie Individual- oder Gruppenadresse unterschieden.

Das 17. Bit fungiert als Indikator für eine funktionale Adresse. Es wird dann auf null gesetzt, wenn Gruppen- und Universaladresse auf null gesetzt sind. Die MAC-Adresse ist also dann lokal und individuell, wenn der Functional Address Indicator null ist.

Funktionale Adressen dienen dazu, auf MAC-Ebene die Struktur des Netzes abzubilden. Die nichtfunktionalen, eingebrannten Adressen der Netzwerkkarten sind dazu ungeeignet.

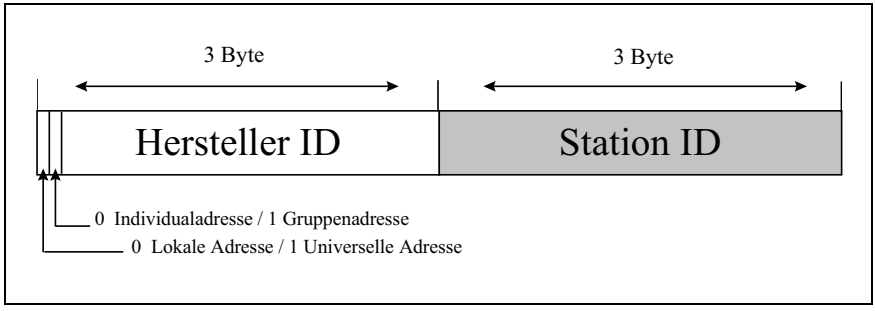


Abbildung 2.11: Ethernet MAC-Adresse

2.4.4 Ethernet – Zusammenfassung

Ethernet-Netze sind stochastische Netze. Wann eine Station sendet, hängt vom »Zufall« ab.

Vorteile des Ethernet

- ✔ Leicht erweiterbar
- ✔ Hohe Übertragungsrate bei geringer Auslastung
- ✔ Hoher Standardisierungsgrad
- ✔ Zuverlässig
- ✔ Sehr hoher Verbreitungsgrad
- ✔ Kostengünstig

Nachteile des Ethernet

- ✔ Sinkende Leistung schon ab Auslastungen >= 30 Prozent
- ✔ Wann eine Station sendet, ist nicht vorhersehbar

2.5 IEEE 802.5 – Token Ring

2.5.1 Zugriffsmethode Token Passing

Der **Token** ist ein definiertes Bitmuster, das als Signal für die Sendeberechtigung von Station zu Station weitergeleitet wird. Der Token steuert den Datenaustausch im Netz.

Im Token Ring übernimmt immer eine Station zentrale Überwachungs- und Managementaufgaben. Diese Station wird Monitor genannt. Da diese Funktion von jeder Station ausgeübt werden kann, hat der Ausfall einer Monitorstation keine Auswirkungen auf die Funktionsweise des Netzes.

Als Übertragungsmedium kommen abgeschirmte Kupferdoppeladern und Glasfaserkabel zum Einsatz.

Der Informationsfluss in einem Token Ring lässt sich in vier Phasen gliedern. In der Phase I kreist ein freier Token im Netz und wird von Station zu Station weitergeleitet. In dieser Phase kann eine Station einige tausendmal in der Sekunde einen freien Token erhalten.

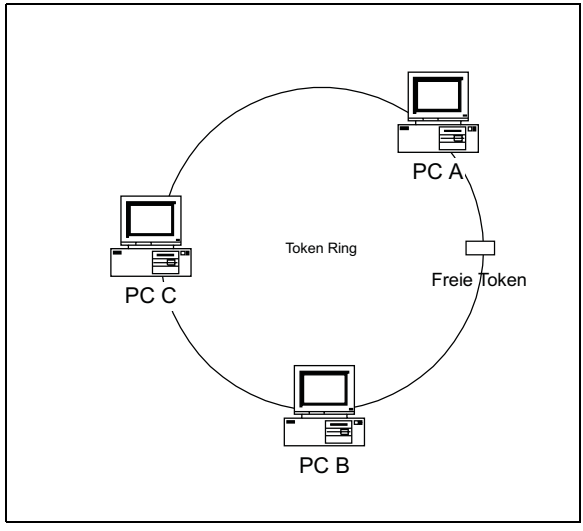


Abbildung 2.12: Token Ring Zugriffsverfahren Phase I: Freier Token kreist im Netz

In der zweiten Phase hat eine sendewillige Station das Tokenbit des Tokens auf eins gesetzt und damit »den Token belegt«. Die sendende Station setzt genau einen Datenrahmen mit der Adresse der Zielstation ab. Alle anderen Stationen im Netz erkennen den Datenrahmen und lesen die Zieladresse. Stimmt diese nicht mit der eigenen überein, dann werden die Daten weitergereicht.

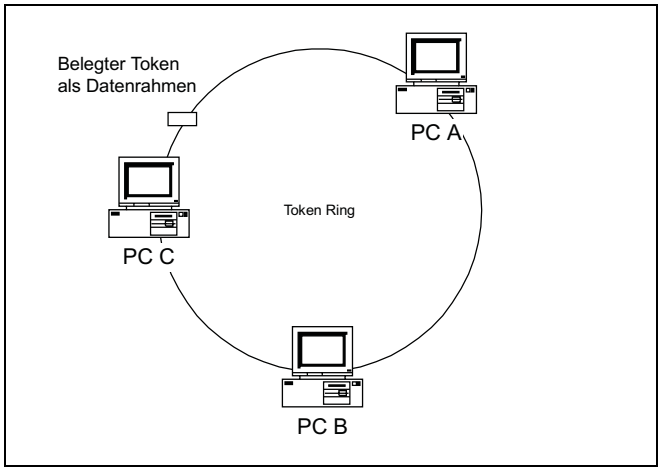


Abbildung 2.13: Token Ring Zugriffsverfahren Phase II: Token belegt, Station sendet

In der Phase III gelangen die Daten zum Empfänger, der diese kopiert. Die Station setzt das Copied-Bit im Rahmenkontroll-Byte auf den Wert eins und bestätigt damit den Empfang des Frames.

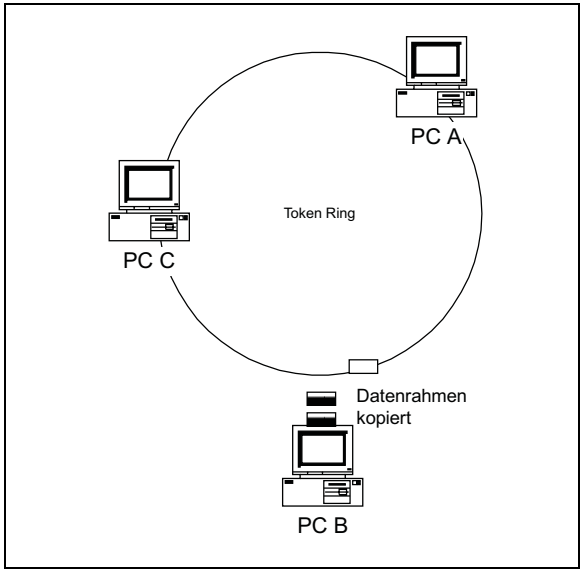


Abbildung 2.14: Token Ring Zugriffsverfahren Phase III: Empfängerstation kopiert Daten

In der letzten Phase gelangen die Daten wieder zur sendenden Station. Diese überprüft den Empfang und nimmt die Daten vom Ring. Abschließend wird ein neuer freier Token generiert.

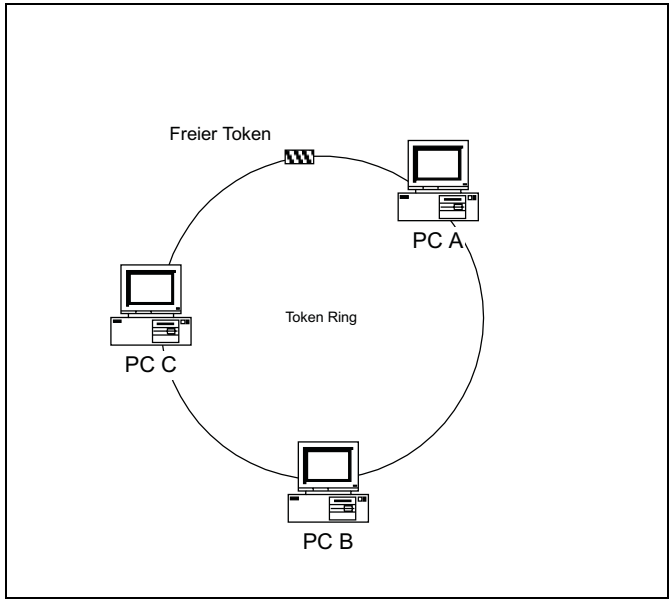


Abbildung 2.15: Token Ring Zugriffsverfahren Phase IV: Sendestation gibt Token frei

2.5.2 Rahmenformate im Token Ring

Auch im Token Ring werden die Daten als Rahmen, Frames, übertragen. Abbildung 2.16 zeigt, dass es zwei Rahmenarten in einem Token Ring gibt.

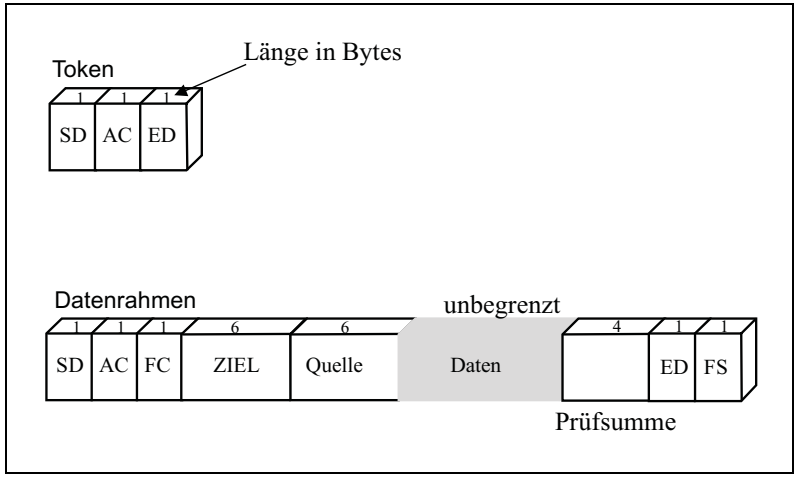


Abbildung 2.16: Die Rahmenformate im Token Ring

Wenn kein Datenverkehr vorliegt, dann kreist der drei Byte lange Token. Das erste Byte wird Start Delimiter, **SD**, genannt und markiert als Startbyte den Beginn des Rahmens. Das Byte **ED**, End Delimiter, markiert das Ende des Rahmens.

Das Byte **AC**, Access Controll, beinhaltet das Token-Bit, das Monitor-Bit, das Prioritätsbit und das Reservierungsbit. Diese Bits steuern den Zugriff auf das Netz. Erhält eine sendewillige Station den Rahmen, dann wird das Token-Bit, Bit null, auf eins gesetzt. Die ersten beiden Byte des Token werden damit zur Startsequenz für einen Datenrahmen.

Das Rahmenkontroll-Byte, **FC** Frame Control, enthält Bitmuster, die der Ringwartung dienen. Über dieses Byte werden insbesondere die Monitorfunktionen gesteuert.

Die Felder für Ziel- und Quelladresse entsprechen dem IEEE Standard 802.3, werden jedoch anders interpretiert, nämlich nichtkanonisch.

Über das Byte Rahmenstatus, FS Frame Status, wird die Übertragung der Datenrahmen kontrolliert. Dieses Byte enthält ein Bit A, das vom Empfänger auf eins gesetzt wird. Das Bit C setzt der Empfänger auf eins, wenn es ihm gelingt die Daten zu kopieren. Es gibt drei Informationsinhalte:

A = 0 und C = 0: Adressat nicht vorhanden oder nicht eingeschaltet.

A = 1 und C = 0: Adressat vorhanden, aber Rahmen nicht angenommen.

A = 1 und C = 1: Adressat vorhanden und Rahmen kopiert.

Die vier Byte lange Prüfsumme entspricht in Aufbau und Funktion der Prüfsumme des Ethernet.

2.5.3 Stationen im Token Ring

In einem Token Ring werden die Stationen über einen Ringverteiler an das Netz angeschlossen. Damit ist die physikalische Topologie des logischen Rings ein Stern. Diese Umsetzung hat Vorteile. Insbesondere ist es sehr einfach eine Station an das Netz anzuschließen bzw. vom Netz zu nehmen. Der Ringverteiler besitzt einen Ringeingang, **RI** Ring Input, und einen Ringausgang, **RO** Ring Output, sowie für jede Station einen Anschluss. In Abbildung 2.17 sind drei Ringstationen angeschlossen. Eine Station ist nicht aktiv.

Die folgenden Absätze beschreiben die Aktivierung einer Ringstation nach den im Token Ring Protokoll definierten und auf der Adapter-Karte implementierten Schritten.

- ✔ Als Erstes führt die Station einen Selbsttest, Lobe-Test, durch. Dieser überprüft in einer internen Schleife die Sende- und Empfangsbausteine der Adapter-Karte. Nach erfolgreichem Selbsttest aktiviert die Karte ein Relais, so dass die Station in den Ringverteiler aufgenommen wird.

- ✔ Als nächsten Schritt überprüft die Station, ob sich bereits ein Monitor im Netz befindet. Wenn nicht, übernimmt diese Station die Funktion des Monitors.
- ✔ Es folgt die Adresskontrolle. Dabei wird überprüft, ob andere Adapter im Netz die gleiche Adresse besitzen.
- ✔ Danach stellt das Gerät die Adresse der nächstfolgenden Station fest, **NAUN** Nearest Active Upstream Neighbor.

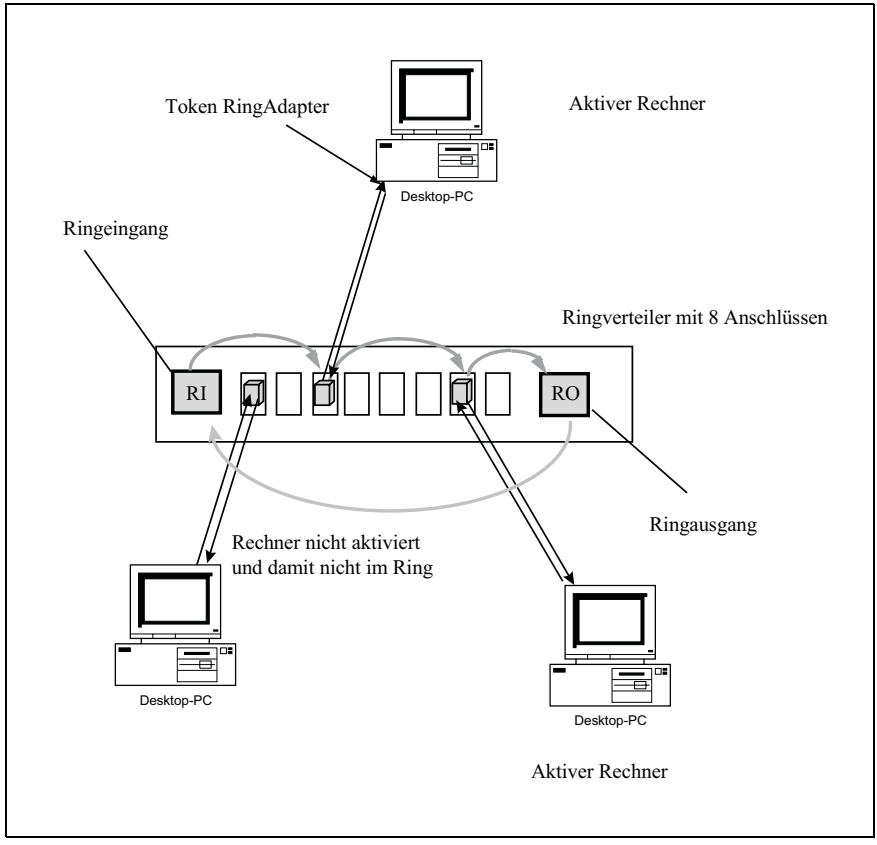


Abbildung 2.17: Stationen im Token Ring.

2.5.4 Zusammenfassung Token Ring

Das Zugriffsverfahren von Token Ring unterscheidet sich damit erheblich von dem des Ethernets.

Token Ring ist ein deterministisches Netz, da die Sendeberechtigung jeder Station vorhersehbar ist und nicht vom »Zufall« abhängt.

Vorteile Token Ring

- ✔ Datendurchsatz und Effizienz bei hoher Auslastung gut
- ✔ Zuverlässig
- ✔ Gute Integration in SNA-Umfeld

Nachteile Token Ring

- ✔ Höhere Kosten als im Ethernet
- ✔ Nicht so skalierbar wie das Ethernet

2.6 HighSpeed LANs

Netzwerke mit einer höheren Geschwindigkeit als 10 Mbit/s werden als Hochgeschwindigkeits- oder Highspeednetze bezeichnet. Die aktuelle Entwicklung zeigt, dass hier eindeutig der Entwicklungsschwerpunkt beim Ethernet liegt.

2.6.1 Fast Ethernet

In der Vergangenheit konkurrierten zwei Ethernet-Verfahren um die Gunst der Anwender, die beide eine Übertragungsrate von 100 Mpbs ermöglichen. Obwohl beide Verfahren sich technisch und auch von den Protokollen her erheblich unterscheiden, werden sie oft unter dem gemeinsamen Begriff Fast Ethernet diskutiert. Die folgenden Absätze geben einen kurzen Überblick.

Ziel des Fast Ethernet ist es, dem Anwender eine Übertragungsrate von 100 MBit zur Verfügung zu stellen. Damit werden aktuelle Anwendungstrends, die unter dem Begriff Multimedia zusammengefasst werden, in lokalen Netzen umsetzbar. Die IEEE hat zwei Arbeitsgruppen gebildet, die die hier vorgestellten Konzepte normieren.

Fast Ethernet nach IEEE 802.3 – 100 BASE X

Das Fast Ethernet Protokoll 100 BASE X wurde von der Firma Grand Function entwickelt. Der Grundgedanke dieses Verfahrens besteht darin, am Zugriffsverfahren CSMA/CD festzuhalten und durch bessere Bitkodierungsverfahren höhere Übertragungsgeschwindigkeiten zu ermöglichen. Für die Unternehmen bedeutet dies, dass eine Migration bei Vorliegen folgender Voraussetzungen möglich wird:

- ✔ Strukturierte Verkabelung
- ✔ 100 Mbps-Netzwerk-Adapter
- ✔ Hubs, die 100 Mbps unterstützen

Für Fast Ethernet sind die in der folgenden Tabelle aufgeführten Standards verabschiedet:

Norm	Technik
100 Base TX	100 Ohm, Kat.5-Kabel, mindestens zwei Adernpaare
100 Base X	150 Ohm, Kat.5 Kabel, mindestens zwei Adernpaare
100 Base FX	LWL, 62,5/125 µm
100 Base T4	100 Ohm, Kat.3-Kabel mindestens vier Adernpaare

Tabelle 2.5: Fast Ethernet Standards im Überblick

Für die verschiedenen Implementierungen des Fast Ethernet lassen sich Designregeln ableiten. Im Folgenden werden zwei dieser Regeln aufgeführt.

Designregeln für 100 Base TX LAN:

- ✔ Grundsätzlich muss Kategorie 5 oder besser verwendet werden
- ✔ Bei Repeater-Repeater-Verbindungen Kabel wie bei 10 Mbps Ethernet drehen
- ✔ Gleiche Kabelbelegung wie bei 10 Mbps Ethernet
- ✔ Maximale Entfernung zwischen zwei Switches: 100 Meter
- ✔ Maximale Entfernung zwischen Station und Repeater bzw. Switch: 100 Meter
- ✔ Maximal zwei Repeater kaskadierbar
- ✔ Maximale Entfernung Station-Repeater-Repeater-Station: 210 Meter

Designregeln für 100 Base FX LAN:

- ✔ Maximal zwei Repeater kaskadierbar
- ✔ Maximale Entfernungen zwischen zwei Stationen oder Switches:
- ✔ 400 Meter ohne Repeater
- ✔ 305 Meter mit einem Repeater
- ✔ 210 Meter mit zwei Repeatern, nach der Formel 400 – (Anzahl der Repeater * 95)

Im Fast Ethernet werden zwei verschiedene Repeater-Klassen eingesetzt. Class I Repeater stellen nur Ports mit gleichartigen Medienanschlüssen, z.B. nur LWL oder nur TP, zur Verfügung. Class II Repeater können, müssen aber nicht, unterschiedliche Portanschlüsse bereitstellen.

Die beiden Protokolle 100 Base FX/TX können im Full-Duplex-Modus, **FDX**, gefahren werden. Dies ist ein wesentlicher Unterschied zum ursprünglichen CSMA/CD-Protokoll, das aufgrund des gemeinsamen Übertragungskanals, Koaxkabel, nur Halb-Duplex vorsieht, d.h. zur gleichen Zeit kann eine Station nur senden oder nur empfangen.

FDX bringt, insbesondere beim Einsatz in Servern, messbare Geschwindigkeitsvorteile. Dabei wird die durch das CSMA/CD-Protokoll vorgenommene Flusskontrolle (wer darf wann senden?) durch lokale Steuerungsverfahren ersetzt. Switches sind in der Lage, mit der Gegenstelle über eine so genannte Auto-Negotiation-Funktion, den FDX-Modus »auszuhandeln«.

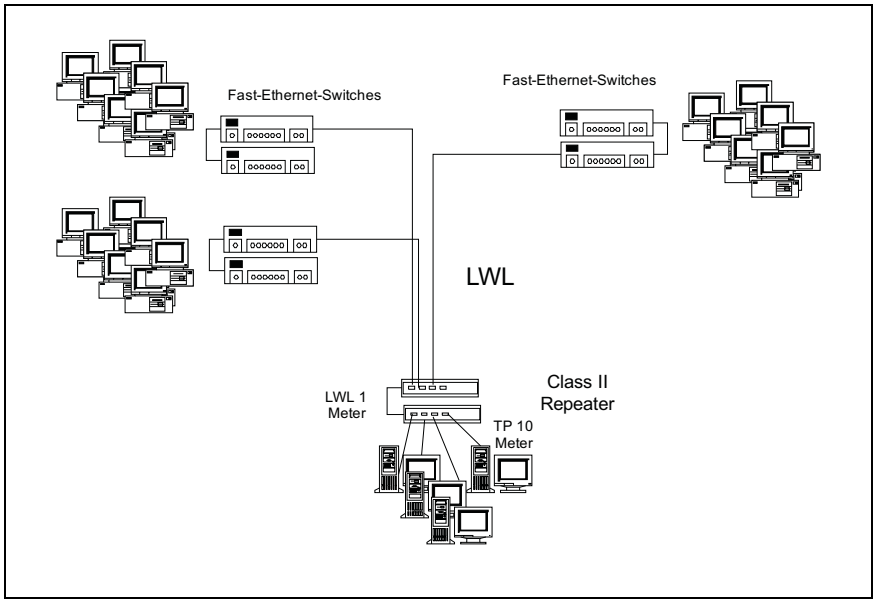


Abbildung 2.18: Beispielkonfiguration für Fast Ethernet

Fast Ethernet nach IEEE 802.12 – 100 BASE VG oder VG Anylan

VG Anylan ist eine von HP und anderen entwickelte Übertragungstechnik, die im Grunde nichts mehr mit dem klassischen Ethernet zu tun hat. Die Ursache hierfür liegt darin, dass dieses Verfahren die Datenpakete nicht mehr nach dem CSMA/CD Protokoll sendet. Es wird vielmehr ein **DPAM**, Demand Priority Access Method, genanntes Verfahren eingesetzt.

Da HP VG Anylan nicht mehr weiterentwickelt wurde, ist diese Technik auch nicht mehr praxisrelevant.

2.6.2 IEEE 802.3z – Gigabit Ethernet

Die Geschichte des Gigabit Ethernet beginnt 1995 mit der Arbeit der IEEE 802.3z Higher Speed Study Group. Im Mai 1996 wurde aus Kreisen der Industrie die Gigabit Ethernet Alliance gebildet. Mitglieder dieser Gruppe, wie z.B. HP oder Texas Instruments, begannen damit, Chips zu produzieren, die sowohl Kupferkabel als auch Lichtwellenleiter unterstützen und eine Übertragungsgeschwindigkeit von einem Gigabit und mehr ermöglichen.

Haupteinsatzgebiet des Gigabit Ethernet ist die Backbone-Technologie für Fast-Ethernet-Netze. Damit kann auch für Multimedia-Anwendungen die erforderliche Übertragungskapazität zur Verfügung gestellt werden. Zum Einsatz kommen kollisionsfreie Punkt-zu-Punkt-Verbindungen im Full Duplex Betrieb zwischen Switch und Rechner oder Switch und Switch. Damit steht Gigabit Ethernet in unmittelbarer Konkurrenz zu ATM.

Die folgende Tabelle gibt einen Überblick über die Gigabit Standards.

	1000 Base CX	1000 Base LX	1000 Base SX	1000 Base T
Wellenlänge		1300 nm	850 nm	
Medium	Twinax oder IBM Typ 1	Single Mode/ Multimode	Multimode	TP Kat.5 4 Adernpaare
Distanz	25 Meter	3 Km / 550 Meter	300 Meter	100 Meter

Tabelle 2.6: Gigabit Ethernet Standards im Überblick

CSMA/CD Erweiterungen des Gigabit Ethernet

Das »traditionelle« CSMA/CD Protokoll kann die erforderlichen Übertragungsraten im Gigabit Ethernet nicht gewährleisten. Aus diesem Grunde sind Anpassungen des Protokolls erfolgt, die im Folgenden beschrieben werden sollen. Unverändert gelten noch die für Ethernet charakteristischen Merkmale:

- ✔ Format der Pakete
- ✔ Minimale, 64 Byte, und maximale, 1518 Byte, Paketgröße

Carrier Extension

Carrier Extension bedeutet, dass alle Pakete, die kleiner als 512 Byte sind, mit so genannten Carrier Extension Symbolen auf 512 Byte aufgefüllt werden. Dadurch werden die Pakete so groß, dass sie auch über längere Strecken kollisionsfrei übertragen werden können.

Diese Technik reduziert allerdings die Nettoübertragungsrate, das sind die tatsächlich übertragenen Nutzdaten, dann erheblich, wenn überwiegend kleine Datenpakete transportiert werden. Die Übertragungswerte werden bei großen Datenpaketen jedoch besser.

Packet Bursting

Packet Bursting bedeutet, dass eine Station mehrere Pakete hintereinander senden darf. Dabei darf die Länge aller Frames die maximale Paketgröße von 1518 nicht überschreiten.

Die folgende Abbildung zeigt, dass über ein so genanntes Interframe Gap von 15 Byte Länge, die hintereinander gesendeten Pakete getrennt werden. Das erste Paket ist kleiner als 512 Byte und wird deshalb mit Hilfe von Carrier Extension Symbolen auf die für Gigabit Ethernet erforderliche Minimalgröße von 512 Byte gebracht.

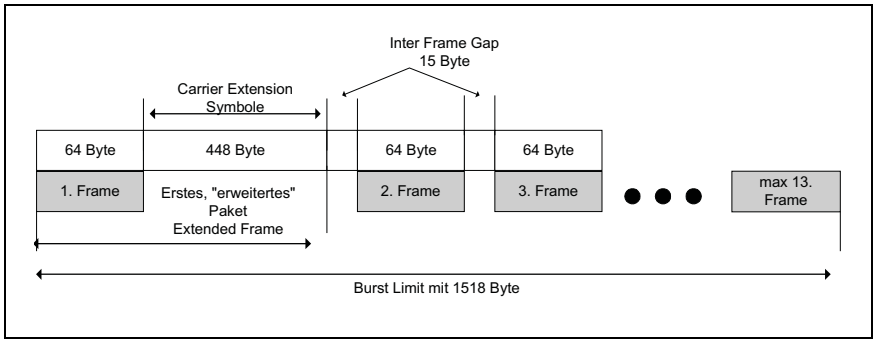


Abbildung 2.19: Packet Bursting im Gigabit Ethernet

Gigabit-Ethernet-Komponenten

Die-Gigabit-Ethernetkomponenten sind

- ✔ Simple oder Halb-Duplex-Repeater
- ✔ Buffered Repeater
- ✔ Switches

Die folgende Tabelle zeigt einen Vergleich:

	Kosten	Betriebsart	max. Netzlänge	Bandbreite
Simple Repeater	gering	Halbduplex	200 Meter	< 1 Gbps
Buffered Repeater	mittel	Vollduplex	Kupfer: 200 Meter, LWL: 2 km	ca. 1 Gbps
Switch	hoch	Vollduplex	Kupfer: 200 Meter, LWL: 2 km	> 1 Gbps

Tabelle 2.7: Gigabit-Ethernet-Komponenten im Überblick

2.6.3 10 Gigabit Ethernet

Die Workgroup 802.3ae arbeitet am aktuellen 10 Gigabit Ethernet Standard, der sich in der Endphase der Entwicklung befindet. Als Interfaces werden Glasfaserschnittstellen definiert, die sich durch verschiedene Längen und Faserdurchmesser unterscheiden. Der neue Standard wird auch unter dem Gesichtspunkt Ethernet-to-the-last-mile diskutiert. Dabei geht es um eine durchgängige Übertragung in 10- oder 100-Mbit/s Ethernettechnik vom Provider bis zum Haushalt oder in die Firma.

2.6.4 FDDI

FDDI, Fiber Distributed Data Interface, ist ursprünglich ein Standard für lokale Netzwerke auf Glasfaserbasis. FDDI wurde zunächst als ANSI-Standard **X3T9.5** dokumentiert. Mittlerweile ist FDDI auch von der IEEE als 802.8 Spezifikation standardisiert und kann auch mit Kupferkabel betrieben werden.

Das typische Einsatzgebiet des FDDI ist der Backbone. Über den FDDI-Ring werden Standard-LANs wie Ethernet oder Token Ring mit Hilfe von Brücken miteinander verbunden. Damit steht FDDI in Konkurrenz zu ATM und Gigabit Ethernet.

FDDI bietet folgende Vorteile:

- ✔ Überbrückung sehr großer Entfernungen
- ✔ Anschluss vieler Stationen
- ✔ Hohe Übertragungsraten, realisiert bis 100 Mbit/s

Übertragungsverfahren im FDDI

FDDI beschreibt ein modifiziertes Token-Ring-Verfahren und ist für 100 Kilometer Netzausdehnung und 100 Mbit/s Übertragungsrate ausgelegt. Bei einem maximalen Abstand von zwei Kilometern können bis zu 500 Stationen angeschlossen werden.

Der wesentliche Unterschied zu Token Ring besteht darin, dass die Sendezeit dynamisch vergeben wird, d.h. je nach Bedarf kann eine Station den Ring für eine längere oder aber auch kürzere Zeit belegen, Timed Token Rotation. Damit wird der wesentlich höheren Übertragungsrate Rechnung getragen. In einem FDDI-Ring können im Unterschied zum Token-Ring-Protokoll mehrere Datenrahmen kreisen. Dies ist möglich, weil der Sender einen neuen Token schon generieren kann, bevor er den von ihm gesendeten Datenrahmen wieder erhält, Early Token Release. Der Sender generiert einen neuen freien Token, nachdem das letzte Bit des Datenrahmens abgesetzt ist.

Damit können in einem FDDI-Netz mehrere Datenrahmen kreisen, aber immer nur ein freier Token.

FDDI sieht je nach Funktionalität unterschiedliche Arten von Stationen vor.

DAS-Stationen, Dual Attachment Station, werden direkt miteinander in beiden Ringen verbunden. Dazu verfügen diese Stationen über zwei Eingänge, die als Ein-/Ausgang für den primären und den sekundären Ring dienen. DAS-Stationen werden auch als A-Stationen bezeichnet.

SAS-Stationen, Single Attachment Station, dagegen werden über Konzentratoren an den Doppelring angeschlossen.

SAS-Stationen werden auch als B-Stationen bezeichnet. An einen Konzentrator können mehrere B-Stationen angeschlossen werden. Der Konzentrator »schaltet« die Datenströme der angeschlossenen Stationen an den FDDI-Ring durch. Aus der Sicht des Ringes verhält sich ein Konzentrator wie eine A-Station.

FDDI als physikalischer Doppelring

FDDI ist als Doppelring konzipiert. Damit wird eine hohe Übertragungssicherheit gewährleistet. Der zweite Ring, Sekundärring, wird bei Ausfall des ersten Rings, Primärring, mitgenutzt.

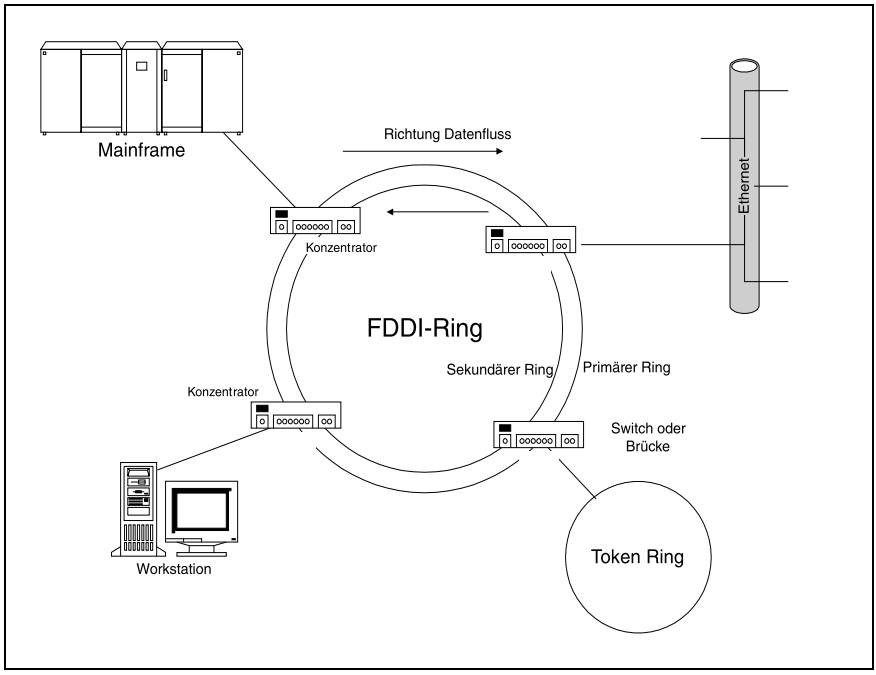


Abbildung 2.20: FDDI als Backbone Ring

Der eigentliche Vorteil des Doppelrings besteht jedoch darin, dass im Falle eines Kabelbruchs die unmittelbar dieser Bruchstelle benachbarten Stationen bzw. Konzentratoren in der Lage sind, beide Ringe zu einem Ring zusammenzuschalten.

Abbildung 2.21 verdeutlicht das Prinzip. Eine Bypass-Switch genannte Einheit in der A-Station unterbricht im Störungsfall die beiden Ringleitungen. Dazu werden die beiden Ringe in der Station miteinander verbunden. Als Ergebnis entsteht ein neuer, einfacher Ring, der die Bruchstelle nicht mehr tangiert.

Server und zentrale Dienste sollten immer an Class-A-Verbindungen geschaltet werden, Workstation-Cluster mit höherer Fehlertoleranz, die keine Netzwerkdienste bereitstellen, können auch als Class B installiert werden.

Da der FDDI-Ring im Vergleich zum Token Ring recht groß ist und die Latenz pro Station minimal fünf Bit beträgt, ist es möglich, mehrere Token in dem Ring zu haben, so dass mehrere Paketrahmen gleichzeitig im Ring unterwegs sein können.

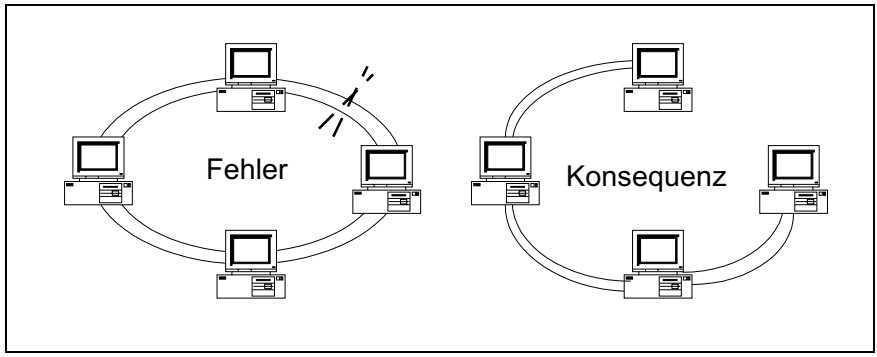


Abbildung 2.21: Zusammenschalten von FDDI Doppelringen zu einem Ring

Die Paketgröße eines FDDI-Paketes beträgt zwischen 17 Byte und 4495 Byte.

Der Einsatz von FDDI rechnet sich unter folgenden Bedingungen:

- ✔ Aufbau großer Backbone Netze
- ✔ Überbrückung großer Strecken
- ✔ Übertragung großer Datenmengen

2.7 ATM-Technologie

ATM – Asynchronous Transfer Mode ist die ultimative Vermittlungstechnik und wurde ursprünglich als die Basis des zukünftigen Breitband-ISDN entwickelt. Es handelt sich also zunächst um eine Vermittlungstechnik in öffentlichen Weitverkehrsnetzen.

Die Standardisierung von ATM ist zurzeit in vollem Gang und wird durch ITU-T für ATM im WAN und das ATM-Forum für ATM im LAN vorangetrieben.

Die wesentlichen Merkmale von ATM sind:

- ✔ Glasfaser für weite Strecken als Übertragungsmedium
- ✔ Übertragungsraten bis zu 9,9 Gbps
- ✔ Übertragung in so genannte Zellen. Das sind kleine Datenblöcke mit fester Länge von 53 Byte, davon 5 Byte Zellkopf und 48 Byte Nutzdaten, Payload.
- ✔ Keine Fehlerkontrolle zwischen den Netzknoten
- ✔ Asynchrones Zeitmultiplexing
- ✔ Virtuelle Verbindungen

Das Zellformat ist ein Kompromiss an die Vielseitigkeit. Für eine optimale Datenübertragung sind die Pakete zu klein und für die Sprachübertragung sind die Pakete eigentlich zu groß.

Das Konzept der Virtuellen Verbindung arbeitet mit so genannten Kanälen, wobei die Beschreibung der Kanäle im ATM-Zellkopf über die Adressen **VPI**, Virtual Path Identifier und **VCI** Virtual Channel Identifier, erfolgt. Der VCI ist eine 16 Bit lange Adresse, die jeweils einen Verbindungsabschnitt, den virtuellen Kanal, in einem ATM-Netz kennzeichnet. Anhand des VCI routet der ATM-Switch zum Empfänger. Dieser VCI ist nur für die erste Teilstrecke der Verbindung gültig. Der Switch benutzt auf der nächsten Teilstrecke einen anderen VCI, der mit dem Empfänger oder nächsten ATM-Switch beim Aufbau der virtuellen Verbindung ausgehandelt wurde.

Der VPI besteht aus mehreren virtuellen Kanälen. Eine Verbindung wird durch VCI und VPI eindeutig beschrieben.

2.7.1 Quality of Services

Ein großer Vorteil der ATM-Technik liegt darin, dass die Bitraten am Anschluss flexibel gehalten werden können. Damit ist diese Technik für die Integration unterschiedlicher Dienste mit je spezifischen Übertragungsraten sehr geeignet.

Der entscheidende Vorteil ist aber, dass ATM die Möglichkeit bietet, verschiedene Übertragungsqualitäten, **QoS** Quality of Services, für die gesamte Dauer einer Verbindung zu garantieren. Beispiele hierfür sind:

- ✔ **CBS** Constant Bitrate für Sprachübertragung
- ✔ **VBR** Variable Bitrate für komprimierte Videos
- ✔ **High Speed Data**

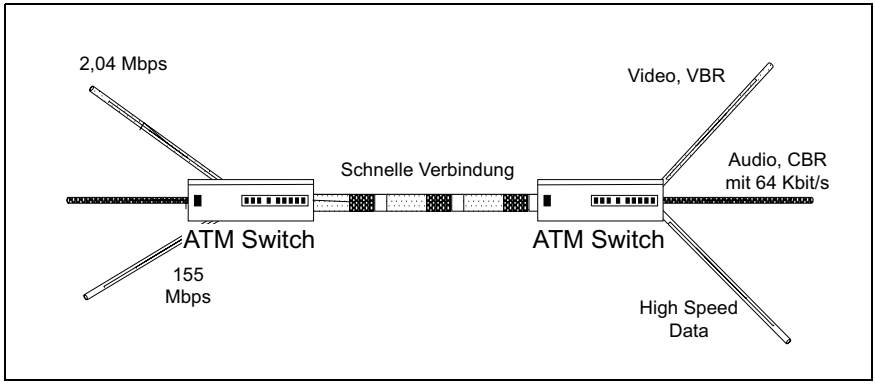


Abbildung 2.22: ATM Multiplexing

Die an einem ATM-Switch mit unterschiedlicher Geschwindigkeit und Qualitätsmerkmalen ankommenden Datenströme können auf eine schnelle Leitung zum nächsten Switch gemultiplext werden. Damit ist eine wichtige Vorgabe für Multimedia-Anwendungen erfüllt, nämlich die gleichzeitige Übertragung von Daten, Sprache und Video.

2.7.2 ATM im LAN

Die aktuelle Entwicklung zeigt, dass ATM zunehmend auch Einzug in den LAN-Bereich hält und hier als Alternative zu FDDI und Fast- bzw. Gigabit-Ethernet eine immer wichtigere Rolle spielt. Beispiel hierfür sind von IBM angekündigte Migrationswerkzeuge zu ATM innerhalb eines SNA-Netzwerkes.

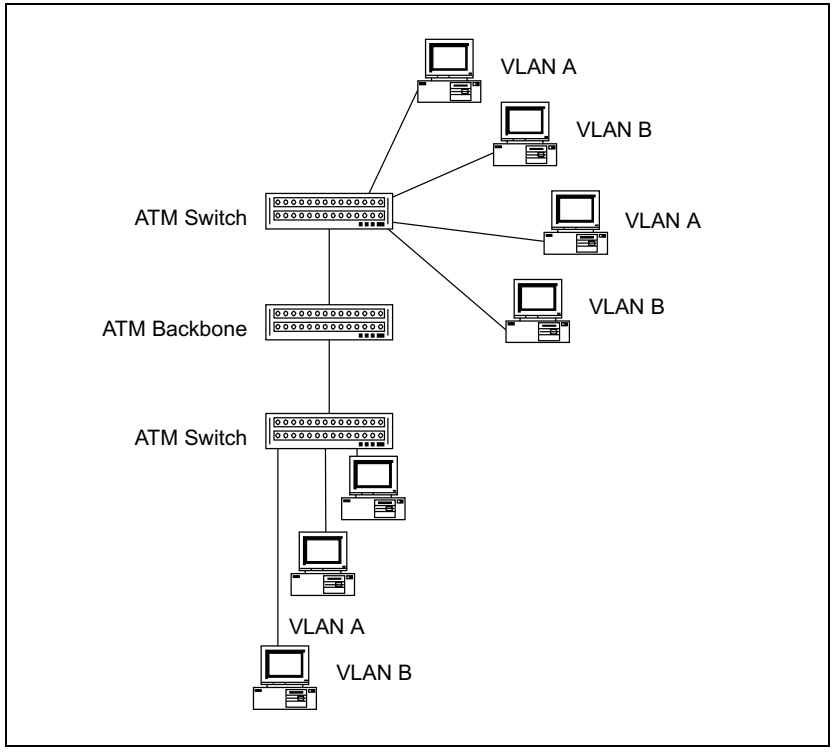


Abbildung 2.23: Virtuelles LAN über ATM-Switches

Beim Einsatz der ATM-Technologie im LAN-Bereich ergibt sich als Problem die Tatsache, dass ATM im Gegensatz zur Soft- und Hardware der »traditionellen« LAN Technologien verbindungsorientiert arbeitet. Punkt-zu-Mehrpunkt-Verbindungen, wie beim Multi- oder Broadcast, sind damit nicht möglich.

Aus dem oben geschilderten Grund wird der verbindungslose Dienst emuliert. Das entsprechende Protokoll wird vom ATM-Forum standardisiert und heißt LANE, ATM/LAN Emulation.

Für eine LAN Emulation muss ein LAN Emulation Server sowie ein Broadcast and Unknown Server zur Verfügung stehen. Der Broadcast and Unknown Server leitet Broadcast-Nachrichten über eine Multicast-Verbindung an alle LAN Emulation Clients weiter. Als weiteren Serverdienst benötigen Sie den LAN Emulation Configuration Server, der die Stationszuordnung für alle emulierten LANs verwaltet.

Der Nachteil von LANE ist, dass damit das typische Merkmal der QoS verloren geht.

LANE ist zur Zeit nur in der Lage, Ethernet und Token Ring zu emulieren. Die angeschlossenen Stationen werden dabei zu einer Multicast/Broadcast Domäne verbunden. Ab einer gewissen Netzgröße, mehr als 200 Stationen, werden mehrere Domains gebildet, die dann als **VLAN**, virtuelles LAN, bezeichnet werden. In einem VLAN werden Endgeräte eines physikalischen Netzwerkes über die Portnummern am Switch zu logischen, eben virtuellen, LANs zusammengeschaltet.

2.7.3 ATM und IP

Die Integration von IP in die ATM-Technologie ist ein aktueller Schwerpunkt der heutigen Entwicklungsarbeit. Ziel ist es, die Geschwindigkeitsvorteile der ATM-Technologie für Internet/Intranetanwendungen zu nutzen. Zwei Protokolle kommen hier zum Einsatz:

CLIP Classical IP over ATM

MBOA Multi-Protocol over ATM

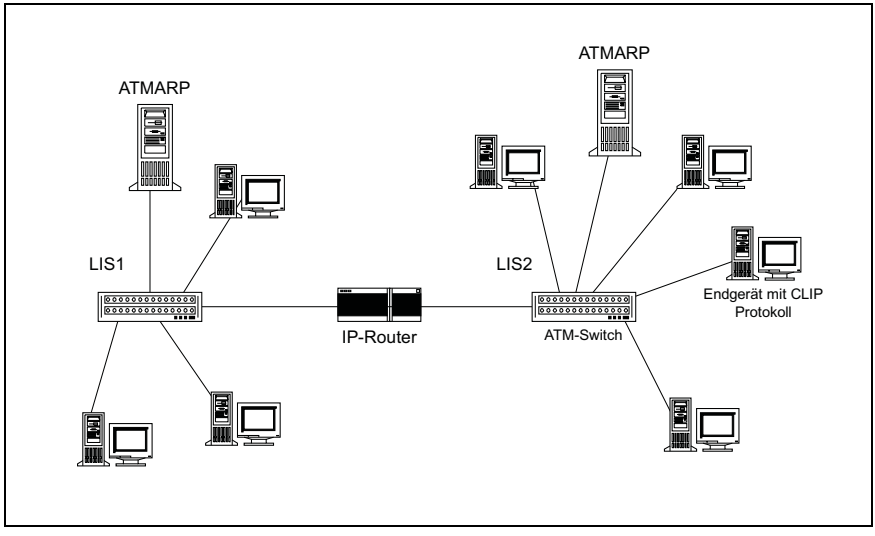


Abbildung 2.24: Classical IP over ATM

CLIP ermöglicht den Aufbau eines Netzwerkes, das mehrere IP-Rechner über ATM-Netzwerkkarten miteinander verbindet. Dazu werden zentrale Server, ATMARP-Server, installiert, die die IP-Adressen in ATM-Adressen umwandeln und umgekehrt. Mit Hilfe dieser Adressumwandlung werden die IP-Paket in ATM-Zellen gekapselt und über ATM zum Endgerät transportiert.

CLIP kann logische Subnetze bilden, die dann über IP-Router miteinander verbunden sind.

Vorteile von CLIP sind:

- ✔ ATM wird zum einfachen und schnellen Transportsystem
- ✔ Keine Änderung der Protokollstruktur in den Endgeräten

Allerdings können die Router zwischen den Teilnetzen zum Flaschenhals werden und das Merkmal der QoS geht verloren.

MPOA ist eine Weiterentwicklung der LAN-Emulation, die im Zusammenhang mit dem Resource Reservation Protocol des IP Version 6 ATM-Dienstequalität bei voller IP-Integration liefert.

2.7.4 AAL

Die Anpassung konventioneller Protokolle erfolgt in einer übergeordneten Teilschicht, dem ATM Adaption Layer AAL. Dies sorgt für Segmentierung und Wiederzusammensetzung der Datenpakete in Zellen. Mehrere Klassen sind definiert:

- ✔ AAL 1: isochron, konstante Bitrate, verbindungsorientiert, z.B. Sprache, Video
- ✔ AAL 2: variable Bitrate, realzeitfähig
- ✔ AAL 3/4: nicht isochron, variable Bitrate, verbindungslos, benutzt für SMDS und Datenverkehr
- ✔ AAL 5: vereinfachte Variante der AAL 3/4, benutzt für IP-Verkehr und andere LAN-Emulationen

KAPITEL 3

3 Internetworking

Die Entwicklung auf dem Gebiet der lokalen Netzwerke hat dazu geführt, dass die in der Vergangenheit entstandenen Insellösungen auf Abteilungsebene den Ansprüchen nicht mehr genügen. Entweder können keine weiteren Stationen angeschlossen werden, oder aber die Arbeitsorganisation erfordert den Austausch von Daten über die Abteilungsgrenzen hinweg.

Eine weitere Ursache ist die ständig wachsende Zahl von PCs in den Unternehmen, die in die bestehende Netzinfrastruktur integriert werden müssen. Diese besteht aus lokalen Netzen mit unterschiedlichen Topologien und aus Mainframe-Architekturen wie z.B. IBMs SNA und Digitals DECNet. Dadurch entsteht der Zwang zur Verbindung von LAN-Segmenten und der Integration von PCs in bestehende Architekturen.

Der Netzadministrator hat es je nach Netzwerkgröße mit einer Vielzahl der in diesem Kapitel beschriebenen Komponenten zu tun, die eine heterogene Struktur bilden. Netzsegmente sind unterschiedlich schnell, befinden sich an entfernten Standorten oder verwenden verschiedene Protokolle.

In dieser Situation sind mehrere Szenarien denkbar:

- ✔ Netzwerke müssen segmentiert werden, weil die Gesamtlast zu groß wird – **Switching – Bridging – Routing**
- ✔ Gleiche Netze, d.h. gleiche Geschwindigkeit und gleiches Protokoll, müssen miteinander verbunden werden – **Switching**.
- ✔ Netze mit verschiedenen Rahmenformaten müssen miteinander verbunden werden – **Translation Switching oder Routing**.
- ✔ Netze mit unterschiedlichen Protokollen auf der OSI-Schicht 3, d.h. unterschiedlicher Adressierung, müssen miteinander verbunden werden – **Routing**.
- ✔ Netze müssen über analoge und/oder digitale öffentliche Netze, Fernsprechnetz, ISDN, Datex-P, Frame Relay oder ATM miteinander verbunden werden – **Routing**.
- ✔ Lokale Netze müssen in Mainframe-Architekturen eingebunden werden – **Gateway**.

3.1 Netzwerkverbindungen im OSI-Modell

Das klassische OSI-Modell beschreibt folgende Komponenten für die Verbindung von Netzwerken.

- ✔ Verstärker oder Repeater
- ✔ Brücke oder Bridge
- ✔ Router oder Vermittlungsrechner oder Layer 3 Switch
- ✔ Gateways

Repeater verbinden Netze, die auf der Ebene der Bitübertragungsschicht gleich sind.

Brücken verbinden Netze auf der Sicherungsschicht. **Router** arbeiten auf der Vermittlungsschicht.

Gateways verbinden unterschiedliche Netzwerkarchitekturen über die OSI-Schicht 7.

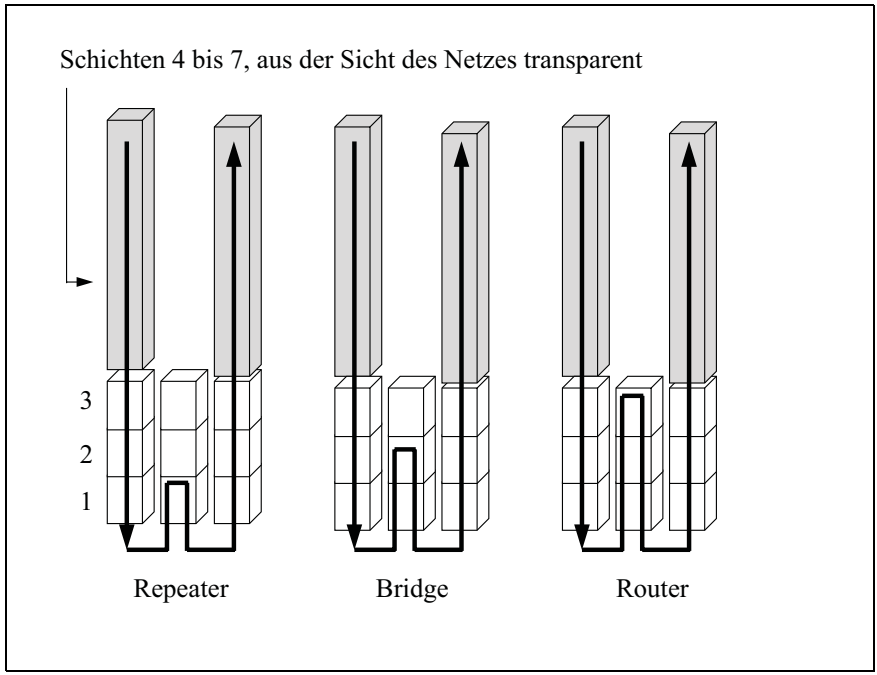


Abbildung 3.1: Internetworking in den Netzwerkschichten des OSI-Modell

3.2 Repeater

Repeater sind Verstärker, die auf der Schicht 1 des OSI-Modells arbeiten. Aufgrund der passiven Anschaltung der Arbeitsstationen an einen Ethernet-Bus ist die Segmentlänge durch die Dämpfung des Kabels beschränkt, d.h. die Signale werden auf dem Bus immer schwächer. Der Repeater verstärkt das Signal und verlängert damit das Gesamtsystem, das nun aus verschiedenen Segmenten besteht und damit den Anschluss von mehr Arbeitsstationen ermöglicht.

Der Repeater verstärkt also auf der Bitübertragungsschicht die Daten. Software ist nicht notwendig.

Verbindet ein Repeater mehrere Segmente miteinander, dann wird er auch als Multiport-Repeater bezeichnet. Bei der sternförmigen Verkabelung von LANs werden diese Multiport-Repeater auch Sternkoppler genannt. In einem Netz mit Ethernet heißen die Repeater dann Hub.

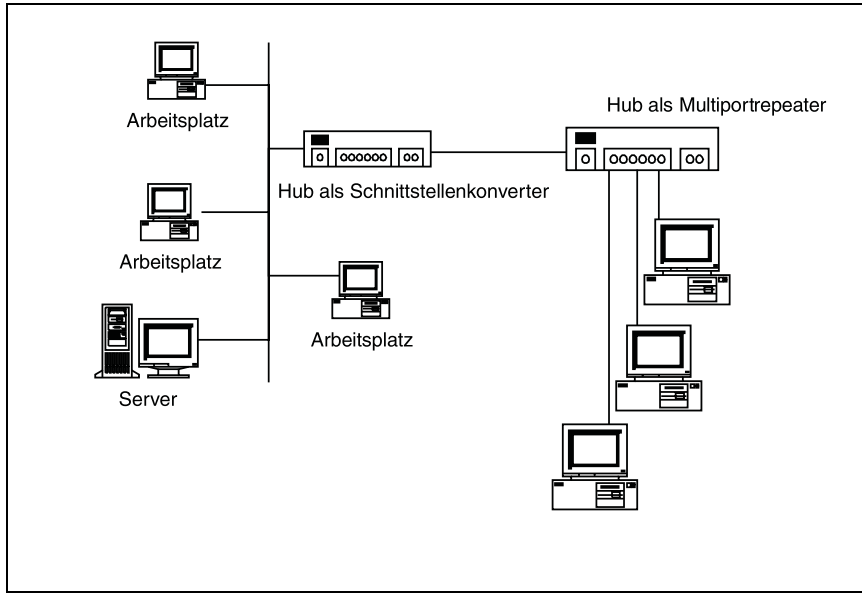


Abbildung 3.2: Repeater

Repeater sind in der Lage als Schnittstellenkonverter Segmente zu verbinden, die mit unterschiedlichen Kabeltypen arbeiten. So können z.B. Ethernetsegmente, die wie im obigen Beispiel unterschiedliche Kabeltypen verwenden, über einen Repeater zusammengeschaltet werden.

Repeater, die in einem Fast-Ethernet-Netz als Schnittstellenkonverter fungieren, werden auch Class I Repeater genannt. Entsprechend steht Class II für Repeater, die nur Segmente mit gleichem Kabeltyp verbinden können.

Die an einen Class I Repeater angeschlossenen Segmente arbeiten mit unterschiedlichen Kabeltypen und mit verschiedenen Kodierungsmethoden. Deshalb muss der Repeater eine Umsetzung des Datenformats vornehmen, was zu Zeitverzögerungen führt. Diese sind die Ursache dafür, dass nur ein Class I Repeater zwischen zwei Endknoten mit maximaler Entfernung liegen darf.

Repeater verbinden also verschiedene Netzwerksegmente zu einem Netzwerk. Alle Stationen eines repeateten Netzwerkes gehören zu einer Collision-Domäne bzw. Token-Domäne.

Generell kann man zwischen duplexfähigen und nichtduplexfähigen Repeatern unterscheiden. Der wesentliche Unterschied zwischen beiden Technologien liegt darin, dass nichtduplexfähige Repeater oder **Halb-Duplex-Repeater** Kollisionen erzeugen, wenn auf den Ports simultane Zugriffsversuche erkannt werden. Die Stationen sind damit gezwungen, das Senden der Daten zu wiederholen.

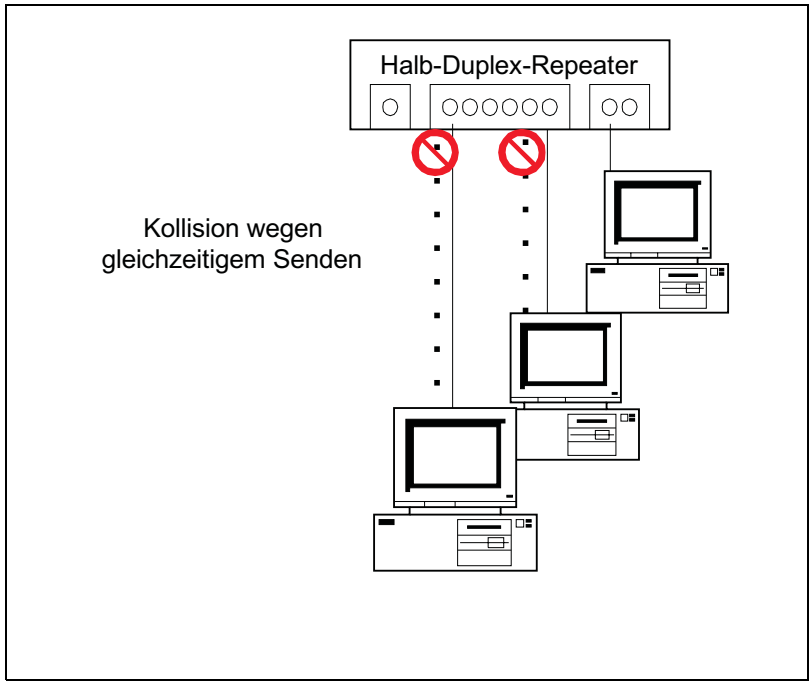


Abbildung 3.3: Halb-Duplex Repeater

Dieses »Verhalten« ist für Hochgeschwindigkeitsnetze, z.B. Gigabit-Ethernet, extrem leistungsmindernd. Aus diesem Grund gibt es für Ethernets nach 802.3x Standard **Full-Duplex**- oder **Buffered Repeater**. Diese arbeiten kollisionsfrei, und es gibt deshalb auch keine Einschränkungen bezüglich der Länge eines Netzes.

Full-Duplex-Repeater sind in der Lage über ein Segment Daten gleichzeitig zu empfangen und zu senden. Durch die in der 802.3x-Norm beschriebene Flusskontrolle mittels MAC Control Frames kann der Repeater an jedem Port das angeschlossene Segment steuern.

Jeder Port kann mindestens einen Frame maximaler Länge puffern, deshalb Buffered Repeater, so dass simultan eingehende Pakete zeitverzögert weitergeleitet werden können.

Gleichzeitig kann der Repeater einen Sender stoppen, ohne dazu eine Kollision erzeugen zu müssen, die alle Stationen in der Collision Domain »lahmlegen« würde.

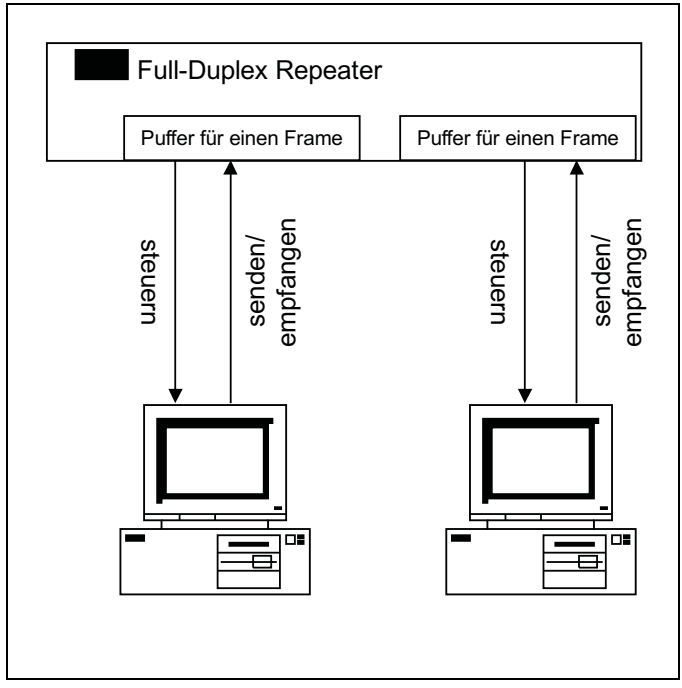


Abbildung 3.4: Full-Duplex Repeater

Netze auf der Basis von Full-Duplex Repeatern arbeiten kollisionsfrei. Damit können Netze aufgebaut werden, deren Ausdehnung nur durch die maximale Reichweite der einzelnen Verbindungen begrenzt wird. Und diese ist wiederum vom verwendeten Medium abhängig und nicht mehr von der Laufzeit eines Signals.

Eine Alternative zum Buffered Repeater sind Switches. Diese bieten mehr Leistung bei vergleichbaren Kosten.

3.3 Brücken

Brücken verbinden Netze auf der Schicht 2 und werden üblicherweise zur Laststeuerung eingesetzt. Brücken segmentieren Collision Domains. Dadurch kann das Gesamtnetzwerk entlastet werden. Je nach Anwendung werden Brücken in verschiedene Kategorien eingeteilt.

3.3.1 Translation Bridge

Die folgende Abbildung zeigt den Einsatz einer Translation Bridge. Diese verbindet LANs mit unterschiedlichen LAN-Protokollen. Wichtiges Kriterium ist hierbei die maximale Framegröße, **MTU** Maximum Transmission Unit, die auf die kleinste Paketgröße im Gesamtnetz beschränkt werden muss. Die Brücke ist nämlich nicht in der Lage, Pakete zu fragmentieren.

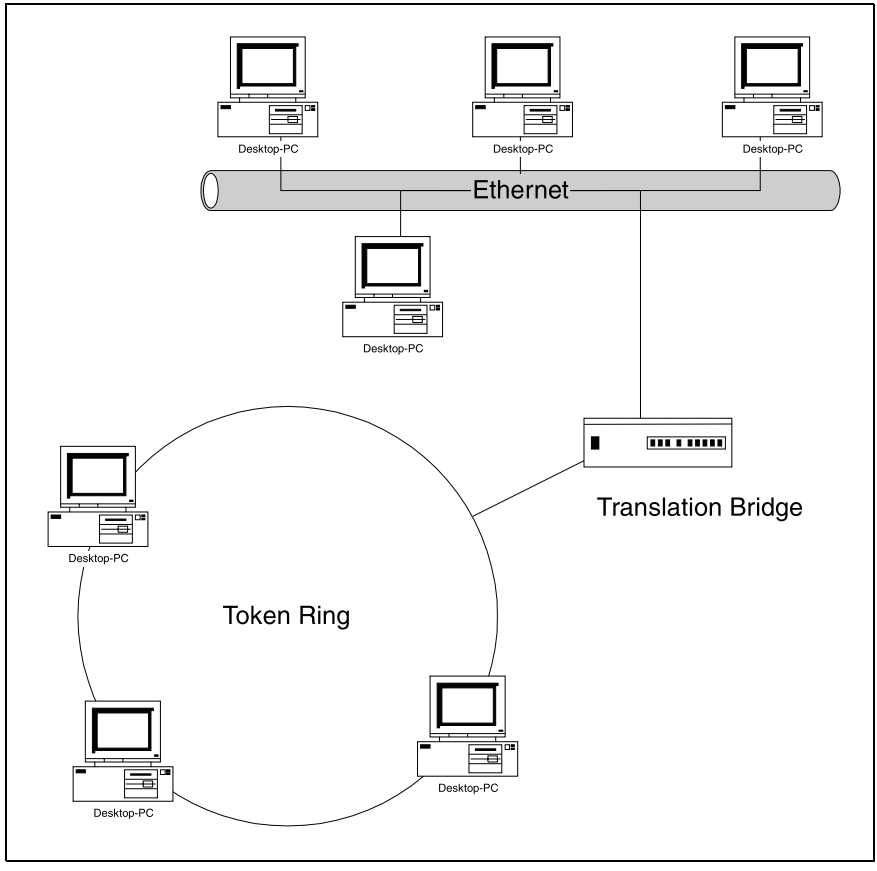


Abbildung 3.5: Brücke zwischen Ethernet und Token Ring

Funktionsweise von Translation Bridges

Eine der wichtigsten Funktionen der Brücke besteht darin, Rahmen umzusetzen. Dazu müssen die protokollspezifischen Informationen der miteinander verbundenen Segmente von der Brücke umgesetzt werden.

Die Translation Bridge wird im gezeigten Beispiel alle ethernetspezifischen Steuerinformationen von IEEE 802.3 entfernen und statt dessen die nach IEEE 802.5 hinzufügen. Dazu wird das Datenpaket bis auf die LLC-Schicht ausgepackt und dann wieder zusammengesetzt. Aus dem Ethernet-Paket wird ein Token Ring Paket.

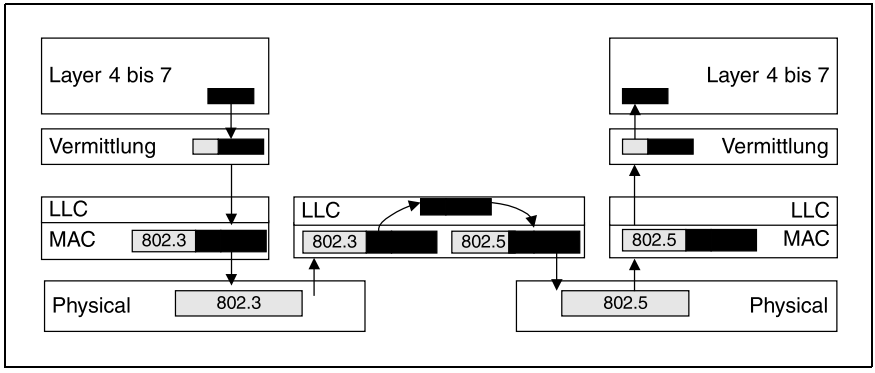


Abbildung 3.6: Funktionsweise einer Translation Bridge

Translation Bridges zwischen Ethernet auf der einen und Token Ring sowie FDDI auf der anderen Seite, müssen zwei technische Probleme lösen, nämlich

- ✔ unterschiedliche Framegrößen
- ✔ kanonische und nichtkanonische Adressierung

Unterschiedliche Framegrößen

Token Ring und FDDI Frames sind mit 4096 bzw. 4500 Byte größer als Ethernet-Frames mit 1518 Byte. Dies hat zur Folge, dass in einem FDDI-Ring nur 1518 Byte große Pakete verwendet werden können, wenn dieser über eine Brücke mit einem Ethernet-Segment verbunden ist.

Eine Fragmentierung der größeren Ringpakete kann höchstens durch ein höheres Protokoll erfolgen, wie z.B. durch IP. Bedingung ist aber, dass die Translation Bridge die IP-Fragmentierung unterstützt.

Umsetzung der Adressformate

Ethernet überträgt das niederwertigste Bit eines jeden Adressbytes als erstes. Dies wird als kanonisches Format oder kanonische Adresse bezeichnet. Token Ring und FDDI machen genau das Gegenteil, übertragen also zuerst das höchstwertige Bit, nichtkanonisches Format oder nichtkanonische Adresse.

Deshalb muss eine Translation Bridge jedesmal Adressen umsetzen, wenn ein Datenpaket zwischen den unterschiedlichen Topologien ausgetauscht wird.

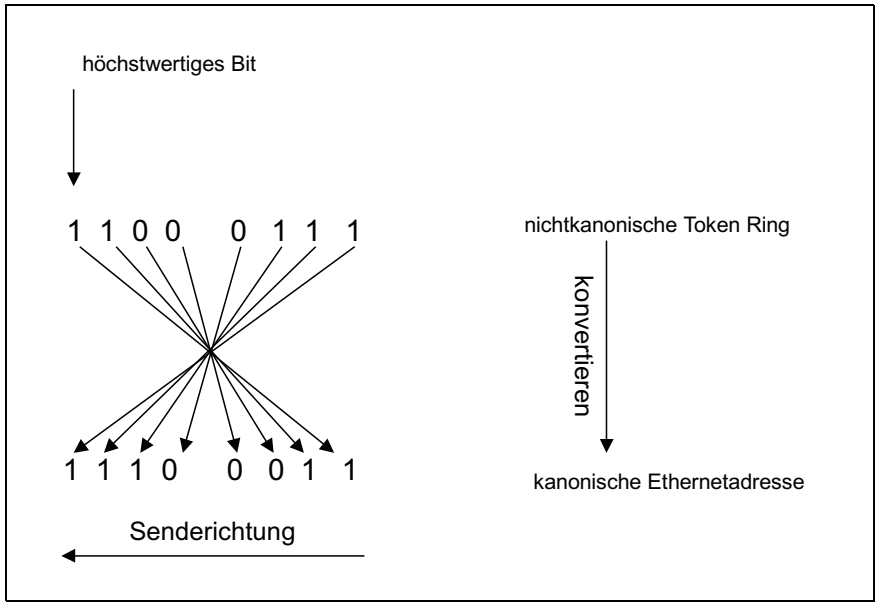


Abbildung 3.7: Konvertierung von Adressformaten am Beispiel von Ethernet und Token Ring

Die Konsequenzen sind, je nach Leistungsfähigkeit der Brücke, hohe Latenzzeiten.

3.3.2 Brücken zum Backbone, Encapsulation Bridges

Abbildung 3.8 zeigt, dass mit Hilfe von Brücken lokale Netzwerke bzw. Netzwerkarchitekturen, z.B. SNA von IBM, über ein Backbone miteinander verbunden werden können. In unserem Beispiel besitzen die Brücken eine FDDI-Karte und eine zum jeweiligen LAN passende Ethernetkarte.

Aus der Sicht der beteiligten Netze ist das Backbone transparent. Die jeweiligen User müssen also nicht wissen, dass es überhaupt ein Backbone gibt.

Das gezeigte Beispiel verweist auf ein weiteres wichtiges Leistungsmerkmal von Brücken, nämlich die Anpassung an unterschiedliche Übertragungsgeschwindigkeiten oder Bandbreiten. Die abgebildeten Brücken müssen in der Lage sein, die 10 Mbit/s des Ethernetsegmentes an die 100 Mbit/s des FDDI anzupassen.

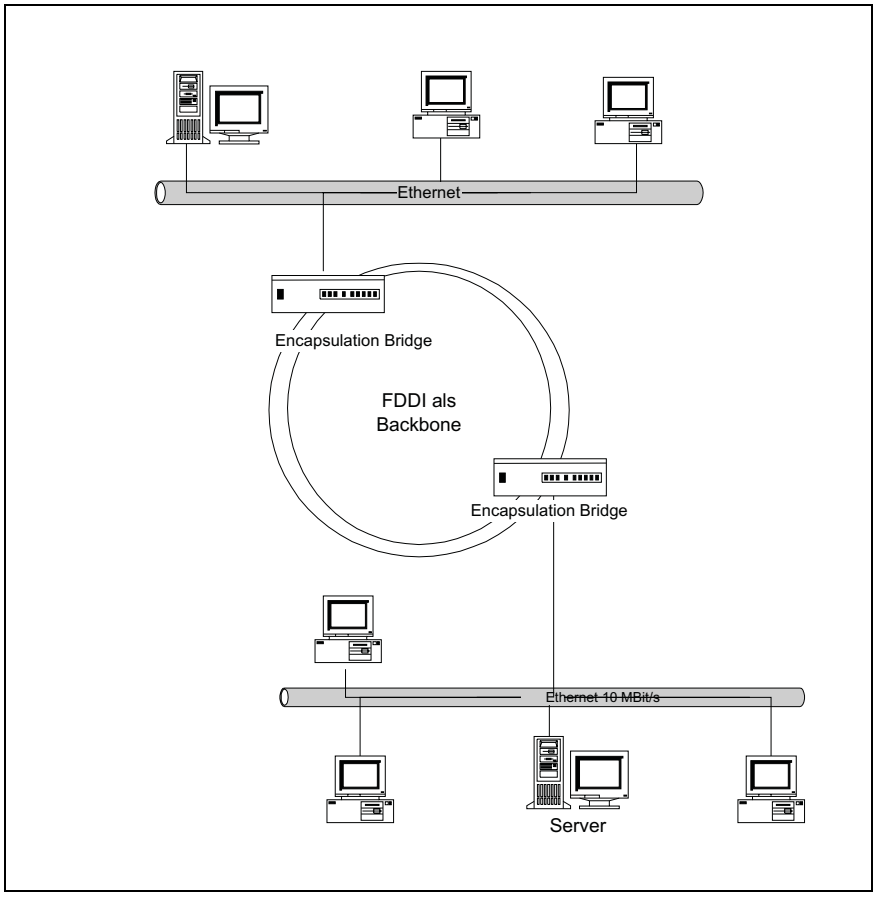


Abbildung 3.8: Encapsulation Bridging

Die Encapsulation Bridge packt das gesamte Ethernet-Paket in das Datenfeld des FDDI-Rahmens. Der Rahmen wird über FDDI dann an die zugehörige FDDI-Adresse transportiert. Hier wird das Ethernet-Paket ausgepackt und dann über Ethernet weitergeleitet.

Damit ist eine Kommunikation zwischen am FDDI angeschlossenen Stationen und Ethernet-Stationen nicht möglich. Der Backbone ist aus der Sicht des Ethernets eine transparente Übertragungsstrecke.

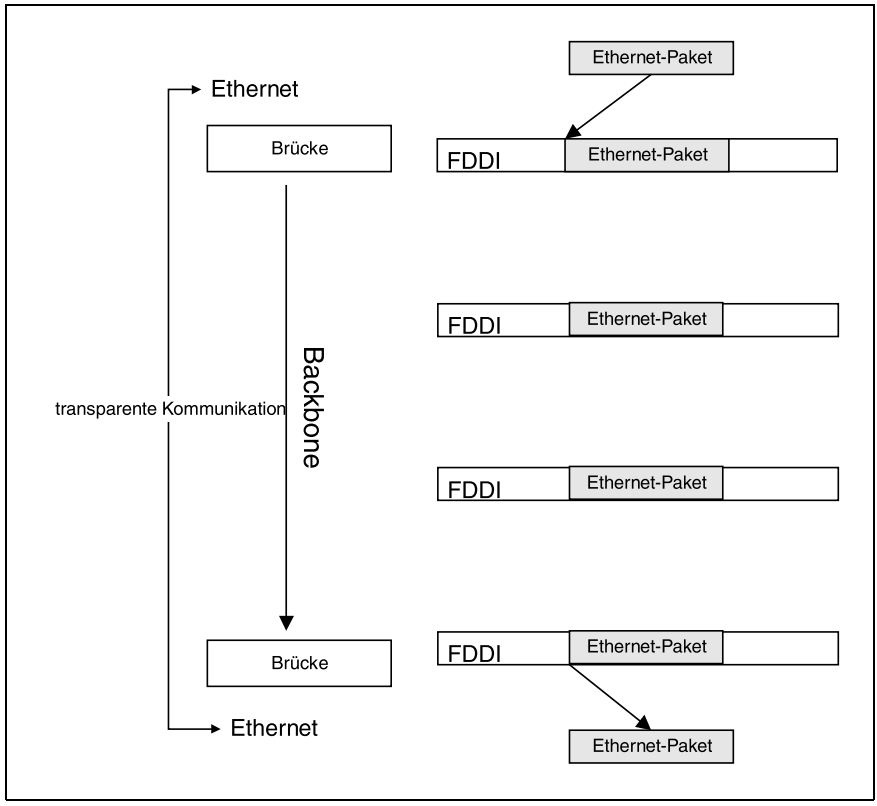


Abbildung 3.9: Encapsulation Bridging am Beispiel von Ethernet und FDDI

3.3.3 Segmentierung mit Hilfe von Brücken

Bisher wurde hervorgehoben, dass Brücken die Fähigkeit besitzen, unterschiedliche Topologien miteinander zu verbinden. Die Hauptaufgabe von Brücken und Switches besteht darin, überlastete LANs durch Segmentierung schneller zu machen.

Dazu wird die Brücke zwischen zwei Segmente geschaltet. Der entlastende Effekt besteht nun darin, dass nicht mehr jedes Datenpaket das Gesamtnetz durchläuft und damit auch belastet. Die Brücke ist vielmehr in der Lage durch einen so genannten Lernmodus zu erkennen, ob der Adressat eines Paketes im anderen Segment liegt. Wenn nicht, wird das Paket nicht weitergeleitet und belastet damit nur das Teilsegment, in dem sich auch der Zielrechner befindet.

Die Brücke unterteilt damit das LAN in so genannte Collision Domains. Berücksichtigt man, dass schon bei 30 Prozent Auslastung die Leistung von Ethernet-Netzen wegen verstärkt auftretender Kollisionen dramatisch abnehmen kann, dann wird der Entlastungseffekt durch die Brücken besonders deutlich.

Die folgende Grafik zeigt das Prinzip, nach dem eine Brücke »lernt«, welche Stationen sich in welchem Segment befinden. Die hier vorgestellte Technik wird auch als transparente Brücke bezeichnet.

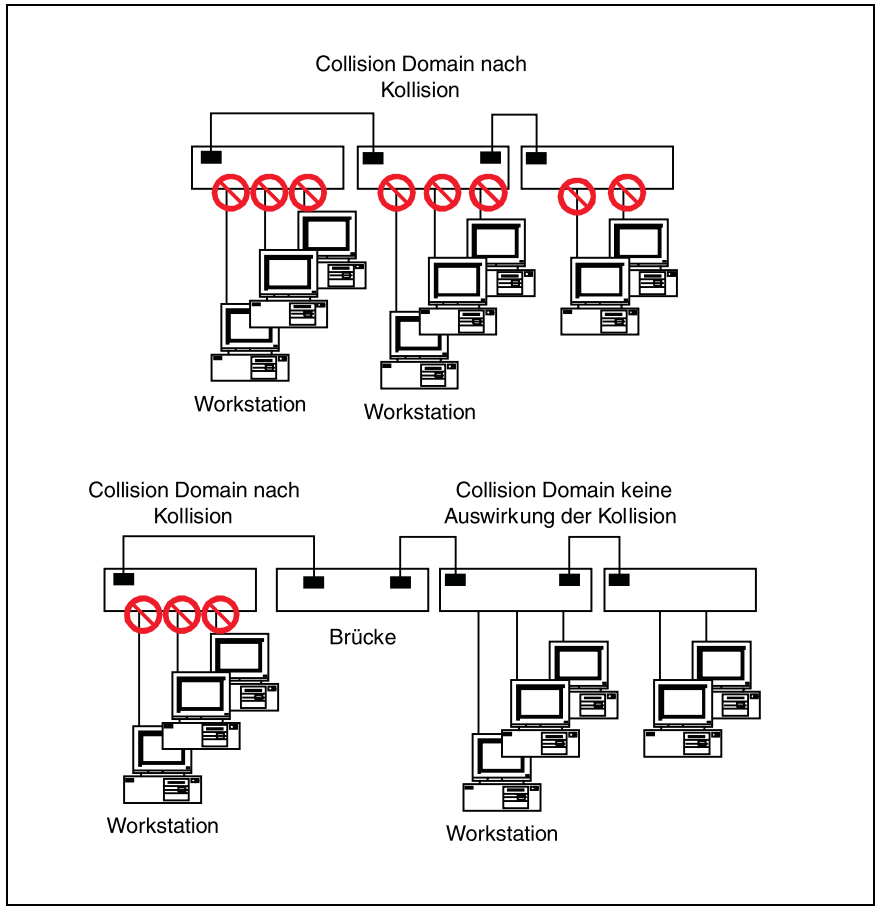


Abbildung 3.10: Segmentierung mit Hilfe von Brücken

Wenn eine transparente Brücke in Betrieb geht, dann kommt der Flutalgorithmus zum Tragen. Dieser bewirkt, dass ankommende Pakete in jedem Fall an alle LAN-Teilsegemente durchgereicht werden.

Anhand von Sender- und Zieladressen lernt die Brücke in der Folgezeit, welche Adressen sich in welchen Segmenten befinden. Diese werden dann in so genannten Hash-Tabellen den einzelnen Ports zugeordnet. In periodischen Abständen von ca. zehn Minuten werden die Hash-Tabellen aktualisiert, indem »alte« Adressen gelöscht werden. Die Adressen von Rechnern, die längere Zeit inaktiv sind, verschwinden damit aus den Tabellen.

Der hier beschriebene Lernalgorithmus, Baran's backward learning, lässt sich wie folgt zusammenfassen :

- ✔ Ziel- und Quell-Adresse sind am gleichen Port, dann Rahmen verwerfen
- ✔ Ziel- und Quell-Adresse sind nicht am gleichen Port, dann Rahmen weiterleiten
- ✔ Ziel-Adresse kann keinem Port zugeordnet werden, dann fluten

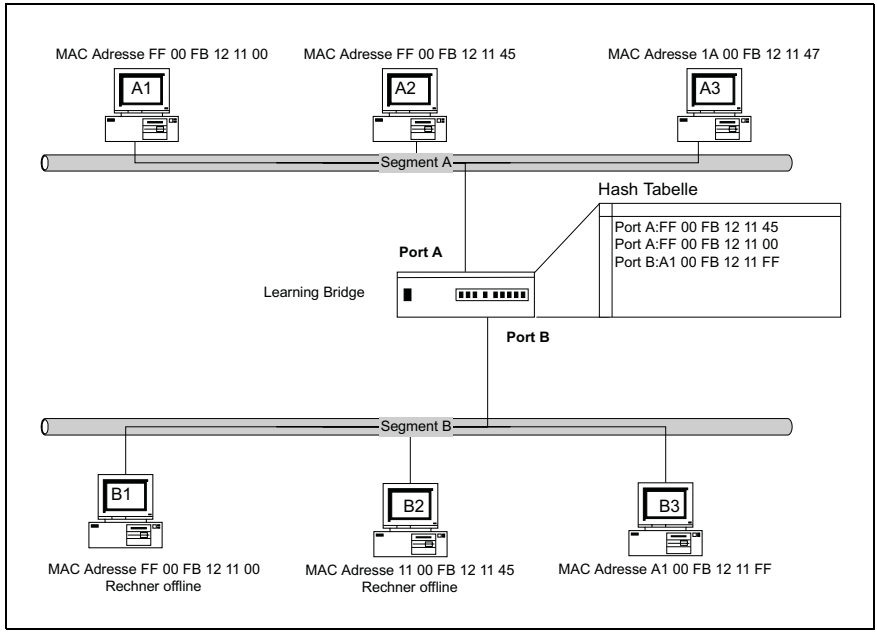


Abbildung 3.11: Lernende Brücke

Die Abbildung 3.11 zeigt an einem Beispiel den oben beschriebenen Algorithmus. In diesem Szenario sind die Adressen der Rechner A1, A2 und B3 in die Hash-Tabelle eingelesen. Der Rechner A3 wurde gerade gestartet und ist noch unbekannt. Daten an diesen Rechner würden »geflutet« werden.

Die Rechner B1 und B2 sind offline, ausgeschaltet oder nicht am Netzwerk. Deshalb ist ihre Adresse und damit auch das Segment, in dem sich die Rechner befinden, unbekannt.

Spanning Tree

Der Spanning-Tree-Algorithmus erlaubt es, redundante Brücken einzusetzen. D.h. zwischen zwei Segmenten werden beispielsweise zwei Brücken eingesetzt, von denen eine aktiv ist und die andere nur zum Einsatz kommt, wenn die aktive Brücke ausfällt. Dadurch werden beim Einsatz von mehr als einer Brücke zwischen zwei Segmenten Schleifen verhindert.

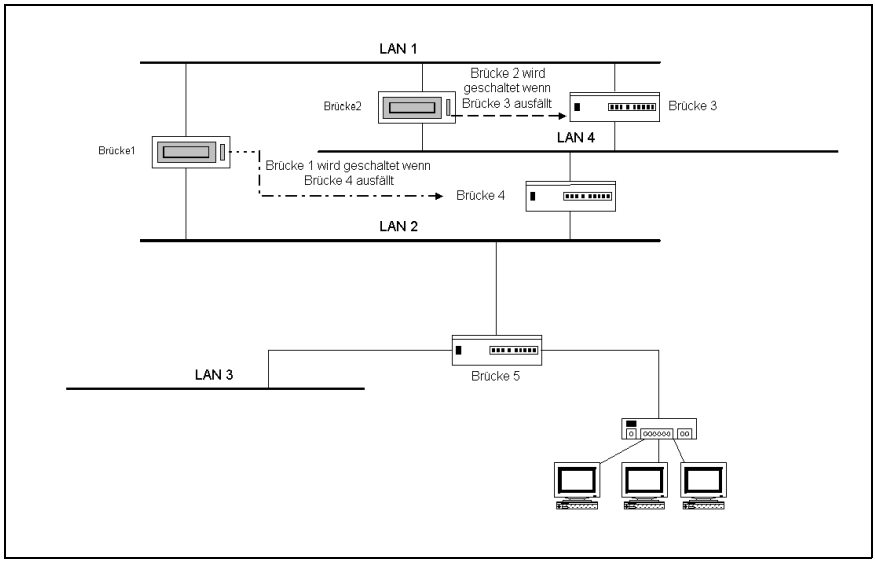


Abbildung 3.12: Spanning Tree

In der oben gezeigten Abbildung bilden die Brücken 1 und 3 Schleifen in den Netzen LAN1, LAN2 und LAN4. Ohne Spanning Tree wäre ein solches Netz nicht funktionsfähig.

Bei Spanning Tree müssen Sie beachten, dass eine Interoperabilität zwischen Geräten unterschiedlicher Hersteller nur bedingt gewährleistet ist.

3.4 Router

Router arbeiten auf der Schicht 3 des OSI-Modells. Hier werden unterschiedliche Protokolle wie IPX, AppleTalk oder IP realisiert.

In den meisten Fällen verbinden Router Netzwerke über Weitverkehrsnetze oder bilden ein internes IP-Netzwerk, das als Transportnetz für ein Intranet fungiert. Router decken dabei sieben Kernfunktionen ab, die im Folgenden beschrieben werden:

- ✔ Segmentierung
- ✔ Adressauflösung
- ✔ Broadcast-Kontrolle
- ✔ Wegewahl
- ✔ Security
- ✔ Layer-3 Special Services
- ✔ WAN-Zugang

Router werden immer dediziert angesprochen. D.h. in einem von Routern kontrollierten Netzwerk werden die Datenpakete direkt an einen Router gesendet, der dann entscheidet, wohin ein Paket weitergeleitet wird, oder ob die Zieladresse sich im eigenen LAN-Segment befindet. Details hierzu werden am Beispiel des IP-Routings in Kapitel 4.6.4 beschrieben.

3.4.1 Subnetting mit Hilfe von Routern

Router können dazu eingesetzt werden, ein großes Inhouse-Netz in Teilnetze, so genannte Subnetze, zu segmentieren. Das Ziel ist, wie beim Einsatz von Brücken, die Entlastung des Gesamtnetzes.

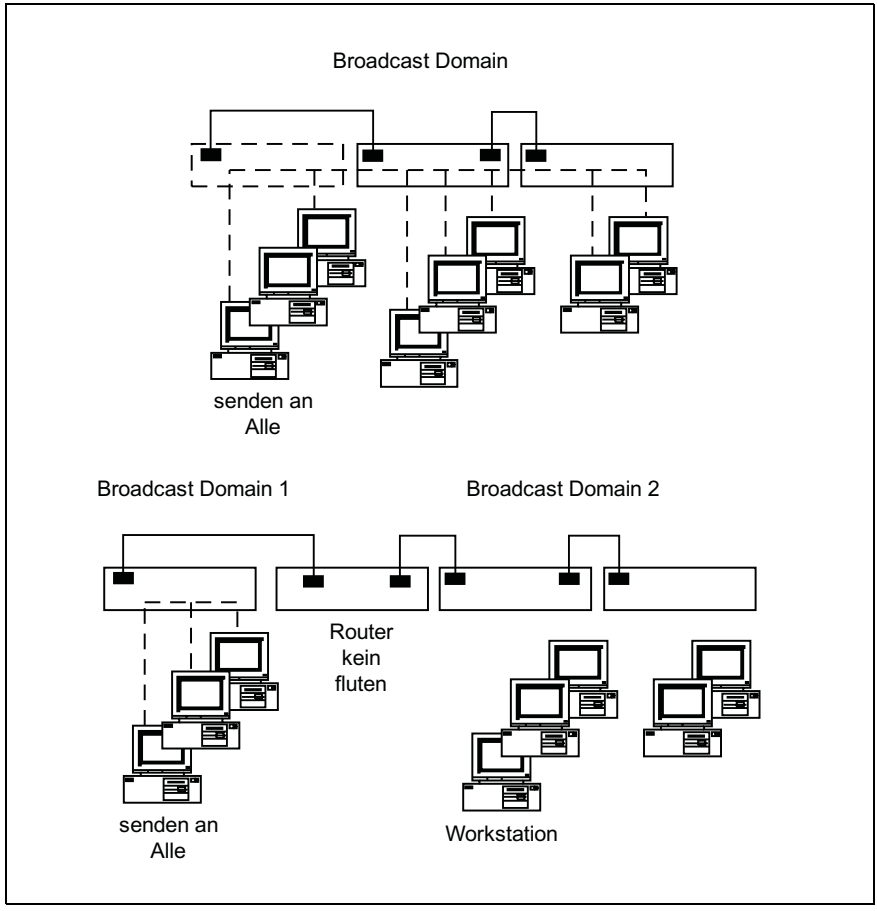


Abbildung 3.13: Segmentierung mit Hilfe von Routern

Der Unterschied zu einer **Segmentierung** durch Brücken besteht darin, dass Router direkt angesprochen werden und Adressen auswerten. Ein Router gibt dabei Datenpakete unmittelbar an einen nächsten Router weiter. Dadurch kann das Zielsegment weit vom Ursprungssegment entfernt liegen.

Brücken entscheiden lediglich, ob Sie ein Paket an ein weiteres direkt angeschlossenes Segment weitergeben oder nicht.

Weil Router im Gegensatz zu Brücken Datenpakete nicht »fluten«, d.h. auf alle angeschlossenen Ports ausgeben, verhindern sie das unkontrollierte Ausbreiten von Broadcasts. Das Ergebnis sind dann so genannte Broadcast-Domänen, die durch die jeweiligen Router begrenzt werden.

3.4.2 Multiprotokoll-Router – MPR

In der Praxis werden Router vor allem auch dazu eingesetzt, LANs mit gleichem Protokoll über Weitverkehrsnetze, z.B. das ISDN-Netz, miteinander zu verbinden. Dazu müssen die Router mindestens ein LAN- und ein WAN-Protokoll »verstehen«. Man spricht in diesem Zusammenhang dann von einem Multiprotokoll-Router, **MPR**.

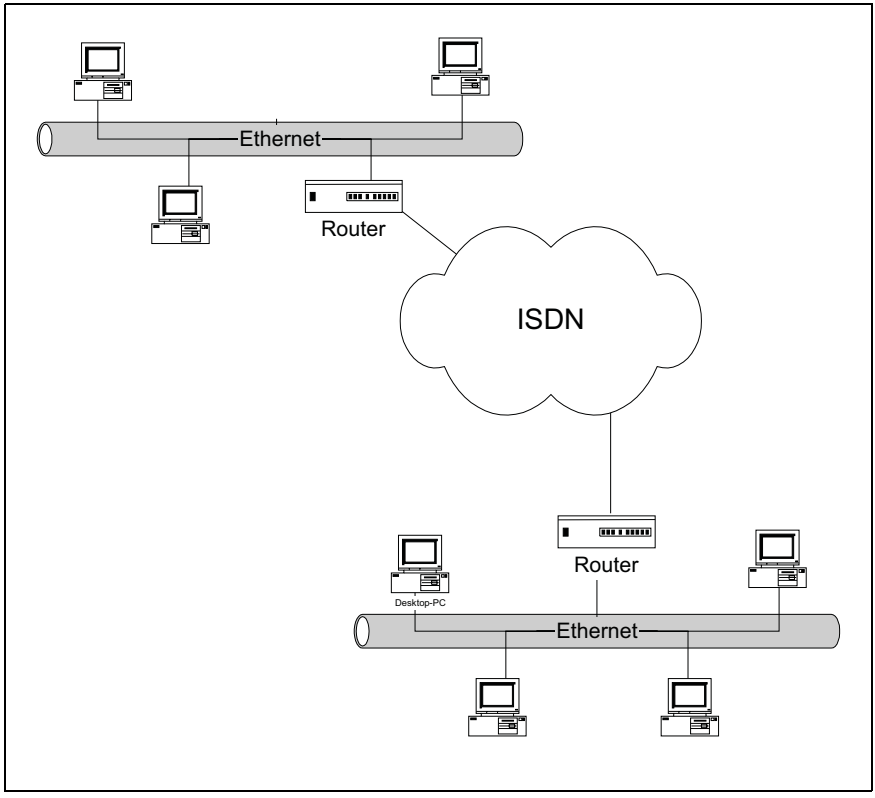


Abbildung 3.14: Multiprotokoll-Router

Als MPR können Router beliebige LANs über beliebige öffentliche Netze wie ISDN, X.25 oder Frame Relay miteinander verbinden.

Die folgenden Abbildungen zeigen weitere Konfigurationsbeispiele für den Einsatz von Routern.

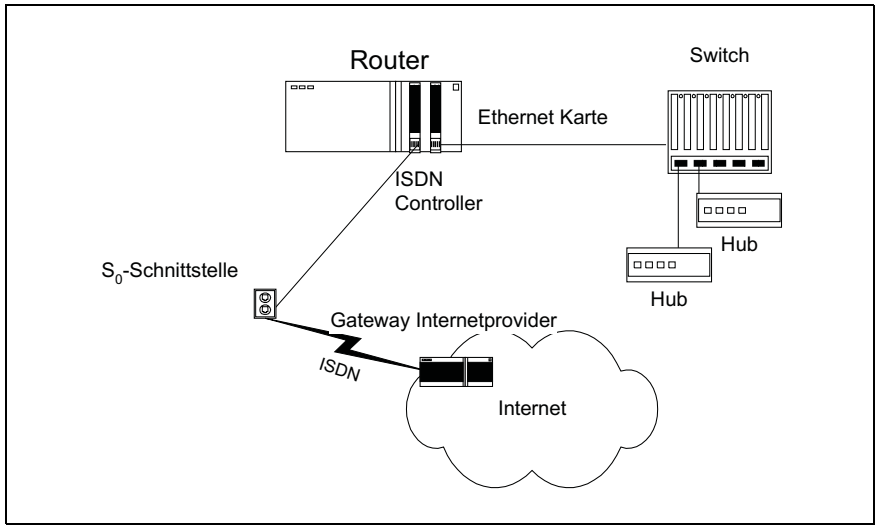


Abbildung 3.15: Multiprotokoll-Router

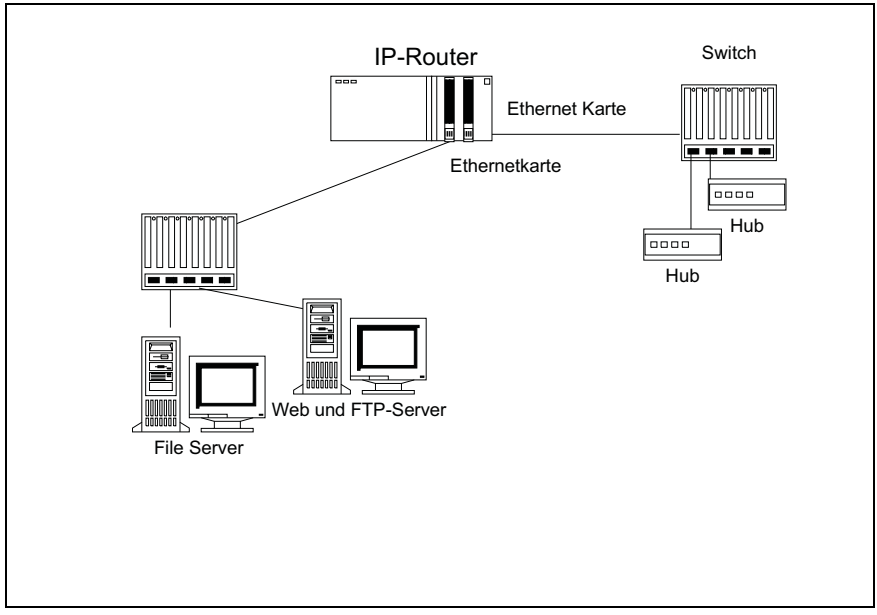


Abbildung 3.16: IP-Router

3.4.3 Wegewahl und Tunneling

Eine weitere wichtige Aufgabe des Routers besteht in der korrekten **Wegewahl**, d.h. die Router-Software muss in der Lage sein mit Hilfe des Address Resolution Protokolls, **ARP**, über verschiedene Netze hinweg einen Adressaten zu lokalisieren. Im Router selbst erfolgt also eine Umwandlung von Adressen. Deshalb arbeiten Router protokollabhängig auf der Schicht 3 des OSI-Modells.

Um die oben beschriebenen Aufgaben lösen zu können, muss ein Router den sich in seinem LAN-Segment befindenden Protokolladressen MAC-Adressen zuordnen können. Wie dies geschieht, erfahren Sie in Kapitel 4 an detaillierten Beispielen zu TCP/IP.

Mit **Layer-3 Special Services** wird die Fähigkeit von Routern bezeichnet, mehrere Schicht- 3-Protokolle zu beherrschen, und dabei Protokolle einpacken zu können. Eine andere Bezeichnung hierfür ist Tunneling. Tunneling ist eine wichtige Voraussetzung für den Aufbau sicherer Virtual Private Networks auf der Basis des Internets. Die folgende Grafik zeigt das Grundprinzip des Tunnelns.

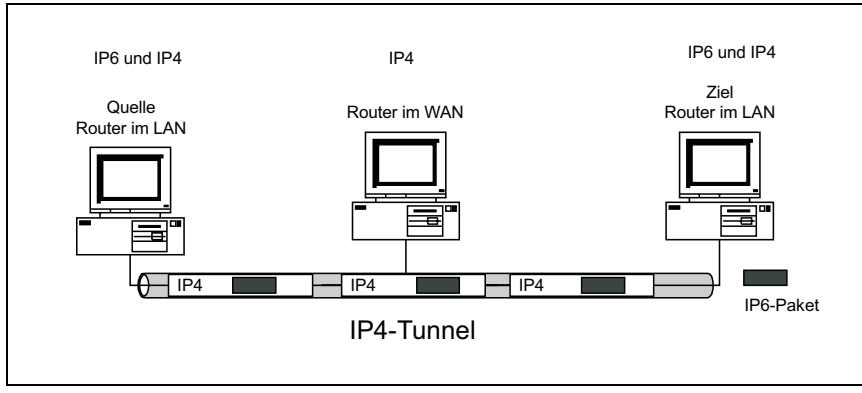


Abbildung 3.17: IP-Router

Das oben gezeigte Beispiel geht von einer Netzwerkkonfiguration aus, die wie folgt beschrieben werden kann:

1. Über das Internet, WAN, sind zwei Host verbunden, die IP4 und IP6 als Routingprotokolle unterstützen.
2. Im Subnet, dem WAN, unterstützt ein Router nur IP4.

Damit dennoch Quelle und Ziel über IP6 miteinander kommunizieren können, müssen die IP6-Pakete in IP4-Pakete **als Nutzdaten** eingepackt werden. Damit bildet IP4 einen Tunnel für den Transport der IP6 Daten von der Quelle zum Ziel, Ende-zu-Ende-Tunneling.

Zusätzlich sind Router in der Lage, Informationen zur Topologie des Netzwerkes zu sammeln und können damit Entscheidungen darüber treffen, auf welchen alternativen Wegen ein Paket übertragen werden kann. Ein Beispiel hierfür ist das Internetprotokoll **RIP**, Routing Information Protocol, das Router untereinander austauschen. Es informiert die Router, welche weiteren Router erreichbar sind.

Leider verwenden viele Praktiker und auch Autoren wie der Netzwerk-Guru Andrew S. Tanenbaum den Begriff Gateway, wenn Sie einen Router meinen. Dies gilt insbesondere für die Internet-Gemeinde.

Hier werden die Router im Rahmen der IP-Konfiguration immer als Gateway bezeichnet. So ist z.B. das Standard Gateway, bzw. Default Gateway, immer der Router, der vom Rechner explizit als erster Router adressiert wird.

Unter Windows 9.x oder NT können bei der TCP/IP Konfiguration zum Standard-Gateway weitere IP-Adressen von Routern eingegeben werden. Diese werden dann direkt adressiert, wenn das Standard-Gateway nicht erreichbar ist.

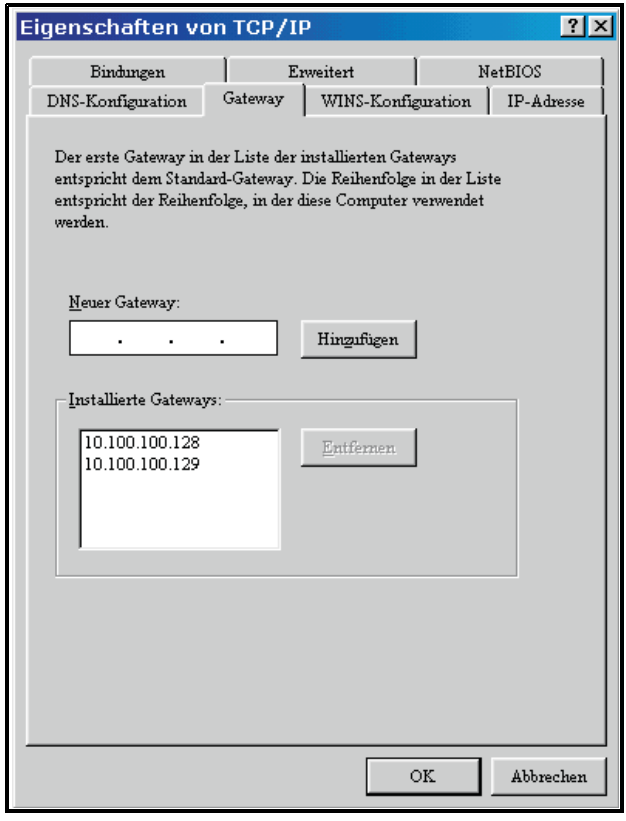


Abbildung 3.18: Routerkonfiguration unter Windows

3.4.4 Das Internet – ein hierarchisches Netzwerk von IP-Routern

Das Internet ist im Grunde ein Netzwerk, das auf der Basis von IP-Routern funktioniert. Diese sind hierarchisch miteinander verknüpft, so dass über Provider an beliebiger Stelle der Erde jeder beliebige Rechner schnell und zuverlässig in das Internet eingebaut werden kann. Dazu muss der betreffende Provider lediglich einen Router zur Verfügung stellen, der alle Verbindungen zu den Hosts seiner Kunden kennt und mit einem übergeordneten Router verbunden ist.

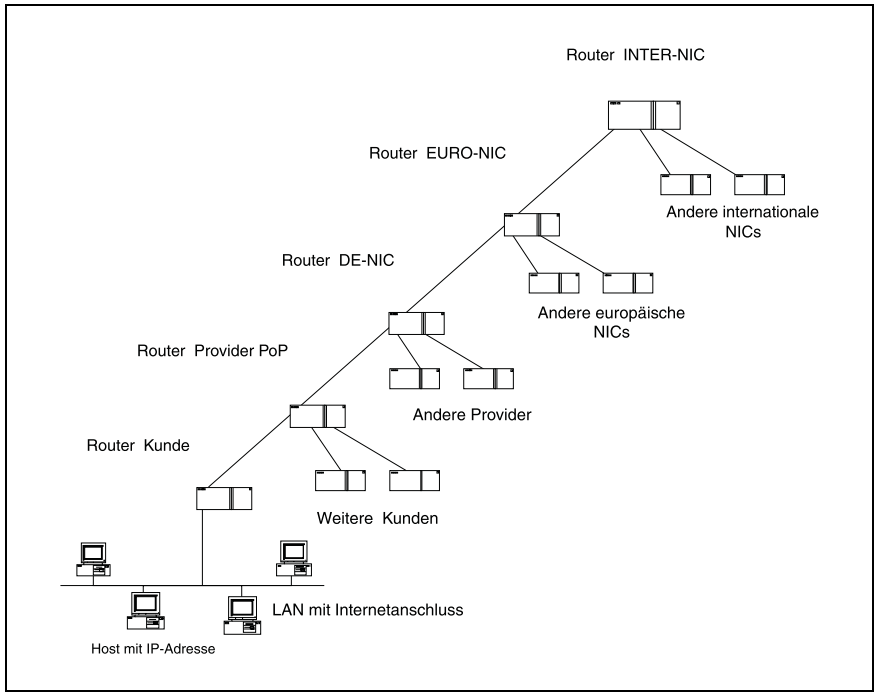


Abbildung 3.19: Router im Internet

3.5 Gateway

Gateways verbinden gänzlich unterschiedliche Netze.

Das typische Gateway wird dazu eingesetzt, lokale Netzwerke mit einer proprietären Architektur zu verbinden. Beispiele sind das SNA-Gateway des Communication Managers unter OS/2 und Novells NetWare for SAA sowie der SNA-Server unter Microsoft Windows NT.

Das Gateway implementiert also immer zwei »Welten«. Die notwendige komplette Umwandlung über alle Schichten hinweg beinhaltet folgende Funktionen:

- ✔ Umwandlung der Adressen
- ✔ Umsetzung von Formaten
- ✔ Code Konvertierung
- ✔ Store and forward, d.h. Zwischenpuffern von Paketen
- ✔ Quittierung
- ✔ Datenflusskontrolle
- ✔ Geschwindigkeitsanpassung

Das SNA Gateway unter OS/2 dient z.B. dazu, für alle Arbeitsstationen im LAN eine Verbindung zum IBM-Host zur Verfügung zu stellen. Aus der Sicht des Hosts ist das Gateway eine Steuereinheit, an die Terminals angeschlossen sind. Aus der Sicht der LAN-Workstations ist das Gateway der Host.

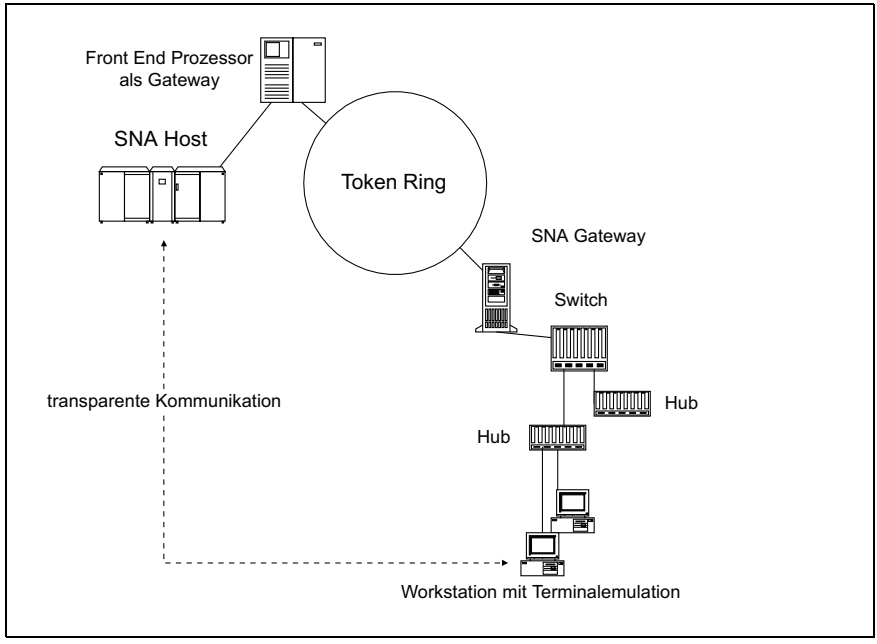


Abbildung 3.20: Gateway

Ein weiteres Beispiel ist das SAA Gateway von Novell, das eine AS/400, eine proprietäre Architektur von IBM, nahtlos in ein LAN integrieren kann. Damit können LAN-Clients gleichzeitig auf AS/400 und auf Novell NetWare Daten und Anwendungen zugreifen. Auch hier erfolgt der Zugriff für den Anwender transparent.

Wie die Abbildung 3.21 zeigt, werden Gateways auch für die LAN-Kopplung über ein Weitverkehrsnetz, WAN, eingesetzt

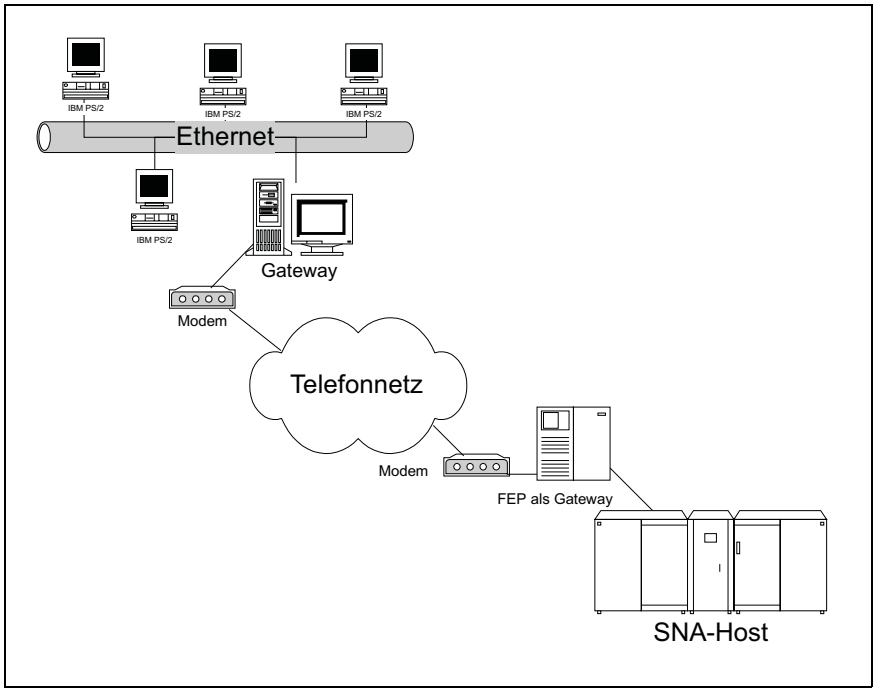


Abbildung 3.21: Gateway in der LAN-WAN-LAN-Konfiguration

Das gezeigte Beispiel macht nochmals den Unterschied zwischen einem Router und einem Gateway deutlich. Router verbinden »gleiche« Technologien, die in unterschiedlichen Netzwerken oder weit entfernt voneinander liegen. Dazu werden bis zur Schicht 3 die Pakete ausgepackt und die Adressformate angepasst. Gateways verbinden im Gegensatz dazu unterschiedliche »Technologien«. Hier reicht es nicht, »nur« Adressen umzusetzen. Die SNA Architektur arbeitet z.B. nach einem völlig anderen Prinzip als lokale Netzwerke. Dies betrifft unter anderem die verwendeten Zeichensätze und die Art, wie Rechner miteinander kommunizieren.

3.6 Switch – Komponente für Highspeed Networking

Der Begriff Switch ist eigentlich nur eine neue Bezeichnung für eine Brücke. Dies gilt, wenn der Switch als Layer 2 Switch konfiguriert ist. In diesem Fall sind die Zieladressen auf MAC-Ebene entscheidend dafür, auf welchen Port eingehende Pakete weitergeleitet werden.

Worin unterscheiden sich nun die Brücken von einem Switch? Der wesentliche Unterschied besteht darin, dass Switches mehr als zwei Segmente miteinander verbinden. Switches sind in diesem Sinne Multiport-Brücken.

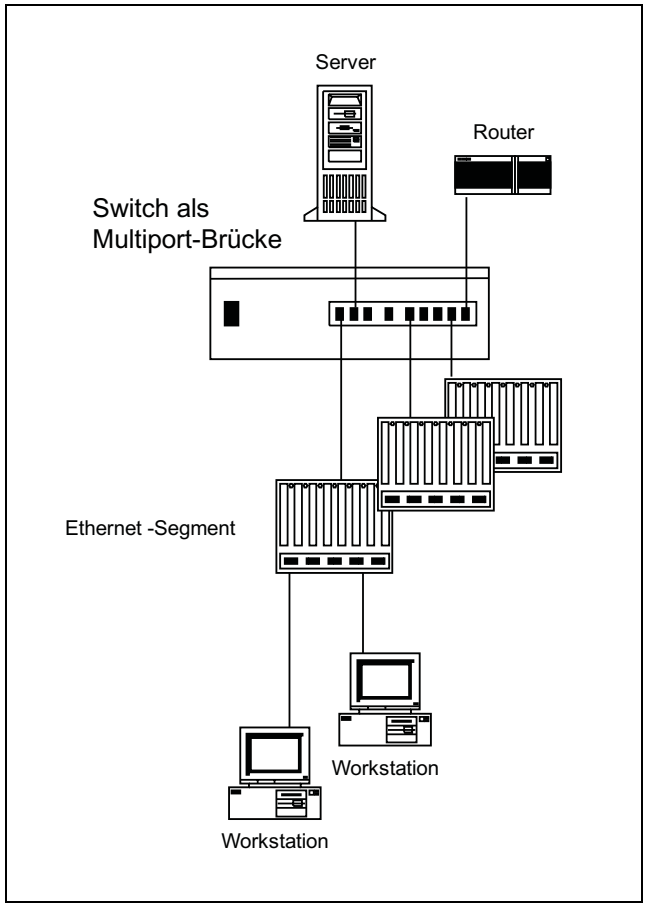


Abbildung 3.22: Switch als Multiport-Brücke

Ein weiterer Unterschied zwischen einer »traditionellen« Brücke und einem Switch liegt in der Geschwindigkeit. Switches verfügen über spezielle Hardwarebausteine, so genannte **ASICs**, Application Specific Interface Circuit, die das Durchschalten, die Forwarding-Entscheidung, wesentlich schneller erledigen als die Software einer Brücke. Damit bilden Switches das Fundament für den Aufbau von Highspeednetzwerken.

Switches werden in die Kategorien

- ✔ Desktop Switch
- ✔ Segment oder Workgroup Switch und
- ✔ Backbone Switch

aufgeteilt.

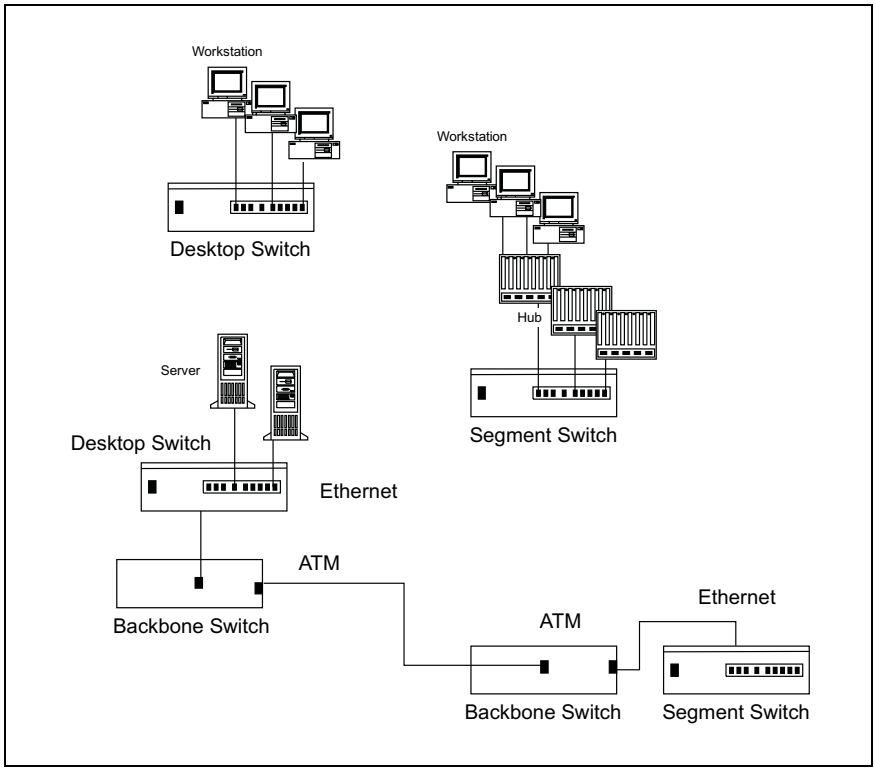


Abbildung 3.23: Switchkategorien

Segment-Switches verfügen über eine hohe Portdichte und an jedem Port ist eine Station angeschlossen.

Workgroup-Switches verbinden über einen Port bis zu 20 Stationen, während Backbone Switches mehrere Switches bzw. Netzwerke miteinander verbinden.

3.6.1 Switching Technologien

Cut-Through-Switching eignet sich für Desktop-Switching, bei dem die Stationen direkt an den Switch angeschlossen sind und es somit nicht zu Kollisionen kommen kann. Dazu wertet der Switch den Frame bis einschließlich der Zieladresse aus und schaltet ihn dann zum Adressaten durch. Diese Methode geht davon aus, dass es keine fehlerhaften Frames gibt. Sie ist sehr schnell, da die Frames nur teilweise »ausgepackt« und nicht gepuffert werden müssen.

Fragment-Free-Switching ist für das Switchen zwischen Workgroups bzw. Segmenten geeignet. Hier ist zwar mit Kollisionen zu rechnen, nicht aber mit fehlerhaften Frames. Da Kollisionen anhand kurzer Frames erkannt werden, wird bei dieser Methode das Datenpaket bis zum 64. Byte im Datenfeld ausgewertet und dann erst weitergeschaltet.

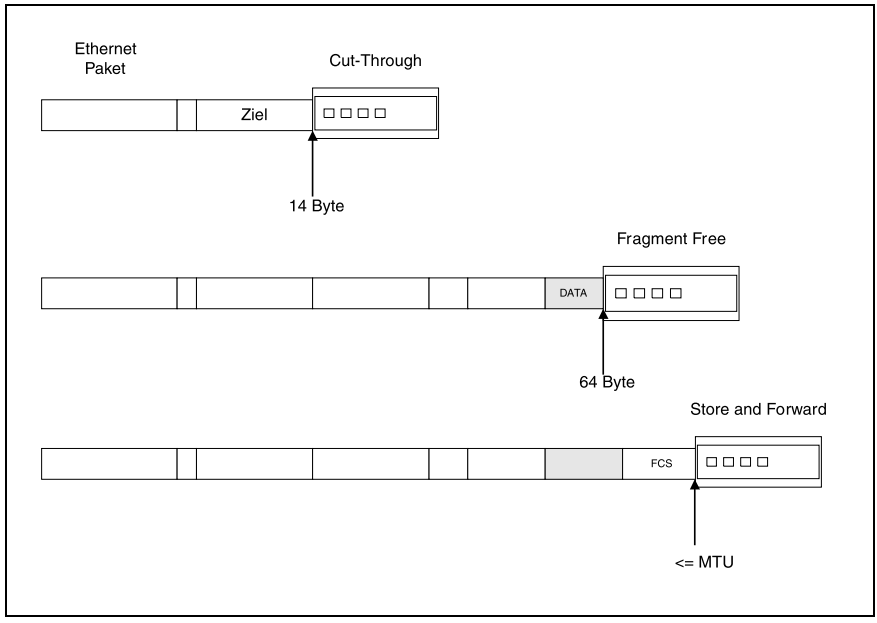


Abbildung 3.24: Switching Technologien

Die letzte Methode, die hier vorgestellt werden soll, ist das Store-and-Forward-Switching. Diese Technik wird bei Backbone-Switches eingesetzt, um das Weiterleiten von fehlerhaften Frames zu unterbinden. Das Datenpaket wird hierzu komplett ausgewertet und dann weitergeleitet, wenn es fehlerfrei ist.

Moderne Switches beherrschen alle die oben aufgeführten Techniken. Sie wechseln je nach Fehlerhäufigkeit automatisch zur besten Methode.

Die Verzögerungszeit bei Cut Through liegt bei etwa 40 Mikrosekunden, bei Store and Forward werden Werte zwischen 98 und 1247 Mikrosekunden erreicht.

Die Architektur eines Switches trägt entscheidend zur Netzwerkleistung bei. Neben den oben beschriebenen Techniken ist die Art und Weise, wie in einem Switch Pakete zwischengespeichert werden, von großer Bedeutung für die Leistungsfähigkeit. Die wichtigsten Techniken sind:

- ✔ Receive Based Port Buffering: Bei diesem Verfahren werden die Datenpakete in einer Eingangswarteschlange, Receive Queue, zwischengespeichert, wenn der Prozessor beschäftigt oder aber der Zielport »belegt« ist. Hier können in der Regel bei 128 KByte ca. 80 Ethernetpakete zwischengespeichert werden.

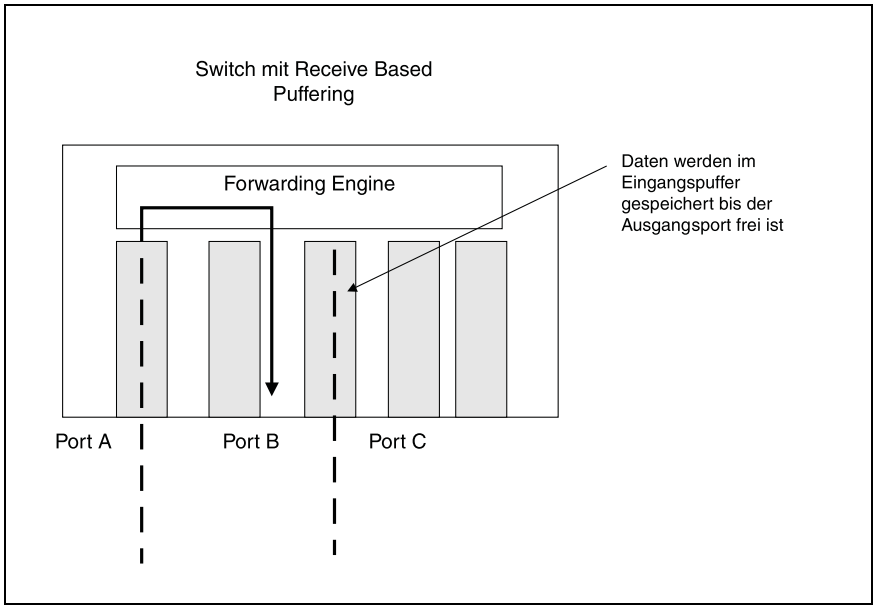


Abbildung 3.25: Switch mit Eingangspuffer – Receive Based Buffering

- ✔ Transmitter Based Port Buffering: Dieses Verfahren geht den umgekehrten Weg wie das oben beschriebene. Hier werden die Datenpakete in einer Ausgangswarteschlange gepuffert, Transmit Queue. Nachteile ergeben sich, wenn Broadcast- und Multicast-Pakete in allen Queues zwischengespeichert werden müssen.
- ✔ Bi-directional Port Buffering: Diese Technik kombiniert die beiden oben beschriebenen Puffertechniken. Es kommt zu weniger Paketverlusten, weil der Speicher für jeden Port doppelt ausgelegt ist.
- ✔ Shared Memory Buffering: Beim Shared Memory Verfahren werden die Speicherkapazitäten dynamisch zugewiesen, d.h. Ports mit hohem Verkehrsaufkommen erhalten mehr Datenpuffer zur Verfügung gestellt. Durch dieses Verfahren werden Datenverluste bestmöglich vermieden.
- ✔ Flow Control Backpressure: Dieses Verfahren wird eingesetzt, um Paketverluste zu vermeiden. Diese sind insbesondere in Netzen mit umfangreichen Fenstergrößen von Nachteil und vermindern erheblich die Effizienz des Netzes. Backpressure bedeutet, dass der Switch bei fast vollem Empfangspuffer am entsprechenden Port Kollisionen simuliert und damit das angeschlossene Segment »lahmlegt«. Dadurch wird ein Überlauf des Puffers verhindert, der zwangsläufig zum Verlust von Datenpaketen führen würde.

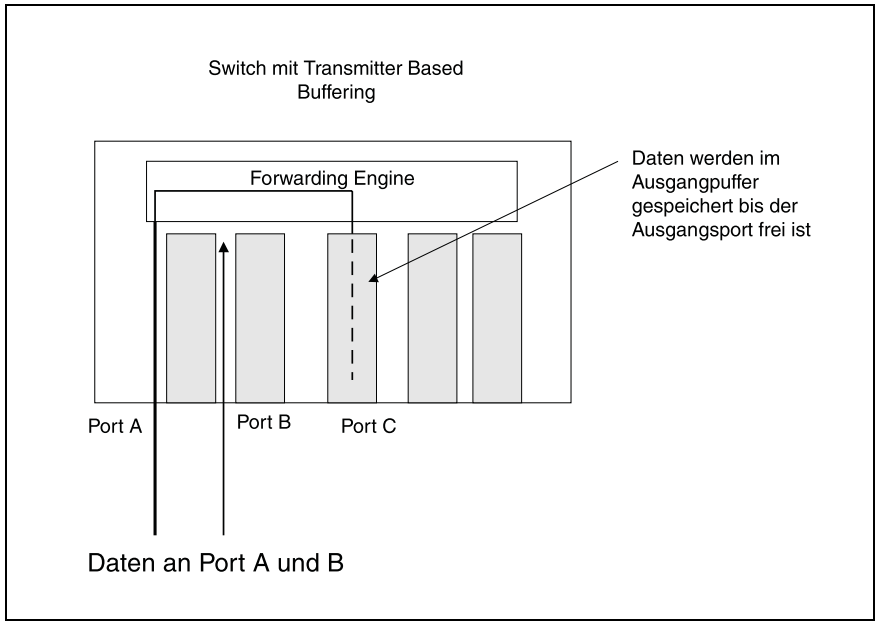


Abbildung 3.26: Switch mit Ausgangspuffer – Transmitter Based Buffering

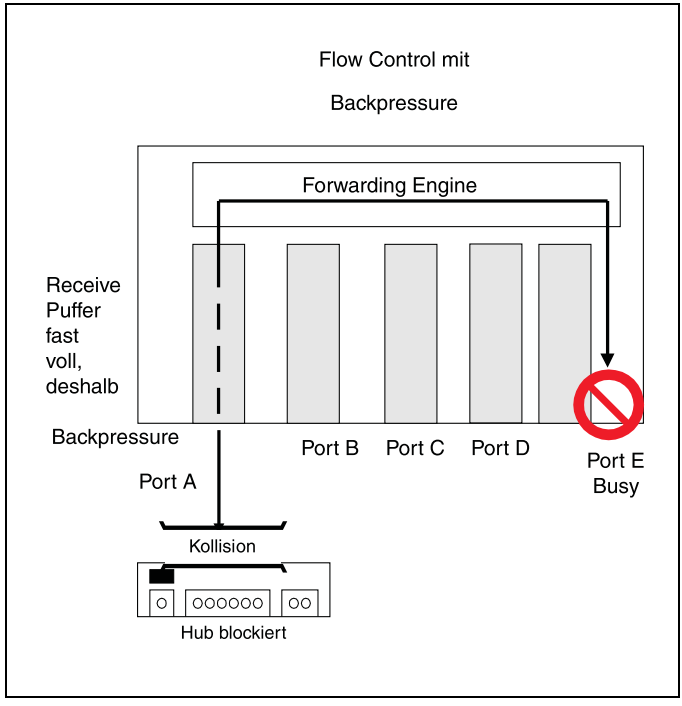


Abbildung 3.27: Switch mit Flow Control Backpressure

3.6.2 Switch als Router – Layer 3 Switch

In größeren Netzwerken sind Router häufig der Flaschenhals für breitbandige Anwendungen. Abhilfe versprechen hier Switches, die Routingentscheidungen mit Leitungsgeschwindigkeit, wired speed, treffen können. Diese Switches arbeiten damit auf der Schicht 3 des OSI-Modells und werden deshalb auch als Layer 3 Switch bezeichnet. Da ein Layer 3 Switch auch die Schicht 2 implementiert, wird die hier beschriebene Technik auch Multilayer Switch genannt.

Routing Switches arbeiten in der Regel mit dem IP-Protokoll. Die IP-Pakete werden dabei anhand von Routingtabellen weitergeleitet, die durch die Routingprotokolle OSPF und RIP angelegt werden.

Routingtechniken

Die Grundlage des Layer 3 Switchings bilden die beiden Verfahren

- ✔ Cut-Through
- ✔ Packet-by-Packet

Cut-Through bedeutet, dass bei der Kommunikation zwischen zwei Endgeräten in unterschiedlichen Subnetzen alle Router, die sich im Kommunikationspfad befinden, durchgeschaltet werden. Das Ergebnis ist eine direkte und damit sehr schnelle Ende-zu-Ende-Verbindung. Die hierfür benötigten Informationen werden vom Switch bei einem Router bzw. Route-Server abgerufen.

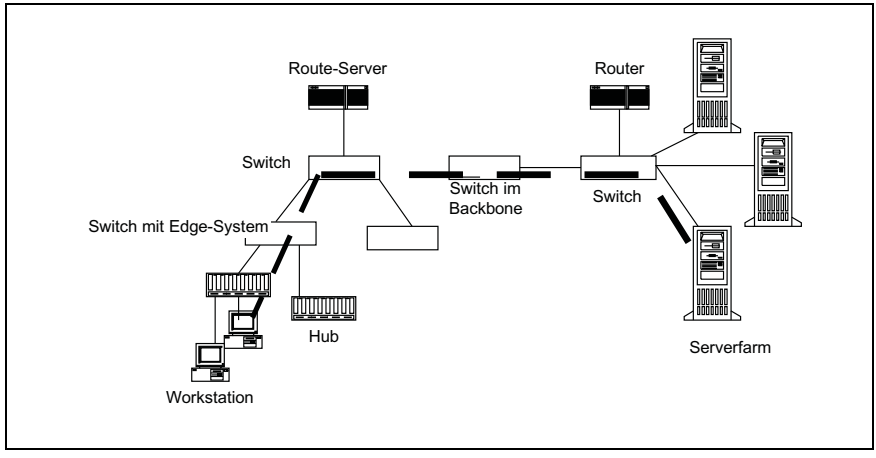


Abbildung 3.28: Cut-Through Switching

Der Kommunikationsstandard **MPOA**, Multiprotocol over ATM, ist ein Beispiel für die Implementierung des Cut-Through Switching auf Layer 3. Die ATM-Switches bilden hierbei ein schnelles Backbone für die angeschlossenen LAN-Segmente, die als Edge- Systeme bezeichnet werden.

Der MPOA-Standard regelt das Übertragen von IP oder anderen Protokollen über ATM-Switches. Weitere Details hierzu finden Sie in Kapitel 3.7.4.

Packet-by-Packet arbeitet nach dem gleichen Prinzip wie traditionelle Router. Die Pakete werden in jedem Switch bis auf Schicht 3 ausgepackt, analysiert und dann wieder weitergereicht. Damit ist dieses Verfahren langsamer als Cut-Through, eignet sich aber sehr gut, um bestehende Routerstrukturen zu ersetzen. So kann die bereits vorhandene IP-Adressstruktur problemlos übernommen werden.

3.6.3 Multimedia mit Layer 4 Switches

Mit Layer 4 Switches können so genannte »regelbasierte« Netze aufgebaut werden. Hinter diesem Konzept steckt die Notwendigkeit zukünftig für bestimmte Anwendungen, wie Video oder Sprache, über einen definierten Pfad garantierte Bandbreiten zur Verfügung stellen zu können, Quality of Services, **QoS**.

Im Wesentlichen geht es beim Layer 4 Switching darum, bestimmte Datenpakete bevorzugt zu transportieren. Die Datenpakete müssen also analysiert werden. Dabei geht es nicht nur darum, wohin ein Paket geleitet werden muss, sondern mit welcher Priorität dies geschehen soll. Dies wiederum ist abhängig von der Art der Daten, die transportiert werden.

Layer 4 Switches, die IP-Daten transportieren, ermitteln den Datentyp anhand der mit TCP bzw. UDP mitgeführten Portnummer. Diese identifiziert eine Anwendung oder einen Dienst und damit den Typ der zu transportierenden Daten. Dieser wiederum ist entscheidend für die Priorität der Übermittlung. Details hierzu finden Sie in Kapitel 4.

IP Layer 4 Switches filtern nach folgenden Entscheidungskriterien:

- ✔ IP-Adresse des Ziel-Hosts
- ✔ Portnummer auf dem Ziel-Host – Datentyp
- ✔ IP-Adresse des Quell-Hosts
- ✔ Portnummer des Quell-Hosts – Datentyp

Die Filtermethoden eines Layer 4 Switches sind als Hardware realisiert. Im Switch befindet sich ein Chip, dessen Programm die hier beschriebenen Filterfunktionen ausführt und damit nahezu Leitungsgeschwindigkeit erreicht.

Wie die Funktionen eines Layer 4 Switches auf Protokollebene abgearbeitet werden, erfahren Sie in Kapitel 4.6.7 RSVP – Resource Reservation Protocol.

3.6.4 Einsatz von Switches in einem Gigabit Ethernet

Die anschließend gezeigte Topologie zeigt eine Implementierung, die eine Bandbreite von 100 Mbit/s bis zum Arbeitsplatz zur Verfügung stellt. Der Switch fungiert hier als Backbone mit hohem Datendurchsatz.

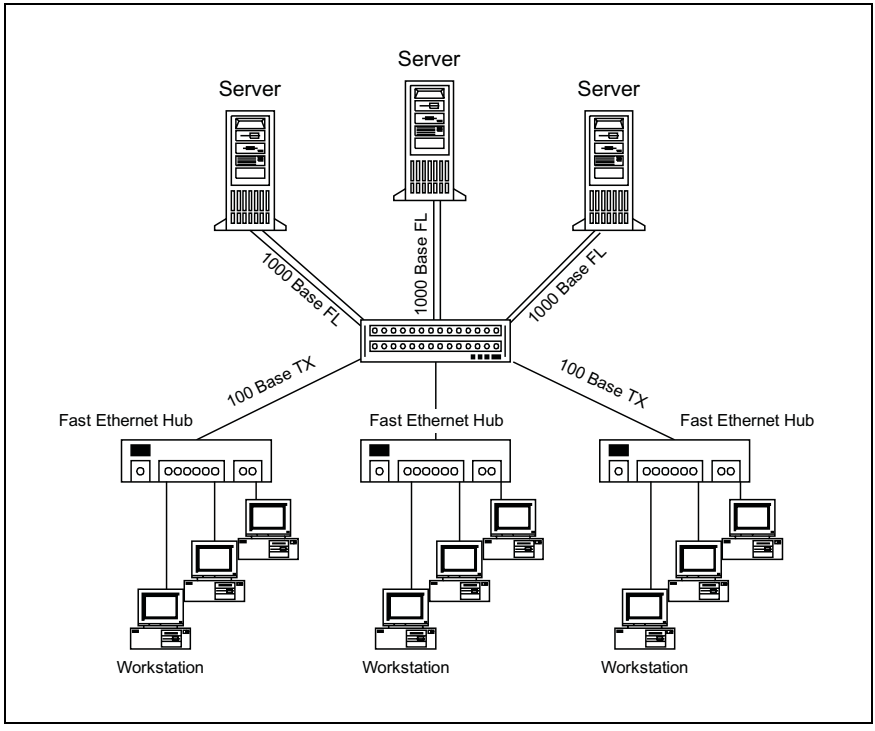


Abbildung 3.29: Optimale Netzkonfiguration mit Switch als Backbone

Im gezeigten Beispiel sind die Workstations an Fast Ethernet Hubs angeschlossen. Diese wiederum hängen Full-Duplex an einem Gigabit-Ethernet-Switch. Die Server sind direkt an den Switch angeschlossen und unterstützen ein Gigabit Übertragungsrate in jede Richtung. Die gezeigte Topologie kann als Endstufe eines Migrationsprozesses angesehen werden, dessen Ausgangspunkt ein Standard-Ethernet war. Voraussetzung ist aber, wie oben schon einmal erwähnt, dass der Standort strukturiert verkabelt ist. Erst dann ist es möglich, nach und nach die Internetworkingkomponenten, also Hubs und Switches, sukzessive auszutauschen.

3.7 Internetworking über Weitverkehrsnetze

In diesem Kapitel erhalten Sie einen Überblick über die WAN-Technologien, die für die entfernte Anbindung von LAN-Segmenten oder einzelnen Arbeitsstationen eingesetzt werden.

WAN Technologien arbeiten im Unterschied zum LAN mit Punkt-zu-Punkt-Verbindungen. Diese werden zwischen Routern aufgebaut, die dann den Zugang zum angeschlossenen LAN ermöglichen. Router zum WAN sind deshalb relativ einfach zu konfigurieren. Als Routinginformation muss lediglich die Adresse der Gegenstelle angegeben werden. Abbildung 3.30 zeigt das Grundprinzip.

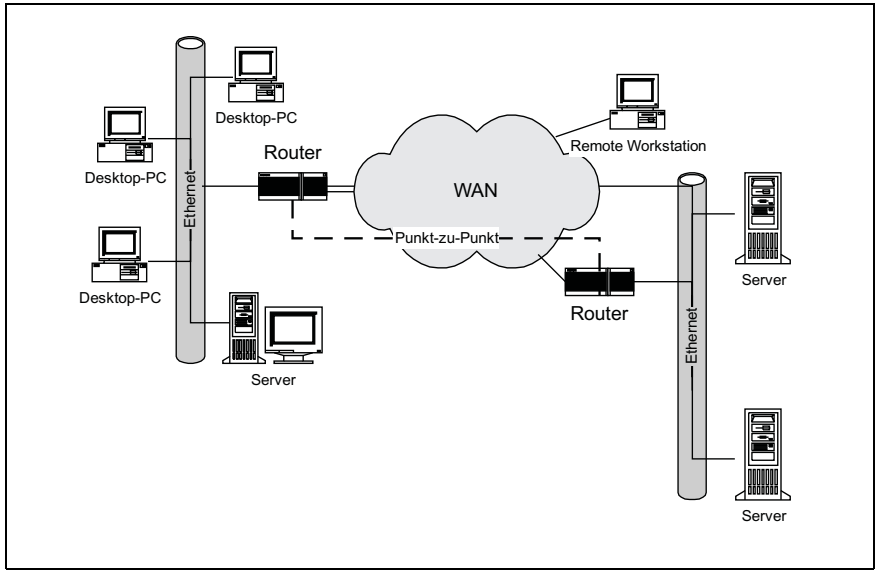


Abbildung 3.30: Prinzip der LAN-WAN-LAN Kopplung.

Die folgenden Kapitel beschreiben die für den Netzadministrator wichtigsten Merkmale der WAN-Technologien. Es sind dies:

- ✔ Schnittstelle
- ✔ Übertragungsgeschwindigkeit
- ✔ Adressierungstechnik
- ✔ Protokoll

Über das »Innenleben« des WAN muss der Netzadministrator relativ wenig wissen. Wichtig ist die Technik am »Rande« des WANs.

Die Architektur eines Routers zum WAN ist im Wesentlichen immer gleich. Es müssen folgende Parameter bekannt sein:

- ✔ Bezeichnung der Schnittstelle
- ✔ Anschlusstechnik dieser Schnittstelle
- ✔ Netzwerkkarte
- ✔ Adresse des Routers im WAN
- ✔ WAN-Protokoll und dessen Implementierung

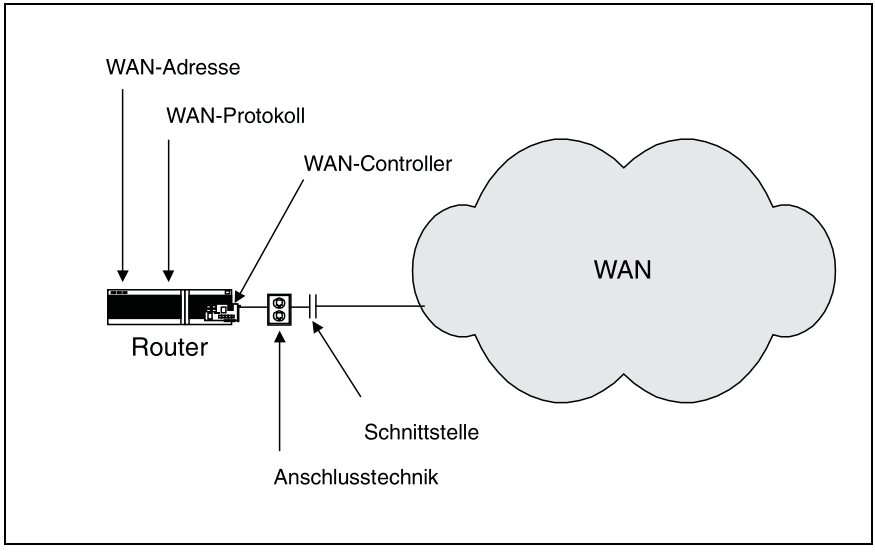


Abbildung 3.31: Architektur eines Routers zum WAN

Im folgenden Kapitel finden Sie konkrete Umsetzungen am Beispiel von ISDN-Routern.

3.7.1 ISDN – Integrated Services Digital Networks

Das Akronym ISDN steht für Integrated Services Digital Networks, was sich etwa übersetzen lässt mit »diensteintegrierendes digitales Netzwerk«. Dieses Netz, das 1989 dem öffentlichen Betrieb übergeben wurde, ist ein universelles digitales Telekommunikationsnetz. Wichtig ist in diesem Zusammenhang, dass ISDN vor allem ein Telefonnetz ist. D.h. die Anforderungen und technischen Grenzen der Sprachübermittlung bilden die Rahmenbedingungen des ISDN.

Langfristiges Ziel ist es, ISDN weltweit zu einem standardisierten Netz auszubauen. Dies und die Tatsache, dass ISDN erhebliche Leistungs- und damit auch Kostenvorteile gegenüber »traditionellen« Netzen wie analoges Telefonnetz

oder X.25 bietet, hat dazu geführt, dass die heutige Telekommunikation und damit auch Datenübertragung zumindest in der Bundesrepublik entscheidend von ISDN geprägt ist.

Aus diesem Grund wird ISDN im Vergleich zu anderen WAN-Technologien in diesem Buch ausführlicher besprochen.

Man unterscheidet zwischen Schmalband-ISDN und Breitband-ISDN. Das letztgenannte Netz wird auf der Basis von Glasfaserkabeln realisiert und bietet Einwählpunkte mit bis zu 155 Mbit/s und mehr Übertragungsrate. Als Vermittlungstechnik kommt ATM zum Einsatz.

Wenn im Folgenden verkürzend von ISDN gesprochen wird, dann ist das Schmalband-ISDN gemeint, das auf dem traditionellen Fernmeldekabel aufbaut. Für die Digitalisierung analoger Sprachsignale wird das PCM-Verfahren eingesetzt. Die Übertragung eines Bytes erfolgt in einem Zeitintervall von 125 Mikrosekunden. Daraus ergibt sich die Übertragungsrate von 64 Kbit/s (8 Bit * 1.000.000/125) in jedem Nutzkanal des Schmalband-ISDN.

In den folgenden Abschnitten lernen Sie die technischen Details des ISDN kennen, die für die LAN-WAN-LAN Kommunikation benötigt werden.

Aus der Sicht eines Netzadministrators sind folgende Leistungsmerkmale des ISDN von Bedeutung:

- ✔ Trennung von Nutz- und Steuerkanal
- ✔ Bis zu 128 Kbit/s Bandbreite
- ✔ Nutzen der vorhandenen Fernmeldeinfrastruktur
- ✔ Schneller Verbindungsaufbau
- ✔ Standardisiertes Protokoll
- ✔ Standardisierte Schnittstelle

ISDN Schnittstellen

Grundvoraussetzung für die Nutzung des ISDN ist der Anschluss an das ISDN-Netz durch den Netzbetreiber. Dazu muss der Fernsprechteilnehmer mit einer digitalen Ortsvermittlungsstelle, in der Telekomterminologie DIVO genannt, verbunden sein. Ist dies der Fall, dann erhält der Teilnehmer einen »ISDN-Hauptanschluss«, auch entsprechend der Schnittstellenbezeichnung als S_0-Anschluss oder als »Kommunikationssteckdose« bezeichnet.

Technisch erfolgt der Anschluss durch die Installation eines **NT,** Network Terminal, genannten Netzabschlusses, der über das Zweidraht-Kupferkabel des analogen Fernmeldenetzes mit der ISDN-fähigen digitalen Ortsvermittlungsstelle verbunden ist.

Das NT wird beim Teilnehmer fest installiert und besitzt einen 220V-Anschluss. Die Überwachung der internen Funktionen und die Notspeisung bei Netzausfall wird von der digitalen Vermittlungsstelle übernommen. Das Netzgerät setzt die zweirädrig geführte Fernmeldeleitung in die vierrädrige S_0-Schnittstelle um. Dies hat den entscheidenden Vorteil, dass kein Kabelaustausch zwischen Teilnehmer und Vermittlungsstelle notwendig ist. Die digitale Verbindung reicht von Endgerät zu Endgerät.

Im ISDN werden je nach Anschlussart 2 oder 30 Nutzkanäle sowie ein hiervon getrennter Steuerkanal zur Verfügung gestellt. Die **Nutzkanäle** werden Basis- oder **B-Kanal** genannt, der **Steuerkanal** heißt **D-Kanal**. Diese Trennung erhöht die Flexibilität des ISDN gegenüber den bisherigen Netzen.

In herkömmlichen Netzen werden Nutz- und Steuerdaten in einem (logischen) Kanal transportiert. Deshalb muss hier zwischen Nutz- und Steuerungsphasen unterschieden werden; das Verhältnis zwischen Nutz- und Steuerdaten, die Effizienz, ist relativ gering. Bei ISDN ist dies nicht der Fall. Signalisierungsvorgänge wie Auf- und Abbau von Verbindungen oder der Austausch von Kontrollinformationen erfolgen unabhängig vom Nutzkanal im D-Kanal.

Die Basiskanäle haben keine dienstespezifischen Eigenschaften und es existieren keine Festlegungen, wie diese Kanäle zu nutzen sind. Das bedeutet, dass sie für jeden Kommunikationsdienst zur Verfügung stehen, für den eine Datenrate von 64 Kbit/s je Datenkanal ausreichend ist.

Die Deutsche Telekom hatte sich 1989 für eine schnelle Einführung des ISDN entschieden. Dies war dann auch die Ursache für die Verwendung einer nationalen Variante der Kommunikationssteuerung. Das entsprechende Protokoll heißt 1TR6. Es handelt sich hier um eine nationale Protokollvariante auf den Schichten 1 bis 3 im OSI-Modell.

Seit 1993 wird neben dem **1TR6**-Protokoll ein europaweit genormtes Protokoll **E-DSS1**, European Digital Subscriber Signalling System No. 1, eingesetzt. Die Anschlussvariante mit diesem Protokoll heißt Euro-ISDN. Für die Praxis bedeutet dies, dass das 1TR6 Protokoll zwar keine Rolle mehr spielt, aber dennoch als Konfigurationsparameter abgefragt wird.

Basisanschluss

Der Basisanschluss bietet die Möglichkeit, zwei unabhängig vermittelbare Datenkanäle, Nutz- oder Basiskanäle mit je 64 Kbps und einen Steuerkanal mit 16 Kbps zu nutzen. Die Basiskanäle werden als B1 bzw. B2 bezeichnet.

Der Steuerkanal, D1, wird in erster Linie dazu verwendet, Steuerinformationen wie z. B. Auf- und Abbau einer Verbindung, zu übertragen. Dabei stellt der D-Kanal keine durchgehende Verbindung von Teilnehmer zu Teilnehmer dar. Er existiert lediglich zwischen dem Teilnehmerendgerät und der ISDN-fähigen **di**gitalen **O**rts**v**ermittlungsstelle **DIVO**.

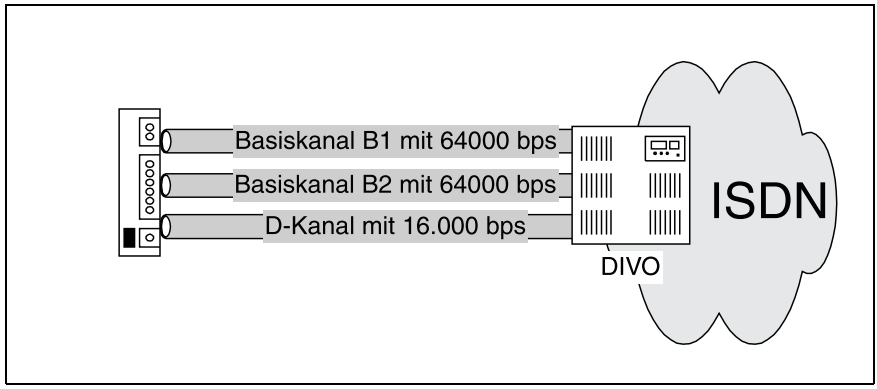


Abbildung 3.32: ISDN-Basisanschluss

Die S_0-Schnittstelle ist als passiver Bus realisiert. Die Schnittstelle funktioniert dabei als »Sammelschiene«, die allen angeschlossenen Geräten den Zugang zum ISDN ermöglicht. Die maximale Länge ist von der Anzahl der am Bus angeschlossenen Endgeräte abhängig. Passiv bedeutet, dass diese Geräte untereinander nicht kommunizieren können, weil die Schnittstelle keine Vermittlungsfunktion wahrnehmen kann.

Der Basisanschluss kann als Einzelendgeräteinstallation mit TK-Anlage und als Mehrfachendgeräte-Installation mit bis zu acht Endgeräten realisiert werden. Das NT heißt **NTBA.**

Merkmal des Euro-ISDN-Anschlusses ist, dass jedes integrierte Gerät eine eigene, **MSN** genannte, Mehrfachrufnummer erhält. Die Multiple Subscribers Number ist eine »normale« Rufnummer, so dass für einen Basisanschluss bis zu zehn verschiedene Rufnummern vergeben werden können.

Primärmultiplexanschluss

Bei einem größeren Bedarf an Anschlussleitungen besteht die Möglichkeit eines Primärmultiplexanschlusses, PMxAs. Dieser bietet 30 Nutzkanäle B1 bis B30 und einen Steuerkanal D2 mit 64 Kbps Übertragungsrate. Die Schnittstelle des Primärmulti-plexanschlusses heißt S_{2M}. Hier ist nur eine Einzelendgeräteinstallation, d.h. Telekommunikationsanlage, möglich. Es handelt sich also um eine typische Punkt-zu-Punkt-Konfiguration. In der Terminologie der Telekom wird die Netzabschlusseinheit für den Primärmultiplexanschluss als **NT2PM** bezeichnet.

Um die Übertragungskapazität des Primärmultiplexanschlusses von 1,984 Mbps zu gewährleisten, verwendet die Telekom ein PCM30 genanntes Multiplexverfahren. Dieses Verfahren ermöglicht die Nutzung von 30 Kanälen für die transparente Datenübertragung.

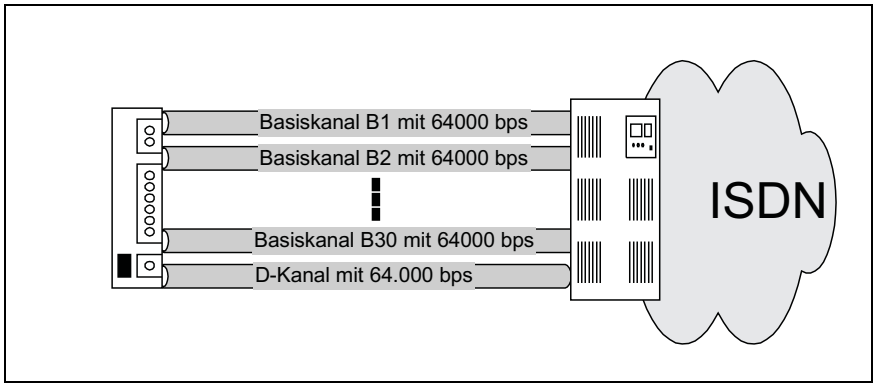


Abbildung 3.33: ISDN-Primärmultiplexanschluss

Der Basisanschluss eignet sich besonders für die Integration von entfernten Arbeitsplätzen in das Unternehmensnetzwerk. Die bei der Kanalbündelung erreichte Übertragungsgeschwindigkeit von 128 Kbit/s ist für einen Zugang zu den File- und Internet-Servern im LAN ausreichend. Die Schnittstelle zum LAN kann dann als Primärmultiplexanschluss ausgelegt sein. Damit haben bis zu 30 Remote-Anwender gleichzeitig Zugriff auf das LAN.

Im ISDN sind zwei verschiedene Verbindungsarten möglich:

- ✔ Wählverbindung
- ✔ Standleitung oder Festverbindung

Ist für den ISDN-Einsatz eine ständige Verbindung erforderlich, dann kann eine »Digitale Festverbindung der Gruppe 2« installiert werden. Festverbindungen können als Basisanschluss und als Primärmultiplexverbindung implementiert werden. Die hierfür in den Endgeräten benötigten Schnittstellen heißen dann S_0FV bzw. S_{2M}FV.

Beide Verbindungsarten werden von ISDN-Internetworkingkomponenten unterstützt. Router können je nach Anforderungen so konfiguriert werden, dass sie bei jedem Verbindungswunsch einen Kontakt herstellen, Dial-on-Demand, oder aber direkt nach dem Booten die Gegenstelle anwählen und die Verbindung via Standleitung aufrechterhalten.

Ein typisches Beispiel für Wählverbindungen ist die Verbindung zwischen einer Zentrale und Außenstellen, die zu definierten Zeiten lokal angefallene Daten an die Zentrale senden, z. B. Kassenbestände oder Bestellungen. Festverbindungen oder Standleitungen sind typisch für den permanenten Zugang zum Internet, also für die Verbindung zwischen eigenem LAN und dem Gateway des Providers.

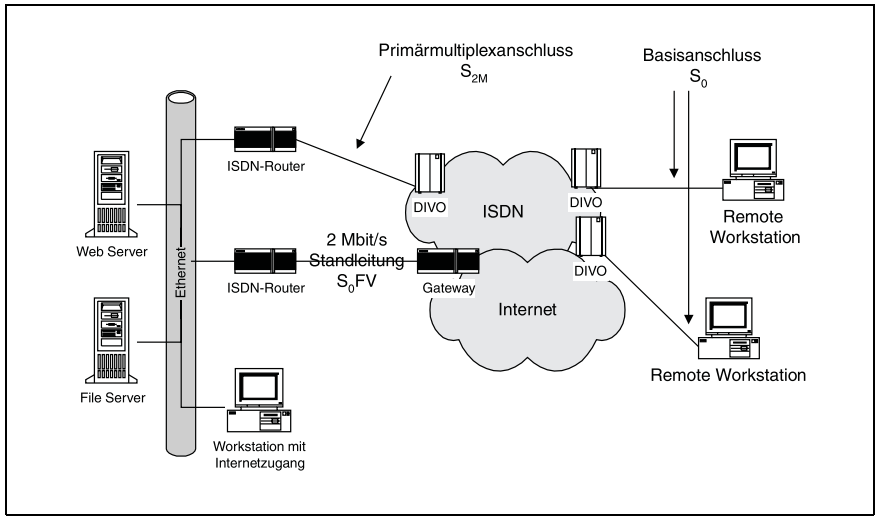


Abbildung 3.34: ISDN-Router und Schnittstellen

ISDN-Controller

Die Datenfernverarbeitung erfolgt im PC über die serielle V.24 Schnittstelle. Über diese asynchrone Schnittstelle ist eine maximale Übertragungsrate von 19200 Bit in der Sekunde möglich. Damit ist sie für den direkten Anschluss an das ISDN-Netz nicht geeignet. Eine Lösung stellt die Aufrüstung mit einer ISDN-PC-Karte, auch als ISDN-Adapter oder ISDN-Controller bezeichnet, dar. Hierbei handelt es sich um Erweiterungskarten, die in einen freien Steckplatz des PC eingebaut werden. Dabei werden im Allgemeinen keine besonderen Anforderungen an den PC gestellt.

Das Leistungsspektrum reicht von kompakten, prozessorlosen Karten über einfache, aber prozessorunterstützte Karten bis hin zum Hochleistungs-Adapter mit eigener Prozessorleistung und bis zu zwei MB Speicherkapazität. Einfache Karten sind für die Abarbeitung eines B-Kanals am Basisanschluss ausgelegt und bieten die Möglichkeit, alle definierten Telekommunikationsdienste wie Telex, Telefax und Btx sowie nichtstandardisierte Anwendungen, wie z.B. Datentransfer, abzuwickeln. Da diese Karten über keinen eigenen Prozessor verfügen, ist der Hardwareaufwand relativ gering. Die gesamte Anwendungssoftware wird von der Festplatte des PC geladen.

Karten ohne eigene Prozessorleistung werden auch als passive Karten bezeichnet.

Hochleistungs-ISDN-Karten sind für den simultanen Betrieb zweier Datenkanäle ausgelegt und besitzen einen Hochleistungsprozessor, Transputer, der bis zu 10 Mips leistet. Auch hier wird die Software von einem externen Speicher geladen. Allerdings entlastet der eigene Prozessor die CPU der Hardware, in die die Karte eingebaut ist.

ISDN-Karten mit eigener Prozessorleistung werden auch als aktive Karten bezeichnet.

Auf ISDN-Karten deutscher Anbieter befindet sich in der Regel das **CAPI**, Common-ISDN-API, Common ISDN Application Programmable Interface. Mit 36 in der Programmiersprache C geschriebenen Funktionen erlaubt dieses Interface den uneingeschränkten Zugriff von Programmen auf die ISDN-Adapterkarte. Damit ist die Grundlage zur herstellerunabhängigen Entwicklung von ISDN-fähigen Programmen gelegt. Anwendungen, die dieses Interface benutzen, sind von zukünftigen Erweiterungen oder Hardwareänderungen nicht betroffen. Ebenso sind zukünftige Erweiterungen unter Erhaltung der Kompatibilität zur vorhandenen Software möglich. Die Common API hat sich in Deutschland zur Standardschnittstelle entwickelt. Eine weltweite Norm ist zurzeit noch nicht in Sicht. Die aktuelle Version der CAPI ist 2.0 und unterstützt 32-Bit-Anwendungen.

Unter Windows werden ISDN-Controller als Netzwerkkarten konfiguriert. Die Bezeichnung für die CAPI-Treiber wird von den Kartenherstellern nicht einheitlich vorgenommen. AVM, einer der bedeutendsten Hersteller von ISDN-Karten, benutzt z.B. den Begriff NDIS-WAN für die CAPI-Treiber.

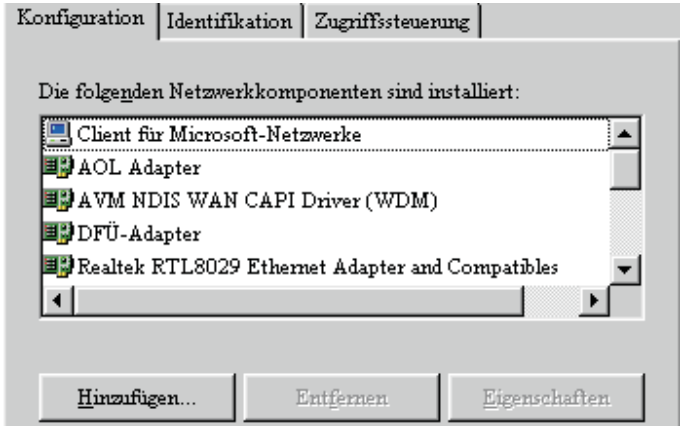


Abbildung 3.35: ISDN-Controller unter Windows 9x

Die CAPI übernimmt die Funktion der Treibersoftware, und jede Karte wird mit einer ISDN-Rufnummer als Adresse konfiguriert. Über das DFÜ-Netzwerk kann dann eine WAN-Verbindung zu entfernten Rechnern bzw. Netzwerken aufgebaut werden.

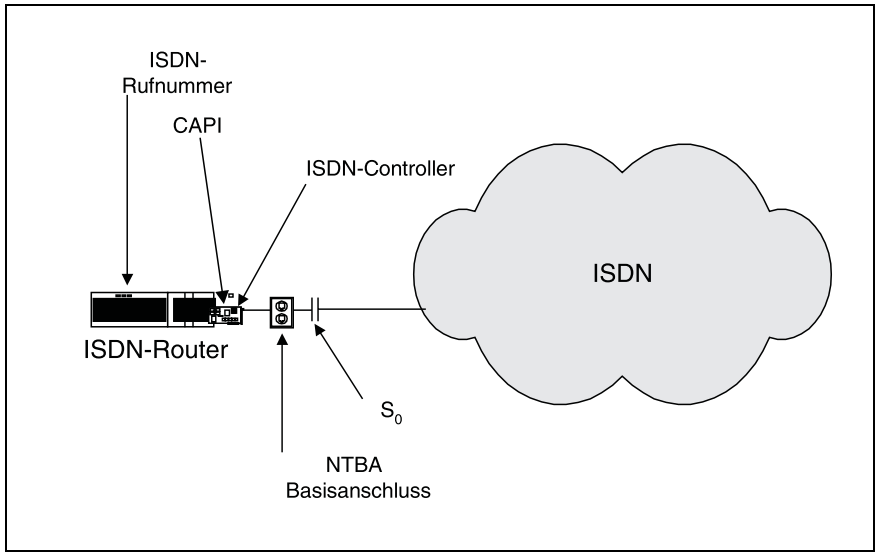


Abbildung 3.36: ISDN-Router am Basisanschluss

3.7.2 X.25

Das X.25-Protokoll ist heute noch das Rückgrat der weltweiten Datenkommunikation über Weitverkehrsnetze. In jedem Land der Erde werden X.25-Netze eingesetzt, die untereinander verbunden sind und ein weltweites Kommunikationsnetz bilden. X.25-Netze spielten in der Vergangenheit auch eine wichtige Rolle bei der LAN-WAN-LAN Kopplung. Da das Protokoll aber relativ langsam und in der Anwendung teuer ist, wird es mehr und mehr von ISDN, Frame Relay und ATM verdrängt.

Sie erhalten in den folgenden Kapiteln einen Überblick über die wichtigsten Fakten. Sie sollen damit in die Lage versetzt werden, bestehende Konfigurationen zu verstehen. Für die Zukunft und für Neuinstallationen spielt X.25 nur noch eine sehr untergeordnete Rolle.

Das entscheidende Merkmal dieser Netztechnologie ist, dass die zu übertragenden Daten in Pakete oder Frames zusammengefasst und dann an den Adressaten übertragen werden. Die Übertragung erfolgt paket- und nicht leitungsvermittelt wie z.B. im ISDN-Netz. Damit entstehen keine entfernungsbedingten Kosten. Kostenrelevant sind das Übertragungsvolumen und die Übertragungsgeschwindigkeit, die vom Nutzer an der Schnittstelle in Anspruch genommen werden.

X.25-Netze sind digitale Datennetze, die nur Daten übertragen. ISDN ist im Unterschied dazu ein Value Added Network, das mehrere Dienste zur Verfügung stellt, ein Mehrwertdienst.

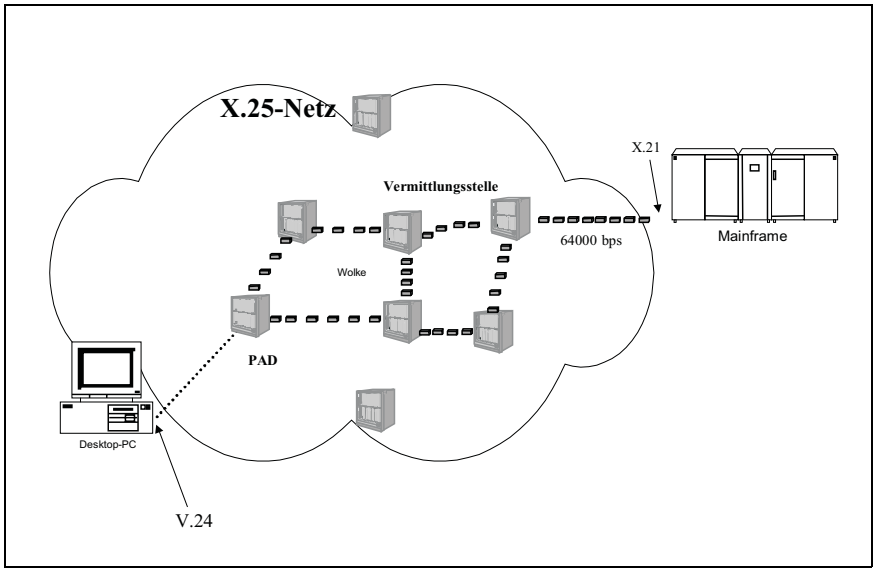


Abbildung 3.37: Paketvermittlung in X.25-Netzen

Abbildung 3.37 zeigt, dass X.25-Netze Daten über verschiedene Wege zum Zielrechner transportieren. Es gibt keine direkte Ende-zu-Ende-Verbindung zwischen Quell- und Zielrechner. Deshalb werden X.25-Verbindungen auch als virtuelle Verbindungen bezeichnet. Über eine physikalische Verbindung können bis zu 255 virtuelle Verbindungen gleichzeitig aufgebaut werden. D.h. ein Zentralrechner mit einer X.25-Schnittstelle kann gleichzeitig mit bis zu 255 angeschlossenen Endgeräten eine Verbindung halten und dabei Daten austauschen.

Bei der virtuellen, scheinbaren, Verbindung werden die Datenpakete immer nur über einen Teilabschnitt der Gesamtverbindung bis zur nächsten Datex-P-Vermittlungsstelle weitergeleitet. Dort werden die Daten so lange zwischengespeichert, bis der nächste Teilabschnitt zur folgenden Vermittlungsstelle frei ist. Diese Methode wird auch store-and-forward-Prinzip genannt. Auf jeder Teilstrecke erfolgt eine Fehlerprüfung.

X.25-Netze arbeiten fensterorientiert. Ein Fenster legt fest, wie viele Datenpakete maximal gesendet werden können, ohne dass der fehlerfreie Empfang vom Postrechner quittiert wurde. So bedeutet eine Fenstergröße von fünf, dass höchstens fünf Datenpakete übertragen werden können, bevor eine positive Bestätigung durch den Empfänger erfolgen muss. Die Deutsche Telekom benutzt in ihrem X.25-Netz z.B. eine maximale Fenstergröße von sieben Segmenten.

X.25-Schnittstellen

Endgeräte, die nicht über eine X.25-Schnittstelle verfügen, wie z.B. der PC, können mit einer entsprechenden Erweiterungskarte nachgerüstet werden. Da dies unter Umständen wegen zu geringer Auslastung des Anschlusses zu teuer sein wird, kann der Anschluss auch über eine sogenannte Anpassungseinrichtung, den **PAD**, Package Assembler/Disassembler, erfolgen. Mit Hilfe des PAD werden die seriellen Daten zu Paketen gebündelt um danach an die X.25 Vermittlungsstelle weitergeleitet. Diese baut sendeseitig die empfangenen Zeichen zu Paketen zusammen und zerlegt empfangsseitig die Datenpakete wieder in einzelne Zeichen.

X.25-Anschlüsse werden mit unterschiedlichen Übertragungsgeschwindigkeiten von 300 Bit/s bis zu 64000 Bit/s angeboten.

Anwendung und Adressierung

Das X.25-Netz der Deutschen Telekom AG heißt Datex-P-Dienst. Der Datex-P-Dienst wird in zwei Versionen angeboten. In der ersten Variante heißt dieser Dienst Datex-P10. Hier wird der Datenaustausch über ein Datenübertragungsgerät gesteuert. Für Datex-P10 benötigen Sie eine Datex-P-Steckdose und eine Datenendeinrichtung mit X.25-Schnittstelle. Hier sind dann Übertragungsraten von bis zu 64000 bps möglich.

In der zweiten Variante, dem Datex-P20-Dienst, erfolgt der Zugang über eine Wählverbindung der Gruppe 5, d.h. über das analoge Telefonnetz. Dabei können maximal 2400 Bit/s übertragen werden. Dieser Wert ist nur noch interessant, wenn Kassensysteme mit geringem Datenvolumen an Hostsysteme angeschlossen werden. Die Telekom verwendet je nach Anschlussart und Übertragungsgeschwindigkeit unterschiedliche Leitungsbezeichnungen für Datex-P-Anschlüsse (siehe Tabelle 3.1).

Leitung	Anschluß	Übertragungsrate
487	Datex-P10H	64 Kbps
492	Datex-P20H	1200 bps
493	Datex-P10H Datex-P20H	2400 bps
494	Datex-P10H	4800 bps
495	Datex-P10H	9600 bps
496	Datex-P10H	48 Kbps

Tabelle 3.1: X.25-Anschlüsse der Deutschen Telekom AG

Damit ein Teilnehmer internationale X.25-Rechner anwählen kann, muss er die entsprechende internationale Rufnummer wählen. Diese ist weltweit standardisiert und auf 14 Stellen begrenzt.

Es sind vier Stellen für die Netzkennzahl und zehn Stellen für die Rufnummer innerhalb des Netzes vorgesehen. Die ersten drei Ziffern der Netzkennzahl bilden die Landeskennzahl **DDC**, Data Country Code. Für den Bereich der Telekom ist dies die 262. Es folgt als letzte Ziffer die Datennetzkennzahl **DNIC**, Data Network Identification Code. Die Kennziffer für Datex-P ist eine Vier.

Damit ist die vollständige Netzkennung für das deutsche Datex-P-Netz die 2624.

Abbildung 3.38 zeigt den Aufbau der Rufnummer eines Datex-P-Teilnehmers.

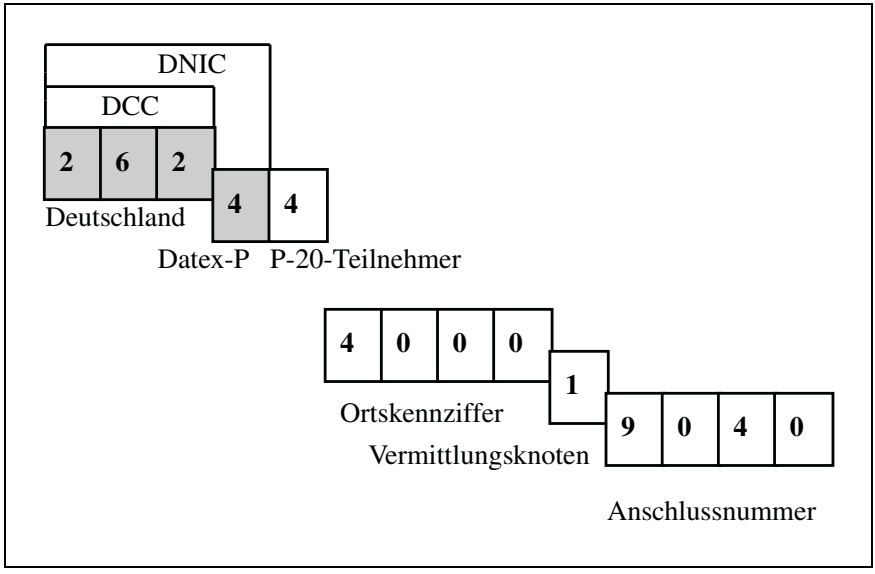


Abbildung 3.38: X.25-Rufnummer

Die nationale Rufnummer setzt sich zusammen aus einer zweistelligen Dienstkennummer, der Ortsnetzkennzahl, **ONKZ**, der Nummer des Vermittlungsknotens und der Anschlussnummer. Die Dienstkennummer besteht aus zwei Ziffern. Die erste Ziffer ist identisch mit der Netzkennung und damit mit der letzten Nummer der Netzkennzahl. Die zweite Ziffer kennzeichnet die Anschlussart. Für P10-Teilnehmer ist dies die fünf, für P20-Teilnehmer die vier. Damit sind die abgebildeten fünf ersten Ziffern einer internationalen Datex-P-Nummer wie folgt zu interpretieren:

26245 Deutscher Datex-P10-Anschluss

26244 Deutscher Datex-P20-Anschluss

Für internationale Verbindungen müssen Sie die Null als Kennziffer für internationale Verbindungen als Erstes eingeben. Dann folgt die Rufnummer mit dem oben beschriebenen Aufbau.

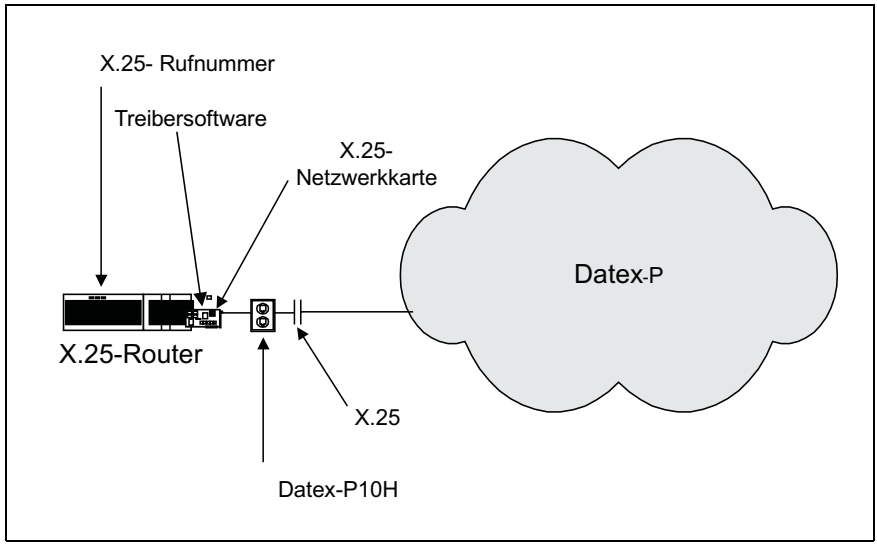


Abbildung 3.39: X.25-Router

3.7.3 Frame Relay

Frame Relay, **FR**, ist ein verbindungsorientiertes Protokoll, das folgende Vorteile bietet:

- ✔ Hohe (relativ) Geschwindigkeit
- ✔ Flexible Anschlusstechnik
- ✔ Kostengünstig

Diese Leistungsmerkmale bietet das Frame Relay Protokoll, weil es nur die unteren beiden Schichten des OSI-Modells abdeckt und zusätzlich auf der Schicht 2 auf eine Fehlerkorrektur verzichtet. Damit ist ein Frame Relay Netz insbesondere im Vergleich zu einem X.25-Netz schneller und technisch weniger aufwändig.

Schicht 1: Frame Relay sieht keine eigene physikalische Schnittstelle für die Bitübertragung vor. Vielmehr können alle Spezifikationen aus dem Bereich der Daten-kommunikation zum Einsatz kommen. Für den Kunden hat dies den Vorteil, dass er seine »alten Anschlüsse« behalten kann, wenn er auf Frame Relay umsteigt. Die Übertragungsgeschwindigkeit kann bis zu zwei Mbit/s betragen.

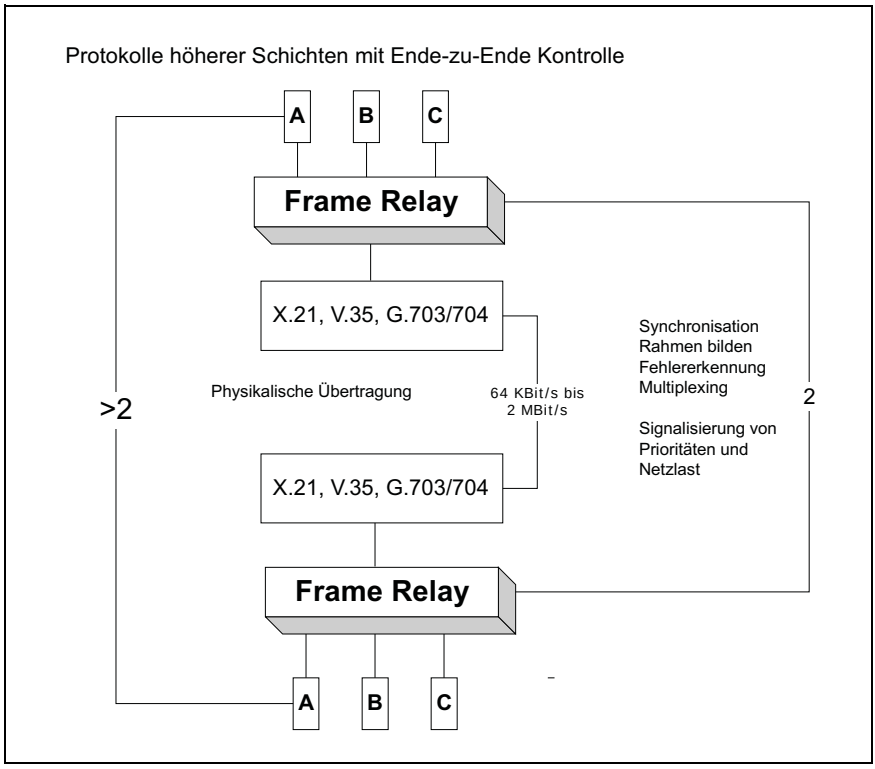


Abbildung 3.40: Architektur Frame Relay

Schicht 2: Die eigentliche Implementierung von Frame Relay erfolgt auf der Schicht 2, Fehlersicherung. Die hier typischen Frame Relay Funktionen sind:

- ✔ Die **Synchronisation** zwischen den Endgeräten. Dazu werden Flags ausgetauscht, die als Blockbegrenzer fungieren.
- ✔ Die Bildung des **Frame Relay Rahmens**, dessen Aufbau die folgende Grafik verdeutlicht.

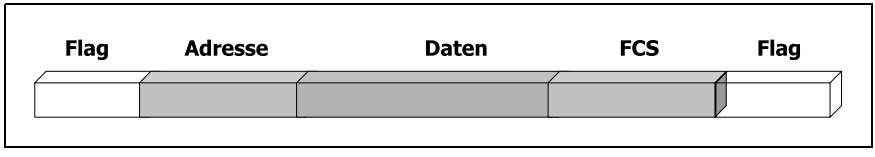


Abbildung 3.41: Frame Relay Rahmenstruktur

- ✔ **Fehlererkennung** mit Hilfe von Prüfsummen. Allerdings werden fehlerhaft erkannte Rahmen nicht korrigiert sondern verworfen.
- ✔ **Multiplexing** von bis zu 255 virtuellen Verbindungen.

Eigenschaften des Frame Relay Protokolls

Frame Relay verwendet Rahmen ohne Sende- oder Empfangsfolgenummern. Damit kann Frame Relay nicht überprüfen, ob Datenpakete verloren gegangen sind.

Aus diesem Grunde gibt es auch im Gegensatz zu X.25 keine Datenflusssteuerung über Sende- bzw. Empfangsfenster. Diese Funktionen müssen übergeordnete Schichten bei Sender und Empfänger übernehmen. Für das Protokoll bedeutet dies deutlich weniger Kontrollinformationen. Der Protokoll-Overhead ist im Vergleich zu X.25, das auf Schicht 2 und Schicht 3 mit Fenstertechnik arbeitet, so gering, dass insbesondere bei großen Datenpaketen Frame Relay wesentlich schneller übertragen kann. Voraussetzung sind allerdings gute Leitungen, damit möglichst wenige Datenpakete verloren gehen.

Variabel lange Informationsfelder führen zu einer weiteren Effektivitätssteigerung. Frame Relay kann Informationsblöcke mit mehreren Kilobyte transportieren. Ein Segmentieren und späteres Zusammensetzen der Datenpakete entfällt. Die folgende Tabelle zeigt für verschiedene Protokolle das Verhältnis zwischen Protokoll- und Nutzdaten.

Nutzdaten	Frame Relay	X.25	ATM
8 Byte z. B. Passwort	50 %	87,5 %	562,5 %
512 Byte	0,8 %	5,5 %	16,2 %
1500 Byte Ethernet 802.3	0,3 %	5,0 %	10,7 %

Tabelle 3.2: Effektivitätsvergleich Frame Relay, X.25 und ATM

Frame Relay ist in der Lage, die Datenübertragung an die Situation des Netzes anzupassen. Mit Hilfe von Statusbits können Prioritäten gesetzt oder netzinterne Lastzustände signalisiert werden.

Zwischen zwei Frame-Relay-Knoten kann je nach aktuellem Bedarf eine Bandbreite zugewiesen werden. Diese Technik wird Bandwidth on Demand oder Verkehrssteuerung genannt. Im Prinzip bedeutet dies, dass einer Verbindung mehr Übertragungskapazität zugewiesen werden kann, als »vereinbart« ist. Die Übertragungsleitung wird optimal genutzt.

Frame Relay unterscheidet zwischen:

- ✔ Verkehrssteuerung am Netzzugang und
- ✔ Netzinterner Verkehrssteuerung.

Am Netzzugang werden die Übertragungsraten mit Hilfe von FR-Parametern festgelegt. Die hierbei festgelegte Übertragungsrate, die unabhängig von der physikalischen Leitungskapazität ist, wird als **CIR**, Committed Information Rate, bezeichnet. Zusätzlich wird eine Committed Burst Size, **Bc**, vereinbart, die festlegt, wie hoch die Datenmenge zu einem bestimmten Zeitpunkt sein

darf. Spitzenbelastungen werden mit Hilfe einer weiteren Einstellung, der »zusätzlichen Datenmenge« abgefangen. Der entsprechende Parameter heißt **Be**, Excess Burst Size.

FR-Parameter können im Duplexbetrieb für die beiden Übertragungsrichtungen unterschiedlich gesetzt werden. Damit sind auch asymmetrische Verbindungen möglich.

Frame-Relay-Anschlüsse werden unter Umständen »überbucht«. Das bedeutet, dass die Summe aller mit CIR festgelegten Verbindungskapazitäten höher sein kann als die Übertragungskapazität der Anschlussleitung. Der Vorteil besteht darin, dass Hardware eingespart wird, allerdings um den Preis möglicher Kollisionen.

Wie die folgende Grafik zeigt, können Datenpakete anderer Protokolle in FR-Frames gekapselt werden. Die Technik des FR Multiprotocol Encapsulating bedeutet in diesem Zusammenhang, dass verschiedene Protokolle über die gleiche Verbindung gekapselt werden.

Internetworking mit Frame Relay

Frame Relay bietet aufgrund seiner Architektur große Vorteile bei der Kopplung lokaler Netzwerke oder Rechnerarchitekturen. Die typische Konstellation ist hier gekennzeichnet durch hohe Datenlast im lokalen Bereich und einen niedrigen Durchschnittswert zwischen den via Frame-Relay verbundenen Segmenten. Hier kommt es aber zu hohen Durchsatzspitzen, burstartigem Datenverkehr, der durch zusätzlich vereinbarte Datenmengen abgefangen werden können, wenn diese die vereinbarte Übertragungsrate überschreiten.

Die Schnittstelle zwischen Datenendeinrichtung und dem Frame-Relay-Netz wird **FR-UNI** Frame Relay User Network Interface genannt. Abbildung 3.42 zeigt unterschiedliche Implementierungen der FR-UNI. Das LAN ist über einen ISDN-Anschluss mit 64000 Bit/s angeschlossen, der Host über X.21. Im Router ist hier eine X.25-Karte eingebaut.

Im gezeigten Beispiel werden die Router über die **DLCI** global adressiert. Der Data Link Connection Identifier ist Bestandteil des Adressfeldes und belegt zehn Bit. Er dient zur Adressierung einer Frame-Relay-Verbindung auf der Anschlussleitung. Bei einer globalen Adressierung hat die DLCI eine netzweite Bedeutung und kann nur einmal vergeben werden.

Frame Relay lässt auch eine lokale Adressierung zu. In diesem Fall ist die DLCI nur lokal eindeutig und kann in anderen nichtöffentlichen Netzen mehrmals verwendet werden.

Für die interne Vermittlung kann der Betreiber der via Frame Relay verbundenen LANs ein eigenes Protokoll oder Frame Relay nutzen. Im gezeigten Beispiel werden die Daten intern entweder über Ethernet weitergeleitet oder via SNA/SDLC.

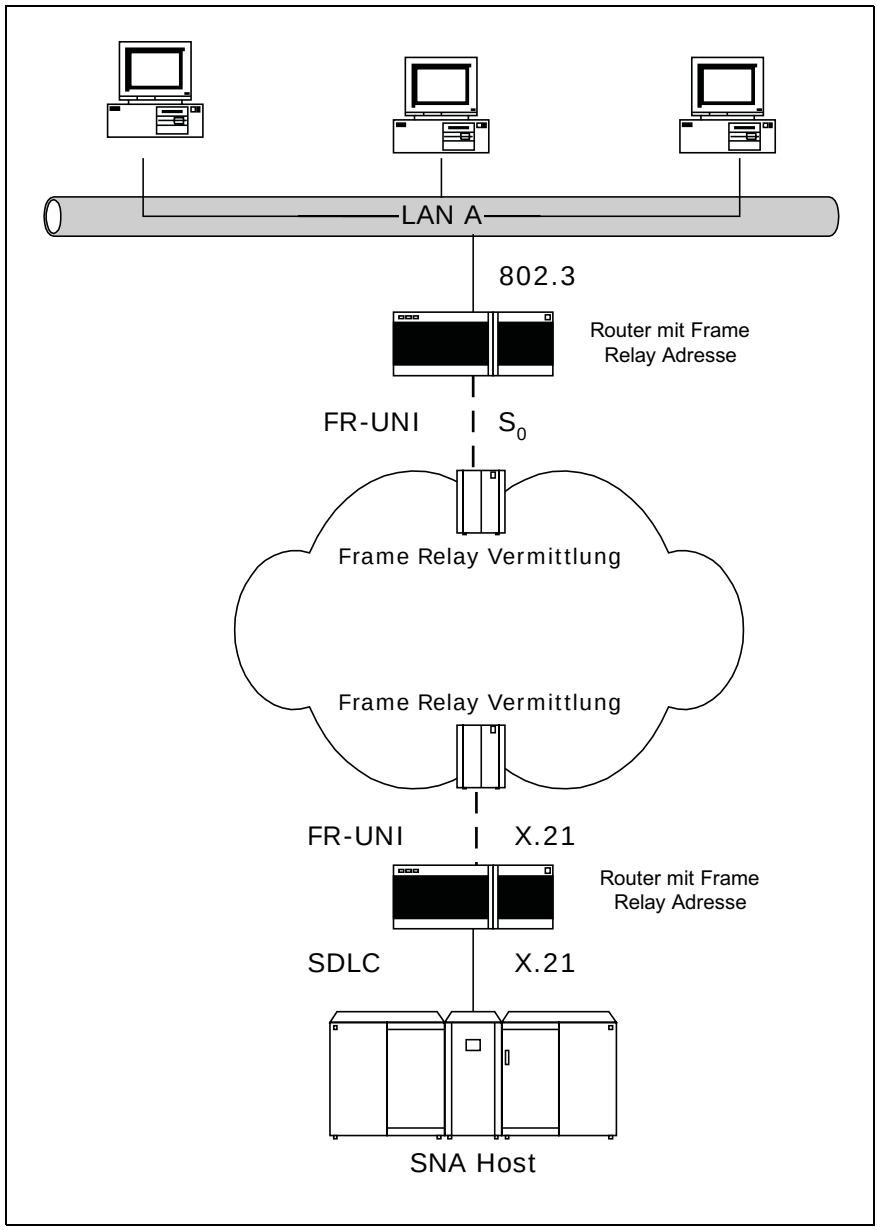


Abbildung 3.42: Internetworking mit Frame Relay

3.7.4 ATM

ATM, Asynchron Transfer Mode, ist eine Vermittlungstechnologie, die für jede Form der Datenübertragung, LAN oder WAN, und für jedes Datenformat, Sprache, Bild und Daten, geeignet ist. Damit unterscheidet ATM sich wesentlich von den bereits oben beschriebenen Techniken.

In den folgenden Abschnitten werden die wichtigsten Details zu ATM beschrieben. Dabei wird deutlich, warum der Einsatz von ATM-Technologien in einem LAN nur mit großem technischen Aufwand realisierbar ist. Aus der Sicht des Netzadministrators sind in diesem Zusammenhang folgende Merkmale relevant:

- ✔ Sehr hohe Übertragungsgeschwindigkeiten
- ✔ Frei wählbare Bandbreite am Anschluss
- ✔ Daten werden als Zellen, nicht als Pakete, übertragen
- ✔ Multiplexing
- ✔ Switching-Technologie
- ✔ Quality of Services
- ✔ Punkt-zu-Punkt-Verbindungen

ATM als WAN-Technologie

ATM Netzwerke sind wie ein Telefonnetz aufgebaut. Das bedeutet, dass jedes Endgeräte über eine »Telefonnummer« adressiert wird. Die öffentlichen ATM-Nummern sind weltweit standardisiert und einmalig. Innerhalb eines geschlossenen Netzes können auch »private« Nummern vergeben werden. ATM-Adressen sind also logische Adressen.

Die Vermittlungsstellen eines ATM-Netzes werden Switches genannt.

Auch der Verbindungsaufbau über ATM gleicht dem des Telefonnetzes. Zuerst wird eine Verbindung zur Gegenstelle geschaltet, dann erst werden die Daten übertragen. Dies ist ein entscheidender Unterschied zu den verbindungslosen Übertragungstechniken in einem LAN.

ATM wird von den großen Telekomgesellschaften vor allem als Backbone-Technologie eingesetzt. Die Schnittstelle zu den Nutzern kann variabel gehalten werden und liegt zwischen 1,54 Mbits/s und 2,5 Gbit/s. D.h. der Kunde kann in der Regel genau die Bandbreite ordern, die er für seine Anwendung benötigt.

Der Zugang zu einem ATM-Netz heißt in der Fachterminologie User Network Interface, **UNI**. Man unterscheidet private und öffentliche UNI. Die Schnittstelle zwischen den Switches im ATM heißt **NNI**, Network Network Interface, manchmal auch Network Node Interface.

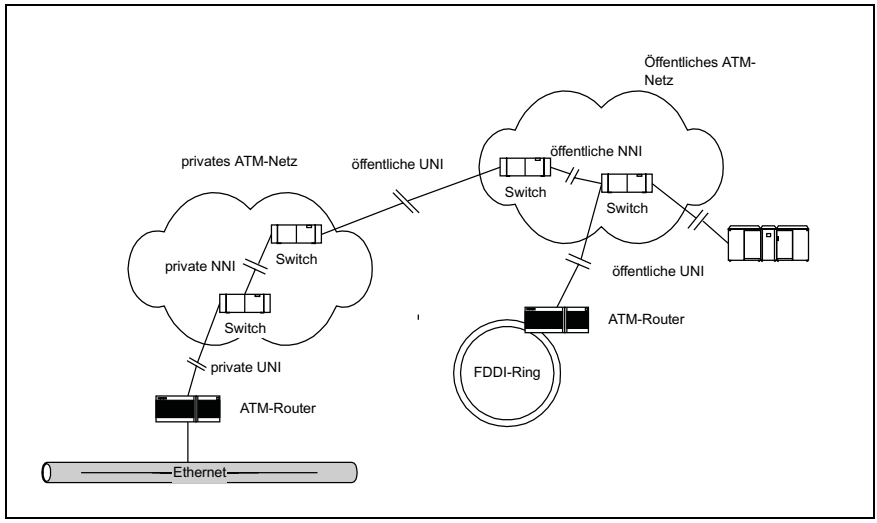


Abbildung 3.43: ATM als WAN-Technologie

ATM Zellen

ATM Daten werden in Paketen mit je 53 Byte übertragen. Diese Pakete werden Zellen genannt. Die Zellgröße ist ein Kompromiss zwischen Sprach- und Datenübertragung. Je kleiner Datenpakete sind, desto vorteilhafter ist dies für Sprachübertragung, während für die Datenübertragung große Pakete von Vorteil sind.

Die ATM-Zelle besteht aus einem fünf Byte großen Header und dem 48 Byte großen Informationsteil. Im Header sind alle für die Adressierung erforderlichen Informationen enthalten. Es sind dies:

- ✔ Routinginformationen, **VCI** und **VPI**
- ✔ Informationen über den Typ der Daten, **PT** Payload Type
- ✔ Informationen zur Datenflusssteuerung, **GFC**, Generic Flow Control und **C** Cell Loss Priority
- ✔ Fehlerbehandlung, **HEC**, Header Control

Die **VCI**, Virtual Channel Identifier, beinhaltet eine 16 Bit lange Adressinformation, die einen Verbindungsabschnitt, virtueller Kanal genannt, kennzeichnet. Diese Adresse wird vom beteiligten Vermittlungsknoten, dem Switch, vergeben. **VPI**, Virtual Path Identifier, bezeichnet einen Pfad bestehend aus den virtuellen Kanälen zwischen Sender und Empfänger.

Der Einsatz von VPI hat den Vorteil, dass bestimmten Anwendungsklassen, z.B. Videoübertragung, bestimmte VPIs zugewiesen werden können. Diese können dann mehrere VCIs für die Anwendung definieren.

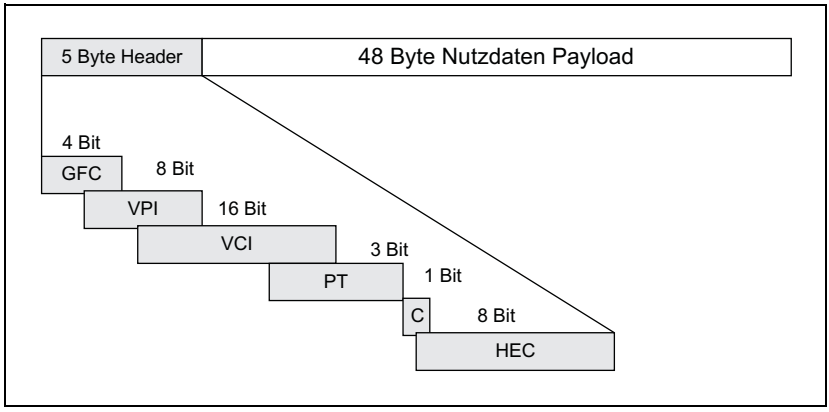


Abbildung 3.44: ATM-Zelle

Im **GFC**-Feld wird der Verkehrsfluss gesteuert. Damit wird ein Endgerät in die Lage versetzt, Überlastungen anzuzeigen und den Datenfluss aus dem ATM-Netz eventuell zu stoppen. Das GFC-Feld wird nur an der UNI genutzt, also dort, wo der Übergang vom ATM-Netz zum Endgerät erfolgt.

Im Feld Header Control, **HEC**, wird eine 8-Bit Prüfsumme berechnet, um Übertragungsfehler erkennen zu können. Das C-Bit kodiert die Priorität einer Zelle.

ATM-Verbindungen können permanent, dann spricht man von **PVC**, Permanent Virtual Connection, oder nur für die Dauer einer Sitzung aufgebaut werden, Switched Virtual Connection, **SVC**. PVCs werden in der Regel manuell vom Administrator konfiguriert. Dazu werden die benötigten VPI/VCI-Werte eingestellt und die erforderlichen Ressourcen »gebucht«. Switched Connections werden von ATM über entsprechende Steuerbefehle aufgebaut.

ATM Adaption Layer – Schnittstellen zu höheren Schichten

Das wesentliche Ziel der ATM-Technologie ist es, einen einheitlichen schnellen Transportdienst für beliebige Anwendungen zur Verfügung zu stellen. Dies hat Konsequenzen für die Architektur von ATM. Das ATM-Referenzmodell sieht drei Schichten vor, wobei Layer 3 die Schnittstelle zu den Anwendungen darstellt.

Die eigentliche ATM-Technologie liegt auf Layer 2. Hier werden die Informationen des ATM-Headers ausgewertet und entsprechende Mechanismen wie z. B. die Wegewahl in Gang gesetzt.

Auf der untersten Schicht isoliert der Sublayer **TC** die ATM-Schicht vom verwendeten Medium. Deshalb können für ATM unterschiedliche Medien wie Glasfaser, Kupferkabel oder Funkstrecken genutzt werden. Auf der **AAL**-Schicht, ATM Adaption Layer, sind die Diensteklassen beschrieben. Wichtig ist, dass über diese Klassen die Qualität eines Dienstes garantiert wird. Durch die Beschreibung der Klasse können alle benötigten Ressourcen abgeleitet und in bzw. von den betroffenen Switches »gebucht« werden.

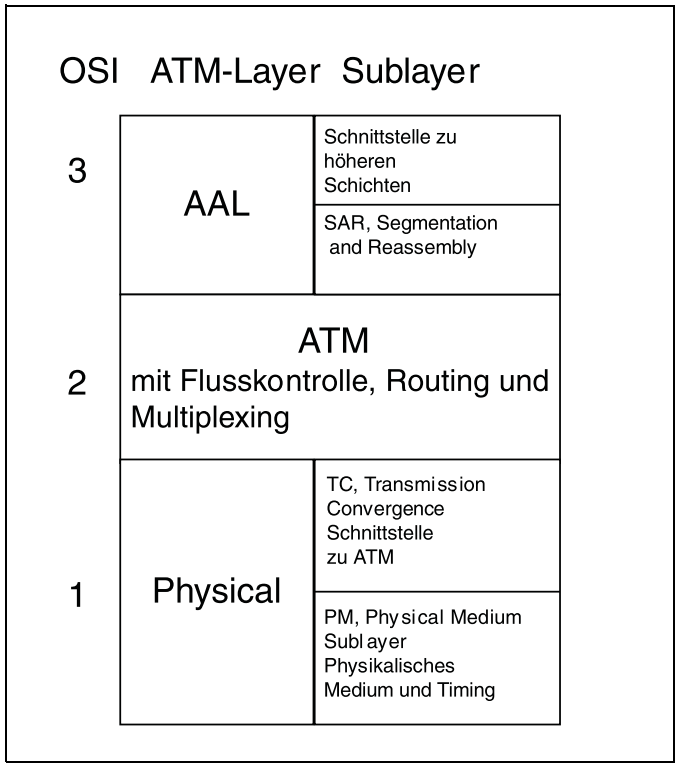


Abbildung 3.45: ATM-Referenzmodell

Die folgende Tabelle gibt einen Überblick.

Adaption Layer	Aufgabe
AAL-Type 1	Zeitkontinuierliche Dienste mit fester Übertragungsrate, z. B. Sprache
AAL-Typ 2	Zeitkontinuierliche Dienste mit variabler Übertragungsrate, z. B. komprimierte Videos
AAL-Typ 3, 5	Gesicherte, verbindungsorientierte Datenübertragung
AAL-Typ 4	Verbindungslose Datenübertragung

Tabelle 3.3: ATM Adaption Layer im Überblick

Die ATM-Norm definiert zusätzlich vier ALL-Dienstklassen, deren Merkmale in der folgenden Tabelle zusammengefasst sind. Die Klassen von A bis D werden wiederum den verschiedenen ALL-Typen zugeordnet.

AAL Klasse	A	B	C	D
Zeitbezug zwischen Quelle und Ziel erforderlich	X	X		
Bitrate konstant	X			
Verbindungsorientiert	X	X	X	
AAL-Typ	1	2	3 / 4, 5	5

Tabelle 3.4: ATM Adaption Layer im Überblick.

Auf den ersten Blick erscheint AAL Typ 4 als die Technik zur Integration von ATM in die verbindungslose LAN-Welt. Dies ist allerdings nicht der Fall. Wird ATM in einem LAN eingesetzt, dann wird ALL-Typ 5 als Schnittstelle genutzt. Die folgende Grafik zeigt dies am Beispiel der LAN Emulation LANE.

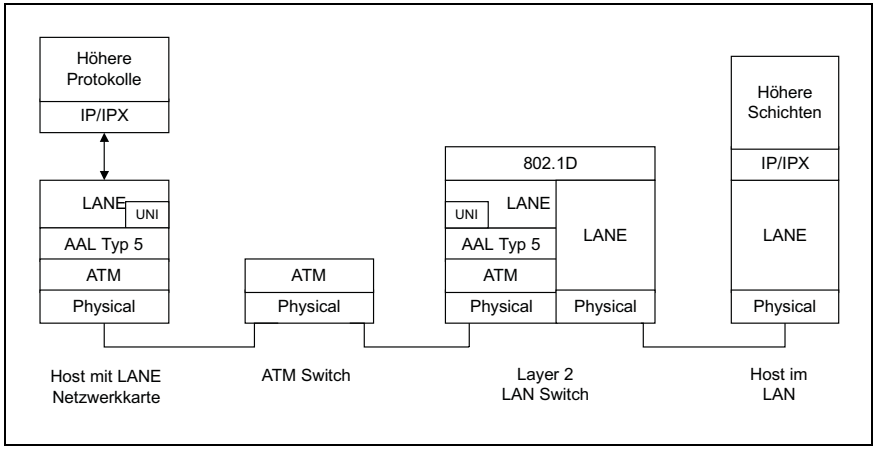


Abbildung 3.46: LANE-Referenzmodell

Abbildung 3.46 vermittelt einen ersten Eindruck davon, wie komplex sich der Einsatz von ATM in einem LAN gestaltet. Hier besitzt Gigabit Ethernet eindeutig Vorteile. Relativ einfach ist es, ATM als Backbone einzusetzen. Die Komponenten, die dann den Übergang vom Backbone zum LAN darstellen, werden Edge Device oder Edge System genannt.

3.7.5 XDSL – Digital Subscribers Line

DSL, Digital Subscribers Line, ist eine Technik, die auf einer Entfernung von drei bis sechs Kilometern eine Bandbreite von bis zu sieben Mbit/s zur Verfügung stellen kann. DSL ist damit eine Alternative zu ISDN oder zu schnellen V.90-Modems in analogen Telefonnetzen und gewinnt seine Bedeutung vor allem im Hinblick auf die schnelle Anbindung des Users an das Internet oder aber auch an ein internes Netz via Internet, Virtual Private Networks.

Es gibt nun verschiedene Anschlussvarianten für DSL. Aus diesem Grund wird die gesamte Technikpalette auch als **xDSL**-Technologie bezeichnet.

Wichtig ist, dass xDSL genau wie das ISDN die gleichen Leitungswege nutzt, die bereits für das analoge Telefonnetz installiert sind. Die xDSL-Technologie bietet daher insbesondere Telefongesellschaften und Internet-Providern die Möglichkeit, kostengünstig auch die »letzte Meile« zum Kunden zu überwinden.

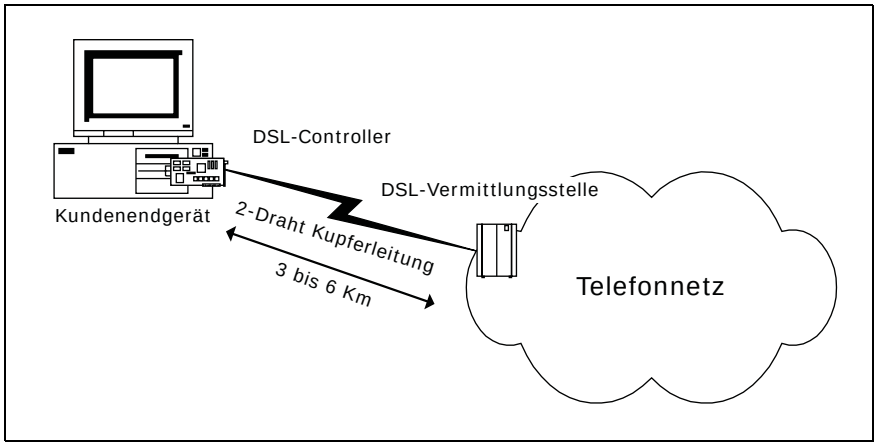


Abbildung 3.47: DSL-Architektur

Die xDSL-Technologie ist sehr variabel. Provider können deshalb unterschiedliche Anschlussvarianten anbieten. Dazu wird die vorhandene Bandbreite in drei Kanäle unterteilt:

Kanal 1 Sprachübermittlung

Kanal 2 Vom Anwender zum Serviceleister, upstream

Kanal 3 Vom Serviceleister zum Anwender, downstream

Die Übertragungskapazität kann asymmetrisch verteilt werden. So macht es Sinn, für downstream höhere Bandbreiten zur Verfügung zu stellen. Dies gilt insbesondere im Hinblick auf das Internet oder Online-Dienste. Hier werden vom Nutzer wesentlich weniger Daten zum Provider bzw. Host übertragen als umgekehrt.

DSL-Varianten sind:

- ✔ **IDSL** ISDN Digital Subscriber Line
- ✔ **SDSL/SDSL2** Symmetric Digital Subscriber Line
- ✔ **ADSL** Asymmetric Digital Subscriber Line
- ✔ **RADSL** Rate Adaptive ADSL
- ✔ **HDSL** High-Date Rate DSL
- ✔ **VDSL** Very High-Speed DSL

IDSL nutzt für die Datenübertragung wie das ISDN ein Verfahren, das die Übertragungsstrecke in zwei 64.000 Bit Nutzkanäle unterteilt. Der Dienstleister benötigt aber keine ISDN-Vermittlungstechnik wie z.B. eine Ortsvermittlung. IDSL ist in der Lage, Sprach- und Datendienste zum Vermittlungsrechner zu übertragen, die dann dort als Sprache bzw. Daten in getrennte Netze weitergeleitet werden. SDSL unterscheidet sich von ADSL durch die gleiche Übertragungsrate in up- und downstream. SDSL arbeitet mit zwei Kupferleitungen, bei SDSL2 sind es vier. Dies erklärt die höhere Übertragungsrate. RADSL bedeutet, dass eine automatische Anpassung an die Leitungsqualität erfolgt, rate adaptive. HDSL ist eine Weiterentwicklung des ISDN. VDSL ist wiederum eine Weiterentwicklung des HDSL auf der Basis von Glasfaserleitungen.

xDSL	Upstream	Downstream	Leitungslänge
SDSL	768 Kbit/s	768 Kbit/s	4 km
SDSL2	1,54 Mbit/s	1,54 Mbit/s	4 km
ADSL	640 Kbit/s	6,14 Mbit/s	4 km
	176 Kbit/s	1,54 Mbit/s	6 km
RADSL	544 Kbit/s	640 Kbit/s	5 km
	1,0 Mbit/s	2,5 Mbit/s	4 km
	1,0 Mbit/s	7,0 Mbit/s	3 km
HDSL	1,54 Mbit/s	1,54 Mbit/s	5 km
VDSL	2,3 Mbit/s	52 Mbit/s	1 km

Tabelle 3.5: xDSL in der Übersicht

3.8 Backbone

3.8.1 Distributed Backbone

Dies ist die klassische Lösung für eine Segmentierung des Netzes. Einzelne Netze, z.B. Ethernet-Netze werden durch Brücken oder Router voneinander getrennt bzw. miteinander verbunden.

Als Verbindung zwischen den Teilnetzen dient ein eigenes LAN, der so genannte Backbone, das Rückgrat des Netzes. Im einfachsten Fall ist dies ein klassisches Ethernet mit entsprechend geringer Übertragungsrate. In der Regel werden jedoch schnellere Übertragungstechniken gewählt, beispielsweise FDDI.

Nur die Daten, die für andere Teilnetze bestimmt sind, werden über den Backbone zu dem entsprechenden Teilnetz übertragen. Der Vorteil dieser Lösung ist eine relativ hohe Ausfallsicherheit. Die Störung einer Komponente beeinträchtigt in der Regel nicht das gesamte Netz.

Entscheidende Nachteile sind die vergleichsweise hohen Kosten, da für jeden Netzübergang relativ teure Komponenten angeschafft werden müssen, insbesondere bei FDDI. Bei Umrüstung des Backbone müssen außerdem alle Komponenten auf die neue Technologie umgestellt werden.

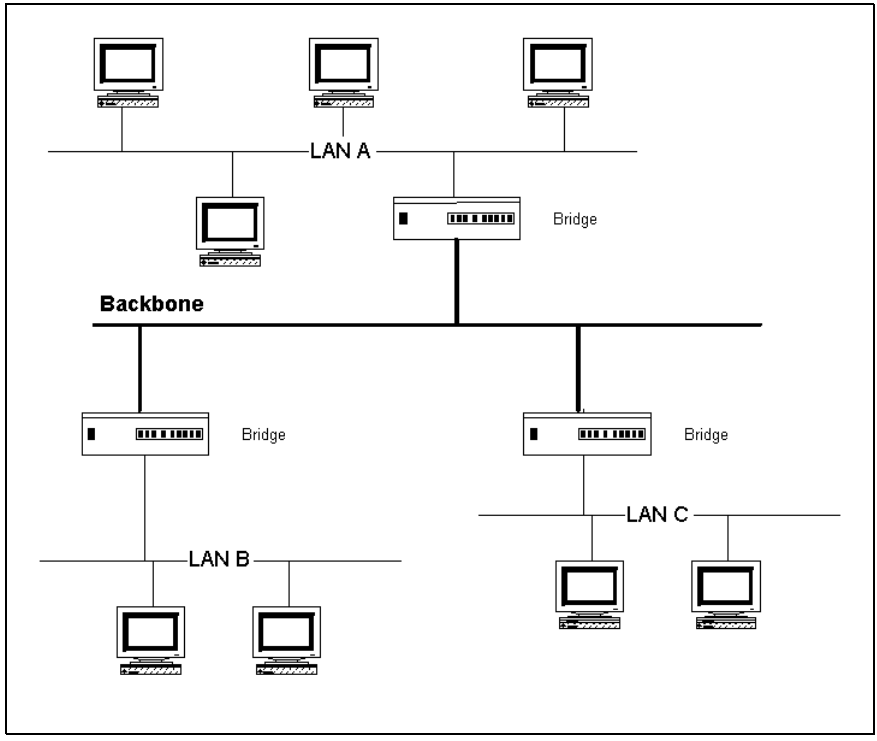


Abbildung 3.48: Distributed Backbone

In der Abbildung 3.48 wird ein klassisches Ethernet-Backbone dargestellt. Mehrere LANs werden über Bridges auf ein zentrales Backbone, hier vergrößert dargestellt, gekoppelt. Die Brücken sorgen dafür, dass auf dem Backbone nur netzübergreifende Daten übertragen werden.

Jedes Datenpaket, das von einem Teilnetz in ein anderes übertragen wird, muss mindestens über zwei Komponenten vermittelt werden. Engpässe in der Übertragung entstehen bei dieser Netzkonfiguration meist durch Laufzeitverzögerungen oder durch Überlastung der Netzkomponenten und damit verbundene Datenverluste.

3.8.2 Collapsed Backbone

Diese Lösung entstand mit der Entwicklung von Hochleistungskomponenten mit sehr leistungsfähigen integrierten Bussystemen (Backplanes). Der Trick bei dieser Lösung ist, dass der Backbone innerhalb einer zentralen Komponente realisiert wird. Hierdurch können Übertragungsraten realisiert werden, die um ein Vielfaches über denen der verfügbaren Übertragungstechniken liegen. Bandbreiten von mehreren Gbit/s werden hier von unterschiedlichen Herstellern angeboten.

Als Schnittstellen bieten diese Geräte in der Regel alle gängigen Übertragungsverfahren wie Ethernet, Token Ring, FDDI und zum Teil auch bereits ATM an. In der Regel können auch die WAN-Verbindungen mit diesen Geräten realisiert werden.

Der Vorteil dieser Lösung ist der meist günstige Preis für eine extrem hohe Bandbreite des Backbones. Außerdem muss ein Datenpaket, das von einem Teilnetz in ein anderes übertragen werden soll, nur eine Komponente passieren.

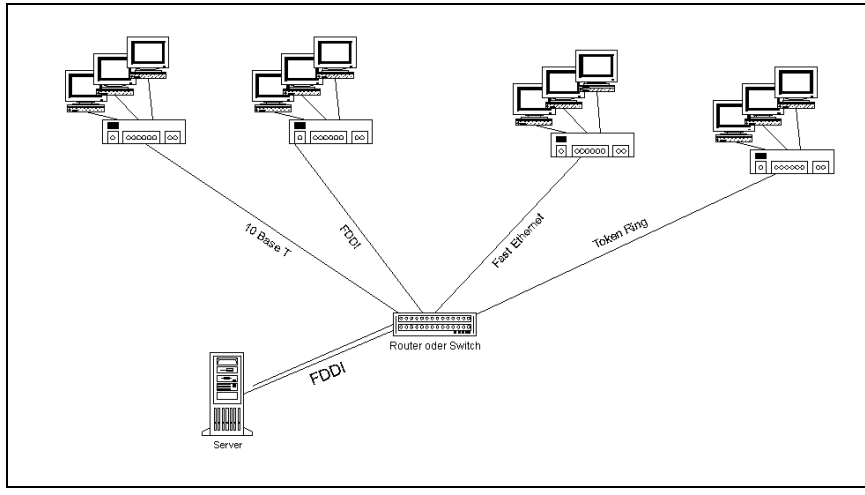


Abbildung 3.49: Collapsed Backbone

Der entscheidende Nachteil dieser Lösung ist der »Single Point of Failure«. Fällt diese zentrale Komponente aus, steht normalerweise das ganze Netz. Mindestens ist jedoch keinerlei Kommunikation zwischen den Netzen mehr möglich. Zusätzlich ist wegen des hohen Preises dieser Komponente die Vorhaltung einer Ersatzkomponente sehr aufwändig. Das Problem wird durch entsprechende Konzeption der Geräte mit redundanten Netzteilen für getrennte Stromkreise, unterbrechungsfreien Stromversorgungen, rein passivem Backplane, Netzmanagement, eigenen Prozessoren auf jeder Einschubkarte etc. teilweise kompensiert. Ein gewisses Restrisiko bleibt jedoch.

3.8.3 ATM Backbone

Ein ATM-Backbone kann in der einfachsten Konstellation aufgebaut werden, wie der Collapsed Backbone. Die zentrale Komponente ist in diesem Fall ein ATM-Switch und die Verbindung zu den Komponenten in den Verteilern erfolgt in ATM-Technik. Der entscheidende Vorteil eines ATM-Backbones ist, dass ohne Wechsel des Übertragungsprotokolls, lediglich durch Austausch der Netzwerkkarten die Übertragungsgeschwindigkeit einer Verbindung verändert werden kann.

Außerdem können vermaschte Strukturen durch Verwendung weiterer ATM-Switches sehr leicht implementiert werden. Damit ist eine redundante Wegewahl möglich und die Ausfallsicherheit des Netzes steigt

Das Einbinden von Workstations oder Servern in das ATM-Netz ist ebenfalls relativ problemlos zu bewältigen. Je nach benötigter Übertragungsrate bzw. Verfügbarkeit von Adaptern können ATM-Adapterkarten direkt in die Systeme eingebaut werden.

KAPITEL 4

4 TCP/IP

In diesem Kapitel erhalten Sie einen Überblick über die unter dem Oberbegriff TCP/IP zusammengefassten Protokolle, die die Infrastruktur des Internets bilden. TCP/IP ist auch die Schlüsseltechnologie für lokale Netzwerke. Der Aufbau von Intranets setzt diese Protokolle zwingend voraus, und der aktuelle Trend zeigt eindeutig, dass TCP/IP zum alleinigen Standard für den Betrieb »traditioneller« LANs wird.

4.1 Grundlagen

Um die Begrifflichkeit und Zusammenhänge der TCP/IP-Protokolle zu verstehen, muss man sich vor Augen halten, dass diese Technik fast 30 Jahre alt ist. Damals wurde eines der ersten größeren Rechnernetze überhaupt, das ARPANET, entwickelt.

Ziel war der Aufbau eines Netzwerkes, das auch dann noch funktioniert, wenn große Teile der Infrastruktur zerstört sind. Gleichzeitig sollten auch unterschiedliche Rechnerarchitekturen miteinander kommunizieren können. Eine Konsequenz dieser Überlegungen war der Aufbau einer paketvermittelten Technologie, in der, im Unterschied zu einem leitungsvermittelten Netz, keine direkte Verbindung zwischen Quelle und Ziel geschaltet werden muss. Die Daten werden in einem paketvermittelten Netz über unterschiedliche Wege zum Empfänger geleitet. Dazu wird der Datenstrom in voneinander unabhängige Pakete aufgeteilt. Diese werden im Transportnetz von Vermittlungsstelle zu Vermittlungsstelle weitergereicht, bis sie an das Zielnetzwerk übergeben werden können.

Die im ARPANET verwendete Terminologie unterscheidet zwischen dem Kommunikationsaspekt, das ist das Leitungssystem oder auch subnet, und dem Anwendungsaspekt, das sind die verbundenen Rechner, die hier Host genannt werden.

Das Leitungssystem besteht aus zwei Komponenten, den Übertragungsleitungen, auch Schaltkreise, circuits, Kanäle, channels, oder Verbindungsleitungen, trunks, oder Links genannt, und den Schalteinheiten. Das sind Computer, die speziell dazu verwendet werden, zwei oder mehr Übertragungsleitungen miteinander zu verbinden. Diese Schalteinheiten wurden auch als **IMP**, Interface Message Processor, Datenvermittlungsstelle, Data Switching Exchange, oder als Transitsystem bezeichnet.

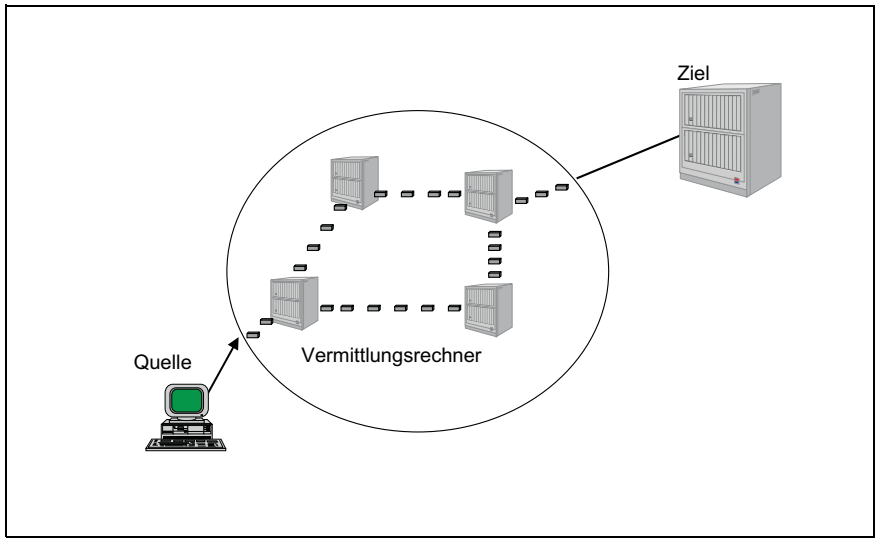


Abbildung 4.1: Paketvermittlung

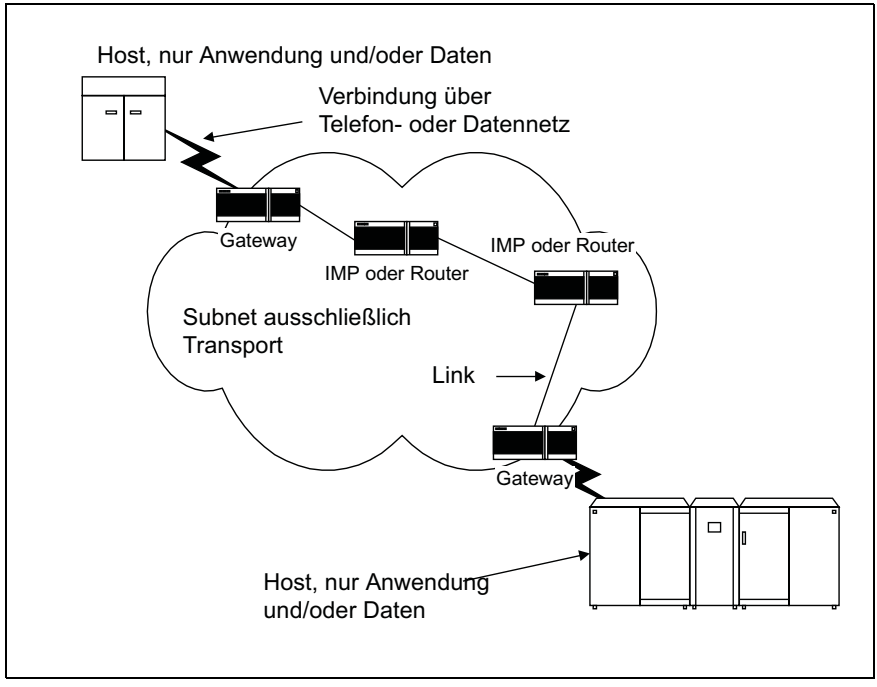


Abbildung 4.2: Das ARPANET – Vorgänger des Internets

Abbildung 4.2 zeigt den Aufbau des ARPANETS. Heute werden die IMPs auch als Router bezeichnet, und der erste Zugangsrechner zum Subnet heißt Gateway. Unverändert geblieben ist die Bezeichnung der Endknoten als Host, unabhängig davon, ob es sich um einen Großrechner, einen PC oder einen Drucker handelt.

In der Terminologie des TCP/IP ist jede Station, die an das Subnet angeschlossen ist, ein Host, alle Rechner im Subnet haben nur eine einzige Aufgabe, das Weiterleiten von Daten bis zum Ziel-Host. Transport und Anwendung werden getrennt. Der Host ist an das Netz angeschlossen und nicht Bestandteil des Netzes. Dies ist wichtig für das Verständnis der folgenden Kapitel.

4.2 TCP/IP – eine Protokollfamilie

Wie bereits aus der Bezeichnung Protokollfamilie ersichtlich ist, handelt es sich bei TCP/IP, Transmission Control Protocol / Internet Protocol, nicht nur um die beiden Protokolle TCP und IP, sondern um eine kompakte Protokollfamilie mit einer Vielzahl von unterschiedlichen Protokollen. Sämtliche Protokolle dieser Protokollfamilie wurden im Laufe der Jahre für die unterschiedlichsten Aufgaben in WANs, Wide Area Network, konzipiert und dabei ständig weiterentwickelt.

Darüber hinaus haben sich die unter dem Oberbegriff »TCP/IP-Protokolle« subsumierten Protokolle als Standardprotokolle im Internet durchgesetzt und stellen damit auch einen Industriestandard im Bereich der Kommunikation zwischen Computersystemen unterschiedlicher Hersteller dar.

Entstanden ist die TCP/IP-Protokollsuite Ende der 60er und Anfang der 70er Jahre. Erstmals realisiert im November 1969 bei der US-Behörde ARPANET, Advanced Research Agency Network, unter Verwendung von NCP, Network Control Protocol, zur Kommunikation zwischen den einzelnen Hosts.

Die wichtigsten Eckdaten zur Entwicklungsgeschichte von TCP/IP sind:

1970	NCP als Kommunikationsprotokoll wird bei der US-Behörde ARPANET eingesetzt.
1972	»Ad hoc Telnet Protocol« wird als erste Telnet-Spezifikation unter RFC 318 festgelegt.
1973	»File Transfer Protocol« wird unter RFC 454 festgelegt.
1974	TCP wird detailliert festgelegt.
1981	»Internet Protocol« wird unter RFC 791 festgelegt.
1982	ARPA und DCA, Defense Communications Agency, legen TCP und IP als TCP/IP-Protokollfamilie fest.
1983	TCP/IP ersetzt das Kommunikationsprotokoll NCP bei der US-Behörde ARPANET.
1984	Einführung von DNS, Domain Name System.

4.3 DoD-Architektur und Schichten

Bereits vor der Realisierung des OSI-Modells regte das **DoD**, Department of Defense, eine Standardisierung im Bereich heterogener Netze an. Diese Standards werden von der **DCA**, Defense Communications Agency, regelmäßig veröffentlicht. Im Einzelnen handelt es sich hierbei um das vierschichtige DoD-Modell oder TCP/IP-Vierschichtenmodell. Dieses Modell beinhaltet Regeln und Normen über die Funktionsweise der Kommunikation zwischen einzelnen Computern in einem Netzwerk. Beschrieben werden eine Netzwerkschnittstelle, eine Internet-, eine Transport- und eine Anwendungsschicht.

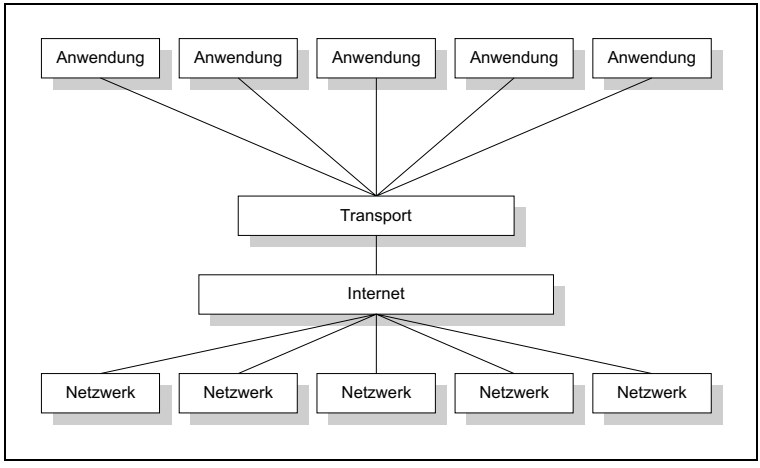


Abbildung 4.3: DoD-Schichtenmodell

Die Grafik 4.4 zeigt eine andere Sichtweise des eben beschriebenen Modells. Sie sehen hier einige der wichtigsten Protokolle der einzelnen Schichten.

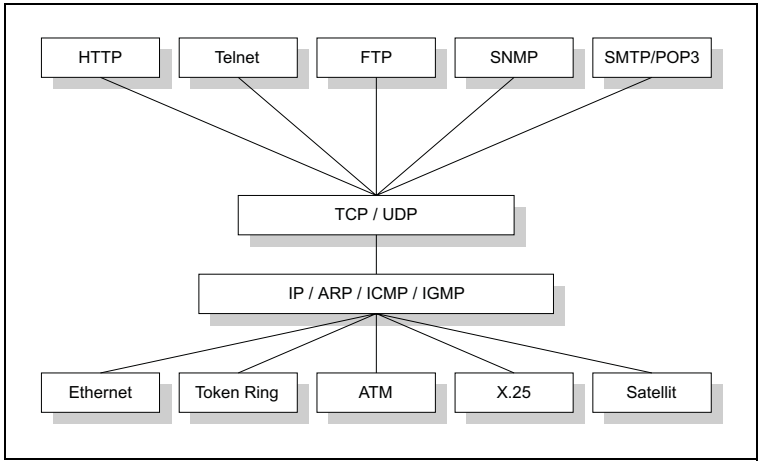


Abbildung 4.4: DoD-Protokolle und Schichten

Der wesentliche Unterschied zum OSI/ISO Modell besteht darin, dass die TCP/IP-Architektur keinerlei Aussagen zur Beschaffenheit des vorhandenen Netzwerkes macht. Mit anderen Worten, die Layer 1 und 2 des OSI-Modells werden als vorhanden vorausgesetzt. TCP/IP-Protokolle gibt es nur für die drei oberen Schichten. Damit können TCP/IP-Protokolle in jedem Netzwerk eingesetzt werden. Will man DoD-Modell und OSI vergleichen, dann ergibt sich folgendes Bild:

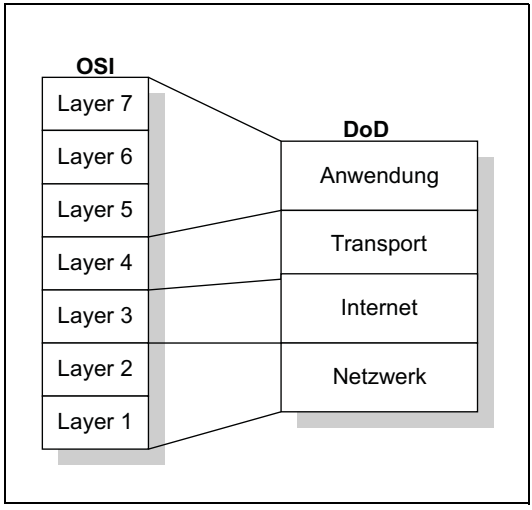


Abbildung 4.5: Vergleich DoD und OSI

Wann immer Daten über das Internet oder im Intranet gesendet werden, müssen sie zuerst den TCP/IP-Protokoll-Stack durchlaufen. Innerhalb des TCP/IP-Protokoll-Stacks stehen wiederum verschiedene Möglichkeiten zur Verfügung. So kann die Anwendungsschicht entweder direkt auf die Vermittlungsschicht zugreifen oder über die Transportschicht laufen.

Greift die Anwendungsschicht auf die Transportschicht zu, so kommuniziert die Anwendung wahlweise mit dem Transmission Control Protocol, TCP, oder dem User Datagram Protocol, UDP. Erfolgt die Kommunikation jedoch direkt über die Vermittlungsschicht, so kommuniziert die Anwendung mit dem Internet Protocol, IP, oder dem Internet Control Message Protocol, ICMP, das wiederum mit IP kommuniziert.

Aber egal, welche Route die Daten passieren, sie müssen immer über das Internet Protocol laufen.

4.3.1 Netzwerkschicht

Die Netzwerkschnittstellenschicht bildet die Plattform des Vierschichtenmodells. Die Zustellung von Informationspaketen zwischen Hosts am selben Netz ist die primäre Aufgabe dieser Schicht. Eine fehlergesicherte Übertragung der Daten erfolgt dabei auf einer höheren Ebene.

Für diese Schicht werden keine Standards vorgegeben. Damit setzt TCP/IP auf jeder beliebigen Netzwerktechnologie auf und ist ideal für den Einsatz in heterogenen Netzen. Für die Praxis bedeutet dies, dass es für jede Netzwerktechnologie, Ethernet, Token Ring, FDDI u.a. eine protokollspezifische IP-Implementierung gibt, die die jeweilige Zugriffsmethode berücksichtigt. Die Schnittstelle zu den Anwendungen, das TCP, ist immer die gleiche.

4.3.2 Internetschicht

Auf dieser Schicht finden sich vier Internet-Protokolle, die die notwendigen Routingfunktionen durchführen. D.h. alle erforderlichen Leitwegalgorithmen zur optimalen Wegesuche werden auf dieser Schicht ausgeführt. Die Routing-Protokolle sind im Einzelnen:

- ✔ IP, Internet Protocol
- ✔ ARP, Adress Resolution Protocol
- ✔ ICMP, Internet Control Message Protocol
- ✔ IGMP, Internet Group Management Protocol

4.3.3 Transportschicht

Abhängig von der verwendeten Datenquelle kommt entweder TCP oder UDP, User Datagram Protocol, als Transportprotokoll zum Einsatz. Diese beiden Protokolle ermöglichen erst die Kommunikationssitzungen zwischen einzelnen Computern. Darüber hinaus wird das Senden von Vorrangdaten ermöglicht. Auch die Datenflusskontrolle wird auf dieser fehlergesicherten Schicht realisiert.

Die Transportschicht ist auf den Hosts, nicht aber im Subnet implementiert.

4.3.4 Anwendungsschicht

Die Anwendungsschicht als die oberste Schicht im TCP/IP-Vierschichtenmodell realisiert für die einzelnen Anwendungen den Zugang zum Netz. HTTP, FTP, Telnet und andere stehen hier als TCP/IP-Diensteprogramme zur Verfügung.

4.4 Standardisierung der TCP/IP-Protokolle

Anders als bei vielen anderen Protokollen, die in der Regel nur von einem Hersteller entwickelt wurden, sind für die Entwicklung von TCP/IP mehrere Träger des Internets verantwortlich. Der Standardisierungsprozess selbst unterliegt einer internationalen Gruppe, der Internet Society, **ISOC**, die 1992 als globale Organisation gegründet wurde. Das Internet Activities Board, **IAB**, auch Internet Architecture Board genannt, verwaltet als eine Gruppe von technischen Beratern der ISOC die Standardisierung. Zu diesem Zweck leitet das IAB weitere Organisationen; die Internet Research Task Force, **IRTF**, die Internet Engineering Task Force, **IETF**, und die Internet Assigned Numbers Authority, **IANA**.

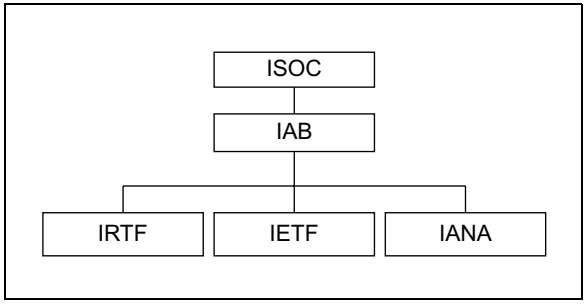


Abbildung 4.6: Standardisierungsgremien des Internets

Langfristige und grundsätzliche Ansätze zur Weiterentwicklung des Internets und somit auch die Weiterentwicklung von TCP/IP, erfolgen durch das IRTF. Diese Ansätze wiederum liefern dann die Basis für die eigentlichen Standards, realisiert durch das IETF. Eindeutige Protokollkennungen im Internet werden von der IANA koordiniert und überwacht.

Request for Comments – RFC

Über ein so genanntes Request for Comments, **RFC**, erfolgt die Standardisierung der TCP/IP-Protokollfamilie und des Internets. Ein RFC selbst stellt einen technischen Bericht des IAB über ein sich abzeichnendes oder bestehendes Problem im Internet dar und beschreibt somit auch den internen Ablauf des Internets.

Ist ein RFC einmal als Standard definiert worden, so wird bei einer notwendigen Änderung eines einzelnen keine Aktualisierung des ursprünglichen RFC vorgenommen. Vielmehr wird bei einer Änderung ein neues RFC mit einer neuen Nummer veröffentlicht. Dies erklärt auch die Tatsache, dass es mittlerweile über 2000 RFCs gibt.

Jedes Mitglied der Internet Society kann ein Dokument zur Veröffentlichung als RFC vorlegen. Aber nicht jedes RFC ist für TCP/IP relevant. Zudem finden viele RFCs in der heutigen Zeit keine Anwendung mehr, und viele wurden niemals veröffentlicht.

Einmal im Quartal publiziert das IAB ein Merkblatt mit dem Namen IAB Official Protocol Standard. Dieses Merkblatt beinhaltet die aktuellen RFCs für jedes Protokoll.

RFCs durchlaufen mehrere Stadien von der Initialisierung bis hin zum anerkannten Standard. Als anerkannter Standard gehört die RFC zum offiziellen Teil der TCP/IP-Protokollreihe. Die Entwicklungsstadien der RFC sind:

- ✔ **Initial**, d.h. das Protokoll wurde für eine Überprüfung eingereicht.
- ✔ **Proposed Standard**, d.h. das Protokoll wurde als Standard vorgeschlagen und einer ersten Überprüfung unterzogen.
- ✔ **Draft Standard**, das Protokoll hat bereits eine erste Überprüfung bestanden. Wenigstens zwei voneinander unabhängige Implementierungen werden realisiert. Die Dokumentation des RFC wird überprüft. Allerdings muss bei einer zukünftigen Implementierung immer noch mit Änderungen gerechnet werden.
- ✔ **Standard**, d.h. das Protokoll wurde überprüft und als gültiger Standard anerkannt.
- ✔ **Experimental**, d.h. das Protokoll wurde nicht für Standardisierungszwecke überprüft. Es wird aber in Tests und Versuchen eingesetzt.
- ✔ **Historic**, d.h. das Protokoll ist veraltet und wird derzeit nicht benutzt.

Das IAB bestimmt für jedes Protokoll einen Status, der Bedeutung genannt wird. Die Bedeutung legt fest, unter welchen Bedingungen das Protokoll eingesetzt werden soll.

- ✔ **Required**, d.h. sämtliche Hosts, Gateways und Router, die TCP/IP benutzen, müssen ein so gekennzeichnetes Protokoll implementieren.
- ✔ **Recommended**, d.h. sämtlichen Hosts, Gateways und Routern wird geraten, dieses Protokoll zu implementieren.
- ✔ **Elective**, d.h. die Internet-Rechner können wählen, ob sie ein so gekennzeichnetes Protokoll implementieren wollen oder nicht.
- ✔ **Limited Use**, d.h. das Protokoll ist nicht für den allgemeinen Gebrauch gedacht. Hier kann es sich z.B. um ein experimentelles Protokoll für die Benutzung durch eine Testgruppe handeln.
- ✔ **Not Recommended**, d.h. die Benutzung des Protokolls ist nicht erwünscht, weil es sich z.B. um eine veraltete Version handelt.

4.5 TCP/IP-Protokollübersicht

Dieser Abschnitt soll Ihnen einen kurzen Überblick über die wichtigsten Protokolle der TCP/IP-Protokollfamilie geben. Eine weitere detaillierte Beschreibung der für die Praxis des Netzadministrators wichtigen Protokolle folgt in den anschließenden Kapiteln.

ARP Adress Resolution Protocol, definiert in RFC 826:

Dieses Protokoll wird verwendet, um die physikalische Adresse, MAC-Adresse, zu lokalisieren, wenn nur die IP-Adresse bekannt ist. Token Ring, Ethernet und andere Netzwerke verwenden eine physikalische Adresse, die vom Hersteller der Netzwerkkarte festgelegt wird. Über ein Broadcast wird die MAC-Adresse erfragt und anschließend im ARP-Cache gespeichert.

RARP Reverse Adress Resolution Protocol, definiert in RFC 903:

Im Gegensatz zu ARP wird diese Varinate des ARP-Protokolls eingesetzt, um bei vorliegender MAC-Adresse eine IP-Adresse von einem Server zu beziehen.

BOOTP Bootstrap Protocol, definiert in RFC 951, 1497:

Das Bootstrap Protocol wird in Kombination mit TFTP eingesetzt, um Clients mit einer IP-Adresse und weiteren notwendigen Information zu versorgen. BOOTSTRAP arbeitet dabei nach dem Client-Server-Prinzip und setzt als Applikation direkt auf dem UDP, User Datagram Protocol, auf. Auch hier kommt ein Broadcast zum Einsatz.

IP Internet Protocol, definiert in RFC 791:

IP ist ein verbindungsloses Protokoll für die Kommunikation in einem oder in mehreren Netzen. Es handelt sich um ein unzuverlässiges Protokoll, da die garantierte Zustellung der einzelnen Datagramme nicht gewährleistet werden kann.

RIP Routing Information Protocol, definiert in RFC 1723:

Das RIP-Protokoll wird eingesetzt, um die Routing-Informationen innerhalb eines IP-Netzwerkverbunds auszutauschen. RIP ist ein dynamisches Routing-Protokoll, das in kleineren und mittleren Netzwerken eingesetzt wird.

OSPF Open Shortest Path First, definiert in RFC 1247:

OSPF ist wie RIP ein Routing-Protokoll, das jedoch speziell zum Zwecke des Routens in großen IP-Netzen entwickelt wurde. Ziel ist unter anderem, eine geringe Netzbelastung zu erreichen.

PING Packet InterNet Groper, definiert in RFC 862:

PING ist ein mächtiges Debugging- und Troubleshootingwerkzeug mit dem bei auftretenden Verbindungs- und Kommunikationsproblemen eine schnelle Eingrenzung des Fehlers vorgenommen werden kann.

ICMP Internet Control Messages Protocol, definiert in RFC 792:

ICMP gibt Statusmeldungen über bestimmte Bedingungen an andere TCP/IP-Protokolle weiter. So nutzt auch PING die Rückmeldungen von ICMP. Die ICMP-Pakete werden als IP-Datagramme geführt und sind unzuverlässig.

IGMP Internet Group Management Protocol, definiert in RFC 1112:

IGMP-Informationen werden an alle angeschlossenen Router mit Multicasting-Funktion weitergegeben, um diese über Hosts-Gruppen zu informieren. Auch die IGMP-Pakete werden als IP-Datagramme geführt und sind somit ebenfalls unzuverlässig.

FTP File Transfer Protocol, definiert in RFC 959:

FTP ist ein einfaches Protokoll, das zum Übertragen von EBCDIC-, ASCII- und Binärdateien unabhängig vom Betriebssystem eingesetzt wird. FTP benutzt die TCP-Ports 21 für FTP-Steuerverbindungen und 20 für FTP-Datenverbindungen.

TFTP Trivial File Transfer Protocol, definiert in RFC 783:

Ein weiteres File-Transfer-Protokoll, das mit einem Minimum an Kommandos ohne aufwändige Sicherheitsmechanismen arbeitet.

SNMP Simple Network Management Protocol, definiert in RFC 1157:

SNMP ist ein Standardprotokoll als Plattform für das Netzwerk-Management in heterogenen Netzen. Es ermöglicht die Verwaltung fast aller verfügbaren Netzwerkkomponenten mit Hilfe einer SNMP-fähigen Netzmanagementsoftware.

SMTP Simple Mail Transfer Protocol, definiert in RFC 821:

SMTP ist verantwortlich für das Versenden von E-Mails über das Internet. Es setzt direkt auf TCP auf und benutzt den TCP-Port 25.

POP3 Post Office Protocol Version 3, definiert in RFC 1460:

POP3 ist das Standardprotokoll für den Empfang von E-Mails. POP3 bietet dem Anwender die Möglichkeit, empfangene E-Mails auf der lokalen Platte zu speichern.

MAPI Messaging Application Programmable Interface:

MAPI ist ein Microsoft-Standard. Das grundlegende Konzept besteht darin, dem Anwender nur einen Client für alle Messaging-Anwendungen zur Verfügung zu stellen.

Telnet definiert in RFC 854, 855:

Telnet erlaubt das Remote-Login über das Netzwerk an entfernten Rechnern. Dabei beschreibt das Telnet-Protokoll die Mechanismen zur Kommunikation zwischen einem Terminal und Rechner, wobei eine fiktive Ein- und Ausgabeeinheit simuliert wird.

TCP Transmission Control Protocol, definiert in RFC 793:

TCP ist ein verbindungsorientiertes Protokoll zur fehlergesicherten Übertragung von Datagrammen, wobei eine Mehrfachnutzung von Verbindungen möglich ist.

UDP User Datagram Protocol, definiert in RFC 768:

UDP ist ein Alternativprotokoll zu TCP, wobei wegen der minimalen Protokollmechanismen keine Ende-zu-Ende-Kontrolle erfolgt.

DHCP Dynamic Host Configuration Protocol, definiert in RFC 1541:

Dieses Protokoll wird eingesetzt, um den Hosts eines IP-Netzwerkverbundes eine gültige IP-Adresse sowie ggf. andere optionale Informationen mitzuteilen.

DNS Domain Name Service, definiert in RFC 881, 882, 883, 1034 und 1035:

DNS ist eine verteilte Datenbankanwendung zur Namensauflösung. Dabei wird ein Domain-Name in eine IP-Adresse umgewandelt. Die im Domain Name Service verwendeten Domain-Namen werden nach einem hierarchischen Namenskonzept vergeben.

4.6 Detaillierte Protokollübersicht TCP/IP

In den folgenden Unterkapiteln finden Sie eine detaillierte Übersicht zur TCP/IP-Protokollgruppe. Hier werden wichtige Kenntnisse zur Funktionsweise einzelner Protokolle vermittelt. Sie erfahren, wie Sie die wichtigsten Standards implementieren und konfigurieren.

4.6.1 TCP (Transmission Control Protocol)

Die Spezifikationen des Transmission Control Protocol sind im Request for Comments 793 veröffentlicht.

Das TCP-Protokoll ist ein verbindungsorientiertes Protokoll, das die TCP-Daten in Segmente unterteilt und zur Übertragung an den Zielrechner an IP weitergibt. Zu diesem Zweck werden vor dem eigentlichen Datenaustausch die notwendigen Sitzungen über virtuelle Verbindungen aufgebaut. Innerhalb des Datenstromes verwendet TCP eine Bytestrom-Kommunikation, d.h. die Daten werden wie eine Folge von Byte behandelt. Zusätzlich ist TCP zuständig für:

- ✔ Fehlererkennung
- ✔ Prioritätssteuerung
- ✔ Virtuelle Full-Duplex-Verbindung
- ✔ Datenflusssteuerung

Datenfluss innerhalb von TCP

Durch ein Protokoll höherer Schichten wird TCP damit beauftragt, eine Verbindung zu einem Ziel-Host herzustellen. TCP bekommt die zu übertragenden Daten byteweise und teilt diese dann in Segmente ein, wobei jedes Segment einen eigenen Header erhält. Im Anschluss daran werden die einzelnen Segmente an das Internet Protocol übergeben, welches sie dann über das Netz schickt.

Nachdem die IP-Pakete, in der TCP/IP-Terminologie Datagramme genannt, den Ziel-Host erreicht haben, werden diese unter Entfernung der IP-Header wieder an das TCP übergeben. Dort werden sie auf Fehler überprüft und in der richtigen Reihenfolge der Anwendung übergeben.

Im Gegensatz zu IP und UDP zeichnet sich TCP dadurch aus, dass eine garantierte Zustellung von Daten gewährleistet ist. TCP ist in diesem Sinne ein zuverlässiges Protokoll.

Zu diesem Zweck muss jedoch jedes TCP-Segment mit einem **ACK,** Acknowledgement, bestätigt werden. In der Praxis bedeutet dies, dass das nächste Segment erst gesendet werden kann, wenn das letzte quittiert wurde. Dieses Verfahren erzeugt allerdings eine sehr hohe Netzlast. Um diese hohe Netzlast zu senken, entwickelte man ein Prinzip namens »Sliding Windows«.

Sliding Windows ist die Vereinbarung darüber, ab welcher übertragenen Anzahl von Segmenten eine Überprüfung und damit auch eine Quittierung erfolgen soll. Um eine bestimmte Anzahl von Segmenten empfangen und speichern zu können, muss der Empfänger den Daten einer Verbindung einen definierten Speicherbereich zuweisen. Dieser Speicherbereich stellt die so genannte Window-Size dar. Die Parameter über diesen Speicherbereich werden beim Aufbau der Verbindung mit dem Ziel-Host vereinbart, können aber vom Quell-Host dynamisch während einer Verbindung angepasst werden, sofern dies seine Ressourcen verlangen. Das Fenster verändert also seine Größe, es »gleitet«, sliding.

Wird nun die vereinbarte Fenstergröße erreicht, erfolgt ein ACK zum Quell-Host. Nach dieser Bestätigung ist der Ziel-Host wieder in der Lage, neue Segmente zu empfangen. Sinkt hingegen die Fenstergröße auf »0«, werden keine Daten mehr übertragen. Wenn die Ressourcen es erlauben, wird die Fenstergröße allmählich wieder erhöht, und die neue Fenstergröße wird dabei mit jedem neuen ACK an den Quell-Host übertragen.

Geht innerhalb einer bestimmten Zeit ein ACK für ein Segment nicht ein, muss dieses Segment und alle nachfolgenden und bereits gesendeten Segmente erneut übertragen werden. Wenn ein Segment in beschädigtem Zustand empfangen wird, so verwirft der empfangende Host es. Weil auch in diesem Fall das ACK-Signal ausbleibt, wird das Segment vom Absender erneut übertragen. Die entsprechenden Zeitintervalle, in denen eine Quittierung erfolgen muss, werden in Abhängigkeit der Netzlast kontinuierlich neu berechnet und im so genannten Round Trip Time Timer hinterlegt.

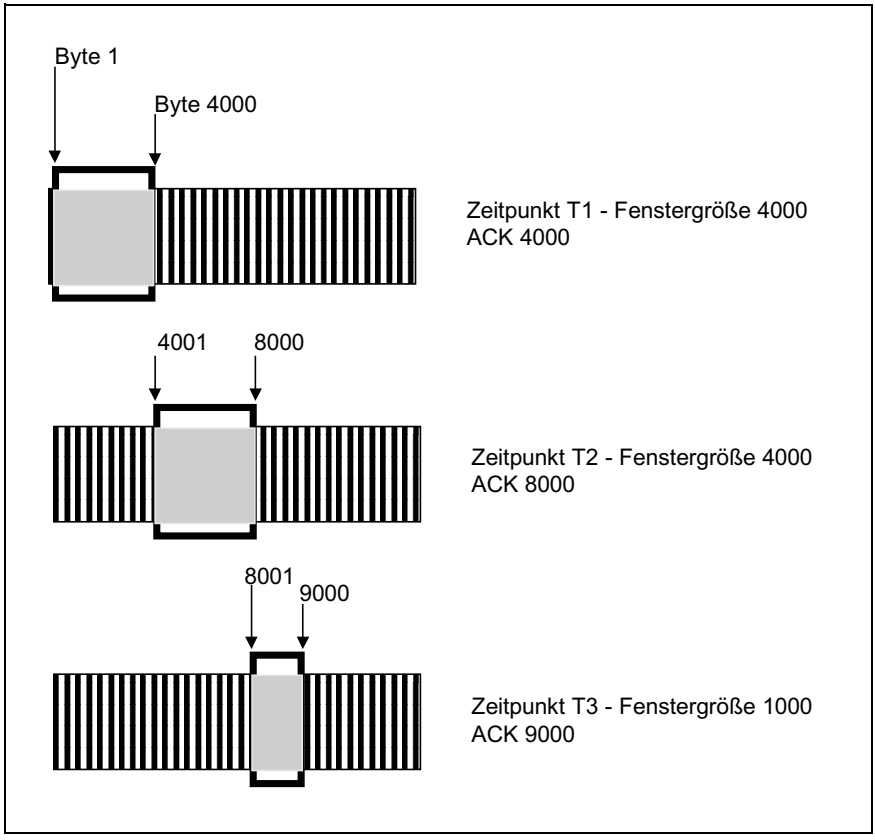


Abbildung 4.7: Sliding Windows

Zeitüberwachung

Das TCP benutzt zur Zeitüberwachung verschiedene Techniken, die als Timer oder Wecker bezeichnet werden. Für die Überwachung der Quittierungsmechanismen wird der Segmentwiederholungswecker oder Retransmission Timeout, **RTO**, verwendet.

RTO läuft ab, wenn in einem vorgegebenen Zeitraum keine Quittierung erfolgt. In diesem Fall muss das Segment nochmals übertragen werden. Da TCP-Pakete verschiedene Netze durchlaufen, deren Signallaufzeit sich um den Faktor Tausend unterscheiden können, wird die RTO dynamisch gesetzt. TCP berechnet dazu für jedes Paket die Zeit, die zwischen dem Senden und der Empfangsbestätigung vergeht. Diese Zeit wird Round Trip Time, **RTT**, genannt. Mit Hilfe einer Formel werden aus der RTT die Spitzen nach oben und unten herausgerechnet. Das Ergebnis ist die mittlere Zeit, die beim Segmentaustausch vergeht. Diese Zeit heißt Smoothed Round Trip Time, **SRTT**. Auch hier erfolgt eine weitere Skalierung, die Spielraum für unvorhergesehene Störungen verschafft.

Sollte nach der Wiederholung eines Segments der RTO zum zweiten Mal ablaufen, dann wird der Wecker neu berechnet und dabei erhöht. Dieser Vorgang wiederholt sich bis zu zwölf Mal. Sollte sich danach immer noch kein Erfolg zeigen, d.h. es erfolgt noch immer keine Quittierung innerhalb der RTO, dann gilt die Verbindung als unterbrochen.

Portnummern

Auf der Transportebene wird von TCP die Kommunikation mit den übergeordneten Prozessen über so genannte Portnummern durchgeführt. Portnummer und IP-Adresse bilden zusammen den Endpunkt einer Kommunikation, den so genannten Socket. Die Portnummern sind dabei Schnittstelle zwischen Anwendung und Transportprotokoll. Sie bieten damit auch gleichzeitig den Zugriff auf die Anwendung. Betrachten Sie dazu das folgende Beispiel aus dem World Wide Web.

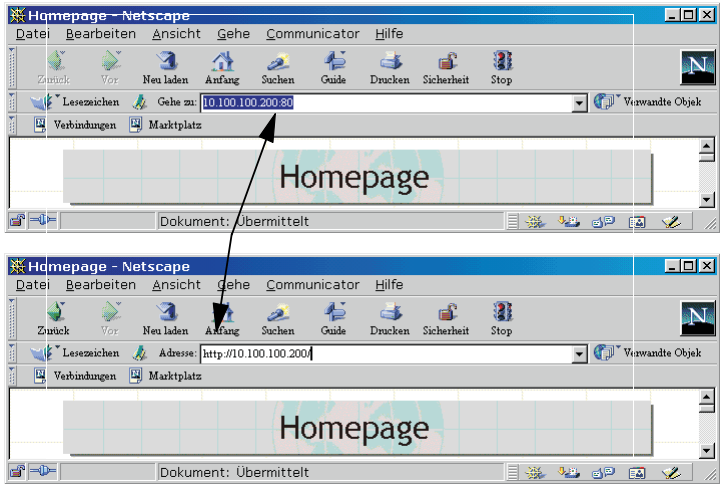


Abbildung 4.8: Portnummern in der Praxis

Das obige Beispiel zeigt, wie auf einen Webserver einmal über die explizite Angabe des Ports, »an dem der Server hängt«, zugegriffen wird und einmal über die explizite Angabe des Protokolls, in unserem Fall HTTP, Hypertext Transport Protocol.

Mit folgender Adresse können Sie zum Beispiel auf einen FTP-Server zugreifen, wenn Sie die IP-Adresse des Hosts kennen, auf dem der Server installiert ist.

Beispiel: Socket eines FTP-Servers

10.100.100.254:21

Eine Portnummer besteht aus 16 Bit, womit sich 65.535 unterschiedliche Ports ansprechen lassen. Für die Standarddienste werden von der Internet Assigned Numbers Authority, IANA, so genannte Well-Known-Portnumbers vergeben.

Diese Portnummern werden im RFC 1010 definiert, sind kleiner als 1024 und werden auch als privilegierte Nummern bezeichnet. Portnummern größer als 1024 können beliebig eingesetzt werden und sind für proprietäre Anwendungen gedacht.

Portnummern bis 255 sind für Standardanwendungen des TCP/IP-Protokollstacks reserviert. Nummern zwischen 256 und 1024 stehen für spezielle UNIX-Anwendungen zur Verfügung.

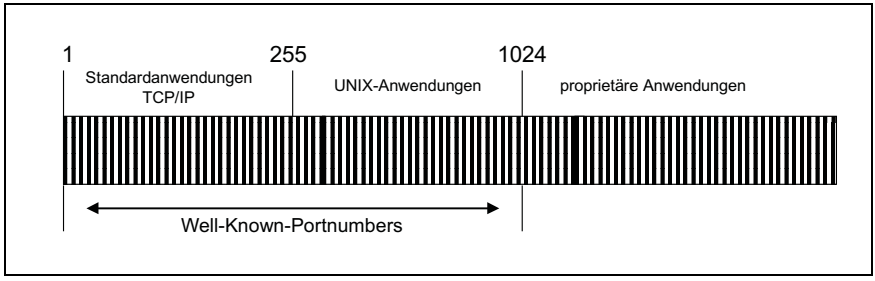


Abbildung 4.9: Well-Known-Portnumbers

Privilegierte Portnummern stellen ein potenzielles Risiko dar, weil sie je nach Dienst, z.B. Telnet, den Zugriff auf Systemressourcen ermöglichen.

In der unten aufgeführten Tabelle finden Sie eine Auswahl von Portnummern. Über die hier aufgeführten Ports können Programme direkt auf die zugeordneten Dienste zugreifen.

Dienst	Portnummer
Telnet	23
FTP	21
SMTP	25
WWW	80
Gopher	70
POP 3	110
SNMP	161

Tabelle 4.1: Well-Known-Portnumbers

Anwendungsbeispiel Portnummern

Die obige Grafik zeigt, dass auf dem hier analysierten Rechner ein Webserver an Port 80 und ein FTP-Server an Port 21 gestartet sind. Gleichzeitig hat ein Webclient über die Portnummern 1034 bis 1036 Verbindungen zu einem Webserver mit Portnummer 80 aufgebaut. Dieser liegt auf dem Host mit der IP-Adresse 10.100.100.200. Das lokale System besitzt die Adresse 10.100.100.254.

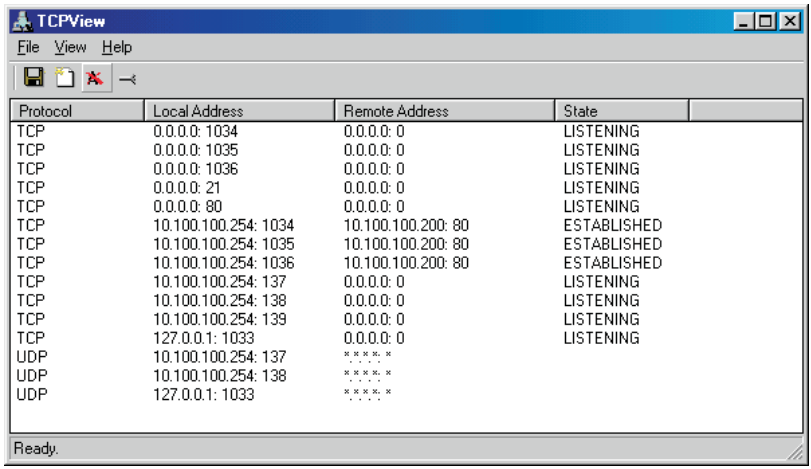


Abbildung 4.10: Portnummern als Kommunikationsendpunkte – Sockets

TCP-PaketstrukturG

Daten und Vorspann, auch Header genannt, bilden die TCP-Segmente.

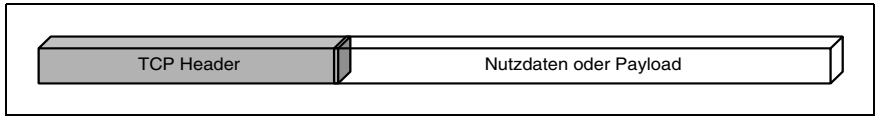


Abbildung 4.11: TCP – Segment

Die Felder, die im Vorspann eingesetzt werden, finden Sie im Folgenden aufgeführt und dann im Detail erläutert.

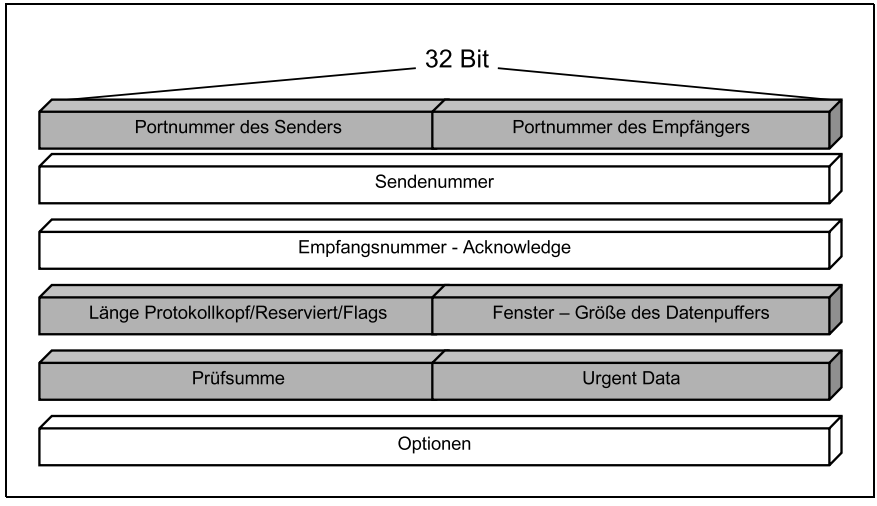
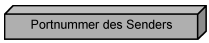
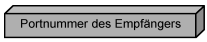


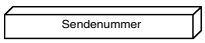
Abbildung 4.12: TCP – Protokollstruktur



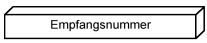
Dieses Feld beinhaltet als Portnummer den TCP-Anschluss des Quell-Hosts. Über diesen Port wird dann die virtuelle Verbindung zwischen Sender und Empfänger hergestellt.



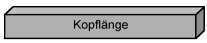
Als Endpunkt der Kommunikation beinhaltet dieses Feld den TCP-Anschluss des Ziel-Hosts.



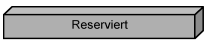
Der Inhalt dieses Feldes gibt an, welches Segment der Sender sendet. Zusammen mit der Folgenummer wird der Austausch der Datenpakete kontrolliert. Sender und Empfänger wissen immer, welche Segmente der Kommunikationspartner sendet, und welche er empfangen hat.



Mit der Empfangsnummer bestätigt der Sender den Empfang von TCP-Segmenten. Segmente, die nicht bestätigt werden, müssen nochmals gesendet werden.

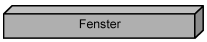


Mit vier Bit wird in diesem Feld die Länge des Protokollkopfs kodiert.



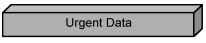
Die sechs Bit dieses Feldes sind für spätere Anwendungen reserviert.

In diesem Block sind sechs Bit für bestimmte Aktionen im TCP-Protokoll definiert. Wird das erste Bit dieses Bitfeldes, **URG,** auf eins gesetzt, dann bedeutet dies, dass das Feld Urgent Data verwendet werden soll. Das zweite Bit heißt **ACK**-Bit und wird gesetzt, wenn die Bestätigungsnummer im Empfangsnummernfeld gültig ist. Bit Nummer drei heißt **PSH**-Bit und bewirkt, dass ankommende Segmente ohne Zwischenspeichern sofort an die Anwendung weitergereicht werden. Mit dem vierten Bit wird eine Verbindung zurückgesetzt, reset- oder **RST**-Bit. Mit dem fünften Bit, **SYN** wird eine Verbindung aufgebaut und mit dem sechsten Bit, **FIN**, beendet. Das SYS-Bit synchronisiert bei Sender und Empfänger die Sende- bzw. Empfangsnummern.

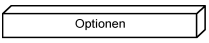


Mit diesem Feld wird der Sliding-Window-Mechanismus kontrolliert. Die verwendeten 16 Bit geben die Größe des Empfangspuffers und damit die Fenstergröße an.

Die Prüfsumme gewährleistet, dass Fehler im IP-Header und den Nutzdaten erkannt werden. Sie wird vom Sender errechnet und vom Empfänger als Prüfsumme verwendet.



Dieses Feld ergibt zusammen mit der Sendenummer einen Zeiger auf ein Byte im Datenfeld. Dieses Byte ist der Anfang eines Datenbereichs, der vom Empfänger sofort gelesen werden soll.



Das Optionsfeld bietet die Möglichkeit, Funktionen zu kodieren, die im »normalen« TCP-Protokollkopf nicht vorgesehen sind. Es sind drei Optionen definiert: End of Option List, No-Operation und Maximum Segment Size. Mit der letzten Option, der wichtigsten in

diesem Zusammenhang, kann ein Host die maximale Segmentgröße, Maximum Transfer Unit, **MTU**, angeben, die er annehmen kann bzw. will.

TCP-Protokollszenarien

Die im Folgenden beschriebenen Szenarien vermitteln einen Einblick in die konkrete Funktionsweise der oben beschriebenen Protokollstruktur. Ausgangspunkt ist die Kommunikation zwischen zwei TCP-Protokollen, die hier TCP-Quelle und TCP-Ziel genannt werden und auf zwei via IP kommunizierenden Hosts residieren.

Szenario 1: Verbindungsaufbau

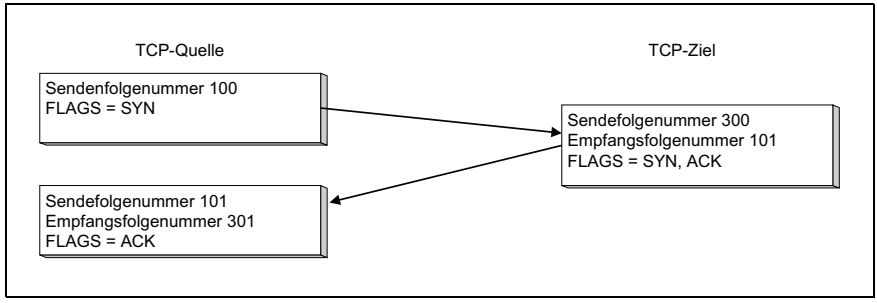


Abbildung 4.13: TCP – Verbindungsaufbau

Abbildung 4.13 zeigt den Verbindungsaufbau unter TCP. Das hier verwendete Verfahren wird auch three-way handshake genannt. Hier wird jede Seite durch das Synchronisationsflag veranlasst, die jeweils empfangene Sendefolgenummer mit der Erhöhung um eins zu quittieren. Das ACK-Flag zeigt jeweils an, dass der Wert der Empfangsfolgenummer, die als Quittierungsfeld fungiert, gültig ist.

Szenario 2: Datenaustausch

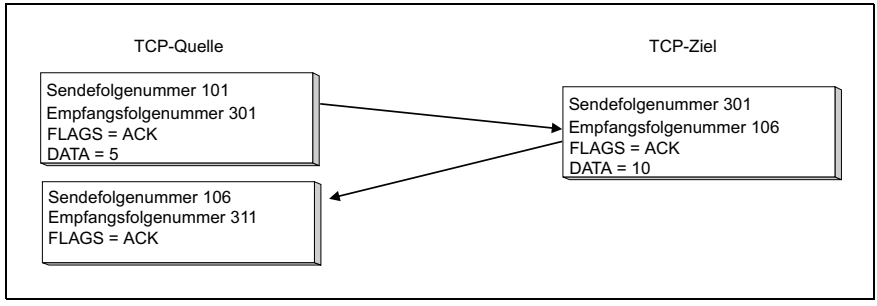


Abbildung 4.14: TCP – Datenaustausch

Abbildung 4.14 demonstriert den Datenaustausch unter TCP. Sie sehen, dass die Zahl der empfangenen Datenbyte in jeder Richtung quittiert wird. Mit der Quittierung werden gleichzeitig Daten in die Gegenrichtung gesendet. Der Datenaustausch findet also gleichzeitig in beide Richtungen statt, Vollduplex.

Szenario 3: Geregelter Verbindungsabbau

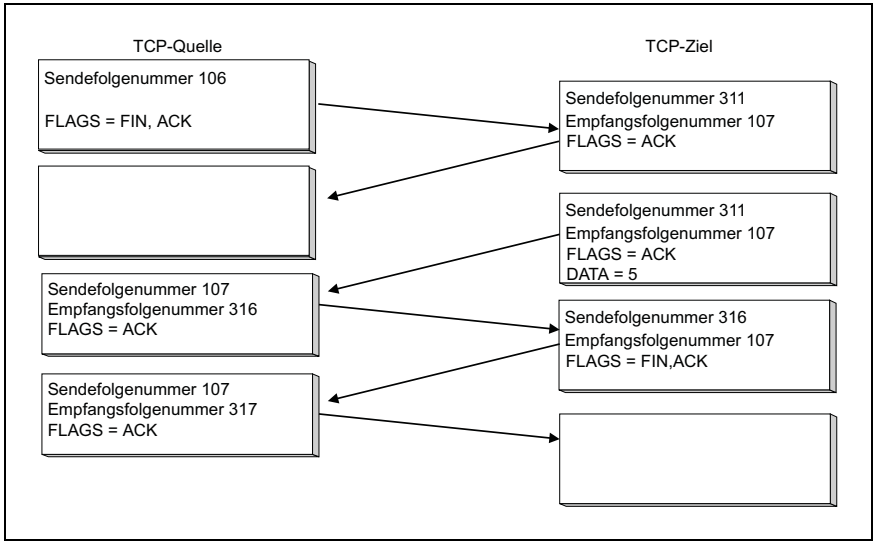


Abbildung 4.15: TCP – Verbindungsabbau

In unserem letzten Szenario werden die bestehenden Verbindungen, je eine in jeder Richtung, abgebaut. Die TCP-Quelle sendet ein FIN-Flag an das TCP-Ziel und baut damit die Verbindung einseitig ab. Nachdem das TCP-Ziel quittiert hat, darf die TCP-Quelle keine weiteren Daten mehr senden. Dies gilt nicht für das TCP-Ziel. Hier werden weiter Daten gesendet, die von der Quelle quittiert werden. Zum Schluss baut auch das zweite TCP die Verbindung über das FIN-Flag ab.

Während beim TCP im Verbindungsaufbau eine Seite aktiv und die andere passiv agiert, sind beide Seiten während der Verbindung und beim Verbindungsabbau gleichberechtigte Partner. Damit ist TCP ein ideales Protokoll für Client/Server-Anwendungen.

4.6.2 UDP (User Datagram Protocol)

Im Gegensatz zu TCP handelt es sich bei UDP, User Datagram Protocol, um ein verbindungsloses und unzuverlässiges Protokoll. Dennoch wurde UDP neben TCP auf der Transportprotokoll-Schicht etabliert. UDP ist wie TCP in der Lage, als eine Art Anwendungsschnittstelle zwischen IP und höheren Schichten zu fungieren. Des Weiteren kann über UDP ein so genanntes Port-Demultiplexing durchgeführt werden. Bei diesem Port-Demultiplexing werden mehrere Prozesse gleichzeitig bedient.

Die in der Tabelle 4.2 aufgeführten Anwendungen/Dienste werden von UDP bedient:

Dienst	Port
TFTP	69
DNS	53
SNMP	161
RPC	111

Tabelle 4.2: UDP-Anwendungen

Datagrammstruktur von UDP

Daten und Vorspann, auch Header genannt, bilden die UDP-Pakete, die Datagramm genannt werden.

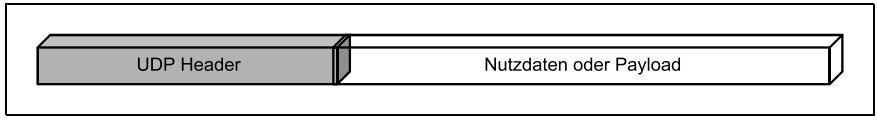


Abbildung 4.16: UDP -Datagramm

Der folgende Abschnitt beschreibt die Felder des UDP-Header.

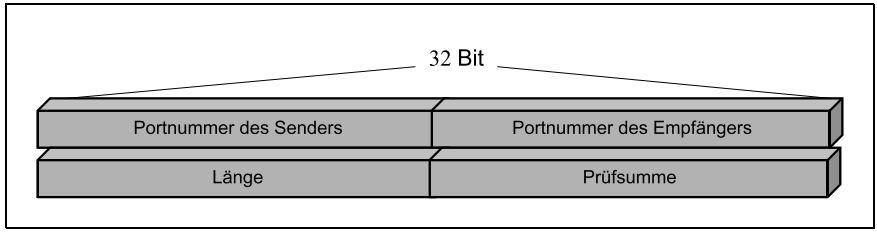


Abbildung 4.17: UDP-Header

Der Source Port ist 16 Bit breit und enthält die Portnummer des sendenden Prozesses. Die umgekehrte Funktion hat der Destination Port mit der Portnummer des empfangenden Prozesses. Im Längenfeld speichert UDP mit 16 Bit die Datagrammlänge inklusive Header. Mit der Prüfsumme werden UDP-Datagramme auf Bitfehler getestet. Die Prüfsumme bezieht sich auch auf den Pseudo-UDP-Header.

Der Pseudo-Header verfügt über eine Länge von zwölf Byte. Der dem UDP-Header vorangestellte Vorspann beinhaltet die IP-Adresse des Quell-Hosts, die IP-Adresse des Ziel-Hosts, den Protokollnamen und die Länge des UDP-Datagramms.

UDP liefert im Unterschied zum TCP lediglich die Portnummern und eine Prüfsumme. Damit wird eine Verbindung möglich, und Fehler können erkannt werden. Weil aber der Quittierungsmechanismus fehlt, ist UDP unzuverlässig. Dieser Nachteil steigert allerdings wegen des fehlenden Protokolloverheads die Effizienz von UDP insbesondere in lokalen Netzwerken mit schnellen und sicheren Übertragungsmedien.

4.6.3 IP (Internet Protocol)

Die Spezifikationen des Internet Protokolls sind im Request for Comment 791 veröffentlicht.

Als eines der Kernprotokolle der TCP/IP-Protokollfamilie ist IP hauptsächlich für die Adressierung und die Steuerung von Datagrammen zwischen den einzelnen Hosts zuständig. Das Internet Protocol arbeitet auf der Internetschicht und stellt den höheren Schichten folgende Dienste zur Verfügung:

- ✔ Adressierung der Netzknoten
- ✔ Datagramm Service
- ✔ Fragmentierung und Reassemblierung der Datenpakete
- ✔ Spezifikation höherer Protokolle: Es wird ein Wert angegeben, der das vom IP-Layer übergebene höhere Protokoll identifiziert.
- ✔ Wahl der Übertragungsparameter
- ✔ Vorrangsteuerung, Prioritäten

Datenfluss von IP

Da es sich um ein verbindungsloses Protokoll handelt, erhält IP die Empfangsbestätigung immer nur vom nächsten Netzknoten, nicht jedoch vom Endempfänger. Dadurch kann auf dem Weg zum Bestimmungsort auch ein Datagramm verloren gehen oder auch außerhalb der Reihenfolge übertragen werden. Geht ein Datagramm verloren, oder wird es außerhalb der definierten Reihenfolge gesendet, so werden weder der Absender noch der Empfänger darüber informiert. Eine Bestätigung über die garantierte Zustellung der Datagramme erfolgt durch die verbindungsorientierten Protokolle höherer Schichten, z. B. durch TCP.

Wenn das IP erkennt, dass es sich bei der Zieladresse um eine lokale Adresse handelt, erfolgt ein direktes Übertragen der Datagramme an den Ziel-Host. Wird die Zieladresse jedoch als eine Remote-Adresse erkannt, so sucht IP in der lokalen Routing-Tabelle nach einem Leitweg zu dem Ziel-Host und sendet das Datagramm auch über diesen Leitweg. In der Praxis bedeutet dies, dass das IP-Paket an den nächsten definierten Router gesendet wird. In der Terminologie des IP heißt dieser Router Standard-Gateway.

TTL – Time to Live

Wird ein Datagramm von der Transportschicht auf die Internetschicht weitergereicht, so werden dabei auch Steuerinformationen wie etwa Absender des Datagramms, Ziel des Datagramms und Lebensdauer des Datagramms in die entsprechenden Felder des IP-Datagramms eingefügt. Um zu vermeiden, dass Datagramme endlos in einem Netz zirkulieren, verfügt jedes IP-Datagramm über einen TTL-Wert, Time To Live, von 32 Sekunden. Dieser Wert ist im RFC 1060 definiert. Windows NT 4.0 verwendet im Unterschied hierzu standardmäßig einen Default-Wert von 128 Sekunden.

Fällt der Wert von TTL auf null Sekunden, dann wird das Datagramm automatisch zerstört und gilt als nicht zustellbar. Werden während des Datenaustausches mehrere Router passiert, so wird jeder der einzelnen Router die Lebensdauer um die Anzahl von Millisekunden, die das Datagramm im Router festsaß, herabsetzen. Der Mindestwert ist hier eine Sekunde. Deshalb kann man in der Regel immer davon ausgehen, dass TTL sich je Router um eine Sekunde vermindert.

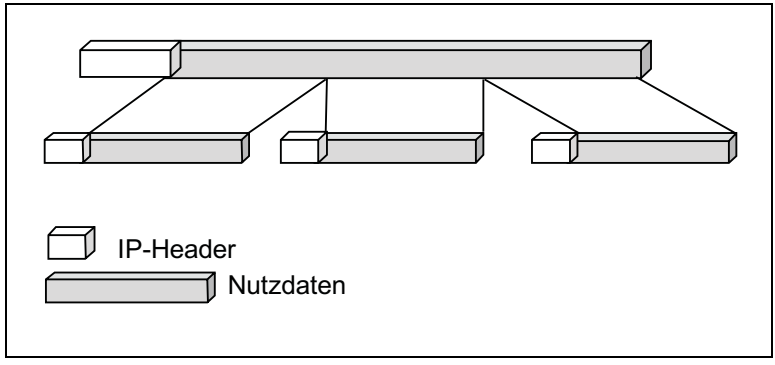


Abbildung 4.18: IP-Fragmentierung

Ist das Datagramm für das verwendete Netzwerk zu groß, kann IP es zu weiteren kleineren Datagrammen fragmentieren. Bei dieser Fragmentierung erstellt IP einen neuen Vorspann für jedes neue Datagramm. Diese Datagramme beinhalten nun unter anderem Informationen darüber, dass weitere Fragmente folgen werden, sowie die Anzahl aller zusammengehörigen Fragmente. Darüber hinaus muss mitgeteilt werden, wie die Datagramme wieder zusammengesetzt werden. Auch eine neue Prüfsumme wird dabei von IP errechnet. Sind die Fragmente endgültig am Ziel angekommen, setzt IP diese wieder zusammen, und es entsteht das ursprüngliche Datenpaket, das an TCP oder UDP weitergeleitet wird.

In jedem Router müssen die IP-Datagramme ausgepackt, neu gesetzt und berechnet werden. Eventuell muss auch eine Fragmentierung erfolgen. Dies bedeutet, dass die Verzögerungszeiten eines Datenpakets in einem Router relativ hoch sind.

IP-Paketstruktur

In diesem Kapitel finden Sie eine detaillierte Beschreibung der IP-Paketstruktur. Als Netzadministrator haben Sie auf den IP-Paketaufbau keinen Einfluss. Detailkenntnisse helfen aber, die Ursache von Störungen einzugrenzen. Sie werden zusätzlich erkennen, dass das IP-Paket sicherheitsrelevante Informationen transportiert, die von Hackern entsprechend genutzt werden können.

Die folgenden Ausführungen beziehen sich auf die IP-Version 4. Relevante Änderungen in der Version 6 werden im nächsten Kapitel beschrieben.

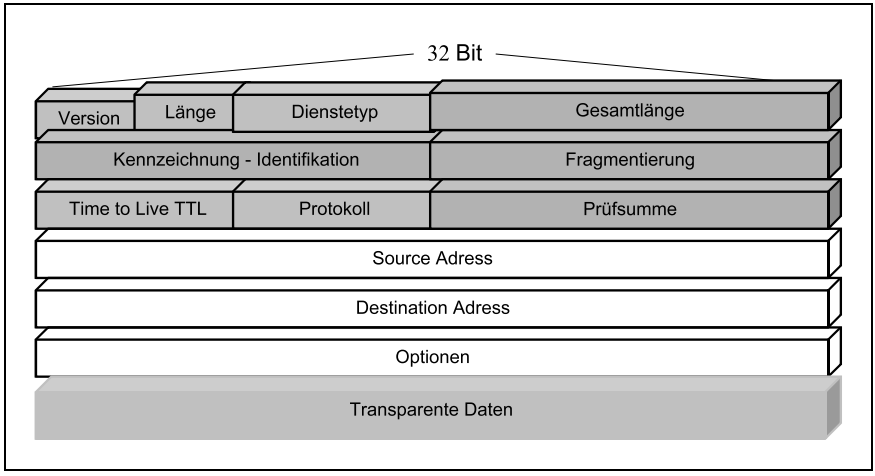
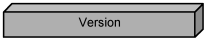


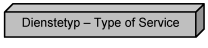
Abbildung 4.19: IP-Paketaufbau

Details zu den Funktionen und zum Inhalt der oben abgebildeten IP-Felder werden in den folgenden Absätzen beschrieben.



Die vier Bit des Versionsfeldes werden zur Bezeichnung der IP-Version verwendet. Die aktuelle Version lautet Version 4. Die nächste Version von IP wird Version 6 sein, früher IpnG IP next Generation.

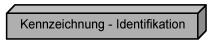
Weitere vier Bit werden im Längenfeld verwendet, um die Anzahl der 32-Bit-Worte im IP-Vorspann anzugeben. IP-Header verfügen über eine Mindestgröße von 20 Byte. Wahlweise kann durch IP-Optionen die Mindestgröße des IP-Vorspanns um jeweils vier Byte erweitert werden. Wenn nicht alle vier Byte von einem IP-Optionsfeld verwendet werden, dann füllt das Protokoll die verbleibenden Bit mit Nullen auf.



Die acht Bit des **ToS**-Felds werden dazu verwendet, die Qualität des Dienstes zu kennzeichnen, der von diesem Datagramm zur Lieferung über Router im IP-Netzwerkverbund erwartet wird. Vorgehensweise, Verzögerung, Durchsatz und Zuverlässigkeit sind die hier kodierten Merkmale. Zurzeit wird der Dienstetyp von nahezu allen Anwendun-

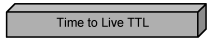
gen ignoriert und hat deshalb in der Regel den Wert Null. Es ist aber durchaus möglich, dass zukünftige Multimedia-Anwendungen in schnellen Netzen dieses Feld nutzen, um für Multimediadaten die benötigten Ressourcen zu reservieren.

Das Feld Gesamtlänge verwendet 16 Bit, um die Paketlänge des IP-Datagramms anzugeben. Die Gesamtlänge beinhaltet dabei den IP-Header und die IP-Nutzdaten höherer Schichten, Payload.

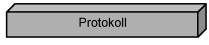


Die 16 Bit des Kennungsfelds werden zur Kennzeichnung dieses speziellen IP-Pakets verwendet. Wird das IP-Paket fragmentiert, verfügen alle Fragmente über dieselbe ursprüngliche Kennung oder Identifikation, die dann vom Ziel-Host für die erforderliche Zusammensetzung, Assemblierung, verwendet wird.

Drei Bit des Fragmentierungsfelds werden als Flag für den eigentlichen Fragmentierungsvorgang reserviert. Davon sind zurzeit nur zwei Bit für die aktuelle Verwendung definiert. Das Bit **DF**, Don't Fragment, legt fest, dass das Paket nicht fragmentiert werden darf. Mit dem zweiten Bit, **MF** More Fragments, wird signalisiert, dass weitere Fragmente des gleichen Datagramms folgen. 13 Bit der Fragmentierung werden als Offset-Zähler verwendet, um die Position des Fragments in Relation zur ursprünglichen IP-Nutzlast anzuzeigen. Bei Nichtfragmentierung ist der Wert des Fragment-Offset Null.



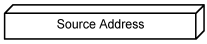
Die acht Bit des TTL-Felds werden dazu verwendet, die Zeit festzulegen, in der ein IP-Paket transportiert werden kann. Ursprünglich wurde TTL vom IP-Router als Zeitzähler benutzt, um festzustellen, wie lange es in Sekunden dauert, ein IP-Paket zu übermitteln. Router der heutigen Generation leiten ein IP-Paket fast immer in weniger als einer Sekunde weiter und müssen nach RFC 791 die TTL um mindestens eine Sekunde reduzieren. Unter diesem Aspekt wird die TTL auch zu einem Zähler für die maximale Anzahl von Hops. Hops entsprechen der Anzahl der Router, die zwischen Sender und Empfänger liegen.



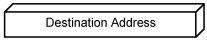
Dieses Feld wird für die Kennzeichnung des IP-Client-Protokolls verwendet, von dem die Nutzlast des IP-Datagramms stammt. Die Transportprotokolle des TCP/IP-Stacks sind Beispiele für IP-Clients. Beim Empfänger der Daten werden im Demultiplex-Verfahren die IP-Datagramme an das jeweils angegebene Protokoll weitergeleitet. Für TCP ist die Protokollnummer 7 festgelegt, UDP besitzt die Nummer 17 und ICMP wird mit der Protokollnummer 1 kodiert.

Für die Prüfsumme des IP-Vorspanns werden 16 Bit verwendet, wobei die IP-Nutzlast selbst nicht in der Prüfsummenberechnung berücksichtigt wird. Wenn ein IP-Datagramm von einem Host empfangen wird, prüft er die Gültigkeit der Prüfsumme. Stimmen selbstberechnete Prüfsumme und die Prüfsumme im Paketfeld nicht überein, dann

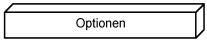
muss ein Fehler aufgetreten sein, und das IP-Datagramm wird verworfen. Übermittelt ein Router ein IP-Datagramm, so muss er die TTL dekrementieren. Aus diesem Grund muss die Prüfsumme bei jedem Hop zwischen Quelle und Ziel neu berechnet werden.



Der Inhalt dieses Feldes entspricht der IP-Adresse des Senders, der Source.



Der Inhalt dieses Feldes entspricht der IP-Adresse des Empfängers, der Destination.



Ein Vielfaches von 32 Bit wird für die Speicherung von IP-Optionen verwendet. Diese Optionen werden in der folgenden Tabelle beschrieben.

Option	Funktion/Bedeutung
End of Option List	Die End of Option List kennzeichnet das Ende der Optionsliste.
No Option	Diese Option kann zum Auffüllen von Bit zwischen den Optionen verwendet werden.
Security	Security kennzeichnet ein Datagramm als geheim. Dies führt aber nicht automatisch zu einer Verschlüsselung der Daten.
Source Routing	Diese Option enthält eine Adressliste mit IP-Adressen, die das Datagramm auf dem Weg zum Ziel-Host durchlaufen soll.
Record Route	Mit dieser Option werden alle Netzknoten aufgefordert, ihre IP-Adresse an das Optionsfeld anzuhängen. Damit kann die Route eines Pakets festgehalten werden.
Time Stamp	Diese Option weist die Router an, die Record Route mit einem zusätzlichen Zeitstempel zu versehen, der den Zeitpunkt festhält, an dem das Datagramm den Router passierte.

Tabelle 4.3: IP-Optionen im Überblick

4.6.4 IP – Adressen und Subnetting

Eine IP-Adresse ist eine 32-Bit breite Adresse, die zur eindeutigen Identifizierung eines Hosts in einem TCP/IP-Netz benötigt wird. Diese Adresse setzt sich aus vier 8-Bit-Feldern, den so genannten Oktetten, zusammen. Dabei werden die einzelnen Oktette durch Punkte voneinander abgegrenzt.

Die IP-Adresse selbst besteht aus zwei Komponenten. Aus der Netzwerk-ID, die das Netz als einmalig auf der Welt repräsentiert und der Host-ID, die den Host als einmalig in diesem Netz kennzeichnet. In der Praxis bedeutet dies, dass für jeden Computer, auf dem TCP/IP ausgeführt wird, mindestens eine eindeutige IP-Adresse notwendig ist. Des Weiteren müssen alle Hosts im gleichen physischen Netzwerk dieselbe Netzwerk-ID verwenden, um eine Kommunikation untereinander zu gewährleisten. Die IP-Adresse selbst kann dabei binär oder dezimal dargestellt werden.

Ein Beispiel für eine IP-Adresse:

Dezimale Schreibweise 145.125.22.97

Binäre Schreibweise 10010001.01111101.00010110.01100001

Dabei hat ein auf null eingestelltes Bit stets den Wert Null. Ist ein Bit auf eins eingestellt, so kann es in einen Dezimalwert umgewandelt werden. Die niederwertigen Bit stehen rechts und beginnen mit dem Dezimalwert eins. Die höherwertigen Bit stehen links und enden mit dem Dezimalwert 128. Der höchstmögliche Dezimalwert eines Oktetts beträgt damit 255 und wird erreicht, wenn alle Bit auf eins gesetzt werden.

IP-Klassen

Um die zur Verfügung stehenden Nummernkreise zu ordnen, hat man diese in so genannte Klassen unterteilt. Diese Klassen reichen von Klasse A bis F, praxisrelevant sind zurzeit jedoch nur A bis C und mit Einschränkungen D als Voraussetzung für Multicast-Anwendungen.

Die in Form von Klassen vergebenen IP-Adressen lassen unter anderem auch einen Rückschluss auf die mögliche Größe eines Netzwerkes zu.

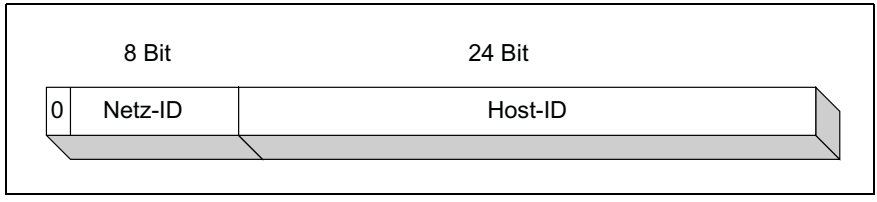


Abbildung 4.20: A-Klasse-Netz

Klasse A Adressen werden ausschließlich Netzwerken mit einer sehr großen Anzahl von Hosts zugewiesen. Bei einer Klasse A ist das höherwertige Bit des ersten Oktetts stets auf null gesetzt. Die restlichen sieben Bit des ersten Oktetts bilden dann die Netzwerk-ID. Die übrigen 24 Bit werden dazu verwendet die einzelnen Hosts zu adressieren. Aufgrund der zur Verfügung stehenden Bitkombinationen können somit insgesamt 126 A-Klasse-Netze mit jeweils bis 16,7 Millionen Hosts realisiert werden.

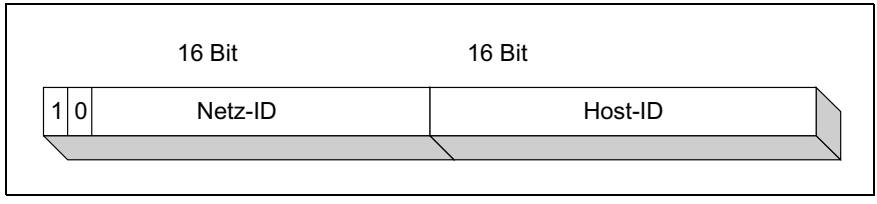


Abbildung 4.21: B-Klasse-Netz

Klasse B Adressen kommen in mittelgroßen bis großen Netzwerken zum Einsatz. Bei einer Klasse B werden die zwei höherwertigen Bit des ersten Oktetts auf die binäre Kombination 1 0 gesetzt. Die übrigen 14 Bit der ersten beiden Oktette bilden die Netzwerk-ID, während die restlichen 16 Bit (die letzten beiden Oktette) für die Adressierung der Host-ID verwendet werden. In einer Klasse B können somit 16.384 Netzwerke mit jeweils bis zu 65.534 Hosts realisiert werden.

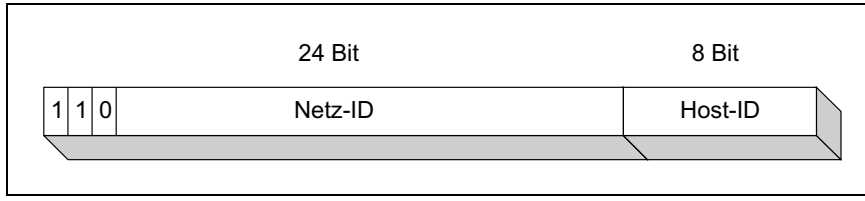


Abbildung 4.22: C-Klasse-Netz

Klasse C wird ausschließlich für kleine LANs verwendet. Bei einer Klasse C werden die drei höherwertigen Bit des ersten Oktetts auf die binäre Kombination 1 1 0 gesetzt. Die restlichen 21 Bit der ersten drei Oktette bilden die Netzwerk-ID. Die acht Bit des letzten Oktetts werden verwendet, um die Host-ID darzustellen. Mit der Netzkategorie Klasse C können fast 2,1 Millionen Netzwerke mit jeweils bis zu 255 Hosts pro Netzwerk realisiert werden.

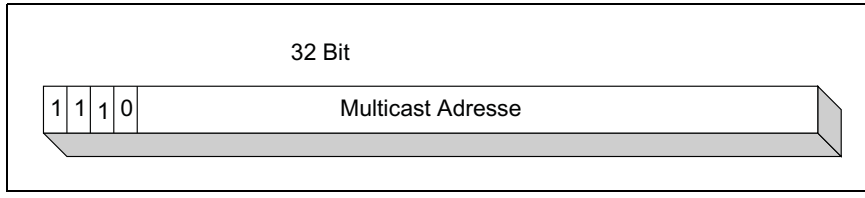


Abbildung 4.23: D-Klasse-Netz

Die **Klasse D** wird bei Verwendung von Multicast-Gruppen eingesetzt. Dabei kann eine Multicast-Gruppe einen, mehrere oder auch gar keinen Host enthalten. Bei einer Klasse D werden die vier höherwertigen Bit auf die Binärkombination 1 1 1 0 gesetzt, wobei die restlichen Bit die Gruppenzugehörigkeit eines Clients festlegen. Da bei diesen Multicast-Operationen keine Netzwerk- und Host-Bit vorhanden sind, werden die Pakete nur an Hosts mit registrierter Multicast-Adresse weitergeleitet.

Bei Adressen der **Klasse E** handelt es sich um eine rein experimentelle Anwendung. Da diese Klasse für zukünftige Verwendungen reserviert ist, wird sie auch öffentlich nicht eingesetzt. Bei einer Klasse E werden die vier höherwertigen Bit auf die Binärkombination 1 1 1 1 gesetzt.

Die folgende Tabelle gibt einen Überblick über die oben beschriebenen Adressklassen.

Adressklasse	Anzahl Netze	Anzahl Hosts	Netzwerk-ID von – bis
Klasse A	126	16.777.214	1 – 126
Klasse B	16.384	65.534	128 – 191
Klasse C	2.097.152	254	192 – 223

Tabelle 4.4: Übersicht IP-Adressklassen

Besondere IP-Adressen – Broadcast – LoopBack und Private Adress Space

Ein über die Broadcast-Adresse gesendetes Datenpaket wird an alle angeschlossenen Hosts des Intranets verschickt. Bei einer Broadcast-Adresse sind alle Bit der Host-ID auf den binären Wert eins gesetzt.

Beispiele:

A-Klasse-Netz 116.255.255.255

B-Klasse-Netz 166.117.255.255

C-Klasse-Netz 201.124.66.255

Jeder Host unter TCP/IP verfügt über die A-Klasse-Adresse 127, die als Loop-Back-Adresse reserviert ist. Diese LoopBack-Adresse wird primär für Testzwecke des eigenen Hosts eingesetzt. So wird ein über **PING 127.0.0.1** gesendetes Paket nicht in das Netzwerk gesendet, sondern gleich wieder an den Sender zurückgeschickt. Alternativ zur IP-Adresse 127.0.0.1 können auch die Adressen 127.0.0.2, 127.0.0.3, 127.0.0.3 usw. verwendet werden.

Wird die Netz-ID mit dem Wert Null angegeben, wird damit automatisch das lokale Netzwerk, This LAN, angesprochen, wobei der Wert Null bei der Host-ID den eigenen Host definiert.

Die RFC 1918 beschreibt Adressen, die nicht im Internet geroutet und als privater Adressenbereich, Private Address Space, bezeichnet werden. Diese können als interne Adressen vergeben werden. Damit können Sie ihre lokalen Hosts vor einem Zugriff aus dem öffentlichen Internet schützen.

Die folgende Tabelle gibt einen Überblick.

A-Klasse:	10.x.x.x
B-Klasse:	**172.16**.xx bis **173.31**.x.x
C-Klasse:	**192.168**.x.x

Tabelle 4.5: Private IP-Adressen

Zuweisen von Netzwerk- und Host-ID

Für jedes LAN/WAN mit Anbindung an das Internet wird eine eindeutige Netzwerk-ID benötigt. Diese erhält man beim **NIC**, Network Information Center, eines jeden Landes. In Deutschland ist das NIC in Karlsruhe für die Vergabe und Registrierung der Netzwerk-IDs zuständig. Liegt jedoch keine Anbindung an das Internet vor, können sie jede beliebige gültige Netzwerk-ID verwenden. Um zu gewährleisten, dass gültige Netzwerk- und Host-IDs eingesetzt werden, ist es jedoch erforderlich, einige allgemeingültige Regeln zu beachten:

- ✔ Es ist nicht zulässig, alle Bit der Netzwerk-ID und der Host-ID auf eins zu setzen, da diese dann als Broadcastadresse und nicht als Host-ID interpretiert wird.
- ✔ Ebenso ist es unzulässig alle Bit der Netzwerk-ID und der Host-ID auf null zu setzen, denn dies wird so gedeutet, dass die Adresse sich nur auf »dieses Netzwerk« This LAN, bezieht.
- ✔ Eine Netzwerk-ID 127 ist ungültig. Denn diese Netzwerk-ID ist als Loop-Back Adresse für Diagnosezwecke reserviert.

Subnetze

Unterteilt man ein Netzwerk in zwei oder mehrere logische Segmente, so bezeichnet man dies als Subnet. Das Unterteilen in mehrere unterschiedliche Subnets wendet man an, um zum einen den administrativen Aufwand zu senken und zum anderen, um die Anzahl der Rundsendungen zu reduzieren. Ein großes Netz wird durch Subnetze in mehrere Broadcast-Domains aufgeteilt.

Wird nun ein Netzwerk in verschiedene Subnets geteilt, dann sollte für jedes Segment auch eine unterschiedliche Netzwerk- oder wahlweise eine unterschiedliche Subnet-ID verwendet werden. Diese Technik bezeichnet man auch als Subnetting, was jedoch in privat genutzten Netzwerken nicht notwendig ist. Das Subnetting wird in einem weiteren Abschnitt näher erläutert.

Subnet-Mask

Die Subnet Mask wird benötigt, um zu erkennen, ob sich der Ziel-Host in einem lokalen oder in einem Remote-Netzwerk befindet. Eine Subnet-Mask ist wie die IP-Adresse ebenfalls 32-Bit breit. Beispiele für Subnet-Masken sind 255.255.0.0 oder auch 255.255.255.0.

Die Subnet-Mask wird zum Sperren eines Teils der IP-Adresse verwendet und TCP/IP kann die Netzwerk-ID von der Host-ID unterscheiden. Bei der Subnet-Mask kann es sich entweder um eine Standard-Subnet-Mask oder um eine benutzerdefinierte Subnet-Mask handeln. Die Standard-Subnet-Mask wird eingesetzt, wenn ein Netzwerk nicht in Subnets unterteilt wird. Dabei werden in der Subnet-Mask alle der Netzwerk-ID entsprechenden Bit auf eins gesetzt, und alle der Host-ID entsprechenden Bit auf null. Eine benutzerdefinierte Subnet-Mask hingegen muss berechnet werden und wird eingesetzt, wenn ein Netzwerk in weitere Subnets unterteilt wird.

Beispiele für Standard-Subnet-Masken

IP-Adresse-Klasse A	104.122.145.78
Subnet-Mask	255.0.0.0
IP-Adresse-Klasse B	172.122.45.188
Subnet-Mask	255.255.0.0
IP-Adresse Klasse C	198.11.201.56
Subnet-Mask	255.255.255.0

Wie bereits erwähnt, wird die Subnet-Mask dazu verwendet, um zu bestimmen, ob ein Paket direkt lokal an einen Host oder über einen Router an einen Remote-Host im Netzwerk gesendet werden soll. Zu diesem Zweck wird ein interner AND-Vergleich durchgeführt. Bei diesem AND-Vergleich handelt es sich um einen Prozess, der transparent im Hintergrund durchgeführt wird.

Bevor ein Paket gesendet wird, werden durch den AND-Vergleich Quell- und Zieladresse miteinander verglichen. Verfügen Quell- und Zieladresse über bestimmte gemeinsame Werte, wird von IP erkannt, dass das Paket zu einem Host im lokalen Netzwerk gehört. Dies ist dann der Fall, wenn die gegenübergestellten Bit beide eins sind. Einzig bei dieser Kombination lautet das Ergebnis immer eins. Bei jeder anderen Kombination lautet das Ergebnis null. Ist das Ergebnis also null, dann ist der Vergleich »ungleich«, und das Paket wird an die IP-Adresse eines IP-Routers gesendet.

Beispiel AND Vergleich – Vergleichstabelle

Bit-Kombination	Ergebnis	Aktion
1 AND 1	1	direktes Senden
1 AND 0	0	an Router senden
0 AND 0	0	an Router senden
0 AND 1	0	an Router senden

Tabelle 4.6: Ergebnisse für den logischen Bitvergleich mit AND

Beispiel AND Vergleich – IP-Quelle und IP-Ziel vergleichen

Im Beispiel aus Abbildung 4.24 führt der logische AND-Vergleich, Bitvergleich, zu dem Ergebnis, dass die Netz-IDs von Ziel- und Quell-Host ungleich sind, weil sie sich im Bitmuster der Netz-ID unterscheiden. Dies bedeutet, dass das Datenpaket über einen Router an den Ziel-Host in einem anderen Segment gesendet werden muss.

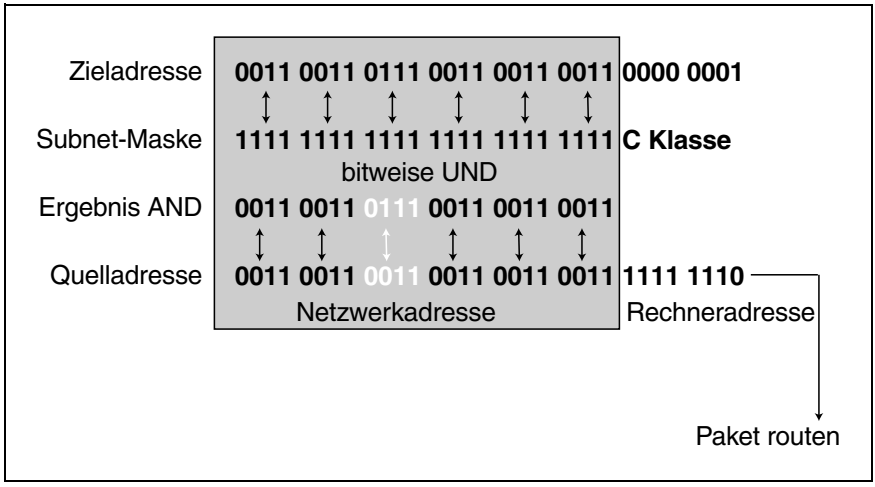


Abbildung 4.24: IP-Routing mit Hilfe von Subnet-Masken

Router

Um mit einem Host in einem anderen Netzwerk kommunizieren zu können, muss ein Router vorhanden sein. Auch dieser Router benötigt eine eindeutige IP-Adresse, damit die einzelnen Hosts ihn auch adressieren können. Zu diesem Zweck verfügen die Router in der Regel über mehrere Netzwerkkarten mit jeweils einer eigenen IP-Adresse.

Sollen nun Daten übertragen werden, so überprüft der Quell-Host, ob er die Hardwareadresse des Ziel-Hosts kennt. Sofern dies der Fall ist, wird der Zielhost direkt adressiert. Aus der Sicht des IP wird eine bekannte Route verwendet. Liegt keine explizite Route vor, werden die Datenpakete für den Remote-Host an den angegebenen Router gesendet, der diese dann an den Ziel-Host weiterleitet. Wie bereits erwähnt, gelangt das Paket im Stack des Ziel-Hosts entweder zu TCP oder UDP.

Subnetting

Im Regelfall bezieht ein Unternehmen die Netzwerk-ID vom DENIC in Karlsruhe bzw. von seinem Provider. Reicht der zur Verfügung stehende Adressbereich nicht aus, oder wird das Netzwerk aus anderen Gründen in mehrere Segmente, z.B. Token Ring und Ethernet, unterteilt, müssen einige Anforderungen für das Subnetting beachtet werden.

Die Spezifikationen des Subnetting sind im Request for Comment 950 veröffentlicht.

Bevor das Subnetting realisiert wird, sollten zunächst die aktuellen Gegebenheiten und die zukünftigen Anforderungen sorgfältig geplant werden.

Vorgehensweise:

1. Im ersten Schritt bestimmen Sie die Anzahl der benötigten physischen Segmente in ihrem Netzwerk. Achten Sie dabei auf die Erweiterbarkeit.
2. Im zweiten Schritt wird die Anzahl der für jedes physische Segment benötigten Host-Adressen festgelegt. Zu beachten ist, dass jeder Host mindestens eine IP-Adresse belegen wird, mehrere IP-Adressen sind möglich.
3. Im dritten Schritt werden anhand der ermittelten Randbedingungen Netzwerkparameter definiert. Dies sind die Subnet-Mask für das gesamte Netzwerk, eine eindeutige Subnet-ID für jedes physische Segment, sowie einen Host-ID-Bereich für jedes Subnet.

Benutzerdefinierte Subnet-Mask

Die folgenden Absätze beschreiben, wie Sie als Netzadministrator alle benötigten Parameter für das Subnetting berechnen können.

Bevor eine benutzerdefinierte Subnet-Mask errechnet werden kann, muss die zukünftig benötigte Anzahl der physischen Segmente und der Hosts je Segment ermittelt werden. Haben Sie diese Anzahl ermittelt, muss diese Zahl in das Binärformat konvertiert werden.

Beispiel: Anzahl der physischen Segmente = sechs Stück

Die Ziffer Sechs als dezimaler Wert entspricht im Binärformat 110, d.h. drei Bit sind für die Darstellung notwendig. Diese drei Bit werden nun von den niederwertigen Bit zu den höherwertigen Bit, d.h von rechts nach links, umgewandelt. In unserem Beispiel lautet der umgewandelte binäre Wert 11100000. Zu beachten ist dabei, dass bei dem Umwandlungsvorgang die Darstellung als komplettes Byte erfolgen muss und somit nach rechts mit Nullen aufgefüllt wird.

Im Anschluss daran muss der umgewandelte Wert wieder in einen dezimalen Wert konvertiert werden. In unserem Beispiel entspricht der binäre Wert 11100000 dem dezimalen Wert 224. Die so ermittelte benutzerdefinierte Subnet-Mask ist dann für ein Klasse-B-Netz

255.255.224.0

Die ersten beiden Byte werden auf 255.255 gesetzt, weil es sich um ein B-Klasse-Netz handelt. Die folgenden Byte 224.0 ergeben sich aus den oben beschriebenen Berechnungen. In einem A-Klasse-Netz wäre das Ergebnis

255.224.0.0

Subnet-ID

Neben der Möglichkeit eine benutzerdefinierte Subnet-Mask zu ermitteln, verfügen Administratoren auch über die Möglichkeit, die niederwertigen Bit bzw. Bit ohne Wertigkeit für das Definieren der Subnet-ID einzusetzen. Diese nie-

derwertigen Bit werden dann von den Routern für die Auswertung der Subnet-ID verwendet. Einige wenige Router älterer Generationen arbeiten jedoch nicht mit dieser Methode.

Konvertierungstabellen

In der nachfolgenden Tabelle finden Sie Subnet-Masks, die bereits unter Verwendung eines Oktetts für Netzwerke der Klasse A konvertiert wurden.

Subnets	benötigte Bit	Subnet-Mask	Hosts im Subnet
0	1	Ungültig	Ungültig
2	2	255.192.0.0	4.194.302
6	3	255.224.0.0	2.097.150
14	4	255.240.0.0	1.048.574
30	5	255.248.0.0	524.286
62	6	255.252.0.0	262.142
126	7	255.254.0.0	131.070
254	8	255.255.0.0	65.534

Tabelle 4.7: Konvertierungstabelle für Klasse-A-Subnetting

In der nachfolgenden Tabelle finden Sie die gleiche Tabelle für Klasse B.

Subnets	benötigte Bit	Subnet-Mask	Hosts im Subnet
0	1	Ungültig	Ungültig
2	2	255.255.192.0	16.382
6	3	255.255.224.0	8.190
14	4	255.255.240.0	4.094
30	5	255.255.248.0	2.046
62	6	255.255.252.0	1.022
126	7	255.255.254.0	510
254	8	255.255.255.0	254

Tabelle 4.8: Konvertierungstabelle für Klasse-B-Subnetting

In der nachfolgenden Tabelle finden Sie Subnet-Masks, die bereits unter Verwendung eines Oktetts für Netzwerke der Klasse C konvertiert wurden.

Subnets	benötigte Bit	Subnet-Mask	Hosts im Subnet
Ungültig	1	Ungültig	Ungültig
1-2	2	255. 255.255.192	62
3-6	3	255. 255.255.224	30
7-14	4	255.255.255.240	14
15-30	5	255.255.255.248	6
31-62	6	255.255.255.252	2
Ungültig	7	Ungültig	Ungültig
Ungültig	8	Ungültig	Ungültig

Tabelle 4.9: Konvertierungstabelle für Klasse-C-Subnetting

Da diese Konvertierung recht umständlich ist, kommt oft eine einfachere Methode zum Einsatz. Befinden sich die verwendeten Computer in einem Intranet, können Sie die Adressen für ein privates Netzwerk verwenden. Das heißt, Computersysteme die keinen direkten Zugang zum Internet haben, können diese reservierten Nummerkreise verwenden. Datenpakete, die »private« Adressen beinhalten, werden von keinem Router im Internet weitergeleitet und sind nach außen hin auch nicht sichtbar. Diese Adressen sind als Private Address Space im RFC 1597 definiert.

Netz-ID von – bis	Anzahl und Netzklasse
10.0.0.0 – 10.255.255.2551	1 Klasse-A-Netz
172.16.0.0 – 172.31.255.255	16 Klasse-B-Netze
192.168.0.0 – 192.168.255.255	255 Klasse-C-Netze

Tabelle 4.10: Adressraum für private Netz-Ids

Welche dieser IP-Adressen eingesetzt werden, hängt von dem Bedarf der zu adressierenden Hosts in einem Intranet ab. Dazu unterscheidet man drei unterschiedliche Typen von Hosts.

1. Hosts, die weder mit dem Internet direkt noch mit anderen Netzwerken über das Internet kommunizieren. Diese Hosts verfügen ausschließlich im Intranet über eine eindeutige IP-Adresse, die nach außen hin nicht sichtbar ist.
2. Hosts, die über einen nach außen hin sichtbaren Router oder ein Gateway eingeschränkte Dienste außerhalb des Unternehmens in Anspruch nehmen können. Auch diese Hosts verfügen lediglich im Intranet über eine eindeutige IP-Adresse, wobei die Verbindung zum Internet über den Router oder das Gateway aufgebaut wird. Auch hier sind die internen IP-Adressen nach außen hin nicht sichtbar.

3. Hosts, die über TCP/IP einen vollständigen Zugang zum Internet haben. Bei diesen Hosts werden global eindeutig definierte IP-Adressen benötigt, was dann jedoch das Benutzerverbot des in dem RFC 1597 definierten IP-Adressraumes bedingt.

Router-Adresse

Wird ein IP-Netzwerk in weitere Subnetze unterteilt, wird für jedes Subnetz ein eigener Router benötigt. Dieser Router ermöglicht dann die Kommunikation mit anderen Subnetzen.

Die Router-Adresse ist dabei keine feststehende und zwingend zu verwendende Adresse, sondern nur eine Empfehlung. Nach dieser Empfehlung wird für die Router die erste Adresse nach der Netzwerknummer verwendet. So sollte in einem Klasse-B-Netzwerk mit der Netzwerk-Nummer 139.122.0.0 die IP-Adresse 139.122.0.1 für den Router verwendet werden.

Auch wenn das Subnetting etwas Planung und Aufwand erfordert, überwiegen doch die Vorteile. So ist durch das Subnetting neben der Trennung unterschiedlicher Technologien auch das Überschreiten von Grenzwerten möglich. Dies betrifft zum einen die Längenausdehnung und zum anderen die maximale Anzahl von Hosts pro Segment. Auch die Netzlast sinkt durch das Umleiten des Datenverkehrs und das gleichzeitige Reduzieren der Rundsendungen.

4.6.5 IPv6 oder IPng der zukünftige Standard

Die zukünftige IP-Generation wird IPv6, oft auch als IP next generation, Ipng, bezeichnet, sein. Für diesen neuen Standard sprechen folgende Gründe:

- ✔ Erweiterter Adressbereich, da 128 Bit breit
- ✔ Höhere Sicherheit
- ✔ Besserer Datendurchsatz bei Spitzenbelastung

Durch den Adressbereich von 128 Bit ist es möglich, hierarchische Adressen aufzubauen, die ein wesentlich schnelleres Routing ermöglichen. Es kommt in diesem Fall also primär nicht so sehr darauf an, möglichst viele Rechner zu adressieren, vielmehr können Adressen logischer aufgebaut werden.

Der größere Adressbereich hat auch zur Folge, dass TCP/IP-Rechner automatisch mit einer Adresse konfiguriert werden können.

Die in IPv6 implementierten Sicherheitsfunktionen werden als IPSec bezeichnet. Das IPSec beinhaltet einen Authentication-Mechanismus und einen Verschlüsselungsalgorithmus nach DES-Standard. Diese Mechanismen sind für alle Anwendungen verfügbar und transparent, d.h. die konkrete Anwendung merkt nichts von diesen Funktionen und muss entsprechend auch nicht verändert werden.

Die Migration nach IPv6 kann aus folgenden Gründen schrittweise erfolgen:

- ✔ Auf einem Host können beide IP-Versionen installiert sein, Dual Stack.
- ✔ IPv6 Netzwerke können über traditionelle IP-Netze miteinander kommunizieren, so genanntes IP-Tunneling.
- ✔ Host und Router können unabhängig voneinander auf IPv6 umsteigen.
- ✔ Durch den Einsatz von Gateways ist eine transparente Kommunikation zwischen »alten« und »neuen« Netzen möglich.

4.6.6 IPSec

Die TCP/IP-Protokolle weisen große Mängel auf, wenn es um die Sicherheit und Unversehrtheit der transportierten Daten und um den Zugriff auf einen IP-Host geht. An dieser Stelle setzt IPSec, IP Security, an. Bei IPSec handelt es sich um eine ganze Protokollgruppe, Framework, die auf der Netzwerkschicht liegt und von der IETF entwickelt wurde. In den folgenden Abschnitten werden die wichtigsten Details zu IPSec Suite beschrieben.

IPSec definiert Tunneling Protokolle für die Verbindung zweier oder mehrerer LANs zu einem VPN. Andere Protokolle, wie z.B. PPTP, L2F und L2TP, werden ergänzend zum Einbinden einzelner Rechner in ein Netzwerk eingesetzt.

Die unter IPSec zusammengefassten Protokolle bieten mehrere Dienste, Services, an, die wahlweise, also auch einzeln, eingesetzt werden können. Zu den Services gehören:

- ✔ Datenverschlüsselung
- ✔ Datenintegrität
- ✔ Überprüfung des Absenders
- ✔ Anti Replay, eine Technik, die es erlaubt, die Annahme wiederholt gesendeter Pakete zu verweigern.

Die folgende Abbildung gibt einen Überblick zur Architektur von IPSec. Sie sehen, dass die drei Protokolle ESP, IKE und AH den Kern des IPSec Framework darstellen.

Die folgenden Details geben einen Einblick, wie Tunneling mit Hilfe von IPSec funktioniert.

Bevor eine sichere Verbindung, der Tunnel, aufgebaut wird, handelt das Key-Management-Protokoll **IKE** die hierfür vorgesehenen Sicherheitsprotokolle aus. Dazu müssen die beiden beteiligten Hosts sich gegenseitig authentifizieren und entsprechende Schlüssel austauschen. Als flexibles Protokoll bietet IKE mehrere Optionen.

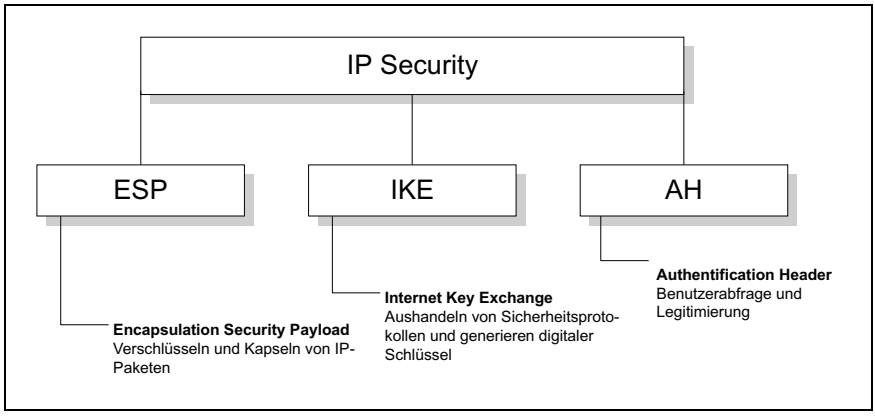


Abbildung 4.25: Die IPSec Protokoll Suite

Bei einer Methode, die Pre-Shared Keys genannt wird, sind die Schlüssel bereits auf den beteiligten Hosts installiert. Die Verbindung wird dann über die Daten dieser Schlüssel gesichert.

Bei der Public Key Cryptography generieren die beteiligten Rechner einen Zufallswert, der mit dem jeweiligen Public Key des anderen Partners verschlüsselt wird. IPSec unterstützt hierbei den RSA-Algorithmus.

Eine weitere Alternative stellt die Digitale Signature dar. Dabei signiert jeder Partner eine gewisse Datenmenge und sendet diese dem anderen zu.

Unabhängig davon, welche Methode verwendet wird, müssen nach der Authentifizierung beide Seiten einen digitalen Schlüssel besitzen, mit dem dann die Daten während der Kommunikationssitzung verschlüsselt werden. In der Terminologie von IPSec heißt dieser Schlüssel Shared Session Key. Mit IKE wird also gewährleistet, dass die Daten bei jedem Datenaustausch anders verschlüsselt werden.

IPSec verwendet als Verschlüsselungstechniken zwei Protokolle:

✔ IP AH, Authentification Header

✔ IP ESP, Encapsulating Security Payload

AH – Authentification Header

AH ist eine digitale Signatur, die die Datenintegrität durch eine Prüfsumme sicherstellt und zusätzlich für die Authentifizierung, also die eindeutige Identifizierung, des Datenursprungs sorgt. Es werden zwei Verschlüsselungsmodi unterschieden.

Im Transportmodus bleibt der ursprüngliche IP-Header erhalten. Durch die Authentifizierung wird lediglich gewährleistet, dass Veränderungen der Daten bemerkt werden. Dieser Modus wird für den Datenaustausch in einem geschlossenen Netz empfohlen. Er vermeidet unnötigen Overhead.

Im Tunnelmodus wird die Sicherheit durch eine Verschlüsselung des Gesamtpakets erhöht. Dabei wird dem Paket ein neuer IP-Header vorangestellt. Damit ist der Tunnelmodus für die gesicherte Verbindung zwischen zwei lokalen Netzwerken über das Internet geeignet.

ESP Encapsulating Security Payload

Das ESP-Protokoll dient ebenfalls der Verschlüsselung. Im Transportmodus wird nur der IP-Inhalt, im Tunnelmodus auch der IP-Header verschlüsselt.

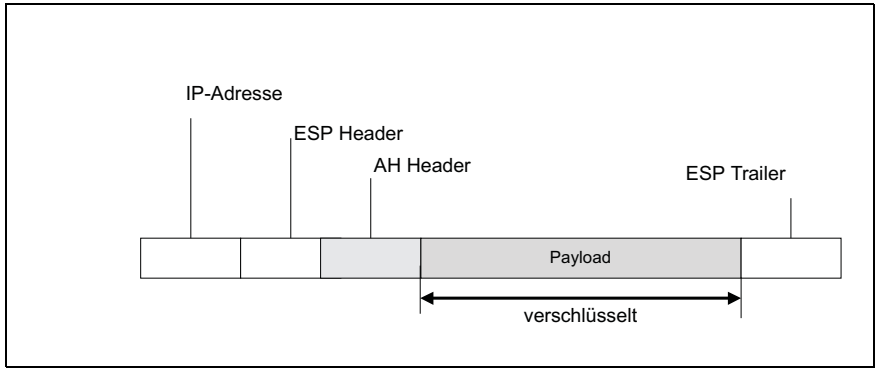


Abbildung 4.26: IPSec-Transportmodus

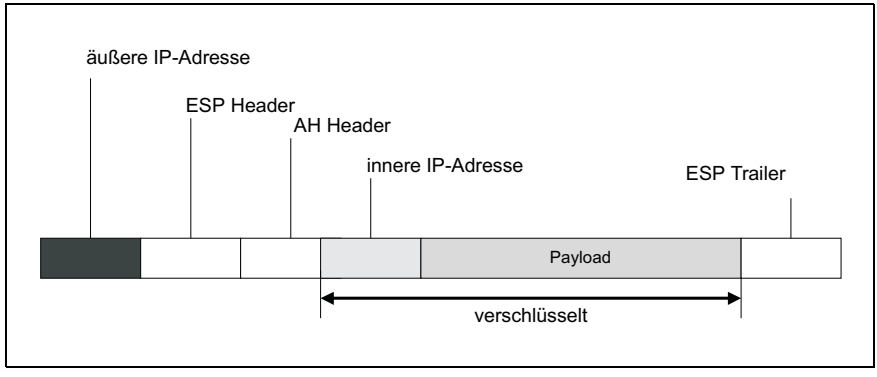


Abbildung 4.27: IPSec-Tunnelmodus

An ESP kann ein so genannter IP-Pseudo-Header angefügt werden. Dieser wird in Klartext übertragen und von den Routern als normaler IP-Header ausgewertet. ESP kann zwischen zwei Stationen, einer Station und einem Router und zwischen zwei Routern eingesetzt werden.

Die Vorgaben des IPSec sehen vor, dass im VPN zwischen den Firewalls der Tunnelmodus verwendet wird, in sicheren Netzen kann dann der Transportmodus konfiguriert sein. Die Verwendung beider Protokolle zugleich, AH und ESP, ist nicht zwingend vorgegeben, erhöht aber die Datensicherheit erheblich.

4.6.7 RSVP (Resource Reservation Protocol)

Die Funktionalität der »klassischen« Internetprotokolle kann keine für Multimediaanwendungen notwendige Übertragungsqualität, Quality of Services, gewährleisten. Diese ist aber fundamentale Voraussetzung für Video- und Audiodatenströme, wie sie z.B. für interaktive Videokonferenzen benötigt werden. Diese Lücke füllt das Resource Reservation Protocol **RSVP**. Dieses Protokoll reserviert in den Routern entlang des Datenstroms die benötigten Ressourcen wie z.B. die Übertragungsrate.

RSVP arbeitet auf der Netzschicht und ist ein reines Reservierungsprotokoll. Das bedeutet, dass RSVP auf die Hilfe von Standardroutingprotokollen und des IP angewiesen ist.

Die wichtigsten Merkmale des RSVP sind:

- ✔ Simplexprotokoll
- ✔ Soft-State-Orientierung
- ✔ Empfängerorientierung

Simplex bedeutet, dass RSVP Ressourcen nur in einer Richtung reserviert. Soft State bedeutet, dass die Reservierungen nach einer gewissen Zeit auslaufen und erneuert werden müssen. Der Grund hierfür liegt in der Charakteristik verbindungsloser Netze. Hier können zum Beispiel Router ausfallen, ohne dass dadurch die Ende-zu-Ende-Verbindung abbricht. Es wird ein neuer Pfad ermittelt, für den dann wieder Ressourcen zu reservieren sind.

RSVP sieht vor, dass die Reservierung der Ressourcen durch das Empfängersystem erfolgt. Dies macht insbesondere im Hinblick auf Multicast-Anwendungen Sinn. Hier haben nicht alle Empfänger notwendigerweise die gleichen Anforderungen an die Ressourcen.

Soft State und Empfängerorientierung sind Merkmale, die RSVP zu einem robusten und für Multicasting besonders geeigneten Protokoll machen. Allerdings gibt es zur Zeit noch sehr wenige Anwendungen, die von RSVP Gebrauch machen.

Begrifflichkeit

Unter einem RSVP-System ist ein Knoten zu verstehen, der RSVP unterstützt. Hierbei handelt es sich um einen Router oder ein Endsystem. RSVP-Systeme implementieren folgende Funktionen:

- ✔ Zulassungssteuerung
- ✔ Paketklassifizierung
- ✔ Paket-Scheduling

Die Zulassungssteuerung aktiviert alle Prozesse, die bei einem Reservierungswunsch notwendig sind und übergibt die hierfür notwendigen Parameter. Der Paketklassifizierer analysiert ankommende Pakete und bestimmt die Route sowie die QoS. Anschließend werden die Daten an den Puffer des Schedulers weitergeleitet. Dieser ist für die Zuteilung der Ressourcen wie CPU-Zeit, Zwischenspeicher und Übertragungskapazität zuständig.

Werden Reservierungen zusammengefasst, so spricht man von einem merge. Hier unterscheidet das Protokoll zwischen drei Reservierungsstilen. Es sind dies:

- ✔ Fixed Filter
- ✔ Shared Filter
- ✔ Wildcard Filter

Beim Fixed Filter gilt die Reservierung für genau einen Sender, beim **Shared Filter** teilen sich mehrere Sender die reservierten Ressourcen und beim Wildcard-Filter stehen die Ressourcen beliebigen Sendern zur Verfügung.

Funktionsweise

RSVP arbeitet mit Nachrichten, die sich in zwei Gruppen einteilen lassen:

- ✔ Pfadnachrichten
- ✔ Reservierungsnachrichten

Der Empfänger benötigt als Initiator die Charakteristika der zu erwartenden Daten und den Pfad zwischen ihm und dem Sender der Daten. Dazu schickt der Sender Pfadnachrichten und Informationen über die Art der Daten und die benötigten Ressourcen an den Empfänger. Der Empfänger merkt sich, von welchem Router er Pfadnachrichten erhalten hat, um dann über diesen Weg seine Reservierungsanforderungen an den Sender zu übertragen.

Eine Pfadnachricht enthält die in der folgenden Tabelle beschriebenen Informationen:

Nachricht	Bedeutung
Sender Template	Beschreibung des Formats der vom Sender stammenden Daten.
Sender Traffic Specification	Voraussichtliche Merkmale des vom Sender generierten Datenstroms.
Advertisement Specific	Informationen über den Datenpfad, wie z. B. minimale Ende-zu-Ende-Verzögerung, verfügbare Bandbreite oder Pfad-MTU, Maximum Transfer Unit.

Tabelle 4.11: RSVP-Pfadnachrichten

Nach dem Erhalt einer Pfadnachricht sendet der Empfänger eine Reservierungsnachricht in Richtung Sender. Die Nachricht beinhaltet zwei Informationen:

- ✔ Flussspezifikation
- ✔ Filterspezifikation

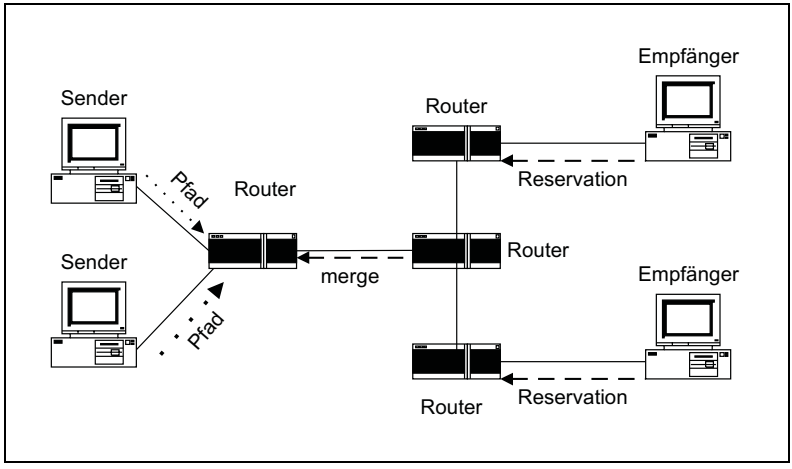


Abbildung 4.28: RSVP und Multicasting

Die Filterspezifikation legt fest, für welche IP-Pakete die Ressourcenreservierung gelten soll. Die Flussspezifikation besteht aus der empfangenen Sender Traffic Spezification und der Reservierungsspezifikation. Diese beschreibt, welche Ressourcen der Empfänger benötigt. RSVP-Reservierungen werden zwischen benachbarten Routern ausgehandelt, Hop-by-Hop.

RSVP arbeitet transparent für Router, die das Protokoll nicht unterstützen.

4.6.8 IGMP

Als Hilfsprotokoll ist das Internet Group Management Protocol, **IGMP**, eine wesentliche Komponente für die Nutzung vom IP-Multicasting. Aufbauend auf IP, wird es von IP behandelt, als sei es ein Protokoll einer höheren Schicht. Deshalb werden IGMP-Daten immer mit einem vollständigen IP-Header verschickt. Die eigentlichen IGMP-Meldungen hingegen befinden sich als Payload im anschließenden IP-Datenteil. Viele Protokolle, wie z.B. OSPF, benutzen das IGMP-Protokoll für Multicast-Anwendungen. Zurzeit existiert noch keine Verpflichtung, dass alle IP-Implementierungen IGMP unterstützen. Die Spezifikationen des Internet Group Management Protocol sind im Request for Comments 1112 veröffentlicht.

IGMP Levels

Unter IGMP sind zwei Arten von Multicast-Unterstützung implementiert.

Level 1 unterstützt das Senden, nicht aber das Empfangen von Multicast-Datagrammen. Damit kann ein Host bestimmte Multicast-Dienste, wie z.B. das Lokalisieren von Netzwerkressourcen, nutzen. Hosts, die Level 1 implementiert haben, sind aber nicht Mitglieder einer Multicast-Gruppe.

Level 2 implementiert die volle Unterstützung von Multicast und erfordert die Implementierung des IGMP.

IGMP-Pakete werden als IP-Datagramme übertragen. Dies bedeutet, dass IGMP-Nachrichten eine Erweiterung des IP-Headers zur Folge haben. Abbildung 4.29 zeigt den Paketaufbau. Das schattierte Feld steht für den normalen IP-Header, dessen Aufbau weiter oben beschrieben wurde.

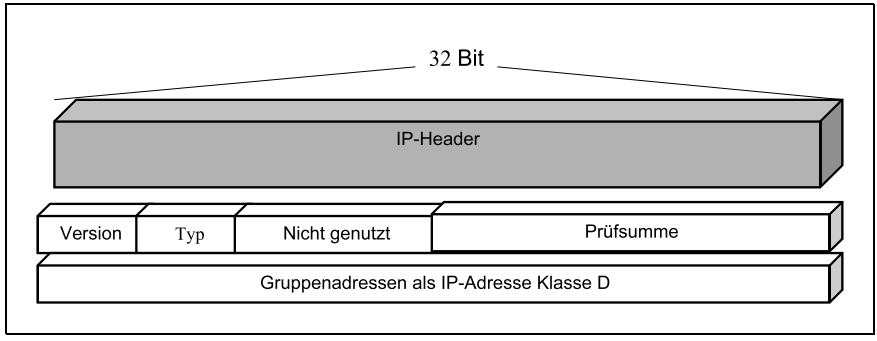


Abbildung 4.29: IGMP-Paketstruktur

Die aktuelle Versionsnummer ist eins. Beim IGMP-Typ eins handelt es sich um eine von einem Router gesendete Anfrage, bei Typ zwei um die Antwort eines Hosts. Im Gruppenadressfeld wird eine Klasse-D-Adresse transportiert, z.B. 224.0.0.1 als Multicast an alle Hosts und Router.

Verwalten von Multicast-Gruppen

Multicast-Gruppen werden über zwei Prozeduren verwaltet:

- ✔ Erstanmeldung
- ✔ Abfragen

Wenn auf einem Host einer Multicast-Gruppe ein entsprechender Prozess startet, dann wird eine IGMP-Nachricht zum Multicast-Router gesendet und der Prozess damit dort angemeldet.

Multicast-Router senden periodisch Abfragen in das lokale Netz. Ziel sind die in der Tabelle eingetragenen Multicast-Adressen. Die Abfragen überprüfen, ob es noch Hosts gibt, die zu der der Multicast-Adresse entsprechenden Gruppe gehören. Jeder Host mit Multicast-Adresse sendet dann eine IGMP-Nachricht zurück.

4.6.9 ICMP

Das Internet Control Message Protocol transportiert Fehler- und Diagnoseinformationen und gehört zu jedem TCP/IP-Protokollstack. Eine ICMP-Nachricht wird entweder von IP oder von den Transportprotokollen TCP und UDP angestoßen. Die folgende Grafik zeigt den Aufbau eines ICMP-Pakets.

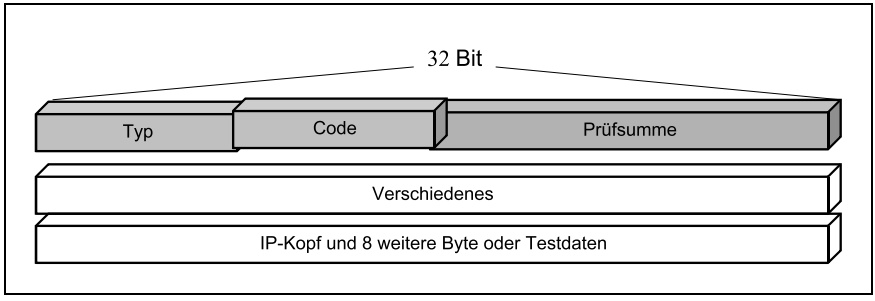


Abbildung 4.30: ICMP-Paketstruktur

Das Typenfeld spezifiziert die Art der von ICMP transportierten Nachricht bzw. deren Funktion. Im Code-Feld können weitere Unterfunktionen des Funktionstyps definiert werden. Die 32-Bit des in seinem Inhalt frei wählbaren Feldes »Verschiedenes« können Informationen wie Sequenznummer, Internetadresse usw. beinhalten. Das Feld »IP-Kopf« enthält das auslösende IP-Datagramm und die ersten acht Byte der darin transportierten Nutzdaten.

Wurde das ICMP-Paket von einem Transportprotokoll wie TCP oder UDP ausgelöst, dann kann mit Hilfe der ersten acht Byte des TCP- bzw. UDP-Paketkopfes das Anwendungsprogramm ermittelt und eine Fehlermeldung übergeben werden. Ein Beispiel hierfür ist die Meldung, dass der Port des adressierten Serverprogramms bei Verbindungswunsch nicht aktiv war.

ICMP transportiert unterschiedliche Informationen, die als Pakettypen kodiert werden. In der folgenden Tabelle finden Sie die Nummern der Typenfelder und die jeweils zugeordnete Funktion bzw. Kodierung.

Nummer	Funktion
0	Echo Reply ist die Antwort eines Hosts, wenn er ein Paket mit Echo Request erhalten hat. Echo Reply wird auch als Ping-Antwort bezeichnet.
3	Destination Unreachable signalisiert eine Störung im Netz, die eine der drei folgenden Ursachen haben kann: Netzwerk, Host, Protokoll oder Port ist nicht erreichbar. Eine Fragmentierung des IP-Pakets wäre notwendig, konnte aber wegen des gesetzten DF-Bit, Don't Fragment, von IP nicht durchgeführt werden. Eine Source Route Option war nicht erfolgreich. Die hier auftretenden Fehler werden im Feld Code numerisch kodiert. Die Fehlercodes sind im Einzelnen: 0 = Netzwerk nicht erreichbar 1 = Host ist nicht erreichbar 2 = Protokoll ist nicht erreichbar 3 = Port ist nicht erreichbar 4 = Notwendige Fragmentierung nicht möglich 5 = Source Routing Fehler 6 = Unbekanntes Netzwerk 7 = Unbekannter Host 8 = Quell-Host ist abgetrennt 9 = Zielnetzwerk ist administrativ nicht zugänglich 10 = Ziel-Host ist administrativ nicht zugänglich 11 = Netzwerk ist für ToS nicht erreichbar 12 = Host ist für ToS nicht erreichbar 13 = Kommunikation nicht erlaubt, weil z. B. Filter eingestellt sind
4	Source Quench wird von einem Host gesendet, wenn der Datenpuffer voll ist. Der Empfänger dieser ICMP-Nachricht wird daraufhin die Übertragungsrate verringern oder das Senden ganz einstellen.
5	Redirect wird dann gesendet, wenn ein Router erkennt, dass der Sender einer Nachricht diese besser direkt an einen anderen Router senden könnte. Der Empfänger dieser ICMP-Nachricht wird die neue Adresse in seine Routingtabelle eintragen. Auch hier sind verschiedene Fehlercodes definiert: 0 = redirect für Netzwerk-ID 1 = redirect für Host-ID 2 = redirect für ToS und Netz-ID 3 = redirect für ToS und Host-ID
8	Echo Request, fordert den Adressaten auf, ein Echo Reply zu senden. Im ICMP-Paket können Testdaten beliebiger Länge gesendet werden, die dann vom Zielrechner als »Echo« zurückgeschickt werden. Echo Request wird auch als Ping-Anforderung bezeichnet
11	Time Exceeded for a Datagram wird immer dann gesendet, wenn ein Paket wegen abgelaufener »Lebenszeit« weggeworfen werden muss. Hier sind zwei Codes definiert: 0 = TTL hat während der Übertragung Null erreicht. 1 = TTL hat während der Zusammensetzung des Paketes Null erreicht

Tabelle 4.12: ICMP-Pakettypen

Nummer	Funktion
12	Parameterproblem on a Datagram wird gesendet, wenn ein Paket wegen fehlerhafter Parameter im IP-Kopf weggeworfen wurde. Die Codes sind hier: 0 = IP-Header beschädigt 1 = Eine erforderliche Option fehlt
13/14	Timestamp Request fordert einen Zeitstempel an, der über Timestamp Replay zurückgegeben wird. Mit Hilfe der beide Timestamps kann die so genannte Koordinierte Universale Zeit eines entfernten Hosts abgefragt werden. Dadurch lässt sich die Zeit berechnen, die Datenpakete im Netz verbleiben.

Tabelle 4.12: ICMP-Pakettypen

4.6.10 ARP (Address Resolution Protocol)

In rundsendungsbasierten Netzen, wie z.B. dem Ethernet, ist das ARP als Adressauswertungsprotokoll zuständig für die Ermittlung und Speicherung der MAC-Adressen aller im Subnet liegenden Hosts. Die Spezifikationen des Address Resolution Protokolls sind im Request for Comments 826 veröffentlicht.

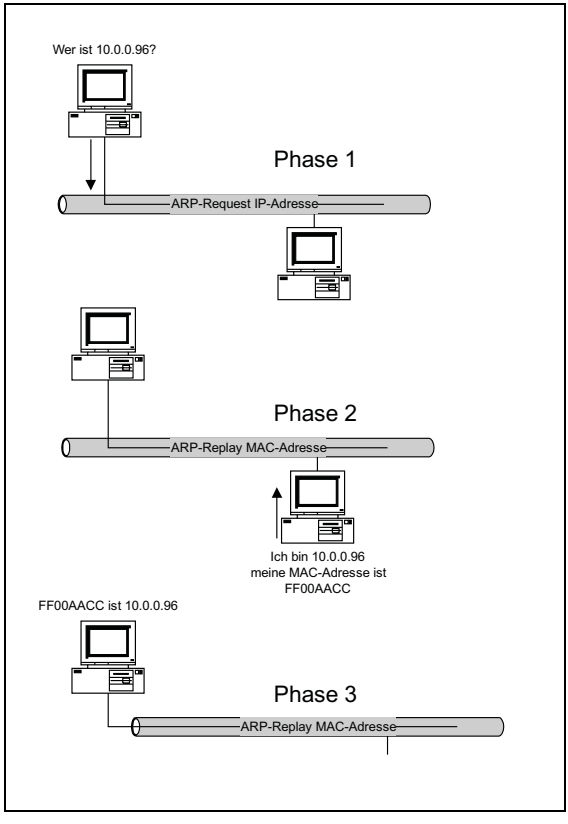


Abbildung 4.31: Funktionsweise ARP

Die Adressauswertung besteht aus einer ARP-Anforderung, Request, und einer ARP-Antwort, Replay. Zu diesem Zweck sendet ARP die IP-Zieladresse als Broadcast an alle lokalen Hosts, um so die MAC-Adresse der Ziel-Hosts zu ermitteln.

Liegt die zu ermittelnde MAC-Adresse vor, wird diese und die dazugehörige IP-Adresse im ARP-Cache gespeichert. Erfolgt nun erneut eine ARP-Anfrage, wird zuerst der ARP-Cache nach einer Übereinstimmung zwischen IP-Adresse und MAC-Adresse überprüft. Bei Übereinstimmung erfolgt keine Rundsendung mehr, sondern ein sogenanntes Unicast, d.h. eine zielgenaue Adressierung an nur einen Empfänger.

BEISPIEL **ARP im Subnet**

1. Sobald ein Host versucht, mit einem anderen Host in Verbindung zu treten, wird jedesmal eine ARP-Anforderung eingeleitet. Erkennt IP, dass die IP-Adresse für das lokale Netzwerk bestimmt ist, überprüft der Quell-Host seinen ARP-Cache nach der MAC-Adresse des Ziel-Hosts.
2. Kann dabei kein Eintrag mit der zur IP-Adresse gehörenden MAC-Adresse gefunden werden, wird ARP eine Anforderung als Broadcast an alle lokalen Hosts senden. Diese Anforderung beinhaltet sinngemäß die Frage »Wem gehört diese IP-Adresse, und wie lautet die dazugehörige MAC-Adresse?«
3. Da diese Anforderung als Broadcast gesendet wurde, führt jeder Host im lokalen Netzwerk eine Überprüfung seiner eigenen IP-Adresse auf Übereinstimmung durch. Wird keine Übereinstimmung festgestellt, wird die Anforderung ignoriert.
4. Stellt der Host hingegen fest, dass die IP-Adresse in der Anforderung identisch mit seiner eigenen IP-Adresse ist, so wird er eine ARP-Antwort unter Angabe seiner MAC-Adresse direkt an den Quell-Host senden. Im Anschluss daran wird er seinen ARP-Cache mit der IP- und Hardwareadresse des Quell-Hosts aktualisieren. Hat der Quell-Host die benötigten Informationen, wird die Verbindung zum Ziel-Host aufgebaut.

Darüber hinaus ermöglicht ARP auch die Auflösung einer IP-Adresse eines Remote-Hosts. Liegen Ziel- und Quell-Host in unterschiedlichen Netzen erfolgt die Rundsendung nach dem Router des Quell-Hosts, der dann die Datagramme an das Netzwerk des Ziel-Hosts weiterleiten kann.

BEISPIEL **ARP im Internet**

1. Durch einen internen logischen AND-Vergleich, Gegenüberstellung der IP-Adresse und Subnet-Mask von Quell- und Ziel-Host, wird die IP-Zieladresse als Remote-Adresse erkannt und entsprechend gekennzeichnet. Im Anschluss daran überprüft der Quell-Host die lokale Routingtabelle auf

einen Eintrag zum Ziel-Host. Kann keine Zuordnung erfolgen, ermittelt der Quell-Host die IP-Adresse des ihm zugeordneten Routers. Dann überprüft der Quell-Host seinen ARP-Cache zur Ermittlung der MAC-Adresse des angegebenen Routers.

2. Kann im ARP-Cache keine Zuordnung für den angegebenen Router gefunden werden, wird ein Broadcast nach der Adresse des Routers gesendet. Der Router reagiert und antwortet auf die ARP-Anforderung des Quell-Hosts, indem er seine MAC-Adresse übermittelt. Nun kann der Quell-Host das Datagramm direkt an den Router senden.
3. Auf dem Router erkennt IP, ob es sich bei der Adresse des Ziel-Hosts um eine lokale oder eine Remote-Adresse handelt. Sofern es sich um eine lokale Adresse handelt, benutzt auch der Router ARP um die MAC-Adresse des Ziel-Hosts zu ermitteln. Der Router selbst wird dann das Datagramm an das Netzwerk des Ziel-Hosts bzw. direkt an den Ziel-Host weiterleiten. Liegt eine Remote-Adresse vor, überprüft der Router in der Routingtabelle, ob ein entsprechender weiterer Router angegeben ist und verwendet dann ARP, um die MAC-Adresse des anderen Routers zu ermitteln.
4. Hat der Ziel-Host das Datagramm erhalten, erfolgt eine ICMP-Rückantwort als Statusmeldung. Da sich der Quell-Host in einem Remote-Netzwerk befindet, wird auch hier die lokale Routingtabelle auf einen Eintrag zu einem Router durchsucht, der sich im Netzwerk des Quell-Hosts befindet. Ist die MAC-Adresse des Routers bekannt, wird die ICMP-Statusmeldung an den Router gesendet, der dann die Rückmeldung an den Quell-Host weiterleitet.

Der ARP-Cache

Um die Anzahl der Broadcasts so gering wie möglich zu halten, werden durch ARP die Adressenzuordnungen, IP-Adresse zu den MAC-Adressen, im ARP-Cache gehalten. Einige Autoren bezeichnen diesen ARP-Cache auch als Internet-to-Ethernet-Translation-Table. Der ARP-Cache kann dabei wahlweise dynamische und statische Datensätze aufnehmen. Der Vorteil von dynamischen Einträgen liegt darin, dass diese automatisch hinzugefügt und gelöscht werden. Dabei beträgt die potentielle Lebensdauer dynamischer Datensätze zwanzig Minuten.

Unter Microsoft Windows NT 4 ist eine Lebensdauer von zehn Minuten definiert.

Nach Ablauf dieser Zeit werden die Einträge automatisch durch den ARP-Timer gelöscht. Einige TCP/IP-Implementierungen vergeben bei erneuter Benutzung eines Datensatzes einen Zeitstempel, der die Lebensdauer um weitere 20 Minuten verlängert.

Statische Einträge müssen manuell eingegeben werden, bleiben dann aber so lange erhalten, bis das Computersystem heruntergefahren wird. Wenn der ARP-Cache seine maximale Kapazität erreicht hat bevor die Einträge verfallen, werden die ältesten gelöscht, um neue Einträge aufnehmen zu können.

Der Einsatz von statischen Adresszuordnungen empfiehlt sich bei häufigen Zugriffen auf die einzelnen Hosts. Durch das Hinzufügen statischer ARP-Einträge kann die Anzahl der Rundsendungen erheblich reduziert werden. Beim Einfügen statischer Einträge ist darauf zu achten, dass die MAC-Adresse die notwendigen Bindestriche beinhaltet.

Übersicht ARP-Befehle

arp -Hostname	Der Befehl arp -Hostname zeigt den Eintrag in der ARP-Tabelle für den angegeben Host an. Der Hostname kann dabei über die IP-Adresse oder in Form eines logischen Namens eingegeben werden.
arp -a	Der Befehl arp -a zeigt den aktuellen Inhalt der ARP-Tabelle an. D.h. über diesen Befehl werden alle IP-Adressen mit den dazugehörigen MAC-Adressen ausgegeben.
arp -d	Der Befehl arp-d wird verwendet, um einen oder mehrere statische Einträge manuell zu löschen.
arp -s	Der Befehl arp -s wird verwendet um statische Einträge in der ARP-Tabelle vorzunehmen. Die physische Adresse wird durch sechs hexadezimale, durch Bindestrich getrennte, Byte angegeben.

Tabelle 4.13: Übersicht ARP-Befehle

Abbildung 4.32 zeigt eine ARP-Anwendung unter Windows. Hier wird zuerst ein statischer Eintrag vorgenommen. Danach wird der ARP-Cache mit Hilfe der Option -a ausgelesen.

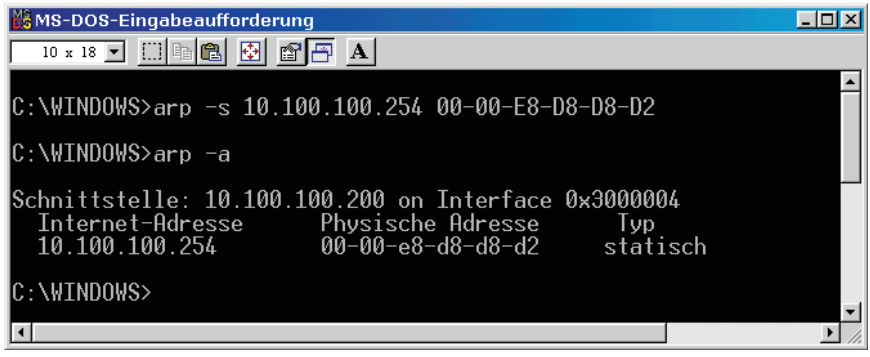


Abbildung 4.32: Anwendungsbeispiele für ARP-Befehle

4.6.11 RARP (Reverse Address Resolution Protocol)

Als sehr einfach gehaltenes Protokoll arbeitet das Reverse Address Resolution Protocol auf der ersten protokollspezifischen Schicht, dem Netzwerk-Layer. RARP wird primär verwendet, um einer Diskless Workstation, einer laufwerklosen Workstation, eine IP-Adresse zuzuordnen. Alternativ dazu kann diese Zuordnung jedoch noch mit anderen Protokollen aus der TCP/IP-Familie erfolgen. Die Spezifikationen des Reverse Address Resolution Protokolls sind im Request for Comments 903 veröffentlicht.

RARP kann aber auch eingesetzt werden, um bei einer vorliegenden MAC-Adresse die dazugehörige IP-Adresse zu ermitteln. Da das RARP von ARP abgeleitet wurde, benutzt es auch ein ähnliches Datenformat wie ARP.

Bei der Installation von TCP/IP wird die IP-Adresse in der Regel fest vorgegeben und abgespeichert. Bei dem Systemstart werden dann die gespeicherten Informationen abgefragt und die Protokoll-Software mit der IP-Adresse initialisiert. Dieser Mechanismus funktioniert jedoch nicht bei den Diskless Workstations, denn diese Geräte verfügen über kein entsprechendes Speichermedium. Technisch ist es für die Hersteller von Diskless Workstations nicht möglich im Initialisierungs-Code eine individuelle IP-Adresse einzufügen.

RARP bietet nun die Möglichkeit mit einem File-Server Kontakt aufzunehmen und von diesem eine spezifische IP-Adresse zu beziehen. Zur Abfrage seiner eigenen IP-Adresse sendet der Quell-Host einen RARP-Request als Rundsendung an alle Rechner. In diesem Datagramm trägt sich der Quell-Host mit seiner eigenen MAC-Adresse in das Quell- und das Ziel-Adressfeld des RARP-Pakets ein.

Diese Rundsendung wird nun von allen aktiven Hosts im Netz empfangen. Reagieren werden jedoch nur die Hosts, die den RARP-Service aktiviert haben und somit als RARP-Server fungieren. Diese Hosts verfügen über eine statische Datei mit allen Ethernet-Adressen der im Netz angeschlossenen RARP-Clients. Befinden sich aus Sicherheitsgründen mehrere RARP-Server in einem Netz, werden dabei alle reagieren.

Sofern mehrere RARP-Server vorhanden sind, untersuchen alle RARP-Server die empfangene RARP-Anforderung und versuchen, diesen Request zu beantworten. Finden die RARP-Server einen entsprechenden Eintrag in ihrer Adressendatei, dann senden sie als Antwort an den RARP-Client die der Ethernetadresse zugeordnete IP-Adresse zurück.

Da die MAC-Adresse des RARP-Clients den Servern bekannt ist, wird die Antwort als Unicast gesendet. Der RARP-Client wird auch alle Antworten der RARP-Server empfangen, jedoch nur auf die erste Antwort reagieren.

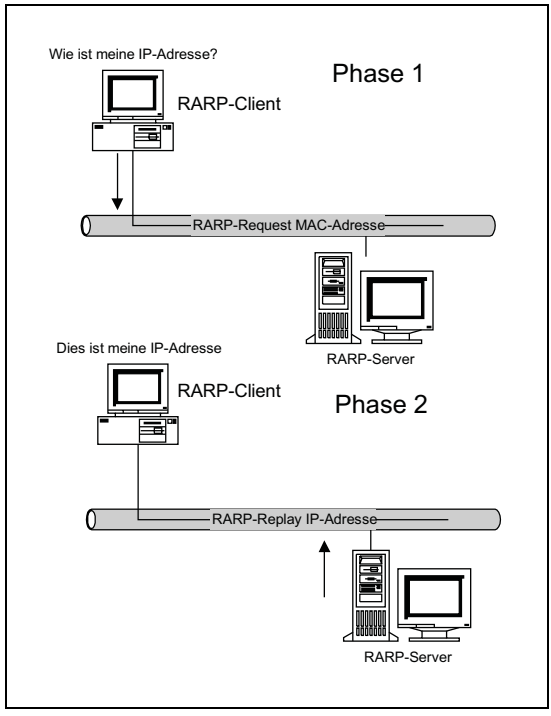


Abbildung 4.33: Funktionsweise RARP

4.6.12 NetBIOS over TCP/IP am Beispiel von Windows NT 4.0

Bei NetBIOS over TCP/IP handelt es sich um einen Netzwerkdienst, welcher die netzwerkspezifischen Ein-Ausgabeoperationen und Steuerungsanweisungen ausführt, die zum Anpassen des Befehlssatzes an die NetBIOS-Schnittstelle erforderlich sind.

Unter Windows NT 4.0 werden dazu alle in den RFCs 1001 und 1002 definierten Knoten zur NetBIOS Namensauswertung unterstützt, wobei die Knoten den Namen auf unterschiedliche Weise auswerten. In diesem Zusammenhang spricht man von NetBIOS over TCP/IP-Knotentypen.

NetBIOS over TCP/IP-Knotentyp

B-Knoten – Broadcast oder Rundsendung

Die Auswertung und Registrierung der Namen wird bei diesem Knotentyp über Broadcast durchgeführt. Da ein Broadcast in der Regel nicht über einen Router weitergeleitet wird, bleibt die Kommunikation auch nur auf das eigene Subnet beschränkt.

P-Knoten – Peer to Peer

Bei diesem Knotentyp werden die auszuwertenden Namen unter Zuhilfenahme eines so genannten NetBIOS-Name-Server, **NBNS**, z.B. **WINS**, Windows Internet Name Service, ausgewertet. Wie aus der Bezeichnung bereits ersichtlich wird, erfolgt hier kein Broadcast sondern ein Unicast, das explizit an den NetBIOS-Name-Server gerichtet ist. Durch diesen Mechanismus kann die Auswertung auch über mehrere Router hinweg erfolgen. Die Netzlast sinkt bei dieser Art der Namensauflösung.

Von Nachteil ist, dass bei einem Ausfall des NBNS keinerlei Kommunikation mehr möglich ist.

H-Knoten – Hybrid

Bei diesem Knotentyp handelt es sich um eine Kombination eines B- und P-Knotens, der jedoch im Regelfall zuerst wie ein P-Knoten die Namensauswertung durchführt. Kann keine Namensauswertung über einen NBNS erfolgen, dann wird das Broadcast eines B-Knoten absolviert.

Erweiterte Microsoft B-Knoten

Dieser Knotentyp kommt zum Einsatz, wenn mit Hilfe der statischen Datei LMHOSTS eine Namensauswertung auf einen Remote-Host erfolgt. Damit dies funktioniert, werden alle mit #PRE gekennzeichneten Einträge aus der Datei LMHOSTS bei der Initialisierung von TCP/IP automatisch in den Cache-Speicher geladen. Details zu dieser Technik finden Sie auf den folgenden Seiten. Es handelt sich hierbei um Auszüge der Beispieldatei LMHOSTS unter Windows.

```
1. # Copyright (c) 1993-1995 Microsoft Corp.
2. #
3. # Dies ist eine Beispieldatei für LMHOSTS, wie sie von Microsoft TCP/IP
4. # für Windows NT verwendet wird.
5. # Sie ist mit der LMHOSTS-Datei von Microsoft TCP/IP für LAN Manager
6. # 2.x kompatibel.
7. # Bearbeiten Sie diese Datei mit einem ASCII-Editor.
8. #
9. # In dieser Datei werden einzelnen IP-Adressen die entsprechenden
10.# NT-Computer-Namen (NetBIOS-Namen) zugeordnet. Jeder Eintrag sollte
11.# aus einer einzelnen Zeile bestehen.
12.# Die IP-Adresse wird in der ersten Spalte eingetragen, gefolgt vom
13.# zugehörigen Computer-Namen. Die Adresse und der Computer-Name
14.# müssen dabei durch mindestens ein Leerzeichen oder ein
15.# Tabulatorzeichen getrennt sein.
16.# Das Zeichen »#« wird gewöhnlich Kommentaren vorangestellt.
17.# Ausnahmen hiervon sind die folgenden Erweiterungen:
18.#
19.# #PRE
20.# #DOM:<Domäne>
21.# #INCLUDE <Dateiname>
22.# #BEGIN_ALTERNATE
23.# #END_ALTERNATE
24.# \Oxnn (Unterstützung nichtdarstellbarer Zeichen)
```

Die Erweiterung »#PRE« wird nach dem Computer-Namen angegeben, wenn dieser Eintrag bereits zu Anfang in den Namen-Cache geladen werden soll. Standardmäßig werden die Einträge nicht zu Anfang in den Namen-Cache geladen, sie werden jedoch auch nur dann ausgewertet, wenn die dynamische Namensauswertung fehlschlägt.

Die Erweiterung »#DOM:<Domäne>« wird nach dem Computer-Namen angegeben, wenn der Eintrag mit einer Domäne verknüpft werden soll. Dies wirkt sich auf das Verhalten des Computer-Suchdienstes und des Anmeldedienstes in der TCP/IP-Umgebung aus.

Die Erweiterung »DOM:<Domäne>« kann zusammen mit der Erweiterung »PRE« für einen Eintrag angegeben werden.

Die Angabe von »#INCLUDE <Dateiname>« veranlasst den so genannten NetBIOS- Helper-Dienst die angegebene Datei zu suchen und sie wie eine lokale Datei auszuwerten. Für <Dateiname> werden **UNC**-Namen, Uniform Naming Convention, akzeptiert. UNC ist die Namenskonvention des Internets.

Durch die UNC ist es möglich, eine LMHOSTS-Datei zentral auf einem Server zu verwalten. Der folgende Name ist ein Beispiel für die Verwendung des UNC-Formats. Der hier adressierte Rechner besitzt den Netzwerknamen maestro. Dies geht aus dem doppelten Backslash vor dem Namen hervor.

Beispiel UNC: *maestro\public\lmhosts*

Befindet sich der Server außerhalb des Broadcast-Bereichs, ist eine Adresszuordnung für diesen Server vor der »#INCLUDE«-Anweisung notwendig.

Die Anweisungen »#BEGIN_ALTERNATE« und »#END_ALTERNATE« ermöglichen die Gruppierung von mehreren »#INCLUDE«-Anweisungen. Ist eine »INCLUDE«-Anweisung erfolgreich, werden alle weiteren »INCLUDE-ANWEISUNGEN« übersprungen und die Gruppe verlassen.

Nichtdarstellbare Zeichen können im Computer-Namen enthalten sein. Solche Zeichen müssen als Hex-Wert in der \0xnn-Notation angegeben werden und zusammen mit dem NetBIOS-Namen in Anführungszeichen eingeschlossen werden. Hier ein Beispiel:

BEISPIEL

```
# 102.54.94.97       maestro  #PRE #DOM:technik # DC von »Technik«
# 102.54.94.102      »spiele \0x14« # besonderer Server
# 102.54.94.123      nordpol #PRE # Server in 3/4317
# #BEGIN_ALTERNATE
# #INCLUDE \\lokal\public\lmhosts
# #INCLUDE \\maestro\public\lmhosts
# #END_ALTERNATE
```

In diesem Beispiel enthält der Server **spiele** ein Sonderzeichen im Namen, und der Server **nordpol** wird bereits zu Anfang in den Namen-Cache geladen. Die Adresszuordnung für den Server »maestro« wird angegeben, um diesen Server

weiter unten in der #INCLUDE-Gruppe verwenden zu können. Wenn der Server **lokal** nicht verfügbar ist, wird die zentrale LMHOSTS-Datei auf **maestro** verwendet.

Knotentypen konfigurieren

Werden auf einem Host unter Windows NT 4.0 die TCP/IP-Konfigurationsparameter manuell eingegeben, muss auch angegeben werden, welcher NetBIOS-Namensauswertungsmechanismus von NetBIOS over TCP/IP zum Registrieren und Auswerten der Namen verwendet wird. Sofern kein NetBIOS-Name-Server, unter NT 4.0 realisiert mit WINS eingerichtet wurde, verwendet NT standardmäßig die erweiterten Microsoft-B-Knoten. Befindet sich ein WINS-Server im LAN, verwendet NT in diesem Fall standardmäßig den H-Knoten.

Sofern man einen anderen Knotentyp verwenden will, muss man dies, wie unter Windows NT 4.0 üblich, in der Registry angeben. Diese Einstellungen werden an folgender Position durchgeführt:

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Netbt\Parameters

Statusabfrage mit NBTSTAT

Um den aktuellen Status aller NetBIOS over TCP/IP-Verbindungen abzufragen, verwendet man das Dienstprogramm NBTSTAT.

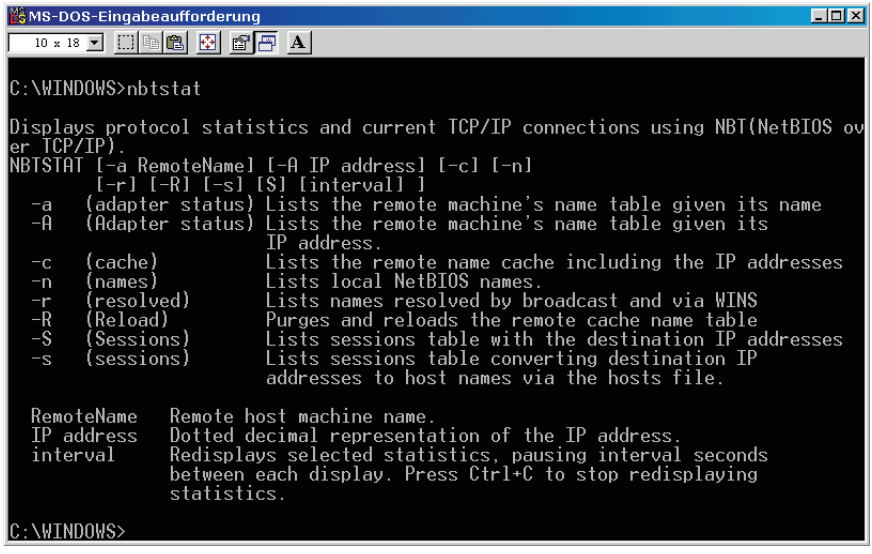


Abbildung 4.34: Statusinformationen für NetBIOS over TCP/IP abrufen

Im Folgenden finden Sie eine Liste mit den wichtigsten Befehlsoptionen. Diese sind für einen schnellen Überblick im Netzwerk unter Umständen sehr hilfreich.

nbtstat -c Zeigt den aktuellen lokalen NetBIOS-Namen-Cache.

nbtstat -n Listet die vom Client registrierten NetBIOS-Namen auf.

nbtstat -R Die mit #PRE gekennzeichneten Einträge aus der Datei LMHOSTS werden manuell in den NetBIOS-Namen-Cache geladen. Dabei wird der eventuell bestehende Cache gelöscht.

nbtstat -S Listet alle Sessions mit den jeweiligen IP-Adressen der Ziel-Hosts auf.

nbtstat -s Listet alle Sessions mit den Namen der jeweiligen Ziel-Hosts auf.

Abbildung 4.35 zeigt die Verwendungen der beiden letzten Optionen. Sie sehen in der jeweils zweiten Zeile der NetBIOS Connection Table, dass der Local-Host mit dem Namen AMDK6 eine Verbindung zu einem Remote-Host mit dem Namen PENTIUM 3 bzw. der IP-Adresse 10.100.100.253 aufgebaut hat.

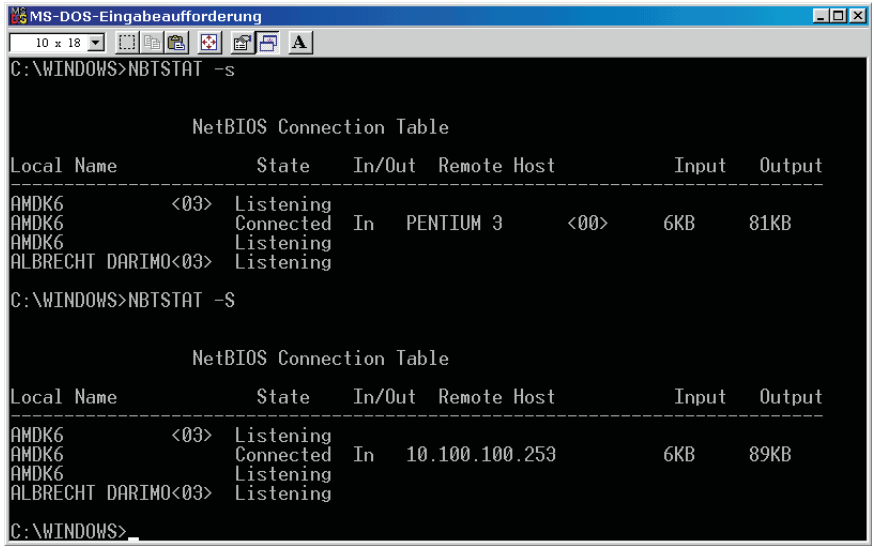


Abbildung 4.35: NetBIOS-Connections mit NBTSTAT anzeigen

Tabelle 4.14 beschreibt, wie durch Kodierung im NetBIOS-Namen die verschiedenen Rechnertypen gekennzeichnet werden. Dazu wird hinter den Namen ein zweiziffriger hexadezimaler Wert in eckigen Klammern angefügt.

NetBIOS-Name	Bedeutung
\\Computer-Name[00h]	Beschreibt den auf dem WINS-Client registrierten Namen für den Arbeitsstationsdienst.
\\Computer-Name[03h]	Beschreibt den auf dem WINS-Client registrierten Namen für den Nachrichtendienst.
\\Computer-Name[20h]	Beschreibt den auf dem WINS-Client registrierten Namen für den Server-Dienst.
\\Benutzername[03h]	Beschreibt den Namen des aktuell angemeldeten Benutzers am Computer. Dieser Name wird vom Nachrichtendienst registriert und ermöglicht das Empfangen von net send Kommandos.
\\Domänenname[1Bh]	Beschreibt den Domänennamen wie er auf dem Primary Domain Controller registriert ist. Da auf dem PDC auch der Domänenhauptsuchdienst ausgeführt wird, verwendet man den Domänennamen zum Durchsuchen von Remote-Domänen.

Tabelle 4.14: NetBIOS-Namen im Überblick

Die Abbildung 4.40 zeigt, wie die oben beschriebenen Namenskategorien eingesetzt werden.

NetBIOS Name Server mit Windows NT 4.0

Da es sich bei der LMHOSTS-Datei um eine statische Datei handelt, muss diese auch manuell gepflegt und aktualisiert werden, was in Abhängigkeit von der Netzwerkgröße recht aufwändig werden kann. Um diesen und andere Nachteile einer LMHOSTS zu kompensieren, kommt unter Windows NT 4.0 ein NetBIOS Name Server, der eine Erweiterung der RFCs 1001 und 1002 darstellt, zum Einsatz.

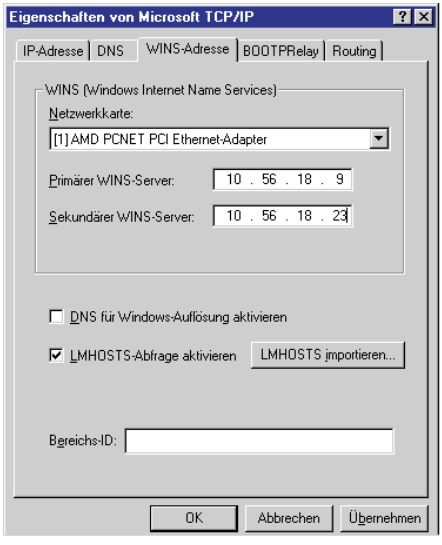


Abbildung 4.36: WINS-Clients konfigurieren

WINS selbst ist eine dynamische Datenbank, in der alle Computer-Namen von WINS-fähigen Clients mit entsprechender IP-Adresse gespeichert werden. Diese Datenbank wird automatisch alle 24 Stunden gesichert, nachdem einmal ein Verzeichnis zur Sicherung angegeben wurde.

Bei der Konfiguration des WINS-Clients wird zur späteren Namensauflösung die IP-Adresse eines primären, optional die IP-Adresse eines sekundären WINS-Servers, benötigt. Über die Registrierkarte WINS werden diese Informationen eingegeben. Als WINS-Clients können Computer mit nachfolgenden Betriebssystemen eingesetzt werden:

- ✔ Windows NT Server und Workstation, Version 4.0 sowie 3.5x
- ✔ Windows 95 und 98, Windows für Workgroups, Version 3.11 mit TCP/IP-32
- ✔ MS Network Client, Ver. 3.0 und LAN-Manager, Vers. 2.2c für MS-DOS

Die aktuell verwendeten Microsoft Clients verfügen somit alle über eine integrierte WINS-Unterstützung.

Namensauflösung unter WINS

Wird ein WINS-Client gestartet, registriert dieser seinen NetBIOS-Namen sowie seine IP-Adresse beim konfigurierten primären WINS-Server, der diese Informationen dann in seiner dynamischen Datenbank speichert. Steht der primäre WINS-Server jedoch nicht zur Verfügung, wird nach drei Fehlversuchen die Anforderung zur Namensregistrierung an den sekundären WINS-Server gesendet. Steht keiner der beiden WINS-Server zur Verfügung, dann erfolgt eine Rundsendung zur Registrierung des Namens.

Wird von einem WINS-Client zu einem späteren Zeitpunkt eine Anforderung zur Namensabfrage gestartet, so wird diese dann direkt als Unicast an den primären WINS-Server gesendet. Findet der primäre WINS-Server in seiner Datenbank eine Zuordnung des gesuchten NetBIOS-Namen, sendet er die IP-Adresse an den WINS-Client.

Kann über den primären WINS-Server keine Namensauswertung erfolgen, wird – wie auch bei der Namensregistrierung – maximal dreimal versucht, den Namen über den primären WINS-Server aufzulösen. Anschließend wendet sich der WINS-Client an den sekundären WINS-Server. Kann auch hier keine Namensauflösung erfolgen, wird eine Rundsendung gesendet. Sollte dies ebenfalls fehlschlagen, besteht noch die Möglichkeit, den Namen über die Datei LMHOSTS, HOSTS oder aber auch mit DNS aufzulösen.

Installation des WINS-Dienstes unter Windows NT

Um die oben aufgeführten Möglichkeiten nutzen zu können, muss natürlich der entsprechende WINS-Server im Vorfeld installiert werden. Wie unter NT 4.0 üblich, wird über das Symbol **Netzwerk, Eigenschaften, Dienste hinzufügen**, der WINS-Dienst geladen. Nachdem der Dienst hinzugefügt wurde, muss das System neu gestartet werden.

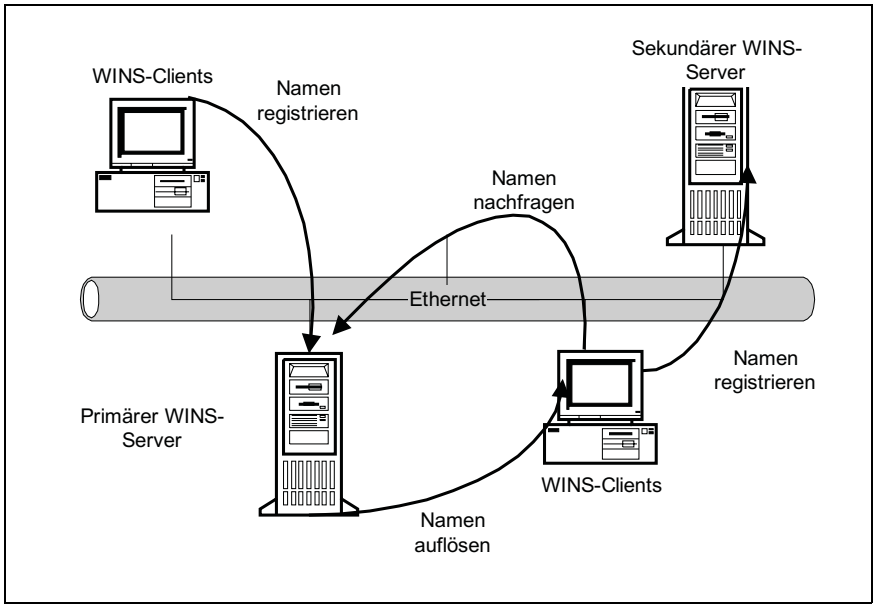


Abbildung 4.37: WINS-Server in einem LAN

Um über die entsprechenden Benutzerrechte für die im Folgenden beschriebenen Schritte verfügen zu können, müssen Sie als Administrator am System angemeldet sein. Anschließend starten Sie den WINS-Manager in der Programmgruppe Verwaltung. Als erster Schritt muss nun manuell ein neuer WINS-Server hinzugefügt werden. Wahlweise kann hier die IP-Adresse oder aber der NetBIOS-Name eingetragen werden. Sofern der NetBIOS-Name verwendet wird, muss ein entsprechender Eintrag in der LMHOSTS vorhanden sein.

Wurde der WINS-Server erfolgreich in die Liste aufgenommen, werden einige Informationen über den Server angezeigt. Von Bedeutung sind hier die Informationen über fehlgeschlagene und erfolgreiche Abfragen im Zusammenhang mit der Gesamtzahl der Registrierungen. Diese Informationen geben Aufschluss über die Funktion des WINS-Servers. Liegt eine hohe Anzahl von fehlgeschlagenen Abfragen vor, so ist dies ein Indiz für eine fehlerhafte Konfiguration bzw. fehlende Verfügbarkeit des WINS-Dienstes. Detaillierte Informationen lassen sich über den Befehl SERVER, DETAILINFORMATIONEN anzeigen.

Alle für WINS konfigurierten Clients, die sich automatisch auf dem WINS-Server registrieren, können Sie über das Menü **Zuordnung, Datenbank anzeigen** auflisten.

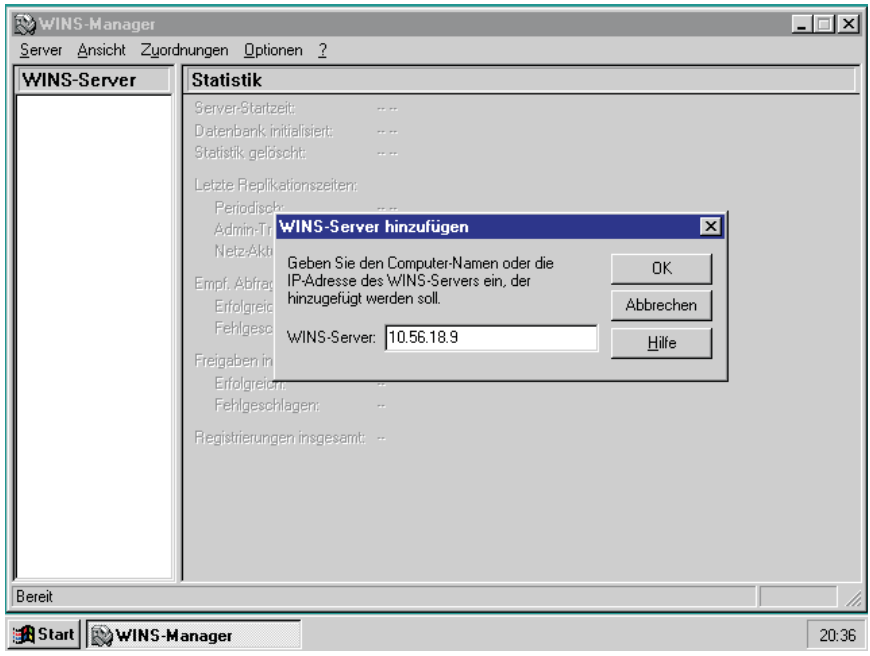


Abbildung 4.38: WINS-Server unter Windows NT einfügen

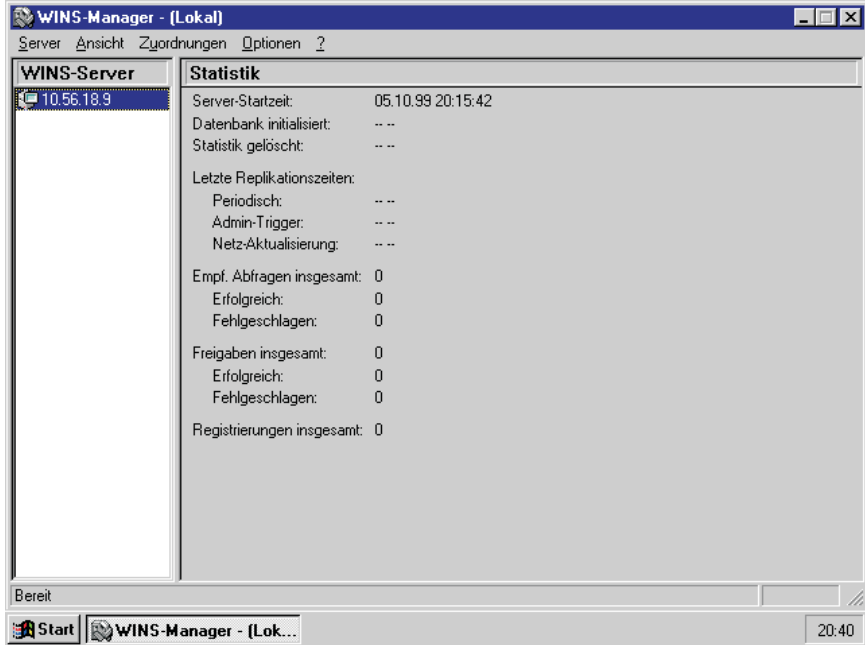


Abbildung 4.39: WINS-Statistik

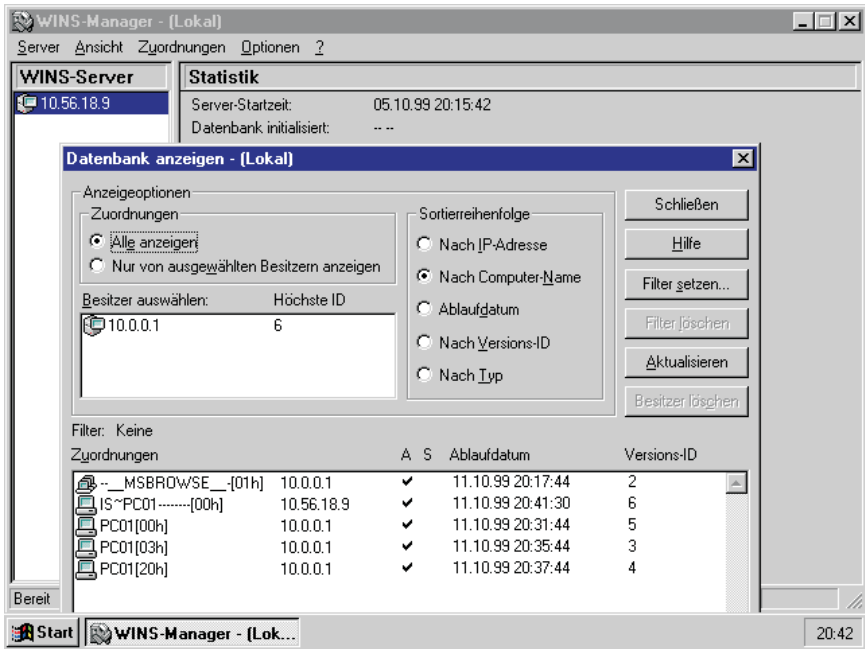


Abbildung 4.40: Registrierte WINS-Clients anzeigen lassen

Die aufgeführten Zuordnungen haben dabei folgende Bedeutung:

Element	Beschreibung
PC-Symbol	Eindeutiger Name
Verschachteltes PC-Symbol	Gruppeneintrag, wie Internet Gruppe oder ein mehrfach vernetzter PC
Name	Registrierter NetBIOS-Name
IP-Adresse	Dazugehörige IP-Adresse
A bzw. S	Aktiver dynamischer Eintrag bzw. statischer Eintrag
A in Verbindung mit Kreuz	Name nicht mehr aktiv
Versions-ID	Eindeutige Hexadezimalzahl, die bei der Replikation benötigt wird
Ablaufdatum	Definiert den Zeitpunkt, an dem der Eintrag abläuft

Tabelle 4.15: Elemente des WINS-Datenbankfensters

Um die einzelnen Intervalle der Namensregistrierung zu ändern, stellt der WINS-Manager unter dem Menüpunkt **Server, Konfiguration** ein Dialogfeld zur Verfügung.

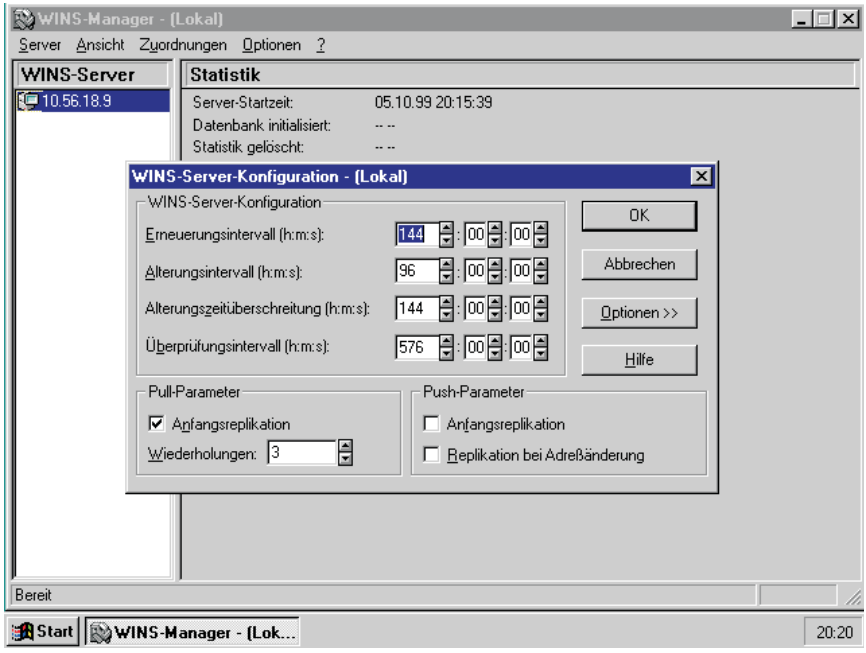


Abbildung 4.41: Aktualisierungsintervalle unter WINS

Die angezeigten Intervalle haben dabei folgende Bedeutung:

Erneuerungsintervall

Hier wird angegeben, wie oft die WINS-Clients ihre Namensregistrierung bei dem WINS-Server erneuern. Als Standardwert werden 144 Stunden vorgegeben.

Alterungsintervall

Kennzeichnet das Intervall zwischen dem Zeitpunkt – nicht mehr registriert – und dem Zeitpunkt – veraltet –. Auch hier beträgt der Standardwert 144 Stunden.

Alterungszeitüberschreitung

Kennzeichnet das Intervall zwischen dem Zeitpunkt – veraltet – und dem Zeitpunkt der Löschung aus der Datenbank. Dieser Wert darf nicht kleiner sein als 24 Stunden, wobei der Standardwert identisch ist mit dem Erneuerungsintervall.

Überprüfungsintervall

Nach Ablauf dieser Zeitspanne überprüft der WINS-Server ob Namen, die wegen Replikationen nicht mehr in seiner Verfügungsgewalt stehen, noch aktiv sind. Als minimaler Standardwert werden hier 576 Stunden zugrunde gelegt.

Datenbankreplikation zwischen WINS-Servern

Um einen Informationsaustausch zwischen mehreren WINS-Servern zu ermöglichen, der die Synchronisation mehrerer Datenbanken voraussetzt, müssen einige Einstellungen im WINS-Manager vorgenommen werden. Grundvoraussetzung für die Datenbankreplikation sind ein WINS-Server, der als Push-Partner und ein zweiter WINS-Server, der als Pull-Partner konfiguriert ist.

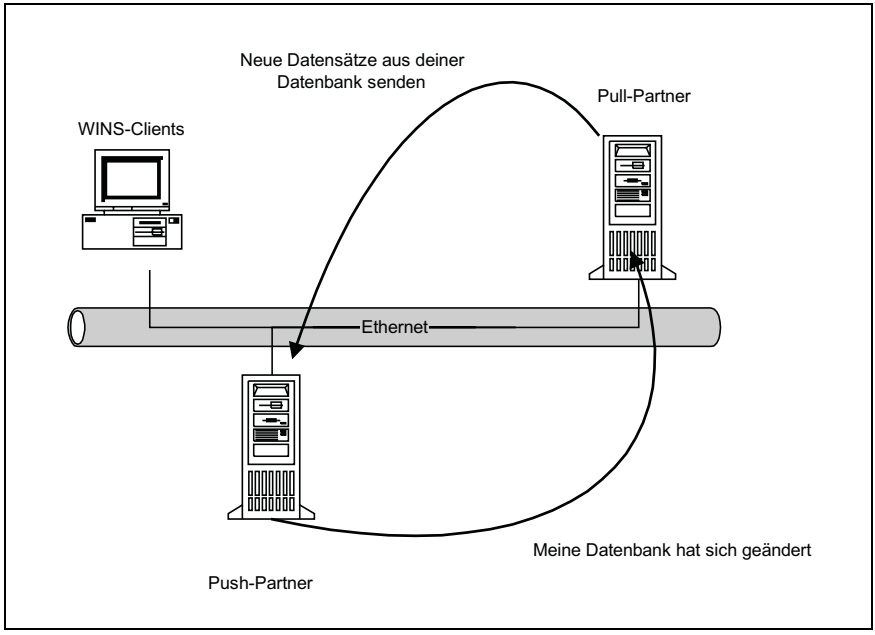


Abbildung 4.42: Datenbankreplikation von WINS-Servern

So fordert ein Pull-Partner neue Datenbankeinträge aus einer WINS-Datenbank an. Der Push-Partner hingegen sendet eine Benachrichtigung an seine Pull-Partner, sobald sich seine WINS-Datenbank geändert hat.

Deshalb muss mindestens ein zweiter WINS-Server über den WINS-Manager hinzugefügt werden.

Sind alle Voraussetzungen gegeben, kann eine Replikation über eine der vier folgenden Möglichkeiten initiiert werden.

Systemstart	Nachdem ein Replikationspartner konfiguriert wurde, fordert der WINS-Dienst bei jedem Start automatisch Kopien von Datenbankeinträgen an.
Zeitintervall	Nach einem festgelegten Zeitintervall wird die Replikation gestartet. Je kleiner dieses Zeitintervall ist, desto synchroner sind die Datenbankeinträge der beteiligten Replikationspartner.

Manuell — Manuell kann die Replikation im WINS-Manager über das Dialogfeld **Replikationspartner, Jetzt replizieren** angestoßen werden.

Schwellenwert — Die Replikation erfolgt, sobald ein WINS-Server einen vordefinierten Schwellenwert überschreitet. Wird dieser Aktualisierungszähler erreicht, benachrichtigt der WINS-Server seine Replikationspartner, in diesem Beispiel die Pull-Partner, die dann ihrerseits Kopien der neuen Datenbankeinträge anfordern.

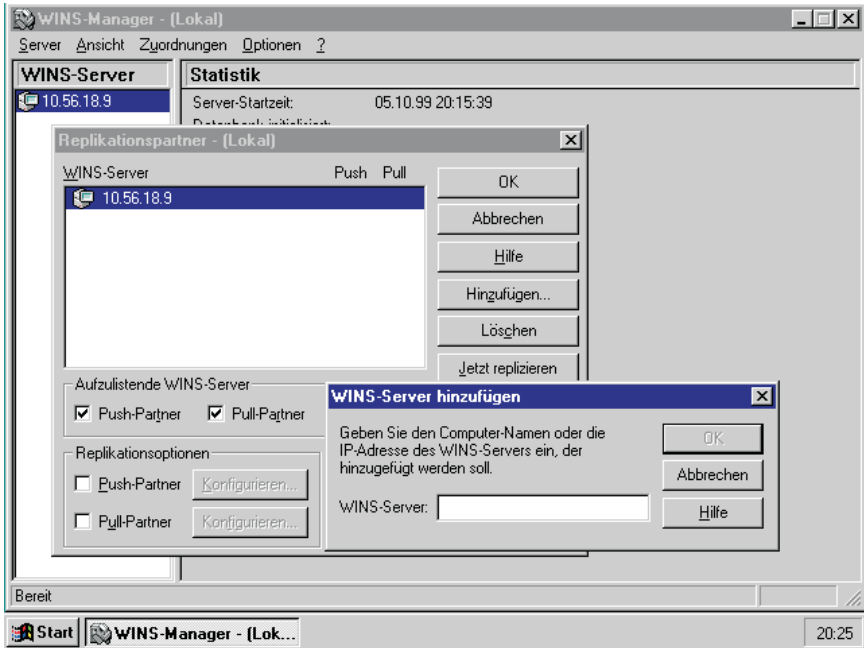


Abbildung 4.43: Konfiguration von WINS-Replikationspartnern

Ein Push mit Ausbreitung bewirkt, dass alle dafür konfigurierten Replikationspartner neue Datenbankeinträge automatisch erhalten.

4.6.13 Ping (Packet InterNet Groper)

Bei Ping handelt es sich um ein Dienstprogramm zum Testen der Connectivity zu anderen Hosts im Netzwerkverbund. Ping verwendet dazu die ICMP-Statusmeldungen »echo request« sowie »echo reply«, um festzustellen, ob ein adressierter Host verfügbar ist und fehlerfrei angesprochen werden kann.

Dadurch wird die Diagnose von Verbindungsfehlern erheblich erleichtert.

Die Spezifikationen des Packet InterNet Groper sind im RFC 862 veröffentlicht.

Praxis

Ping ist ein sehr einfaches Programm, das auf der DOS-Befehlsebene mit mehreren Parametern aufgerufen wird.

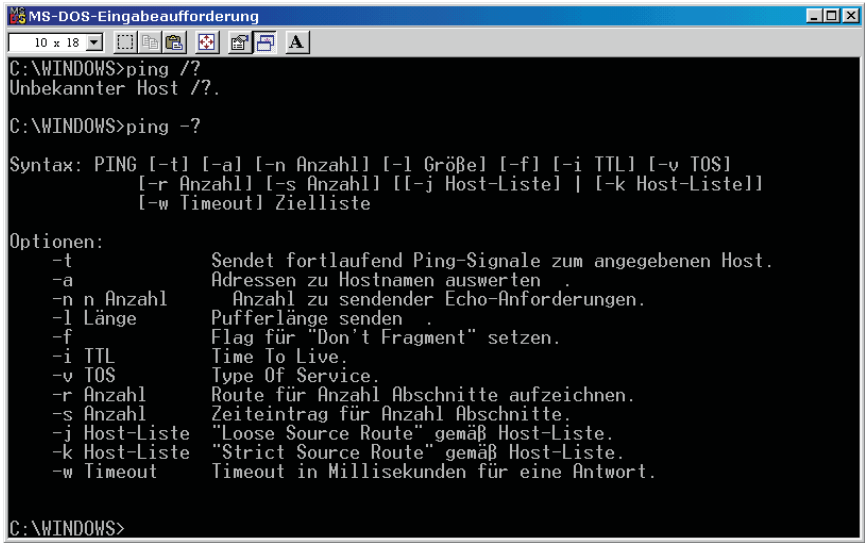


Abbildung 4.44: Parameterübersicht Ping

Die einfachste Anwendung besteht darin, eine IP-Adresse oder einen Host-Namen als Parameter einzugeben. Sofern das Ping erfolgreich ausgeführt werden konnte, wird z.B. unter Windows folgende Statusmeldung angezeigt:

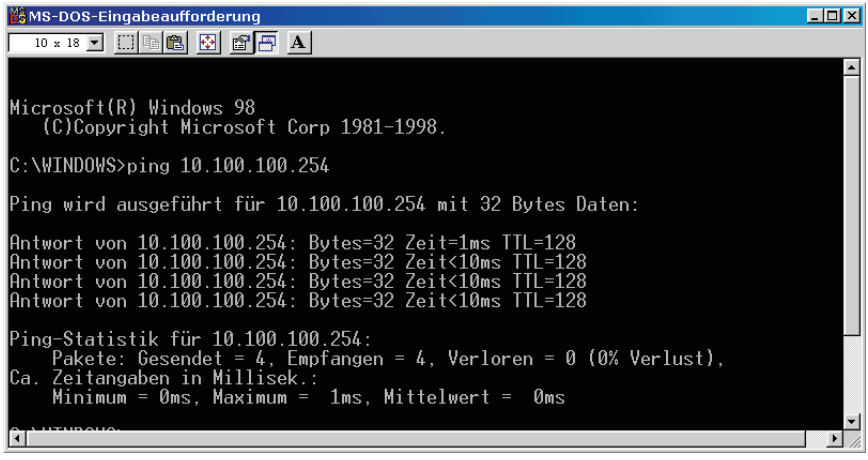


Abbildung 4.45: Ping in der Anwendung

Ping kann auch eingesetzt werden, um die ordnungsgemäße Installation von TCP/IP auf dem eigenen Host zu testen. Zu diesem Zweck wird ein Ping auf die eigene IP-Adresse durchgeführt. Diese kann mit dem Dienstprogramm IPCONFIG an der Eingabeaufforderung abgefragt werden. Wird ein Ping auf die real existierende IP-Adresse durchgeführt, dann wird auch die Funktionalität der Netzwerkkarte überprüft.

Alternativ zur eigenen IP-Adresse kann auch die für jeden Host gleiche Loopback-Adresse 127.0.0.1 verwendet werden. Ein über die Loopback-Adresse abgesendetes Ping umgeht jedoch dabei die Netzwerkkarte vollständig. Wurde TCP/IP nicht ordnungsgemäß installiert oder falsch konfiguriert, überschreitet Ping die zulässige Zeit, und es wird eine entsprechende Statusmeldung angezeigt.

Damit stellt Ping ein einfaches, aber sehr mächtiges Diagnoseprogramm dar. So kann es auch dazu eingesetzt werden, die IP-Adresse eines Hosts zu ermitteln, dessen Domänenname bekannt ist. Dazu müssen Sie nur den Domänennamen als Parameter übergeben.

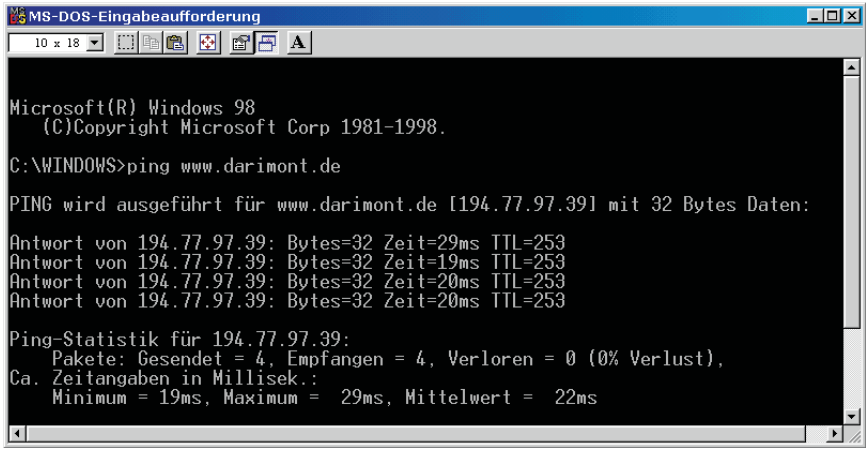


Abbildung 4.46: IP-Adresse mit Ping ermitteln

Netzadministratoren nutzen Ping, um eine erste Fehlerdiagnose durchzuführen. Alle aktiven Komponenten im Netz, Hosts, Router, Switches oder Drucker, besitzen eine IP-Adresse und können damit »angepingt« werden, um festzustellen, ob sie noch betriebsbereit sind.

4.6.14 DNS (Domain Name System)

Geschaffen wurde Domain Name System, um Computern anstelle der rechnerfreundlichen IP-Adresse auch menschenfreundlichere logische Namen zuordnen zu können. So ist es einfacher, den Domain-Namen coni.edelsteine.de einzugeben, als beispielsweise die zugehörige IP-Adresse 132.109.155.67. Die Spezifikationen des Domain Name System sind in den RFCs 881, 882, 883,1034 und 1035 veröffentlicht.

Ein Domain Name System Computer-Name besteht dabei aus zwei Teilen, dem Host-Namen und dem Domänen-Namen. Diese beiden Komponenten bilden dann den so genannten FQDN, Fully Qualified Domain Name.

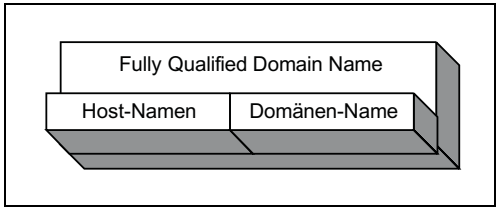


Abbildung 4.47: Struktur eines Domänennamens

Bevor DNS zum Einsatz kam, verwendete man zum Zweck der Namensauflösung im Internet eine Datei mit dem Namen »HOSTS.TXT«, die zentral über das Stanford Research Instituts Network Information Center des Defense Data Networks, SRI-NIC.DDN.MIL, verteilt wurde. Diese statische, manuell erstellte und gepflegte Datei enthielt die Zuordnung aller im Internet angeschlossenen Host-Namen mit den dazugehörigen IP-Adressen. Mit dem File Transfer Protocol wurde diese Datei dann an alle im Internet angeschlossenen Computer verteilt. Um die Daten auf allen Computern synchron zu halten, musste dieser Vorgang natürlich nach jeder Änderung an der Originaldatei wiederholt werden.

Beispieldatei HOSTS:

```
# Copyright (c) 1993-1995 Microsoft Corp.
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows NT
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#       102.54.94.97     rhino.acme.com     # source server
#       38.25.63.10      x.acme.comz        # x client host
127.0.0.1    localhost
```

Bedingt durch den rasanten Anstieg der im Internet angeschlossenen Computer war dieses Verfahren schon bald nicht mehr einsetzbar. Denn proportional mit dem Ansteigen der Dateieinträge nahm auch die Größe der Datei zu, und konnte so nicht mehr synchron auf allen Rechnern gehalten werden. Deshalb ging man dazu über, die Daten auf Domain Name Servern in einer Datenbank

zu verwalten. Darüber hinaus hat ein Administrator mit dem Domain Name System in Verbindung mit Subnetting die Möglichkeit, das eigene Netzwerk in autonome Zonen aufzuteilen.

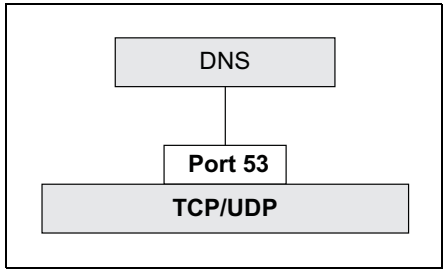


Abbildung 4.48: DNS-Socket

Das Domain Name System selbst stellt eine verteilte, hierarchische Datenbankanwendung dar und verwendet die Protokolle TCP und UDP über den Port 53.

Domain Name Space

Die im Domain Name Service verwendeten Domain-Namen basieren ausgehend von einer so genannten Root auf einem baumartigen, hierarchisch strukturierten Namenskonzept. Jede Verzweigung stellt eine Verwaltungseinheit dar, die Domain, die im Zusammenhang mit DNS Zone genannt wird. Der Domain-Name selbst dient dazu, ein Netzwerk im Internet eindeutig zu identifizieren. Deshalb müssen Internet-Domains zentral registriert werden. Innerhalb der eigenen Domain kann der Besitzer eine weitere Strukturierung durchführen. Dabei entstehen so genannte Subdomänen, für deren Verwaltung der Domain-Besitzer selbst verantwortlich ist. Dies führt dazu, dass er in der Regel einen eigenen DNS-Server installieren und warten muss. Sie erfahren unter anderem in den folgenden Abschnitten, wie DNS-Server unter Windows NT installiert und konfiguriert werden. Damit ist ein wichtiger Grundstein für den Aufbau heterogener IP-Netzwerke gelegt.

Zonen

Eine Zone ist eine Verzweigung innerhalb der Baumstruktur der DNS-Datenbank, die als autonome Einheit verwaltet wird. Die Zone kann dabei aus einer einzelnen Domäne oder einer Domäne mit Teildomänen bestehen. Die Teildomänen der unteren Ebenen einer Zone können wiederum in eigene Zonen aufgeteilt werden.

Somit stellt eine Zone die verwaltungstechnische Einheit des Domain Name System dar und definiert, welche Adressinformationen auf welchem Domain Name Server verwaltet werden, wobei ein Domain Name Server mehrere Zonendateien verwalten kann. In diesen Zonendateien werden die Internet-Namen mit den dazugehörigen Adressinformationen verwaltet. Durch das Anlegen von Zonen kann zusätzlich eine dezentrale Administration erreicht werden.

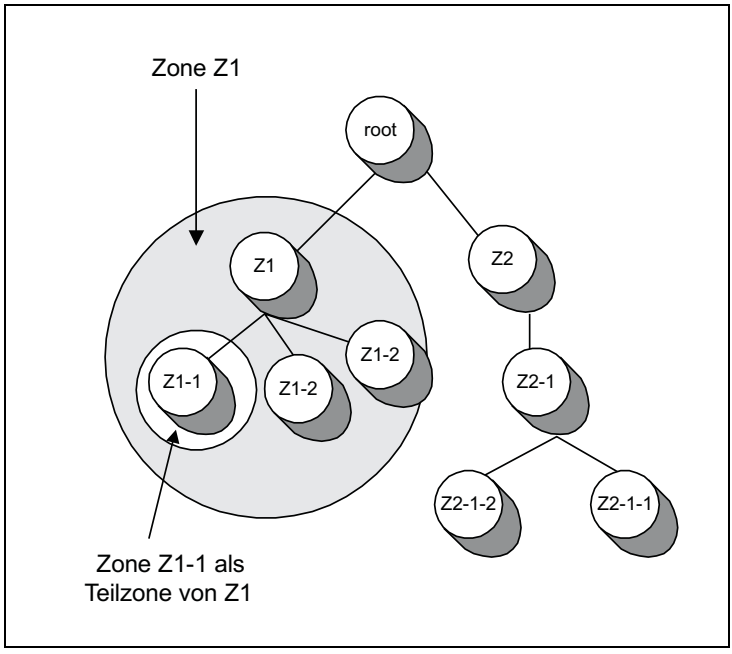


Abbildung 4.49: Zonen im DNS

Allgemein kann man auch sagen, dass eine Zone den Bereich darstellt, für den ein DNS-Server verantwortlich ist.

Aufbau von Domain-Namen

Domain-Namen werden mit Hilfe der Punktnotation unterteilt. Der Domain-Name ist dabei ein Abbildung des hierarchischen Name Space und beginnt mit der Angabe des Pfades vom Zweig bis zur Root.

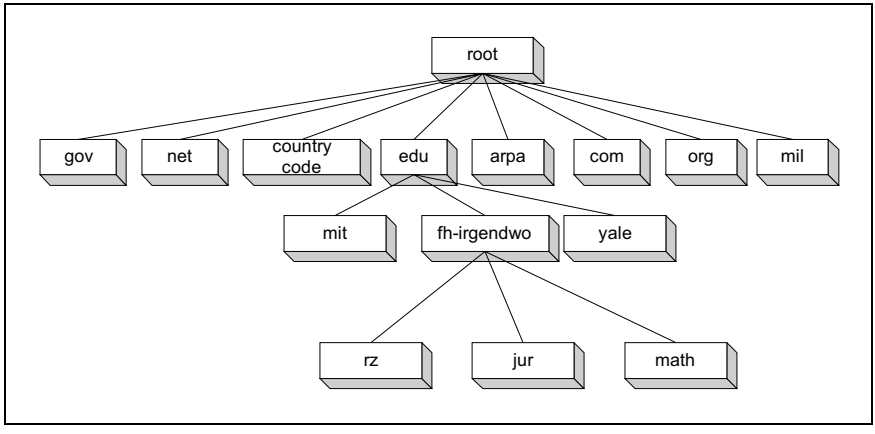


Abbildung 4.50: Der Name Space des Internets als hierarchischer Baum

Beispiel: **rz.fh-irgendwo.edu**

Im obigen Beispiel heißt die Domain **rz**. Diese liegt in der Domain **fh-irgendwo** und diese wiederum gehört zur Domain **edu**. Die Domain **edu** liegt unmittelbar unter der Root des Internets und gehört deshalb zu den Top Level Domains.

Abbildung 4.50 zeigt den für das Internet gültigen Namensraum. Hier wird zwischen den Top Level Domains direkt unterhalb der Root und den sich dann anschließenden Sublevel Domains unterschieden.

Üblicherweise verwendet man die Top Level Domain des Country Codes, z.B. de für Deutschland oder it für Italien. Eine Aufnahme in eine organisatorische Top Level Domain, das sind dann alle anderen, ist nur unter bestimmten Voraussetzungen möglich und ist sorgfältig zu begründen. Liegt keine stichhaltige Argumentation vor, wird der Antrag von dem zuständigen Network Information Center und den Internet-Registraturen abgelehnt.

Top Level Domains

Zurzeit stehen im Internet nachfolgende Top Level Domains zur Verfügung.

Domain Name	Bedeutung
arpa	ARPANET Domain
com	Commercial Organisation
edu	Educational Institutions
gov	Government Institutions
mil	Military Groups
net	Major Networking Support Centers
Org	Alle anderen Organisationen
Country Code	Alle Länder Codes, außer USA

Tabelle 4.16: Top Level Domains des Internets

Organisatorische Top Level Domains stammen aus der Zeit, als das Internet noch hauptsächlich auf Nordamerika beschränkt war. Aus diesem Grund werden diese Domains auch ausschließlich vom Inter-NIC vergeben und verwaltet. Die im Februar 1997 von der International Ad Hoc Committee, **IAHC**, vorgestellten sieben weiteren Top Level Domains konnten sich bis zum heutigen Tag nicht durchsetzen.

Domain Name	Bedeutung
store	Waren und Dienstleistungen im Internet
firm	Unternehmen
web	Webbezogene Aktivitäten

Tabelle 4.17: Top Level Domains des IAHC

Domain Name	Bedeutung
arts	Kunst
rec	Unterhaltung
info	Informationsanbieter
nom	Individuelle Namengebung

Tabelle 4.17: Top Level Domains des IAHC

Seit 1998 ist die ICANN, Internet Corporation for Assigned Names and Numbers, damit beauftragt, Top Level Domains und die Vergabe von IP-Adressen zu verwalten.

Um eine Domäne weiter zu strukturieren, kann es innerhalb einer Domäne weitere Subdomänen geben, wobei diese Strukturierung auf unterschiedliche Weise erfolgen kann. Denkbar ist eine räumliche oder aber auch eine organisatorische Strukturierung, wobei, wie schon oben erwähnt, das Unternehmen selbst für die Strukturierung verantwortlich ist.

Wie bereits beschrieben, dient der Domain-Name dazu, ein Netzwerk eindeutig zu identifizieren. Der Domain-Name wird bei der Arbeit im Internet über das IAB vergeben und sollte sorgfältig ausgewählt werden, da Änderungen recht aufwändig sind und von den Providern auch nicht mehr kostenlos durchgeführt werden.

Ein einprägsamer Name, aus dem die Firmenbezeichnung hervorgeht, bietet sich geradezu an. Um jedoch die Eindeutigkeit des Domain-Namen zu gewährleisten, sollte man sich vor der Beantragung des Domain-Namens vergewissern, dass keine andere Institution diesen Namen verwendet. Auskunft darüber erteilt das zuständige Network Information Center oder der Provider. Auch der Host-Name sollte sorgfältig und einprägsam gewählt werden.

Domain Name Server

Wie in hierarchischen Systemen üblich, kennt ein Domain-Name-Server immer nur den nächsthöheren und nächsttieferen Domain Server der jeweiligen Domain. Wenn ein DNS-Server eine Anfrage zu einer Namensauflösung nicht beantworten kann, dann sendet er die Anforderung an den ihm bekannten nächsthöheren Server. Dieser Vorgang wiederholt sich so lange, bis ein DNS-Server die Anfrage beantworten kann und diese dann wieder nach unten weitergibt. Der DNS-Server, der die Anfrage weitergeleitet hat, wird die erhaltenen Daten in einem lokalen Cache-Speicher ablegen. Nachfolgende Anfragen zur gleichen Namensauflösung können dann direkt beantwortet werden.

Bei einem Domain-Name-Server kann es sich um einen Primary-, Secondary- oder Master- Name-Server handeln. In jeder Zone befindet sich immer ein Primary-Domain-Name- Server, der alle Namen mit den dazugehörigen Adressen im Original beinhaltet. Jede Änderung von Informationen für diese Zone wer-

den demzufolge auch auf diesem Server durchgeführt. DNS-Server, die auf einer Hierarchieebene alle Zoneninformationen verbindlich zur Verfügung stellen, werden als zuständige Autorität bezeichnet, authoritativ.

Aus Sicherheitsgründen verfügt jede Zone über einen Secondary-Domain-Server, der bei Bedarf einspringt. Dieser Bedarf entsteht unter anderem, wenn der Primary-Domain-Name- Server ausgefallen oder belegt ist. Ein Secondary-Name-Server erhält über einen so genannten Zonentransfer vom Primary-Name-Server oder von einem anderen Secondary- Name-Server eine Kopie der Zoneninformationen.

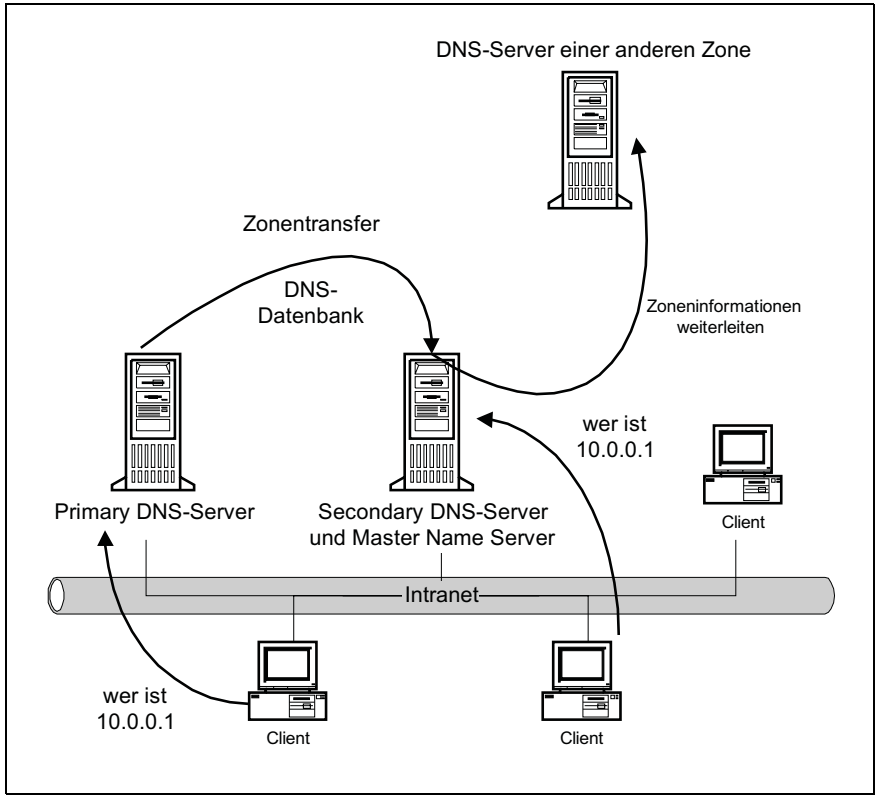


Abbildung 4.51: DNS-Server im Netz

Damit stellen der Primary- und der Secondary-Name-Server die gleichen Informationen zur Verfügung. Darüber hinaus wird mit dem Einsatz eines Secondary-Name-Servers die Datenlast reduziert und ein schnellerer Zugriff für Remote-Standorte erreicht. Der Master- Name-Server wird zur Weiterleitung von Zoneninformationen eingesetzt. Dabei kann es sich um einen Primary- oder aber auch um einen Secondary-Name-Server handeln, da beide Zoneninformationen weiterleiten können.

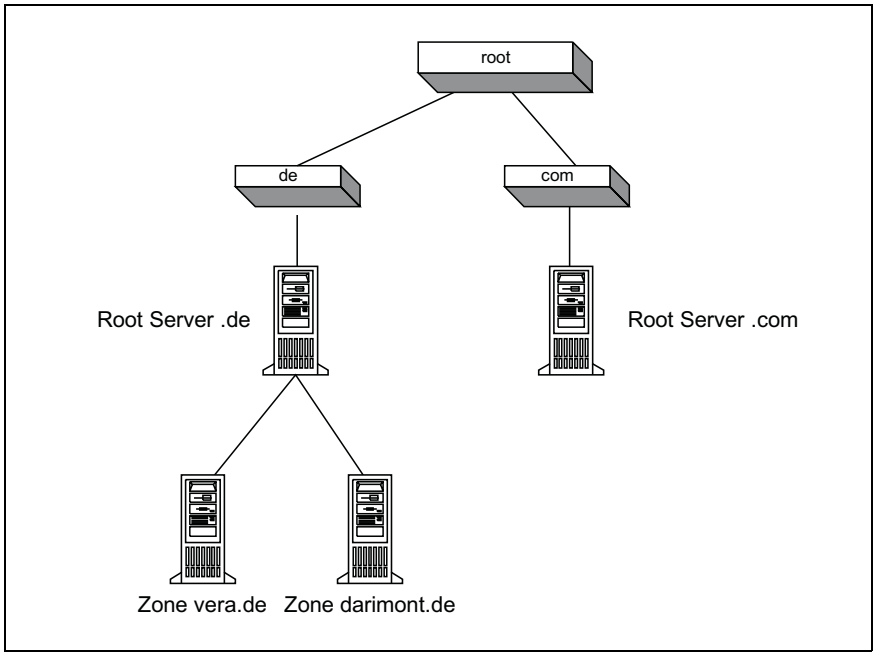


Abbildung 4.52: Root-Server im DNS-Baum

DNS-Autoritäten auf der Ebene der Top-Level-Domains-Server werden als *Root-Server* bezeichnet. Root-Server enthalten alle Informationen, die von DNS-Servern auf der Zonenebene benötigt werden, um einen beliebigen Namen auflösen zu können. So kann z.B. der Root-Server der Domain .de nicht alle Namen auflösen, er kann aber untergeordneten Servern mitteilen, welche anderen Server diese Informationen bereithalten. Abbildung 4.52 zeigt das hier beschriebene Prinzip.

Domain Name Service Resolver

Domain Name Service Resolver sind Programme, die für einen Client Namensanforderungen zwischen Anwendungen und Name Server weiterleiten. In der Regel verfügt ein Resolver zu diesem Zweck über die Adressen von zwei DNS-Servern. Durch diese Weiterleitung wird ein logischer Name der dazugehörigen IP-Adresse zugeordnet. Häufig ist der Domain Name Service Resolver in der Anwendung integriert oder wird alternativ dazu als Bibliotheksroutine ausgeführt.

Bei einer **Resolver-Abfrage** wird auf den ersten der beiden Name-Server zugegriffen. Ist dieser Name-Server nicht dazu in der Lage, eine Abfrage zu beantworten, werden gegebenenfalls andere Name-Server kontaktiert, um die benötigten Informationen zu erhalten. Wird dieses Kontaktieren vom Resolver nicht gewünscht, übermittelt der Name- Server standardmäßig eine positive Antwort oder aber eine Fehlermeldung. Insgesamt unterscheidet man dabei drei unterschiedliche Abfragen:

Bei einer **rekursiven Abfrage** wird der adressierte DNS-Server aufgefordert, die angefragten Informationen auszugeben. Liegen die angeforderten Informationen bzw. ein aufzulösender Domain-Name nicht vor, erfolgt statt dessen eine Fehlermeldung. Ein Verweis auf einen anderen Name-Server zur Beantwortung der Abfrage kann dabei nicht erfolgen.

Erfolgt hingegen eine **iterative Abfrage**, dann gibt der abgefragte DNS-Server die am ehesten geeignete Antwort an den anfragenden Resolver zurück. Diese Antwort beinhaltet entweder die angefragten Informationen oder aber einen Verweis auf einen anderen DNS-Server, der in der Lage ist, die Abfrage des Resolver zu beantworten.

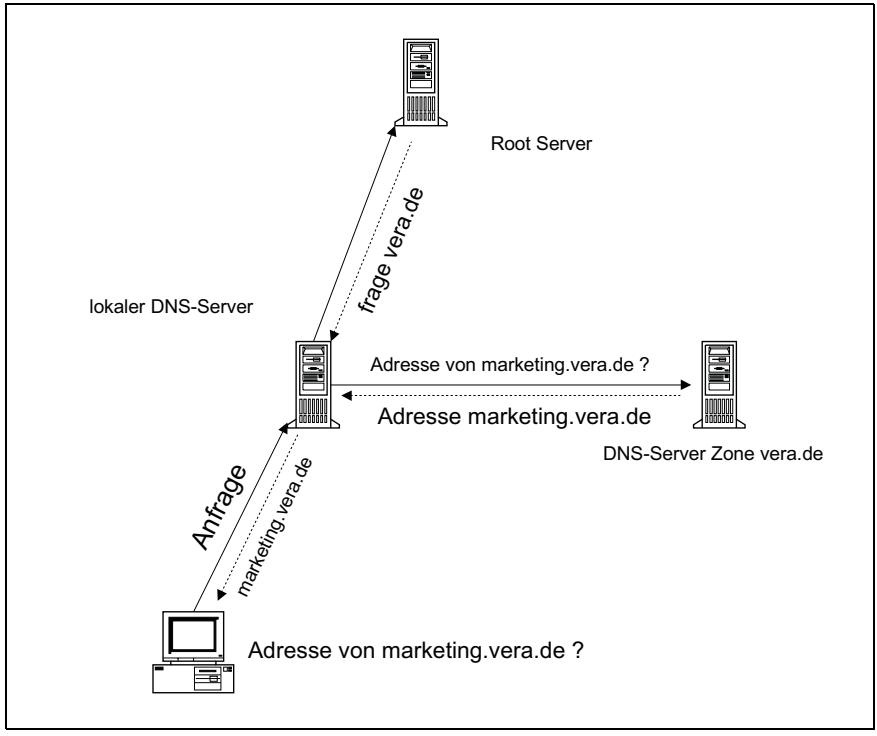


Abbildung 4.53: Iterative Namensauflösung im DNS-System

Bei einer **inversen** Abfrage wird die Suche in allen angeschlossenen Domänen durchgeführt.

Beispielkonfiguration DNS unter Windows NT 4.0

Anhand des nachfolgenden Beispiels soll die Einrichtung von DNS unter Windows NT 4.0 demonstriert werden.

Der DNS-Server-Dienst von Microsoft realisiert einen RFC-kompatiblen DNS-Server und kann dadurch mit anderen DNS-Servern zusammenarbeiten. Dazu werden standardmäßig von dem DNS-Server die notwendigen DNS-Zonendateien mit Unterstützung aller Typen von Standard-Ressourceneinträgen, die in RFC 1034, 1035 und 1183 definiert sind, erstellt und verwendet. Diese Informationen werden Resource Records, **RR**, genannt. Wird der DNS-Server-Dienst in der richtigen Reihenfolge installiert, dann werden die benötigten SOA-, A- und NS-Records, basierend auf den angegebenen Domänen- und Host-Namen, automatisch generiert. Dazu ist es notwendig, vor dem Hinzufügen des DNS-Dienstes über die Registrierkarte des DNS-Servers die später verwendeten Angaben einzutragen.

Konfigurationsdateien

Für den DNS Server Dienst unter Windows NT 4.0 werden standardmäßig vier Konfigurationsdateien erstellt, die auch manuell editiert werden können.

Datenbankdatei	In dieser Datei werden die Records für eine Domäne gespeichert. Abhängig von dem verwendeten Zonennamen lautet diese Datenbankdatei bei einem Zonennamen von sydney.com beispielsweise sydney.com.dns. Windows NT 4.0 stellt als Dateivorlage eine Datenbankdatei mit dem Namen place.dns zur Verfügung, die bei Verwendung jedoch an die vorhandene Struktur des Unternehmens angepasst werden sollte.
Cache-Datei	Alle Einträge der Root-Name-Server sind in dieser Datei enthalten. Root-Name-Server stellen alle Informationen zur Verfügung, die ein DNS-Server für den Zonenaustausch mit höheren Hierarchieebenen benötigt. In der Standard Cache-Datei unter NT 4.0 sind Datensätze für alle Root-Server im Internet vordefiniert. Erfolgt jedoch kein Zugang zum Internet, muss diese Datei entsprechend der Unternehmensstruktur geändert werden. Eine Standard-Cache Datei kann über die Adresse *ftp.rs.internic.net* aus dem Internet kopiert werden.
Reverse-Lookup-Datei	Diese Datei wird benötigt, damit ein Name-Server inverse Abfragen auswerten kann. Generiert werden dazu SOA-, NS- und Pointer-Einträge, die den Einträgen anderer Zonendateien der DNS-Datenbank entsprechen.

Boot-Datei	Die Boot-Datei überwacht den Startvorgang des DNS-Servers bei der **BIND**-spezifischen, Berkeley Internet Name Daemon, Implementierung. Da sie in keinem RFC definiert ist, ist sie auch nicht zwingend erforderlich.

Ressourceneinträge nach RFC 1034, 1035 und 1183

Die folgenden Abschnitte bieten einen Überblick über die DNS-Datensätze. Die hier beschriebenen Kennungen müssen Sie dann manuell eintragen, wenn Sie mit einem Server arbeiten, der keine grafische Benutzerschnittstelle mit entsprechenden Dialogfenstern zur Verfügung stellt. Mit anderen Worten, die unten beschriebenen Details müssen nur bekannt sein, wenn Sie die oben erwähnten vier Dateien von Hand editieren müssen.

SOA-Eintrag (Start of Authority)

In jeder Datenbank muss sich als erster Eintrag ein SOA-Eintrag befinden, der die allgemeinen Parameter für die DNS-Zone definiert. Bei dem Hinzufügen von SOA-Records sind folgende Regeln zu beachten:

- ✔ Gehen Zeilenumbrüche über mehr als eine Zeile, müssen diese in Klammern (geschweift) gesetzt werden.
- ✔ Endet ein Host-Name nicht mit einem Dezimalpunkt, wird dieser Host-Name an die Stammdomäne angehängt.
- ✔ Das @-Zeichen bedeutet »dieser Server«.
- ✔ In der E-Mail-Adresse des Administrators wird das @-Zeichen durch einen Dezimalpunkt ersetzt.
- ✔ Ein Internet-Eintrag wird durch IN gekennzeichnet.

Die folgenden Zeilen zeigen ein Beispiel. Nach dem Semikolon stehen die Kommentare zu den in der gleichen Zeile stehenden Werten. Der SOA-Record selbst definiert den Rechner clara als DNS-Server für die Domäne darimont.im.netz.de.

BEISPIEL

```
@ IN     SOA    clara.darimont.im.netz.de        root.darimont.im.netz.de (
97070700        ; Seriennummer, muß einmalig sein und dient der Replikation
10800           ; Refresh-Zeit, hier 3 Stunden
; Zeit, hier 1 Stunde, nach der eine erneute Kontaktaufnahme
 erfolgen soll, wenn ein übergeordneter Server nicht erreicht werden kann
3600000
; Zeit, die ein sekundärer Server Zoneninformationen speichert, die er nicht
 aktualisieren kann, hier 1 Jahr
86400; Standardzeit für die Gültigkeitsdauer von Zonen-
informationen, hier 24 Stunden  )
IN A 10.100.100.004  ; Adresse des DNS Servers
IN MX admin.darimont.im.netz.de; E-
Mail Adresse für den Administrator des DNS
```

NS-Eintrag (Name-Server)

Über einen NS-Eintrag werden zusätzliche Name-Server aufgelistet. Dabei ist es durchaus möglich, dass eine Datenbankdatei mehr als einen Name-Server beinhaltet.

Beispiel: `@ IN NS nameserver3.jager.com`

Host-Eintrag (A-Eintrag)

Über einen A-Eintrag wird eine endgültige Zuordnung zwischen einem Host-Namen und einer IP-Adresse hergestellt. Da über die A-Records die Host-Namen zugeordnet werden, repräsentieren sie naturgemäß die meisten Einträge.

Beispiel: `vincent IN A 12.2.9.98`

PTR-Einträge (Pointer-Einträge)

Über die Pointer-Einträge erfolgt eine Zuordnung von Adressen und Namen innerhalb einer Zone, wobei die Suche in umgekehrter Reihenfolge erfolgt. Deshalb wird bei der Erstellung eines Pointer-Datensatzes die IP-Adresse in umgekehrter Reihenfolge geschrieben und an die Adresse »in-addr.arpa« angehängt. Dieser Vorgang heißt reverse Abbildung. Soll beispielsweise der Name für die IP-Adresse 12.2.9.98 ermittelt werden, ist eine Pointer-Abfrage für den Namen »98.9.2.12.in-addr-arpa« notwendig.

Beispiel: `98.9.2.12.in-addr.arpa. IN PTR vincent`

Reverse Abbildungen sind notwendig, weil IP-Adressen sich nicht wie Domain-Namen hierarchisch strukturieren lassen. Aus diesem Grunde wurde die Domäne **arpa** aufgebaut, die die Wurzel einer Baumstruktur bildet, deren Zweige aus den Bytes der IP-Adresse bestehen. Diesen Zweigen werden dann die Domain-Namen zugeordnet. Die folgende Abbildung zeigt das hier beschriebene Prinzip und erklärt das oben aufgeführte Beispiel für einen Pointer-Datensatz.

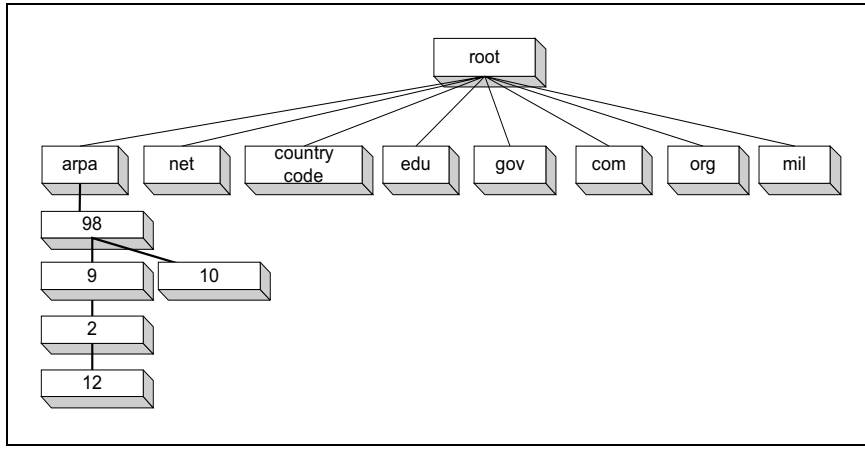


Abbildung 4.54: Pointer Adressen in der DNS.

CNAME-Eintrag (Canonical Name)

Über einen CNAME-Eintrag eröffnet sich die Möglichkeit, einer IP-Adresse mehrere Host-Namen als Alias-Namen zuzuordnen.

Beispiel:
```
Fileserver2   CNAME   sydney
www           CNAME   sydney
```

DNS-Implementierung

Grundvoraussetzung für die Installation des DNS-Dienstes ist die Installation von TCP/IP auf dem Server unter Verwendung des aktuellen Service Pack. Sollen die standardmäßigen SOA-, NS- und A-Einträge automatisch erstellt werden, müssen entsprechende Informationen vorgegeben werden. Gehen Sie dazu wie folgt vor:

Festlegung der Suchreihenfolge für den DNS-Server-Dienst

- ✔ Bringen Sie Ihre aktuell verwendete IP-Adresse in Erfahrung, und wechseln Sie über die Netzwerkumgebung zu den Eigenschaften von TCP/IP auf die Registrierkarte DNS.
- ✔ Geben Sie einen Domänennamen an, und legen Sie unter der Suchreihenfolge des DNS-Dienstes Ihren eigenen Server unter Angabe der IP-Adresse fest.

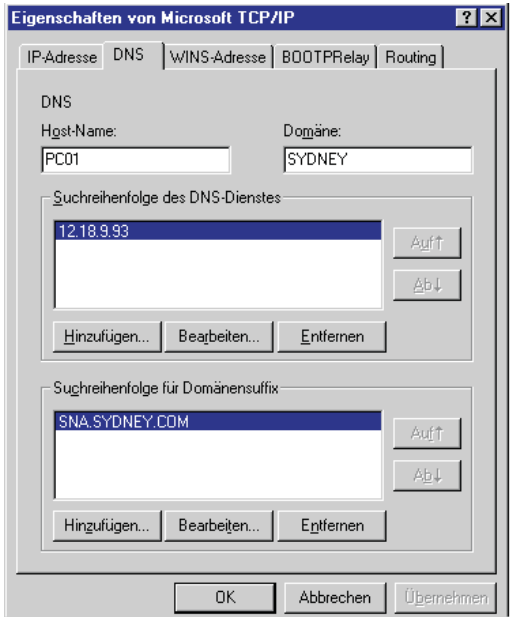


Abbildung 4.55: DNS-Suchreihenfolge unter Windows NT konfigurieren

Erläuterung zur Grafik

Host-Name	In diesem Eingabefeld wird der Name des eigenen Computersystems eingetragen, wobei standardmäßig der Setup-Name vorgegeben wird. Unter anderem wird dieser Name zu einem späteren Zeitpunkt auf dem DNS-Server mit entsprechender Zuordnung zur IP-Adresse gespeichert.
Domäne	Hier muss ein Name für die Domäne angegeben werden. Zusammen mit dem Host-Namen bildet dies dann den **FQDN**, Fully Qualified Domain Name. Erfolgt ein Zugang bzw. eine Namensauflösung über das Internet, muss dieser Domänenname aufgrund der Eindeutigkeit auch registriert sein.
Suchreihenfolge des DNS-Dienstes	In diesem Eingabefeld können bis zu drei DNS-Server aufgelistet werden, die sequentiell abgefragt werden. In der Praxis bedeutet dies, dass der erste DNS-Server auch über die normalerweise abgefragten Adressen verfügen sollte, um eine schnelle Namensauflösung zu gewährleisten.
Suchreihenfolge für Domänensuffix	Um zu gewährleisten, dass unterschiedliche Domänen durchsucht werden, erfolgt hier die Angabe unterschiedlicher Domänen.

Wird zum Beispiel der Name PC100 gesucht, und es liegen zwei Einträge mit den Namen arge.de sowie level.com vor, wird wie folgt aufgelöst:

PC100.arge.de

PC100.level.com

Installieren des DNS Server Dienstes

Die Installation des DNS-Servers kann relativ schnell durchgeführt werden. Es sind nur die drei folgenden Schritte notwendig.

- ✔ Klicken Sie in der Systemsteuerung auf das Symbol **Netzwerk/Dienste.**
- ✔ Über **Hinzufügen/DNS-Server** erfolgt das Laden der Software.
- ✔ Nachdem der Dienst hinzugefügt wurde, muss das System neu gestartet werden.

Konfiguration des DNS Server Dienstes mit Hilfe des DNS-Managers

Wie bereits erwähnt, kann der DNS-Server-Dienst manuell oder aber mit Hilfe des DNS-Managers konfiguriert und verwaltet werden. Die Konfiguration mit Hilfe des DNS-Managers wird im folgenden Abschnitt näher erläutert. Nachfolgende Grafik zeigt die automatisch erstellten Zonen unter dem DNS-Manager.

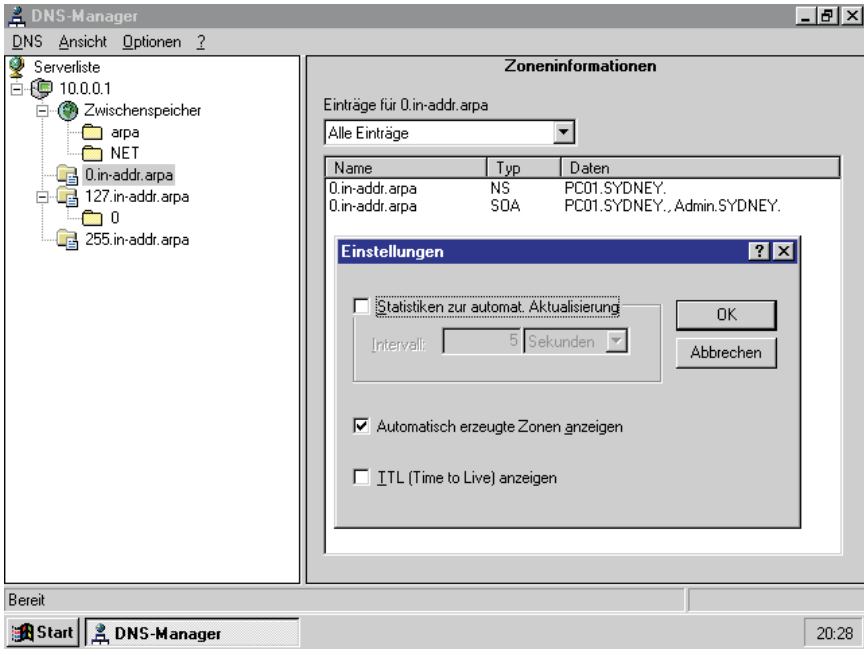


Abbildung 4.56: Implementierung DNS unter Windows NT – Zoneninformationen

Um über die entsprechenden Benutzerrechte verfügen zu können, ist es notwendig, dass Sie als Administrator am System angemeldet sind. Anschließend starten Sie den DNS-Manager in der Programmgruppe Verwaltung. Nach dem Start des Programms muss über die Registrierkarte DNS ein neuer Server hinzugefügt werden. Wahlweise kann hier die IP-Adresse oder aber der NetBIOS-Name angegeben werden. Für diesen neu definierten DNS-Server wird dann eine Zone angelegt, die als Zwischenspeicher bezeichnet ist. Zu diesem Zeitpunkt handelt es sich bei dem DNS-Server um ein ausschließlich cachendes System, dessen Einträge nach dem Abschalten verloren gehen würden.

Deshalb muss als nächster Schritt die Definition der Zonen für diesen Server erfolgen. Je nach Struktur erfolgt nun das Definieren des Zonentyps. Wie bereits im oberen Abschnitt erwähnt, wird beim Anlegen einer Zone mit dem Namen sydney.com automatisch die Zonendatei sydney.com.dns angelegt. Damit ist die Erstellung einer Zone bereits abgeschlossen. Als nächstes müssen nun die einzelnen Computer in Abhängigkeit der gültigen Ressourceneinträge definiert werden.

Unter der Voraussetzung, dass der Zwischenspeicher markiert ist, lassen sich über die Option **DNS/Neuer Host** neue Hosts hinzufügen. In dem angezeigten Dialogfeld müssen die IP-Adresse und der Host-Name angegeben werden. Alternativ dazu kann auch mit dem Befehl **Neuer Eintrag** gearbeitet werden, wodurch sich alle Typen von Ressource Records angeben lassen.

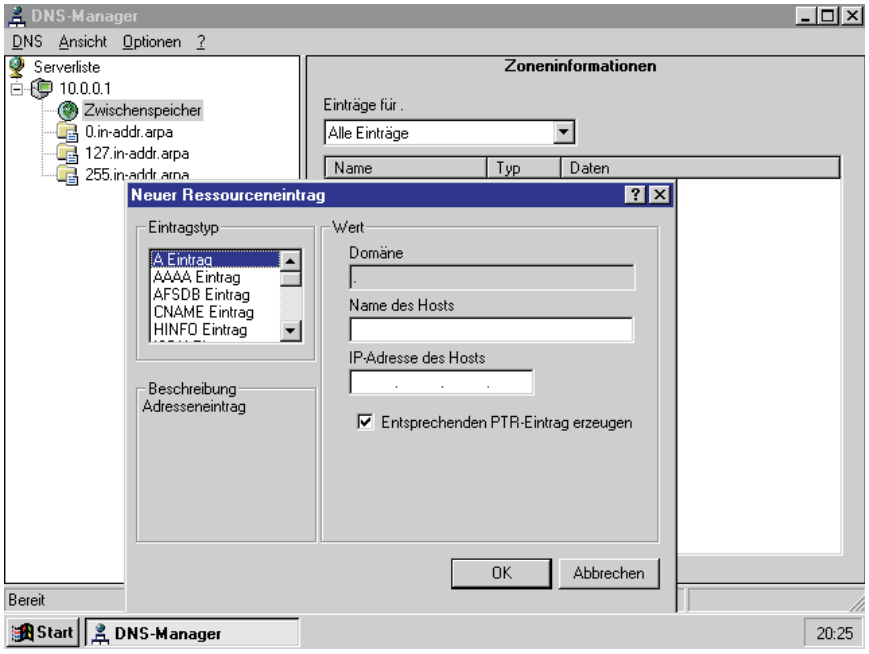


Abbildung 4.57: Implementierung DNS – Hinzufügen neuer Ressourceneinträge

Wahlweise können nun noch die Eigenschaften des DNS-Servers bzw. der Zonendatei verändert werden. Unter den Konfigurationseinstellungen für die Zone befinden sich die Registrierkarten Allgemein, SOA-Eintrag, Benachrichtigen und WINS-Reverse-Lookup.

Allgemein	Unter dieser Registrierkarte kann der Zonentyp sowie der Zonenname geändert werden.
SOA-Eintrag	Unter dieser Registrierkarte kann der Name des primären Name-Servers der Zone angegeben werden.
Benachrichtigen	Unter diesem Menüpunkt kann man eine Liste von DNS-Servern angeben, die bei Änderungen in der Zonendatei des primären Name-Servers benachrichtigt werden sollen. Daraufhin erfolgt dann der Zonentransfer.
WINS-Reverse-Lookup	Hier werden Einstellungen für die Interaktion zwischen DNS-Server und WINS-Server definiert.

So kann die dynamische Datenbank von einem WINS-Server mitbenutzt werden, ohne dass manuelle Einträge in der DNS-Datenbank vorgenommen werden müssen.

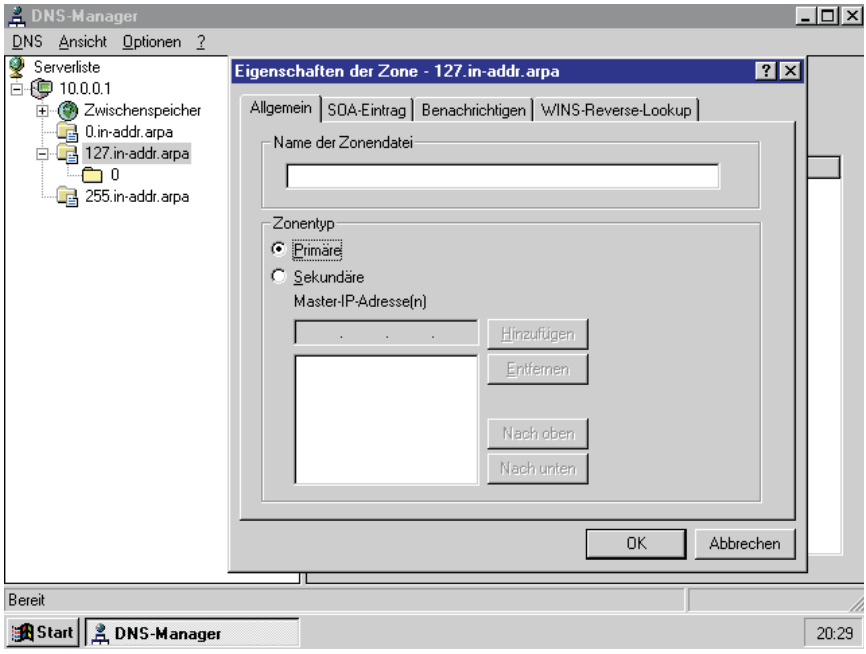


Abbildung 4.58: Implementierung DNS – Eigenschaften einer Zone festlegen

4.6.15 DDNS, Dynamic Domain Name Service

Wie Sie oben erfahren haben, wird DNS (Domain Name Service) verwendet, um in Netzwerken mit TCP/IP als Protokoll eine Namensauswertung von Computernamen zu IP-Adressen durchzuführen. Vereinfacht ausgedrückt übersetzt DNS einen für Menschen leicht verständlichen Namen wie www.snav.de in eine IP-Adresse, da diese von Computern leichter interpretiert werden kann, z.B. 93.18.9.01. DNS selbst ist ein statisches Datenbanksystem. Werden Namen und die zugeordneten Adressen allerdings nicht manuell eingegeben, so existieren sie auch nicht. Mit dem Betriebssystem MS-Windows 2000 arbeitet DNS nun dynamisch. Jedoch sollte ein dynamisches DNS nur in einer reinen Windows 2000-Umgebung eingesetzt werden, da dieser Dienst elementar auf den Funktionen von DHCP 2000 (Dynamic Host Configuration Protocol, siehe Kapitel 4.6.16) und Active Directory aufbaut. Umgekehrt wird für die Verwendung von Active Directory auch unbedingt ein DNS-Server benötigt.

Windows 2000 benutzt den DNS-Server aber nicht nur zur reinen Namensauflösung, sondern auch dafür, um Dienste und Ressourcen im Netzwerk zu finden. Allerdings wird dieser neue Standard noch nicht von allen DNS-Servern unterstützt. Aus diesem Grund kann auch nicht irgendein beliebiger DNS-Server verwendet werden. Vielmehr benötigt Windows 2000 zur Funktion von Active Directory einen DDNS-Server. Nur hier kann Windows 2000 auch automatisch die Dienste und Ressourcen registrieren. Diese dynamische Registrierung von DNS-Einträgen für Windows 2000-Clients erfolgen über DHCP.

Standardmäßig ist ein DHCP-Server auch so konfiguriert, dass die DNS-Client-Informationen automatisch aktualisiert werden. Nachdem ein Client eine IP-Adresse vom DHCP-Server geleast hat, gibt es nun unterschiedliche Verhaltensweisen, die von dem verwendeten Betriebssystem des Clients abhängen.

Verhalten von Windows 2000 Clients:

- ✔ Ein Client sendet eine IP-Adressanforderung.
- ✔ Ein DHCP-Server bietet eine IP-Adresse an und genehmigt den Lease.
- ✔ Der DHCP-Client registriert seinen A-Eintrag (A=Address Record) beim DNS-Server.
- ✔ Der DHCP-Server registriert den PTR-Ressourceneintrag zur Reversezone des Clients beim DNS-Server.

Verhalten von Windows 95/96 und NT-Clients:

- ✔ Ein Client sendet eine IP-Adressanforderung.
- ✔ Ein DHCP-Server bietet eine IP-Adresse an und genehmigt den Lease.
- ✔ Der DHCP-Server registriert den A-Eintrag des Clients beim DNS-Server.
- ✔ Der DHCP-Server registriert den PTR-Ressourceneintrag zur Reversezone beim DNS-Server.

Der wesentliche Unterschied liegt also bei der Registrierung des A-Eintrages. So registriert ein Windows 2000-Client sich selbst beim DNS-Server, während ansonsten der DHCP-Server die Registrierung vornimmt.

Installation von DNS-Server

Ein DNS-Server kann wahlweise zusammen mit Windows 2000 oder aber auch nachträglich installiert werden. Wie bei NT 4.0 muss auch bei Windows 2000 darauf geachtet werden, dass der DNS-Server eine statische IP-Adresse verwendet. Um einen DNS-Server in eine bestehende Windows 2000 Umgebung zu installieren, gehen Sie wie folgt vor:

1. Starten Sie über einen Doppelklick in der Systemsteuerung den Ordner Software.
2. Im Ordner Software klicken Sie dann auf **Windows-Komponenten Hinzufügen/Entfernen**.
3. Aktivieren Sie die Option Netzwerkdienste und klicken Sie auf die Schaltfläche **Details**.
4. Aktivieren Sie anschließend im Dialogfeld Netzwerkdienste das Kontrollkästchen **DNS-Server**.
5. Bestätigen Sie Ihre Auswahl mit **OK** und dann auf **Weiter**.

6. Zuletzt müssen Sie noch den Pfad zu den Windows 2000-Installationsdateien angeben (z.B. C:\i386). Auch hier bestätigen Sie mit **OK**, um die Installation zu starten.

Startdatei

DNS benötigt zum Starten eine so genannte Startdatei. Diese Startdatei enthält wichtige Informationen über Pfadangaben zu den DNS-Konfigurationsdateien und deklariert, für welche Domänen ein DNS-Server zuständig ist. Diese Startdatei sollten Sie auf jeden Fall sichern damit sie verfügbar ist, wenn der DNS-Server erneut eingerichtet werden muss.

Cachedatei

In dieser Datei sind alle Hostinformationen, die eine grundlegende DNS-Verbindung ermöglichen, gespeichert. Im Detail handelt es sich dabei um die Adressen von Root-Nameservern wie .com und .edu.

Zonendatei

In einer Zonendatei ist jede Domäne, für die ein DNS-Server zuständig ist, eingetragen.

Konfiguration von DNS

Bei der Installation von DNS sind beim ersten Öffnen der DNS-Konsole einige Fragen zu beantworten. Der Assistent für die DNS-Serverkonfiguration öffnet sich dabei.

Zuerst werden Sie gefragt, ob der Server, den Sie installieren, der erste Server in der Domäne ist. Treffen Sie die entsprechende Auswahl und klicken Sie anschließend auf **Weiter**.

Bestätigen Sie im nächsten Schritt die Auswahl der Option mit **Ja**, um eine Forward-Lookupzone zu erstellen.

1. Klicken Sie auf **Weiter**.
2. Wählen Sie als Zonentyp Primär oder Sekundär und klicken Sie auf **Weiter**.
3. Geben Sie den neuen Zonennamen ein und klicken Sie auf **Weiter**.
4. Erstellen Sie eine neue Zonendatei und klicken Sie auf **Weiter**.
5. Zum Erstellen einer Reverse-Lookupzone wählen Sie die Option **Ja**, und klicken Sie anschließend auf **Weiter**.
6. Wählen Sie als Zonentyp die Option Primär oder die Option Sekundär und klicken Sie auf **Weiter**.
7. Geben Sie die Netzwerkkennung und den Namen für die Reverse-Lookupzone ein. Diese Angaben sind identisch mit dem sekundären Domänennamen des FQDN, Fully Qualified Domain Name. Klicken Sie anschließend auf **Weiter**.

8. Akzeptieren Sie den Dateinamen und klicken Sie auf **Weiter**.
9. Klicken Sie auf **Fertigstellen**.

Damit ist die Konfiguration abgeschlossen und Sie können mit der Verwaltung der Domänen und Zonen beginnen.

DNS-Server verwalten

Nachdem der DNS-Server installiert wurde, erfolgt nun die Verwaltung. Hierfür stehen einem DNS-Server drei wesentliche Aufgaben zur Verfügung:

- ✔ Zonen hinzufügen und entfernen
- ✔ Untergeordnete Domänen hinzufügen und entfernen
- ✔ Neue Ressourceneinträge hinzufügen und entfernen

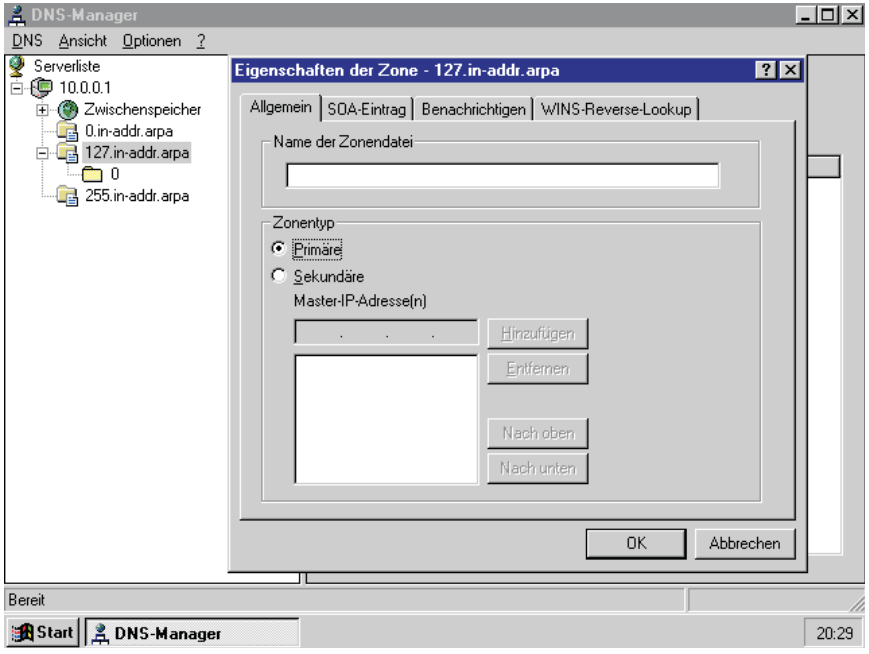


Abbildung 4.59: Die DNS-Konsole

Eine Zone unter DNS stellt eine logische Gruppierung von mehreren Domänen dar. Wenn ein DNS-Server installiert ist und das erste Mal gestartet wird, so erfolgt das Erstellen der Ersten Zone mit einer Reverse Lookup-Zone. Möchten Sie weitere Zonen hinzuzufügen, klicken Sie in der DNS-Konsole mit der rechten Maustaste auf das entsprechende Serverobjekt und wählen im Kontextmenü den Befehl Neue Zone. Danach öffnet sich der Assistent zum Erstellen einer neuen Zone. Um eine neue Domäne anzulegen, müssen Sie die Zone, in

der Sie eine neue Domäne erstellen wollen, mit der rechten Maustaste markieren. Aus dem Kontextmenü wählen Sie den Befehl Neue Domäne und geben im gleichnamigen Dialogfeld den Namen der neu zu erstellenden Domäne ein.

WINS zu DNS migrieren

Um die Netzlast in einem Netzwerk zu reduzieren, kann man nun durch die Dynamik von DDNS auf die Verwendung von WINS verzichten. Dies empfiehlt sich jedoch nur in einer Umgebung in der keine Windows 95/98, NT 4.0 oder DOS-Clients verwendet werden. Um eine reibungslose Migration zu gewährleisten, sollten Sie WINS erst dann entfernen, nachdem Sie den DNS-Server ausführlich auf seine Funktion getestet haben. Um von WINS zu DNS zu migrieren gehen Sie wie folgt vor:

Entfernen Sie unter den TCP/IP Eigenschaften der Clients die Einträge von primären und sekundären WINS-Servern.

Stellen Sie sicher, dass alle Clients für die Verwendung von DNS konfiguriert sind.

Entfernen Sie alle Einträge aus dem oder den WINS-Servern. Anschließend entfernen Sie alle WINS-Server.

Deaktivieren von DDNS

Gelegentlich kann es notwendig werden den DDNS abzuschalten. Ein Deinstallieren ist in dieser Situation jedoch nicht erforderlich. Vielmehr reicht ein Deaktivieren.

Klicken Sie mit der rechten Maustaste auf das Symbol **Netzwerkumgebung** auf dem Desktop, und wählen Sie **Eigenschaften** aus.

Klicken Sie mit der rechten Maustaste auf die gewünschte Verbindung (z.B. LAN-Verbindung) und wählen Sie auch hier wieder **Eigenschaften** aus.

Klicken Sie in dem nun folgenden Fenster auf **Internetprotokoll** (TCP/IP) und anschließend auf die Schaltfläche **Eigenschaften**.

Klicken Sie auf die Schaltfläche **Erweitert**. Es öffnet sich nun ein weiteres Fenster: Wählen Sie dort die Rubrik **DNS** aus und deaktivieren Sie die Option **Adressen** dieser Verbindung **in DNS registrieren**.

4.6.16 DHCP (Dynamic Host Configuration Protocol)

Als Erweiterung des BOOTP-Protokolls weist **DHCP** Computern automatisch eine IP-Adresse, die Subnet-Mask, und bei Bedarf weitere Informationen zu. Die Spezifikationen des Dynamic Host Configuration Protocol sind in den RFCs 1533, 1534, 1541 und 1542 veröffentlicht.

Durch die Implementierung von DHCP in einem großen Netzwerk können so viele Probleme, die bei der manuellen Zuweisung von Adressen auftreten, vermieden werden. DHCP ist somit ein leistungsfähiges Protokoll, mit dessen Hilfe ein Administrator sehr viel Zeit und Mühe einsparen kann. Dazu ist allerdings eine sorgfältige Analyse der vorhandenen Netzstruktur und die Planung der Server-Konfigurationen erforderlich.

Vorteile DHCP

Wird TCP/IP auf einem Host manuell konfiguriert, besteht die Gefahr, dass IP-Adressen doppelt oder ungültige IP-Adressen vergeben werden. Des Weiteren kann es bei der Eingabe der Subnetmaske oder beim Router zu falschen Adressen kommen. Nicht zu unterschätzen ist auch der erhebliche administrative Aufwand bei manueller Konfiguration.

Um die oben aufgeführten Probleme zu vermeiden, empfiehlt sich die Implementierung von DHCP. Bei der automatischen Vergabe von IP-Adressen wird einem Computer eine IP-Adresse mit der dazugehörigen Subnet Mask für einen bestimmten Zeitraum, eine so genannte Leasedauer, zugeteilt. Die so geleaste IP-Adresse kann aber auch von dem Client selbst bei Bedarf vor Ablauf der Lease freigegeben werden. Der Vorteil besteht darin, dass eine von einem Client nicht mehr benötigte IP-Adresse an einen anderen Client vergeben werden kann.

Darüber hinaus unterstützt das DHCP-Protokoll auch die im Bootstrap Protocol definierten Boot Relay Agents. Diese Agents haben die Aufgabe, DHCP-Nachrichten abzufangen und an andere Netzsegmente weiterzuleiten, die nicht über einen eigenen DHCP-Server verfügen.

Der Einsatz eines Boot Relay Agents hat den Vorteil, dass nicht für jedes Subnetz ein eigener DHCP-Server zur Verfügung gestellt werden muss. Als Nachteil soll aber auch erwähnt werden, dass bei einem Ausfall eines Boot Relay Agents oder eines DHCP-Servers die Clients mit einer IP-Lease nicht mehr dazu in der Lage sind, mit anderen Clients zu kommunizieren.

Je nach Ausfallsicherheit ist es mitunter doch sinnvoll, in jedem Segment einen DHCP-Server aufzusetzen. Verfügt ein Computer dabei über mehrere Netzwerkkarten, so wird die Zuweisung der IP-Adressinformationen für jede Karte getrennt durchgeführt, und jeder Karte wird eine eindeutige IP-Adresse zugewiesen.

IP-Lease

In den folgenden Abschnitten wird beschrieben, wie ein Client eine IP-Adresse für eine definierte Zeit von einem DHCP-Server zugewiesen bekommt. Dieser Vorgang der temporären Verfügung über eine IP-Adresse heißt Lease. Zum besseren Verständnis wird das »Leasing« in der Abbildung 4.61 in vier Phasen dargestellt.

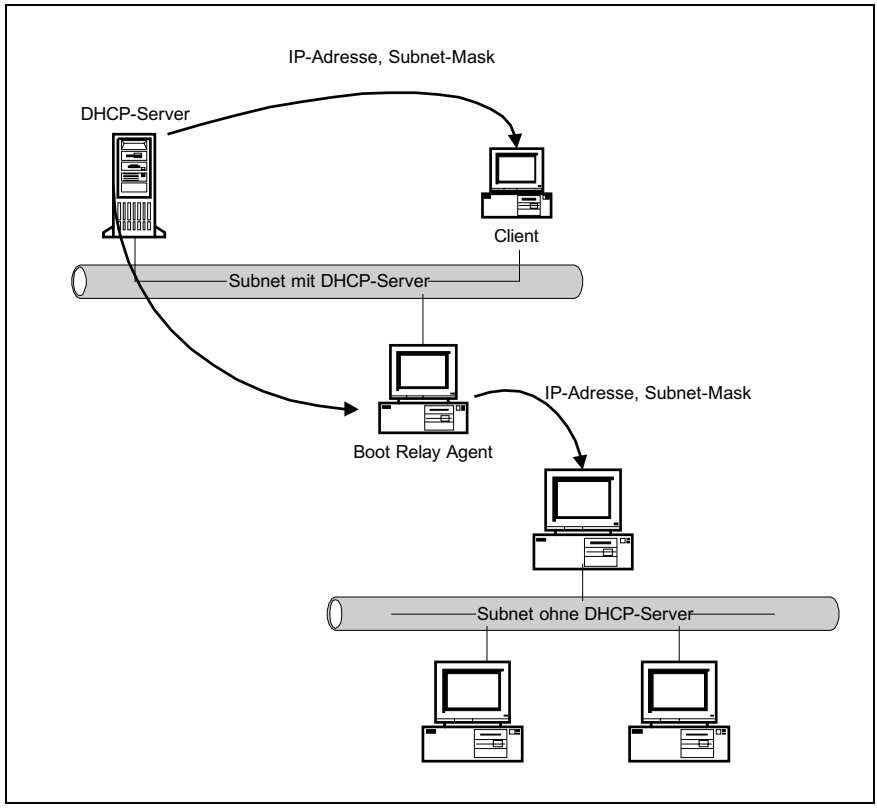


Abbildung 4.60: DHCP – Boot Relay Agent

Phase 1: IP Adresse anfordern

Der Client initialisiert eine eingeschränkte Implementierung von TCP/IP und fordert über ein Broadcast den Standort des DHCP-Servers sowie die dazugehörigen IP-Adressinformationen an. Da der fordernde Client zu diesem Zeitpunkt weder über eine gültige IP-Adresse verfügt noch die IP-Adresse eines DHCP-Servers kennt, verwendet er dazu als Quelladresse 0.0.0.0 und als Ziel die Broadcast-Adresse 255.255.255.255.

Phase 2: Angebot als Reaktion der DHCP-Server

Alle DHCP-Server, die über das Broadcast erreicht werden und über gültige IP-Adressinformationen verfügen, senden ein Angebot an den fordernden Client.

Phase 3: Auswahl

Der Client wählt nun die IP-Adressinformationen aus dem ersten Angebot aus und sendet eine Nachricht, mit der er eine Lease für die in dem Angebot enthaltenen IP-Adressinformationen anfordert.

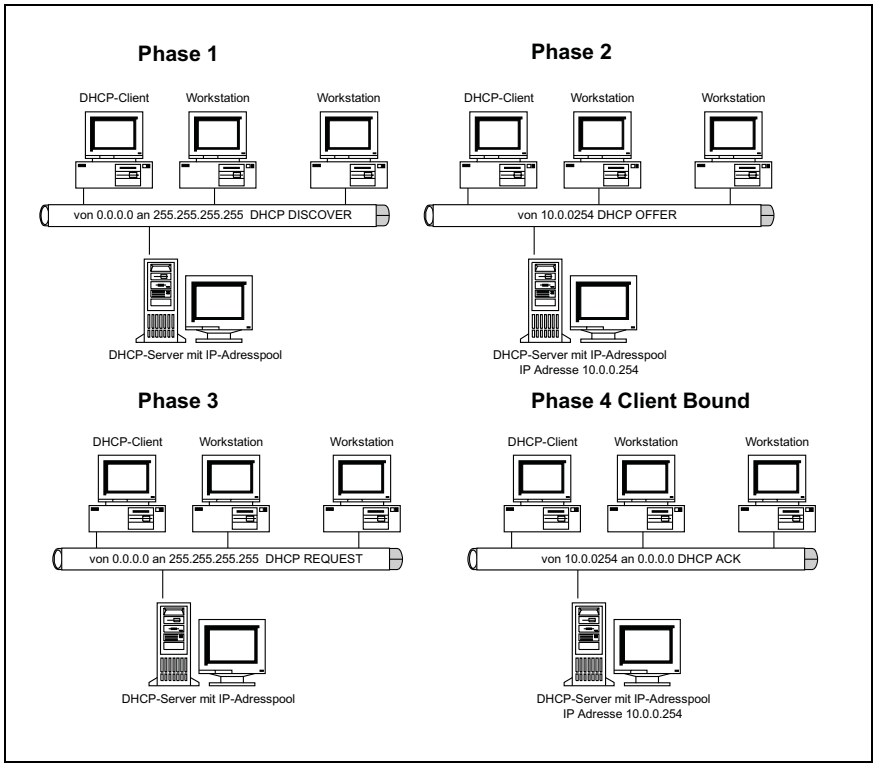


Abbildung 4.61: DHCP – Lease

Phase 4: Bestätigung

Der DHCP-Server, von dem das Angebot ausging, reagiert auf diese Nachricht, worauf alle anderen DHCP-Server ihre Angebote zurücknehmen. Im Anschluss daran werden die IP-Adressinformationen dem Client zugewiesen, und eine Bestätigung wird gesendet.

Ein DHCP-Client wartet eine Sekunde auf ein Angebot. Ist in dieser Zeit jedoch kein DHCP-Server verfügbar oder ist der zur Verfügung stehende Adresspool ausgeschöpft, kann der Client nicht initialisiert werden, und es werden drei weitere Anforderungen als Broadcast gesendet. Dies geschieht in Zeitintervallen von 9, 13 und 16 Sekunden sowie einer zufälligen Zeitspanne zwischen 0 und 1.000 Millisekunden. Erhält der Client auch nach diesen vier Anforderungen kein Angebot, unternimmt der Client alle fünf Minuten einen neuen Versuch.

Überblick DHCP Nachrichten

Nachricht	Bedeutung
DHCP DISCOVER	Eine Nachricht, die ein fordernder Client als Broadcast verschickt, um im Netz einen DHCP-Server zu lokalisieren.
DHCP OFFER	Nachricht eines DHCP-Servers auf ein DHCP-Discover, die über ein Broadcast oder Unicast verschickt wird. Dem fordernden Client werden dabei IP-Adressinformationen angeboten.
DHCP REQUEST	Nachricht als Broadcast eines DHCP-Clients an alle DHCP-Server. Durch diese Nachricht werden die in der DHCP OFFER-Nachricht eines DHCP-Servers angebotenen IP-Adressinformationen angenommen und alle anderen Angebote abgelehnt.
DHCP ACK	Nachricht des DHCP-Servers an den Client, mit der gültigen Lease.
DHCP NAK	Nachricht eines DHCP-Servers an einen Client, die eine Anfrage für geforderte IP-Adressinformationen ablehnt.
DHCP RELEASE	Nachricht eines DHCP-Clients an einen DHCP-Server, dass eine geleaste IP-Adresse nicht mehr benötigt wird und wieder zur Verfügung steht.

Tabelle 4.18: DHCP-Nachrichten

Mit den in der Tabelle 4.18 aufgelisteten Nachrichten zwischen DHCP-Clients und DHCP-Servern wird der gesamte Informationsaustausch gesteuert. So werden über diese Nachrichten auch mögliche Reservierungen für einen Client kontrolliert. Ein wichtiger Parameter ist hierbei der »Zustand«, in dem sich der Client befindet.

Liegt eine Reservierung für einen Client vor, dann müssen die anderen Server darüber informiert werden, dass sich der Client für einen bestimmten Server entschieden hat. Zu diesem Zweck wird diese Nachricht als Broadcast versendet. Die betreffenden Server können dann die durch DHCP OFFER reservierten IP-Adressinformationen wieder freigeben und anderen Clients anbieten. Sollten weitere DHCP OFFER Nachrichten auf dem Netz auftreten, werden diese im Zustand Requesting vom Client ignoriert und stillschweigend verworfen.

Der Server, der vom Client ausgewählt wurde, antwortet mit der Nachricht DHCP-ACK, die alle IP-Adressinformationen für den Client enthält. Mit dem Empfang von DHCP-ACK wechselt der Client dann in den Zustand Bound. Befindet sich der Client in dem Zustand Bound werden alle weiteren Nachrichten DHCP OFFER, DHCP-ACK und DHCP NAK ignoriert und stillschweigend verworfen.

Von nun an ist der Client dazu in der Lage, TCP/IP-Pakete von anderen Hosts zu empfangen und selbst TCP/IP-Pakete zu senden. Da die Leasedauer zeitlich festgelegt ist, steuern auf dem Client zwei Timer, T1 und T2, den weiteren Ablauf der Lease.

Diese Timerwerte werden vom Server vorgegeben und haben, solange nichts anderes vereinbart wurde, folgende Werte:

T1=0,5 * Lease-Dauer

Erstes Erneuerungsintervall nach Ablauf von 50 Prozent der Leasedauer

sowie

T2=0,875 * Lease-Dauer

Nachfolgende Erneuerungsintervalle nach 87,5 Prozent der Leasedauer

Ist die Zeit des Timers T1 abgelaufen, so geht der Client in den Zustand Renewing über. Dazu sendet der Client einen DHCP-Request direkt an den Server, von dem er seine IP-Lease bezogen hat. Durch diesen DHCP-Request wird versucht, nach Ablauf von 50 Prozent der Leasedauer seine IP-Adresse zu verlängern.

Empfängt der Client nun innerhalb einer Zeitspanne, die kleiner als der Timer T2 ist, ein DHCP ACK mit einer erneuerten Lease vom Server, so geht der Client wieder in den Zustand Bound über. Erhält der Client innerhalb der Zeit T2 keine Nachricht vom Server, wechselt der Client in den Zustand Rebinding und sendet einen DHCP-Request als Broadcast an alle DHCP-Server um seine Lease-Dauer zu verlängern. Erhält der Client von einem DHCP-Server ein DHCP ACK, so ist die Zeitspanne des Lease erneuert, und der Client wechselt wieder in den Zustand Bound.

Empfängt der Client jedoch im Zustand Renewing oder Rebinding ein DHCP NAK oder läuft die Lease-Dauer ab, so wechselt er in den Zustand Init. In diesem Zustand werden alle Netzwerkaktivitäten eingestellt, und die gesamte Initialisierungsprozedur muss erneut durchlaufen werden.

Freigeben einer IP-Lease

Mit Hilfe des Dienstprogramms ipconfig kann eine Lease von einem Client manuell zur weiteren Verwendung freigegeben werden.

Beispiel: ipconfig /release

Diese Option bewirkt, dass der DHCP-Client eine DHCP RELEASE-Nachricht an den DHCP-Server sendet und damit die Lease freigibt. In der Praxis kommt die Freigabe zum Einsatz, wenn ein Client in ein anderes Subnet wechselt und die ursprüngliche Lease nicht mehr benötigt wird. Unmittelbar nach der Freigabe kann jedoch keine Kommunikation mehr mit anderen Clients durchgeführt werden.

Manuelles Erneuern einer IP-Lease

Mit Hilfe des Dienstprogramms ipconfig kann eine Lease von einem Client auch manuell erneuert werden.

Beispiel: ipconfig /renew

Diese Option bewirkt, dass der DHCP-Client eine DHCP REQUEST-Nachricht an den DHCP-Server sendet und somit versucht, die Lease zu erneuern. Steht kein DHCP-Server zur Verfügung, werden die bisherigen IP-Adressinformationen verwendet.

Alle DHCP-Nachrichten werden über die UDP-Anschlüsse 67 und 68 gesendet.

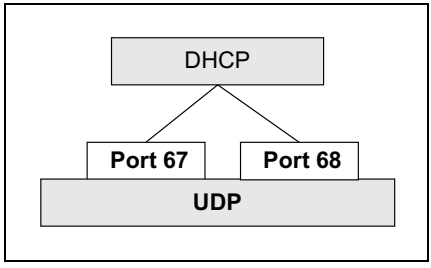


Abbildung 4.62: DHCP-STack

4.6.17 NAT und PAT

Wie bereits erwähnt stehen unter IP Version 4 nur eine begrenzte Anzahl von IP-Adressen zur Verfügung. Um dennoch mit diesem zur Verfügung stehenden Adresspool arbeiten zu können, wird das Protokoll **NAT,** Network Address Translation, eingesetzt. Die Spezifikationen des Network Address Translation sind im Request for Comments 1631 veröffentlicht.

Als Vorläufer des NAT findet auch das etwas ältere Verfahren **PAT**, Port and Address Translation, Verwendung. Beide Protokolle haben die Aufgabe, mittels einer einzigen »echten« IP-Adresse eine volle Anbindung zum Internet zu ermöglichen. Das PAT übersetzt dabei automatisch die IP-Adressen sowie die Port-Nummern von ein- und ausgehenden IP-Datagrammen und wandelt die Adressen der Quell-Hosts in die dynamische IP-Adresse des Routers um. Handelt es sich dabei um ausgehende Pakete, so speichert der Router die IP-Adresse und den Port des Quell-Hosts in einer internen Tabelle und ersetzt diese durch seine eigene dynamische IP-Adresse sowie einen neuen Port.

Sofern es sich um eingehende Pakete handelt, wird die Adresse des Ziel-Hosts anhand derselben internen Tabelle auf die IP-Adresse des lokalen Hosts abgebildet. Im Gegensatz zu PAT werden bei Verwendung des NAT nur die IP-Adressen umgewandelt, was von außen einen vollständigen Zugriff auf die lokalen Rechner im Netzwerk ermöglicht.

Man unterscheidet zwischen statischem und dynamischem NAT. Um einen vollen Zugriff nach außen zu garantieren, z.B. für E-Mail oder Webdienste, bzw. um uneingeschränkt von außen auf einen lokalen Host zugreifen zu können, sind statische IP-Adressen notwendig. Dabei kann wahlweise die globale IP-Adresse des Routers selbst, eine dynamische IP-Adresse des Internet Service Providers oder aber eine statische IP-Adresse eingesetzt werden.

Durch Kombination von mehrfachem NAT und PAT auf einem Router wird ein vollständiges klassenloses TCP/IP-Routing sowie eine dynamische Adressierung über IP ermöglicht. Router, die diese Technologie unterstützen, können jede interne IP-Adresse und Port-Nummer aus einem Intranet in eine nach außen hin sichtbare Internet-Adresse und die dazugehörige Port-Nummer umwandeln.

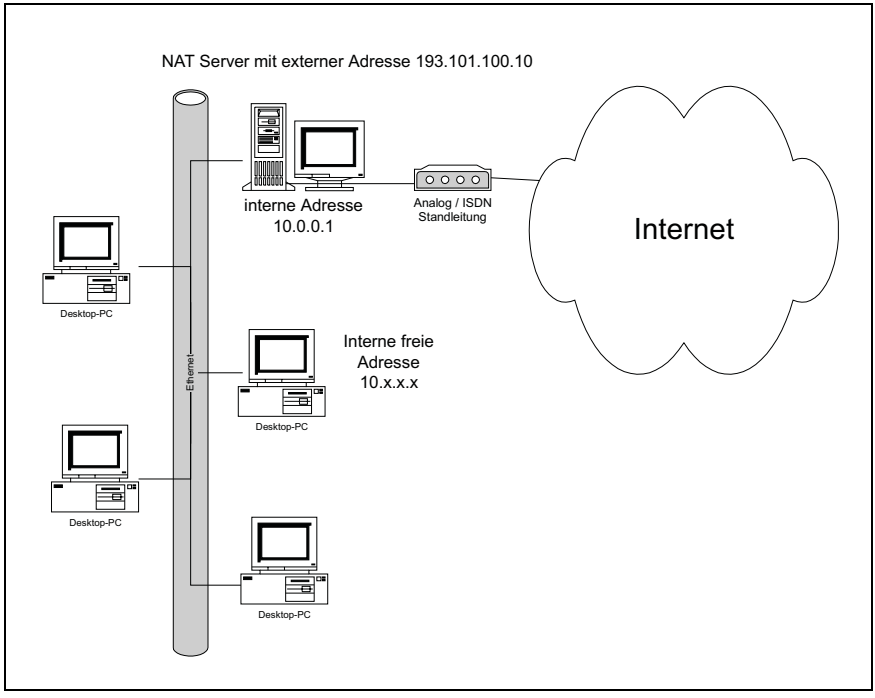


Abbildung 4.63: Anwendungsbeispiel NAT

Um nicht mit real verwendeten IP-Adressen in Konflikt zu geraten, sollten die nach RFC 1918 definierten privaten IP-Adressen im Intranet benutzt werden, z.B. 10.x.x.x. für den Aufbau eines internen A-Klasse Netzes.

Das in Abbildung 4.63 gezeigte Beispiel demonstriert diese Vorgehensweise und zeigt, dass NAT und PAT als so genannte Firewall-Technologien eingesetzt werden können. Server mit der oben gezeigten Funktion werden auch als Proxy-Server bezeichnet. Sie bauen stellvertretend für die Hosts im geschützten LAN Internetverbindungen auf und kontrollieren damit sowohl den Zugriff von außen auf interne Hosts, als auch den Zugriff von innen auf das Internet.

NAT Router

Um NAT einsetzen zu können werden auch Router benötigt, die NAT beherrschen. Als Produkte kommen hier unter anderem in Frage:

- ✔ 3COM Connect Remote 5xx
- ✔ CISCO 1003
- ✔ Passage 22

Unter Linux, einem Betriebssystem, das insbesondere beim Einsatz von TCP/IP-Servern zum Einsatz kommt, kann ab dem Kernel 2.0 NAT verwendet werden. Dazu muss im Kernel MASQUERADING aktiviert werden. MASQUERADING-HOWTO beschreibt dann die weiteren notwendigen Schritte.

Die folgende Liste zeigt eine Auswahl von Sharewareprodukten, die NAT mit Windows 95/98/NT realisieren.

- ✔ Trumpet Firesock
- ✔ Winroute
- ✔ Proxy

4.6.18 RIP (Routing Information Protocol)

RIP ist ein **IGP** Routing Protokoll**,** Interior Gateway Protocol, das in kleinen und mittleren Netzen eingesetzt wird. Die Spezifikationen des Routing Information Protocol sind in den RFCs 1058 und 1388 veröffentlicht.

Routing-Verfahren und Techniken

Generell unterscheidet man zwei unterschiedliche Verfahrensweisen beim Routing, nichtadaptives und adaptives Routing.

Beim nichtadaptiven oder statischen Routing werden die einzelnen Routen in den Routern fest eingestellt. In der Praxis bedeutet dies, dass die Datenpakete zwischen Quell- und Ziel-Host immer die gleiche Strecke passieren. Von Nachteil ist, dass dadurch nicht automatisch auf Überlastungen oder Ausfälle von Routern reagiert werden kann, da statische Router keinerlei Statusinformationen untereinander austauschen. Die Router selbst benötigen in diesem Fall auch keine Routing-Protokolle. Dies führt in großen Netzen zu einem nicht zu unterschätzenden hohen administrativen Aufwand, denn alle Veränderung an der Netzstruktur müssen manuell in allen Routern eingetragen werden.

Beim adaptiven oder dynamischen Routing bilden die Router Metriken, die durch Routing-Algorithmen errechnet werden. Die so erworbenen Informationen werden dann in den einzelnen Routing-Tabellen abgelegt. Dazu müssen nun natürlich wieder Routing-Protokolle verwendet werden. Wie bereits oben erwähnt, werden als Metriken alle Merkmale wie Hopcount, Leitungslast, Bandbreite, neue oder weggefallene Leitungsstrecken berücksichtigt. Dadurch wird

erreicht, dass sich die Wegwahl immer wieder automatisch an die vorhandene Situation im Netz anpasst. Auch der administrative Aufwand ist bedeutend geringer als beim nichtadaptiven Routing, da die Router ja alle Änderungen in der Netztopologie selbständig propagieren. Dennoch ist die Konvergenz eine kritische Größe bei großen Netzen mit dynamischem Routing.

Für das dynamische Routing stehen verschiedene Techniken zur Verfügung. Beim Reverse Poison werden Änderungen nicht in die Richtung propagiert, aus der sie gelernt wurden. Split Horizon vermeidet unnötige Broadcasts und beim Hold Down werden Routing Loops verhindert.

Arbeitsweise von RIP

RIP wird zum Austausch von Nachrichten innerhalb eines autonomen Systems verwendet. Autonome Systeme sind Teilnetzwerke des Internets, deren innere Struktur nach außen hin transparent ist. In der Beziehung zwischen den Routern unterscheidet man zwischen internen Nachbarrechnern, Interior Neighbours, und externen Nachbarrechnern, Exterior Neighbours.

Abbildung 4.64 zeigt die hier beschriebene Systematik. Interior Neighbours sind im gleichen autonomen System angesiedelt, externe Nachbarn werden über Protokolle erreicht, die als **EGP**-Protokolle bezeichnet werden, Exterior Gateway Protocol. Details zu EGP finden sie in den RFCs 827, 888 und 904.

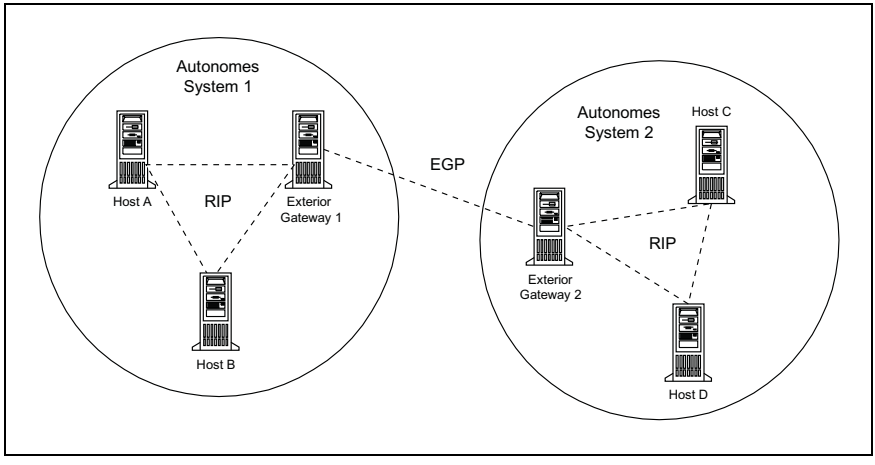


Abbildung 4.64: Gateway Protokolle und autonome Systeme.

Das Routing Information Protocol verwendet den DVA-Algorithmus**,** Distance Vector Algorithmus auch Bellman Ford Algorithmus. Dieser Algorithmus dient dem zyklischen Austausch von Routing-Tabellen zwischen dynamischen Routern eines autonomen Systems. Zu diesem Zweck verfügt jeder Router über eine Routing-Tabelle, in die er einträgt, wie er alle ihm bekannten Netzwerke erreichen kann. Diese Tabellen werden dann über ein Broadcast auf die betroffenen Router verteilt.

Als Metriken werden dabei ganz unterschiedliche Größen wie Leitungslast, Leitungsverzögerung, Hopcount, Zuverlässigkeit oder auch die zur Verfügung stehende Bandbreite verwendet. Da diese Routing-Tabellen regelmäßig komplett ausgetauscht werden, kommt es zu so genannten Broadcaststürmen. Darüber hinaus treten immer wieder Situationen auf, in denen schon gelernte Änderungen wieder von Routern überschrieben werden, welche die Änderungen noch nicht gelernt haben. Dies führt dazu, dass der reine DVA über eine sehr schlechte Konvergenz verfügt. Bedingt durch diese schlechte Konvergenz, werden heute verstärkt modernere Protokolle wie OSPF eingesetzt. Als eines der ältesten und einfachsten Routing-Protokolle ist RIP auch eines der verbreitetsten.

4.6.19 Open Shortest Path First

OSPF ist ein hierarchisches Link-State-Protokoll, das von der Internet Engineering Task Force, IETF, speziell für das Routen in komplexen TCP/IP-Netzen entwickelt wurde. Die Spezifikationen des Open Shortest Path First sind im RFC 1247 veröffentlicht.

Die OSPF-Spezifikation ist frei verfügbar und kann deshalb auch ohne zusätzliche Lizenzgebühren implementiert werden. Von Nachteil sind allerdings die recht hohen Anforderungen an die Ressourcen, die von den Herstellern der Router, ob als Hard- oder Software, erfüllt werden müssen. Insofern nur ein Router zum Einsatz kommt, hält sich der Preis dafür noch in Grenzen. Werden jedoch in einem großen Netz viele Router mit OSPF-Implementation eingesetzt, so schlägt sich dies deutlich im Preis nieder.

Die Routenberechnung selbst erfolgt unter der Verwendung eines modifizierten LSA-Algorithmus, Link State Algorithmus. Bei einem herkömmlichen, nicht modifizierten LSA, legt jeder Router eine Routing-Tabelle an, in welche die vollständige Topologie des Netzwerks abgebildet wird. Änderungen eines Links, einer Verbindung, werden dann über ein Link State Anouncement den benachbarten Routern sofort mitgeteilt. Diese Änderungen werden verbindungsorientiert an die benachbarten Router propagiert und verfügen somit über eine gute Konvergenz.

Wie bereits oben erwähnt, sendet LSA in seiner ursprünglichen Form periodisch Link-Status-Meldungen an die angeschlossenen Router. Da OSPF eine modifizierte Variante des LSA verwendet, sieht OSPF für jedes Multi-Access-Netz einen eigenen designierten Router vor, welcher stellvertretend für alle anderen Router in diesem Multi-Access-Netz Meldungen versendet. Unter Verwendung von Hardware Broadcasts kann darüber hinaus die Anzahl der Nachrichten reduziert werden.

Im Unterschied zu RIP verfügt OSPF über folgende Leistungsmerkmale:

- ✔ ToS-Routing
- ✔ Berücksichtigung anfallender Leitungskosten
- ✔ Partitionierung von Netzen
- ✔ Authentifizierung

ToS-Routing, Type of Service

Bei diesem Verfahren verfügen alle Router über eine Datenbank, in der die Topologieinformationen des autonomen Systems, in dem sich der Router befindet, vorgehalten werden. Sofern eine Partitionierung des autonomen Systems vorgenommen wurde, sind diese Topologieinformationen für alle Router eines Autonomous Systems bzw. einer Area gleich.

Jeder Router sendet Statusinformationen wie »Gegenwärtiger Zustand« oder »Erreichbare Nachbarn« über Broadcasts an die anderen Router, die sich im gleichen autonomen System oder in der gleichen Area befinden. Zum Kalkulieren der optimalen Routen werden die Type of Service-Bit, die im IP-Header der einzelnen Datagramme codiert sind, berücksichtigt.

Zu diesem Zweck werden die Delay-, Throughput- und Realibility-Bit eines IP-Datagramms ausgewertet. Da der Type of Service durch vier Bit codiert wird, können maximal 16 Metriken berechnet werden. Ist das Bit eins, Delay-Bit, gesetzt, dann bedeutet dies: »Minimiere die Verzögerung«. Das zweite Bit ist das Throughput-Bit. Es signalisiert »Maximiere den Durchsatz«. Das dritte Bit bedeutet »Maximiere die Zuverlässigkeit« und das vierte Bit steht für »Minimiere die Kosten«. Anhand der besonderen Anforderungen an den zugrunde liegenden Datendienst wählt OSPF dann die optimale Route aus. Das dialogorientierte Telnet ist ein typisches Beispiel für ein Routing, das eine minimale Verzögerung erfordert. Entsprechend müsste hier das ToS-Feld auf das Bitmuster 1000 gesetzt sein. File Transfer setzt einen möglichst hohen Datendurchsatz voraus. Sinnvoll wäre hier das Bitmuster 0100.

OSPF kann die Datagramme gleichmäßig auf die einzelnen Verbindungen verteilen und entlastet so die einzelnen Leitungen. Als eines der ersten nicht-proprietären Routing-Protokolle verfügt OSPF über das hier beschriebene Leistungsmerkmal.

Berücksichtigung anfallender Leitungskosten

Um die anfallenden Leitungskosten zu berücksichtigen, werden Informationen über das zu erwartende Lastaufkommen, die zur Verfügung stehende Bandbreite sowie Leitungstarife kalkuliert und den einzelnen Schnittstellen zum WAN zugeordnet. Dadurch erhält ein Router eine weitere Möglichkeit zur Berechnung der Routing-Metrik.

Partitionierung des Netzes in Teilnetze

OSPF bietet die Möglichkeit, ein Netzwerk in mehrere Teilnetze, so genannte Areas, zu partitionieren. Diese Technik ermöglicht es, Topologieänderungen einzelner Areas durchzuführen, ohne dass diese Änderungen über die Area hinaus propagiert werden müssen. Außerdem muss nicht jeder Router innerhalb einer Area über die gesamten Topologieinformationen des übergeordneten autonomen Systems informiert sein. Deshalb belasten Änderungen nicht das gesamte Netzwerk, und OSPF kommt dadurch mit relativ wenig Overhead aus.

Im Allgemeinen sind OSPF-Topologien hierarchisch aufgebaut. Dabei wird zwischen den folgenden Ebenen unterschieden:

- ✔ Netz
- ✔ Area – Gruppe von Netzen
- ✔ Backbone – Verbindung von Areas
- ✔ Autonomous System – Zusammenfassung der über das Backbone verbundenen Netze

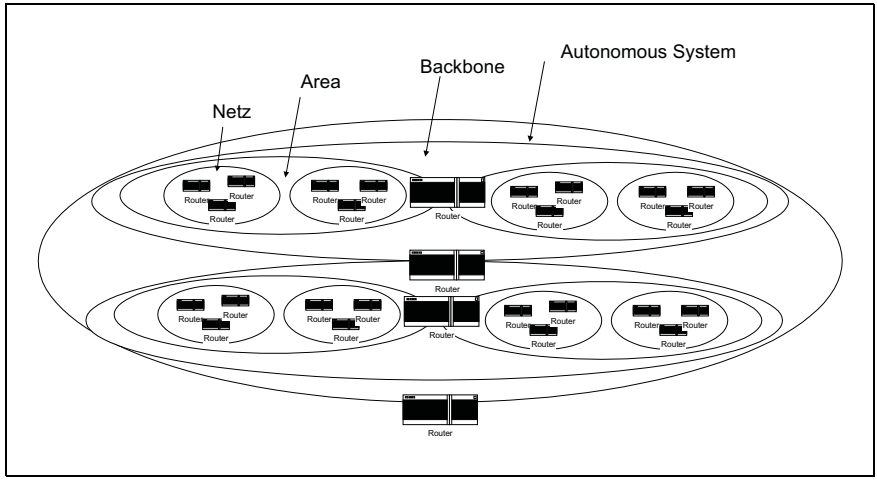


Abbildung 4.65: Hierarchische Topologie mit OSPF

Analog dazu werden auch die Router in einer OSPF-Topologie eingeteilt in:

- ✔ Interne Router
- ✔ Designierte Router
- ✔ Area Border Router
- ✔ Autonomous System Boundary Router

Interne Router sind Router, bei denen sämtliche direkt angeschlossenen Netze innerhalb einer Area liegen. Auch Router, die nur auf dem Backbone routen, werden als interne Router bezeichnet, da das Backbone als eigene Area angesehen wird.

Designierte Router sind Router, die stellvertretend für sämtliche anderen in einem LAN eingesetzten Router mit anderen Netzen Topologieinformationen austauschen.

Area Border Router verbinden zwei Areas miteinander oder binden eine Area in das Backbone ein.

Autonomous System Boundary Router verfügen über Verbindungen zu mindestens einem oder mehreren anderen autonomen Systemen und propagieren diese Informationen an andere Systeme.

Authentifizierung zwischen verschiedenen Routern

Mittels mehrerer Authentifizierungsverfahren wird sichergestellt, dass nur autorisierte Router die Routing-lnformationen in das Netz propagieren können. Auch die Integration von außenstehenden Routern ist unter OSPF möglich. Authentifizierung bedeutet, dass ein Router bekannt geben muss, wer er ist und diese Identität durch einen Schlüssel oder Passwort verifizieren muss.

Um jedoch das gezielte Einstreuen falscher Routing-Informationen zu vermeiden, werden außenstehende Router entsprechend gekennzeichnet. Dies erhöht auch die Sicherheit gegen Angriffe von außen, da diese dadurch effizient unterbunden werden.

Darüber hinaus unterscheidet man zwischen Intra- und Inter-Area-Routing. Das Intra-Area-Routing bezieht sich dabei ausschließlich auf das Routen innerhalb einer Area. Dazu werden nur die areainternen Topologie-Informationen verwendet. Muss ein Datagramm über die Area-Grenzen hinaus geroutet werden, kommen die Inter Area-Informationen zum Einsatz. Dadurch wird der Overhead des Protokolls erheblich reduziert. Zudem trägt die streng hierarchische Gliederung zur Stabilisierung des Algorithmus bei.

Den Austausch von Topologie-Informationen nennt man in der Terminologie von OSPF Advertising. Die einzelnen Router verschicken so genannte Advertisements, in denen sie ihre Link States bekanntgeben.

4.7 TCP/IP-Anwendungsprotokolle

In den folgenden Unterkapiteln erhalten Sie einen Überblick über die TCP/IP-Anwendungen, die Sie als Administrator nutzen und/oder konfigurieren können sollten. Dazu sind je nach Anwendung Detailkenntnisse der Protokolle hilfreich.

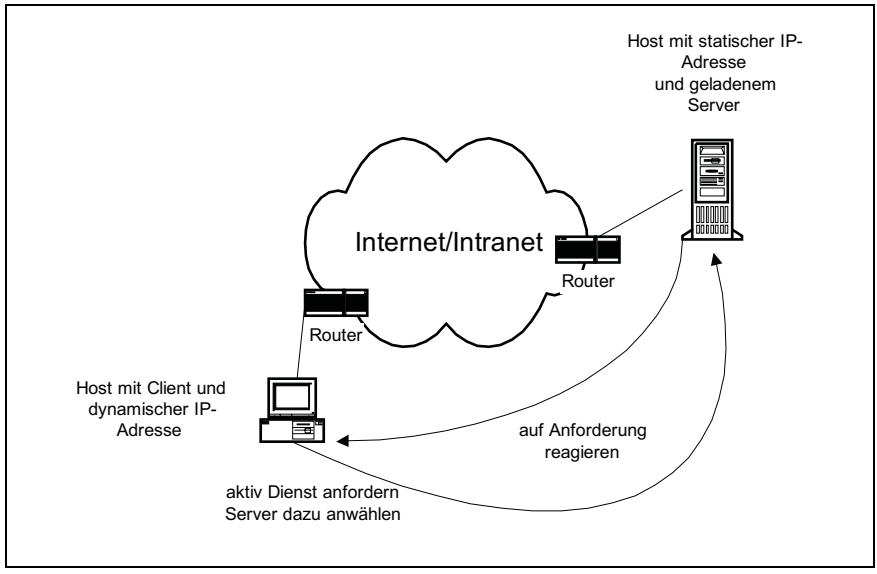


Abbildung 4.66: TCP/IP-Anwendungen als Client/Server Systeme

Generell arbeiten alle im Folgenden vorgestellten Protokolle nach dem Client/Server-Prinzip. Die Protokolle sehen dazu eine Implementierung vor, die Dienste zur Verfügung stellt und dabei »passiv« auf eine Anforderung wartet. Diese Implementierungen werden Server genannt und sind permanent auf den Hosts geladen. In der UNIX-Welt werden TCP/IP-Server häufig als Deamon bezeichnet. So heißt z.B. eine Implementierung des FTP-Dienstes ftpd, ftp deamon, der Telnet-Server heißt telnetd etc.

Die Clients sind Protokollvarianten, die aktiv die Dienste der Server anfordern. Sie werden bei Bedarf geladen.

Clients benutzen für die Kommunikation Portnummern größer als 1024 und Server Portnummern zwischen 1 und 255. Ein weiterer Unterschied zwischen Servern und Clients besteht darin, dass Clients in der Regel eine dynamische via DHCP zugewiesene Adresse haben und Server eine statische.

Nach dem Verbindungsaufbau wird die Kommunikation in der Regel symmetrisch abgewickelt. Das bedeutet, dass Server und Client gleichberechtigt die Kommunikation steuern und z.B. jeder selbstständig die Verbindung abbauen kann.

4.7.1 FTP (File Transfer Protocol)

Das File Transfer Protocol wird für die Übertragung von Dateien über das Internet eingesetzt. Darüber hinaus ist FTP auch ein Dienst, der, wie viele Internet-Dienste, nach dem Client/Server-Prinzip arbeitet. Eine Besonderheit dieses Dienstes ist jedoch die Trennung von Kontroll- und Datenverbindung. Die Spezifikationen des FTP sind im RFC 959 veröffentlicht.

Bei einer FTP-Sitzung baut der Client eine Kontrollverbindung zum Server über den Port 21 auf. Über diesen Port werden nun Kommandos und Anworten zwischen Client und Server ausgetauscht.

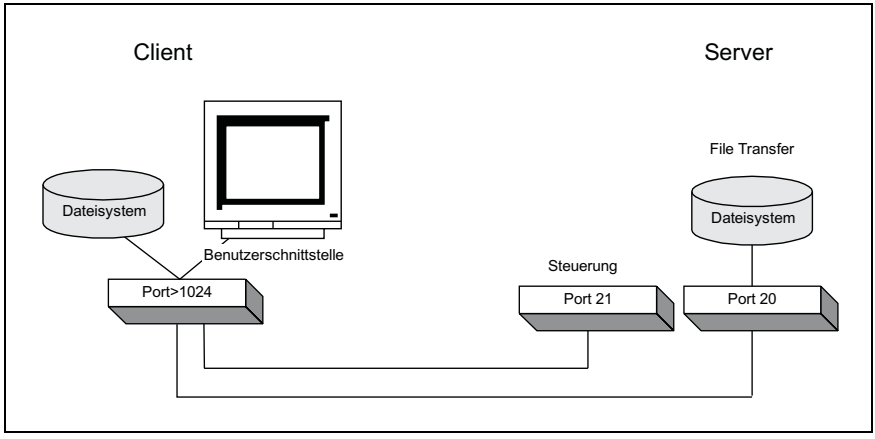


Abbildung 4.67: TCP/IP-Protokollarchitektur des FTP-Dienstes

Nachdem eine Festlegung der Kommunikations- und Übertragungsparameter stattfand, wird nun die eigentliche Übertragung der Dateien über den Port 20 durchgeführt.

Anonymous FTP

Anonymous-FTP-Server sind öffentliche FTP-Server auf denen Millionen von Dateien abgespeichert sind. Dort findet man Programme, Text-, Bild-, Audio- und Videodateien. So bieten viele Unternehmen aus dem Computerbereich über FTP die neuesten Treiber und Programmversionen an. Wird man bei der Verbindungsaufnahme zu einem anonymen FTP-Server zur Eingabe eines Benutzernamens aufgefordert, so lautet dieser **anonymous**. Als Passwort gibt man seine eigene E-Mail-Adresse an.

Eine Liste mit anonymen FTP-Servern findet man unter:

http://tile.net/ftp-list/ oder

shttp://askhp.ask.uni-karlsruhe.de/ftp/ftp-list-de.html

Soll der Zugriff auf einen FTP-Server benutzerorientiert erfolgen, dann muss der Administrator Konten anlegen. Diese bestehen aus einem Benutzernamen und einem Passwort. Jedem Konto können dann Zugriffsrechte auf unterschiedliche Verzeichnissysteme zugewiesen werden.

Beim Einsatz von FTP gibt es zwei grundlegende Möglichkeiten, den Dienst zu nutzen. Die komfortabelste Art ist der Dateitransfer über einen FTP-Client. Ist diese Möglichkeit nicht gegeben, z.B. bei einem eingeschränkten Zugang zum Internet, dann kann man über E-Mail-Dateien von FTP-Archiven anzufordern.

FTP mit FTP-Client

Über einen FTP-Client erfolgt der direkte Zugriff auf einen FTP-Server. Einfache Versionen von FTP-Clients sind textorientierte Programme, die bei den gängigsten Betriebssystemen wie Unix, Microsoft Windows 95/98 und NT 4.0 zum Funktionsumfang gehören. Da bei einem textorientierten Client keine grafische Benutzeroberfläche zur Verfügung steht, muss man auch die Syntax der FTP-Kommandos kennen.

Kommando	Bedeutung
Help	Aufrufen der Hilfefunktion
open Rechnername Open IP-Adresse	Es wird eine Verbindung über FTP hergestellt. Mögliche Parameter sind der Rechnername oder die IP-Adresse des Ziel-Hosts. Wenn eine Verbindung zustande kommt, dann wird nach einer Benutzeridentifikation und einem Passwort gefragt.
pwd	Anzeige des aktuellen Verzeichnisses auf dem Server
dir <Verzeichnis>	Ausführliche Inhaltsangabe des Verzeichnisses auf dem Server
ls <Verzeichnis>	Kurze Inhaltsangabe des Verzeichnisses auf dem Server
cd <Pfad>	Wechseln des Verzeichnisses auf dem Server
cdup	Wechseln in das nächsthöhere Verzeichnis auf dem Server
lcd <Pfad>	Wechseln des Verzeichnisses beim Client
ascii	Übertragungsmodus für ASCII-Dateien
binary	Übertragungsmodus für Binärdateien (Programme, Bilddateien und komprimierte Dateien)
type	Zeigt den eingestellten Übertragungsmodus an
hash	Anzeige der Fortschrittsanzeige einer Datenübertragung mit dem #-Zeichen
get <Datei>	Kopieren einer Datei vom Server zum Client, download
mget <Dateien>	Kopieren mehrerer Dateien vom Server zum Client
put <Datei>	Kopieren einer Datei vom Client zum Server, upload
mput	Kopieren mehrerer Dateien vom Client zum Server
mkdir	Erstellen eines Verzeichnisses auf dem Server
rmdir	Löschen eines Verzeichnisses auf dem Server
delete	Löschen einer Datei auf dem Server
mdelete	Löschen mehrerer Dateien auf dem Server
close	Verbindung wird geschlossen
quit oder exit	Verbindung wird geschlossen und der FTP-Client beendet

Tabelle 4.19: FTP-Befehlssatz

Grafisch orientierte FTP-Clients sind in der Bedienung natürlich wesentlich benutzerfreundlicher. Diese Clients sind in der Regel so aufgebaut, dass die Verzeichnisse des lokalen Rechners und die des FTP-Servers nebeneinander dargestellt werden. Der Anwender kann jetzt mit Hilfe der Maus und der Download- bzw. UpLoad-Buttons Dateien beliebig zwischen den beiden Host-Systemen hin und her kopieren, wenn er über die hierzu notwendigen Zugriffsrechte verfügt.

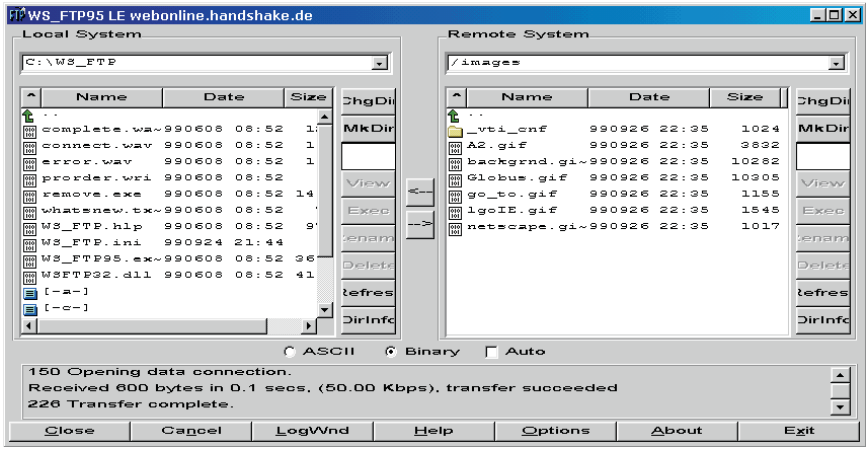


Abbildung 4.68: FTP-Client mit grafischer Benutzerschnittstelle

Windows-Clients bieten die Möglichkeit, für jede Verbindung die zugehörigen Verbindungsparameter in einem Datensatz zu speichern. Bei jedem Eintrag können die erforderliche Benutzerkennung, das Passwort und weitere Parameter so konfiguriert werden, dass der Login-Vorgang automatisch erfolgen kann.

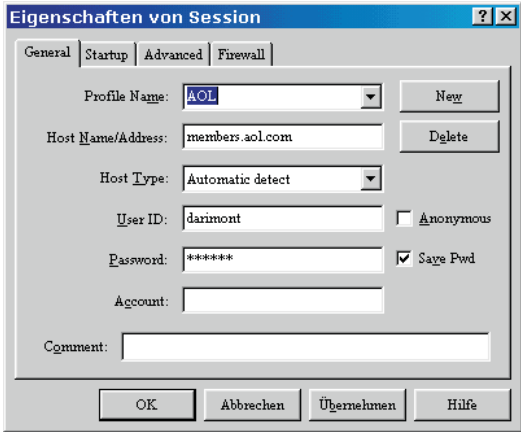


Abbildung 4.69: FTP-Verbindungen konfigurieren

FTP mit E-Mail

Ist kein uneingeschränkter Zugang zum Internet möglich, besteht noch die Möglichkeit über FTPMAIL-Server auf FTP-Archive zugreifen. Diese Server bearbeiten die Anweisungen, die der Benutzer per E-Mail zuschickt. Die Syntax der Anweisungen ist ebenfalls fest vorgegeben und steht im Body einer E-Mail.

Liste einiger FTPMAIL-Kommandos

Kommando	Bedeutung
reply	Mit dem Kommando reply wird die Rücksendeadresse angegeben. Hier sollte die eigene E-Mail-Adresse eingegeben werden, damit auch sichergestellt ist, dass die Rückantwort die richtige Adresse erreicht.
Connect	Connect gibt den FTP-Server an, von dem man Dateien erhalten möchte.
Ascii	Ascii legt fest, dass die georderten Dateien ASCII-Dateien sind.
Binary	Binary legt fest, dass die georderten Dateien Binär-Dateien sind.
Chdir /nnn	Gibt das Verzeichnis /nnn an, in dem die georderten Dateien liegen.
uuencode	Die georderten Dateien werden im uuencode-Format versendet. Dieses Format wird für die Verschlüsselung von Dateien unter UNIX verwendet.
btoa	Die georderten Dateien werden im btoa-Format versendet.
ls /nnn/ccc	Es wird das Inhaltsverzeichnis von /nnn in Kurzform versendet.
dir /nnn	Es wird das Inhaltsverzeichnis von /nnn versendet.
index xyz	Im Indexverzeichnis des Servers wird nach dem Begriff »xyz« gesucht.
get nnn.ab	Fordert die Datei nnn.ab vom FTP-Server. Dabei sind je FTPMAIL-Anfrage maximal zehn get-Befehle erlaubt.
quit	Zeigt das Ende der Befehlsfolge an.

Tabelle 4.20: FTPMAIL-Befehlssatz

Sieht man sich den Inhalt von FTP-Servern an, so stellt man fest, dass die Dateien ganz unterschiedliche Dateiformate haben. Ein Merkmal dafür sind die unterschiedlichen Dateierweiterungen wie z.B. .exe, .com oder .doc. An diesen Dateierweiterungen kann man in der Regel erkennen, um welches Dateiformat es sich handelt.

In den so genannten Dateiarchiven finden sich in der Regel mehrere Dateien samt der Verzeichnisstruktur zusammengefasst. Diese Informationen können nun weiter komprimiert werden, um die Größe der Dateien zu reduzieren.

Je nach Betriebssystem kommen unterschiedliche Archivierungs- und Komprimierungsprogramme zum Einsatz. Einige Programme unterstützen beide Funktionen, d.h. die Dateien werden in einem Vorgang gepackt und komprimiert. Wird ein Dateiarchiv von einem FTP-Server auf die Festplatte des FTP-Clients übertragen, muss die Datei im Anschluss daran mit den entsprechenden Programmen wieder dekomprimiert und entpackt werden. Die nachfolgende Tabelle beinhaltet die gängigsten Formate von Dateiarchiven:

Dateierweiterung	Dateiformat
.arj	Mit arj komprimiert (MS-DOS)
.cpt	Compact Pro Archiv (Mac)
.exe	Selbstextrahierendes Archiv (MS-DOS)
.gz	Mit GNUs gzip komprimiert
.sea	Selbstextrahierendes Dateiarchiv (Mac)
.sit	StuffIt Archiv (Mac)
.tar	Mit tar gepacktes Dateiarchiv (Unix)
.tgz	Zuerst mit tar gepackt und dann mit gzip komprimiert (identisch mit .tar.gz)
.zip	Mit pkzip komprimiert (MS-DOS)
.z	Mit pack komprimiert
.Z	Mit compress komprimiert (Unix)

Tabelle 4.21: Formate von Dateiarchiven.

4.7.2 Trivial File Transfer Protocol

Neben FTP ist das Trivial File Transfer Protocol das zweite File Transfer Protokoll, das von den TCP/IP-Services unterstützt wird. Die Spezifikationen des TFTP sind im RFC 783 veröffentlicht.

Im Gegensatz zu FTP verfügt TFTP nur über ein Minimum an Kommandos und arbeitet ohne aufwändige Sicherungsmechanismen. Ein weiterer Unterschied ist der verwendete Port. Denn anders als FTP, das auf der Transportschicht TCP nutzt, verwendet **TFTP** das User Datagram Protocol, UDP, über den Port 69. Da es sich bei UDP um ein unzuverlässiges Protokoll handelt, verfügt TFTP über einige wenige Sicherungsmechanismen. Diese gewährleisten allerdings, dass die zu übertragenden Daten auch wirklich beim Empfänger ankommen.

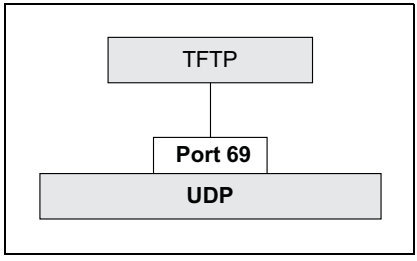


Abbildung 4.70: TFTP-Socket

TFTP wird häufig zusammen mit so genannten Diskless Workstations eingesetzt. Das Programm dient dabei zum Übertragen der Initialisierungsprogramme, die nach dem Kaltstart in den Arbeitsspeicher der Workstation geladen werden müssen. Dazu benötigt TFTP aber die IP-Adresse des bootenden Systems. Diese wird von RARP und BOOTP ermittelt.

Da es sich bei TFTP um ein recht einfaches Protokoll handelt, sind auch die Konventionen nach denen das TFTP abläuft sehr simpel gehalten.

OPCode	Funktion
1	Read Request, RRQ
2	Write Request WRQ
3	Acknowledgement ACK
4	Error
5	Data

Tabelle 4.22: Funktionen von TFTP

So stehen für die Kommunikation mit TFTP nur fünf Funktionen, so genannte OPCodes zur Verfügung. In den folgenden Absätzen erhalten Sie eine Kurzbeschreibung der in Tabelle 4.22 aufgelisteten Funktionen.

Das Read Request-Kommando sendet eine Datei an den Ziel-Host. Gleichzeitig wird die UDP-Verbindung über Port 69 zu diesem Host etabliert. Der OpCode für Read Requests ist der Wert Eins. Mit RRQ werden Parameter übertragen, die den Filetransfer steuern. Dabei legt ein Feld mit dem Namen Read Request Mode fest, wie die Daten übertragen werden. Dafür stehen die Optionen: NetASCII, Binary und Mail zur Verfügung. Der Name der zu übertragenden Datei steht im Feld Read Request File Name.

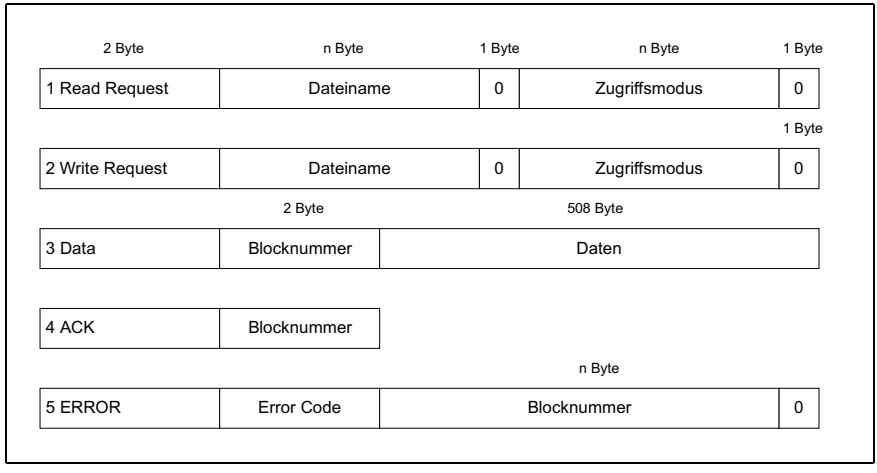


Abbildung 4.71: TFTP-Paketformate

Das Write Request-Kommando leitet das Empfangen einer Datei von dem angewählten Rechner ein. Der OpCode von WRQ ist der Wert Zwei. Auch hier werden die gleichen Parameter wie die oben beschriebenen übergeben. So legt z.B. das Feld Write Request File Name fest, wie die Datei heißt, die vom entfernten Rechner gesendet werden soll.

Das Kommando Data überträgt die eigentlichen Daten. Dabei erfolgt die Übertragung in fester Blockgröße von 512 Byte. Sind die Blöcke kleiner als 512 Byte, wird der eigentliche File-Transfer beendet, weil auf Datenblöcke kleiner 512 keine weiteren Daten folgen können. Der OPCode von Data hat immer den Wert Vier. Bei der Übertragung wird die Data-Blocknummer mit dem Wert Eins initialisiert. Dieser Wert erhöht sich mit jedem weiteren übermittelten Datenblock.

Bis auf die Pakete, die den File-Transfer beenden, werden alle Datenpakete von TFTP individuell bestätigt. Die Pakete TFTP Write Request und TFTP Data werden dabei immer mit einem Acknowledgment oder, falls notwendig, mit Error-Paketen quittiert. Die Acknowledgement-Pakete und TFTP-Read Request-Pakete werden immer mit Data- oder mit Error-Paketen bestätigt. Der OPCode von Acknowledgements hat immer den Wert Vier. Die Acknowledgement-Blocknummer enthält immer die Blocknummer des zu bestätigenden Datenblocks. Write Requests werden dabei immer mit einer Blocknummer = Null bestätigt.

Mit Error werden Fehler bei der Übermittlung von Files angezeigt. Ein Error-Paket kann von jedem anderen TFTP-Pakettyp bestätigt werden. Der Error OPCode hat immer den Wert Fünf. Error-Pakete kodieren die gemeldeten Fehlerursachen. Die folgende Tabelle gibt einen Überblick.

Error Code	Beschreibung
0	Nicht definiert
1	File nicht gefunden
2	Kein Zugriff
3	Disk voll
4	Unzulässige TFTP-Operation
5	Unbekannte Transfer-ID

Tabelle 4.23: Error Codes von TFTP

Je nach Implementierung kann eine so genannte Error-Message dem Benutzer detaillierte Hinweise auf Fehler geben.

Treten nun während der Kommunikation Fehler auf, so führt dies immer zum Abbruch des File-Transfers. Der Kommunikationspartner, der den Fehler während der Datenübertragung erkennt, generiert eine Fehlermeldung. Diese bedingt dann den Abbruch des File-Transfers.

Im Gegensatz zum FTP-Protokoll werden verloren gegangene Datenpakete dabei nicht erneut gesendet. Diesen Nachteil kompensiert das TFTP durch einen so genannten Timeout-Retransmission-Mechanismus. Über diesen Mechanismus verfügt jeder der an der TFTP-Sitzung beteiligten Hosts. Empfängt der Quell-Host nach Ablauf des Timers keine Bestätigung, so wird automatisch der nicht quittierte Datenblock erneut übertragen. Wird auf eine Bestätigung auf einen empfangenen Block nicht innerhalb einer bestimmten

Zeit ein neuer Datenblock empfangen, so wird die letzte Bestätigung erneut gesendet. Die Datenpakete verfügen dabei mit Ausnahme des letzten Pakets immer über eine statische Größe von 512 Byte.

4.7.3 Telnet

Als erster Dienst im Internet, bekannt unter der Bezeichnung »Ad hoc Telnet Protocol« (1972), bietet Telnet die Möglichkeit, sich über ein Remote-Login an einem entfernten Rechner anzumelden. Durch Telnet arbeitet man so, als ob der Bildschirm und die Tastatur direkt an den entfernten Rechner angeschlossen wären. Die Spezifikationen von Telnet sind im RFC 854 veröffentlicht.

Viele der Dienste, die im Internet angeboten werden, können auch über Telnet genutzt werden. Dies hat den Vorteil, dass man nicht für jeden Dienst das entsprechende Client-Programm installieren muss. Da es sich bei Telnet um ein Terminalprogramm ohne grafische Benutzeroberfläche handelt, erfolgt die Darstellung der Informationen jedoch im reinen Textmodus. Darüber hinaus kann Telnet auch für die Konfiguration und Administration der Remote-Systeme genutzt werden.

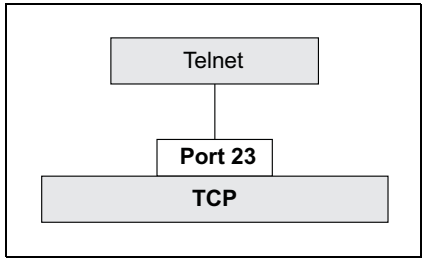


Abbildung 4.72: Telnet Socket

Funktionsweise von Telnet

Durch das Konzept des virtuellen Terminals arbeitet Telnet plattformunabhängig.

Im Grunde geht es darum, dass die Eingaben auf dem Client auf dem verbundenen Server als lokale Eingaben eines Terminalbenutzers an die Anwendung weitergegeben werden. Umgekehrt sendet der Server alle Ausgaben der Anwendung an das Ausgabegerät des Clients.

Ein so genanntes Network Virtual Terminal, **NVT**, bildet die Grundlage für die Kommunikation zwischen zwei Rechnern über Telnet. Das NVT definiert eine Reihe von Regeln und Eigenschaften, die bei einer Telnet-Sitzung unbedingt erforderlich sind. Jeder Endpunkt einer Telnet-Sitzung besteht logisch aus einer NTV-Tastatur und einem NTV-Drucker. Dadurch wird es möglich, dass Computersysteme mit völlig unterschiedlichen Architekturen und Leistungsmerkmalen miteinander kommunizieren können. NTV besteht aus einer virtuellen Tastatur, die definierte Zeichen erzeugen kann, und einem virtuellen Bildschirm bzw. Drucker, der entsprechende Zeichen darstellen kann.

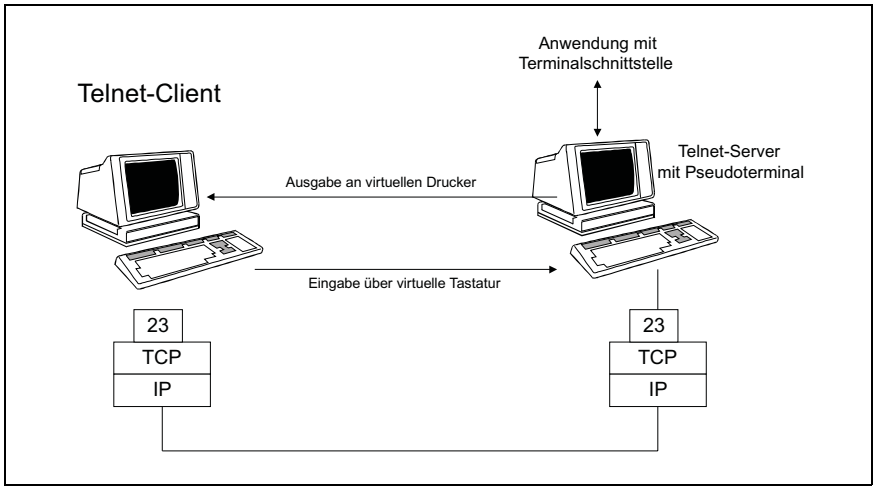


Abbildung 4.73: Architektur von Telnet

Negotiated Options

Jede Telnet-Sitzung beginnt immer auf der Basis des NVT. Das Negotiated Options-Konzept, aushandelbare Optionen, ermöglicht es den beteiligten Kommunikationspartnern, zusätzliche Optionen auszuhandeln, die nicht über das NVT abgedeckt werden. Dadurch lassen sich weitere Eigenschaften definieren, die denen der reellen Terminals entsprechen. So gehört z.B. die Interpretation von Funktionstasten zu den verhandelbaren Optionen.

Symmetrische Verbindung

Die zur Verfügung stehenden Protokollfunktionen und -mechanismen können von beiden Kommunikationspartnern der Telnet-Sitzung gleichberechtigt benutzt werden. Die Aushandlung von Optionen bzw. Parametern kann deshalb von beiden Partnern initiiert werden. Verbindungen, in denen die Kommunikationspartner gleichberechtigt sind, werden auch symmetrische Verbindungen genannt.

Gestartet wird ein Telnet-Client mit dem Kommando **telnet**. Zu diesem Zeitpunkt kann auch direkt der Name oder die IP-Adresse des Ziel-Hosts angegeben werden, um die Telnet-Sitzung sofort mit einem Remote-Rechner zu öffnen.

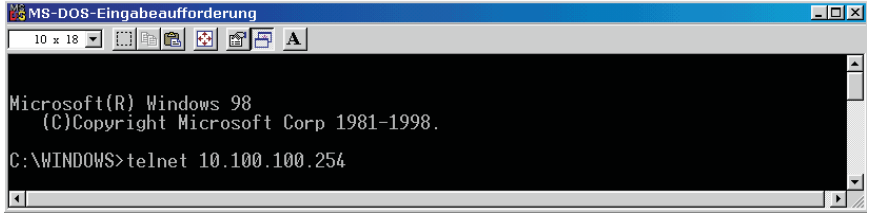


Abbildung 4.74: Telnet-Verbindungen aufbauen

Ist ein Telnet-Client bereits gestartet, wird die Verbindung zum Ziel-Host mit dem Kommando open <ziel-host> hergestellt. Nachdem eine Verbindung zustande gekommen ist, muss man sich auf dem Rechner anmelden.

Handelt es sich um kein öffentliches System, dann ist ein Benutzername und ein Passwort zwingend notwendig. Auf öffentlich zugänglichen Systemen hingegen ist es in der Regel ausreichend, sich mit einem speziellen Benutzernamen anzumelden. In vielen Fällen finden Sie diesen auf dem Eröffnungsbildschirm. Wird über Telnet auf einen anderen Internet-Dienst zugegriffen, so muss der entsprechende Port explizit angegeben werden. Zu diesem Zweck wird beim Verbindungsaufbau mit den Befehlen telnet oder open die Portnummer hinter die Rechneradresse des Zielsystems gesetzt.

Beispiel: telnet 10.100.100.254 21

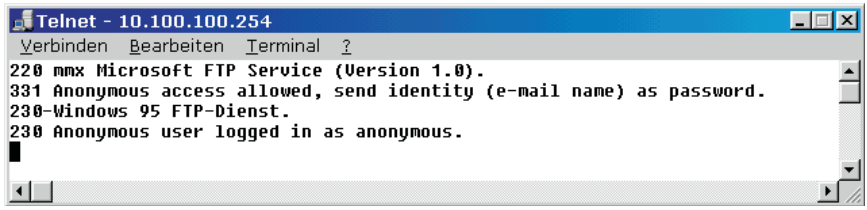


Abbildung 4.75: FTP-Verbindung über Telnet aufbauen

Abbildung 4.75 zeigt den Verbindungsaufbau zu einem FTP-Server über Telnet. Dieses Beispiel macht nochmals das Prinzip des Pseudoterminals deutlich. Aus der Sicht des FTP-Servers, der in diesem Beispiel die Funktion einer Anwendung mit Terminalschnittstelle hat, erfolgt das Login lokal, d.h. so als würde der User alle Tastatureingaben über ein angeschlossenes Terminal eingeben.

Telnet-Befehle

Wird Telnet ohne Angabe einer Zieladresse gestartet, so gelangt man in den Kommandomodus. Im diesem Modus können dann Kommandos zur Steuerung und Konfiguration abgesetzt werden.

Kommando	Bedeutung
open Rechnername open IP-Adresse	Über dieses Kommando wird versucht, eine Verbindung zu dem adressierten Host aufzubauen. Wird die Verbindung ohne Angabe einer Portnummer initiiert, erfolgt der Verbindungsaufbau über Port 23.
close	Das Kommando close bewirkt, dass die Verbindung abgebrochen wird.
quit	Das Kommando quit beendet die Telnet-Sitzung.
z	Durch Eingabe von z gelangt man zur Eingabeauforderung des Betriebssystems zurück, ohne jedoch die Telnet-Sitzung zu beenden. Zu einem späteren Zeitpunkt kann die Telnet-Sitzung wieder aufgenommen werden.

Tabelle 4.24: Telnet Befehlsübersicht

Kommando	Bedeutung
mode	Mit mode wird festgelegt, zu welchem Zeitpunkt Telnet die Eingabe überträgt. Im Character-Mode wird jedes eingegebene Zeichen direkt übertragen. Im Line-Mode werden die Zeichen erst übertragen, wenn eine Zeile mit <Return> abgeschlossen wird. In den meisten Fällen arbeitet man jedoch im Character-Mode.
set	Durch set werden spezifische Parameter gesetzt.
toggle	Mit toggle werden Parameter ein-, aus- oder umgeschaltet.
options	Sofern options aktiviert ist, können die Verhandlungen von Client und Server auf dem Bildschirm mitverfolgt werden.
?	Aufruf der Hilfefunktion

Tabelle 4.24: Telnet Befehlsübersicht

Bei den Telnet-Clients unter MS-Windows ist in der Regel kein Kommandomodus implementiert. Dort erfolgt die Konfiguration der Verbindungsparameter menügesteuert. Die grafische Benutzeroberfläche wird automatisch gestartet, wenn der Anwender im DOS-Fenster das Programm telnet aufruft.

Als Verbindungsparameter werden im in Abbildung 4.76 gezeigten Beispiel der Host-Name oder alternativ die IP-Adresse, der Anschlusstyp, in unserem Beispiel der Telnet-Port, und der Terminaltyp angegeben.

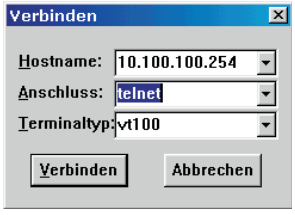


Abbildung 4.76: Verbindungskonfiguration eines Telnet-Clients unter Windows

Netzadministration mit Telnet

Telnet ist für den Netzadministrator ein mächtiges Werkzeug zur Fernsteuerung der über TCP/IP miteinander verbundenen Rechner. Wenn auf einem Rechner ein Telnet-Server läuft, dann kann dieser Rechner über Telnet vollkommen kontrolliert werden. Ein typisches Beispiel hierfür ist das Herunterfahren, shutdown, des entfernten Rechners.

Dieser Vorteil von Telnet ist allerdings auch ein Nachteil. Rechner, auf denen Telnet-Server laufen, sind für Hacker ein beliebtes Ziel und stellen eine große Gefahrenquelle dar. Noch schwerwiegender ist die Tatsache, dass der gesamte Datenaustausch über Telnet unverschlüsselt als Klartext erfolgt. Wenn es gelingt, ein Überwachungsprogramm, einen Sniffer, in die Verbindung einzuklinken, dann können Benutzernamen und Passwörter ausgespäht werden.

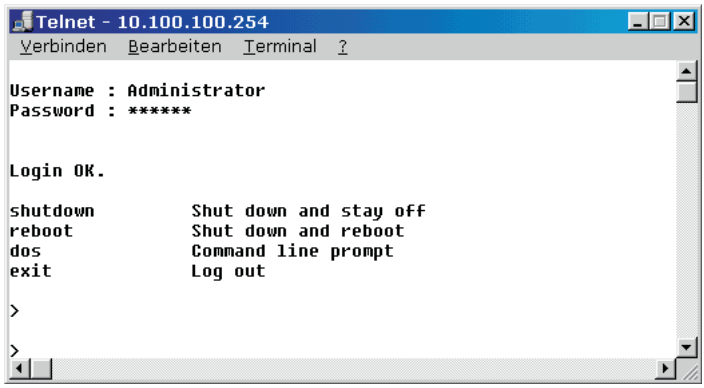


Abbildung 4.77: Systemadministration mit Telnet

4.7.4 SMTP (Simple Mail Transfer Protocol)

Für den Transport einer E-Mail in einem TCP/IP-Netzwerk ist das Simple Mail Transfer Protocol zuständig. Um eine gesicherte Übertragung der E-Mail zu gewährleisten, werden TCP und der Port 25 benutzt. Die Spezifikationen des Simple Mail Transfer Protocol sind im RFC 821 veröffentlicht. Weitere in diesem Zusammenhang wichtige RFCs sind RFC 822 »Standard for the Format of Arpa Internet Text Messages«, RFC 1049 »Content-Type Header Field for Internet Messages« und RFC 1154 »Encoding Header Field for Internet Messages«.

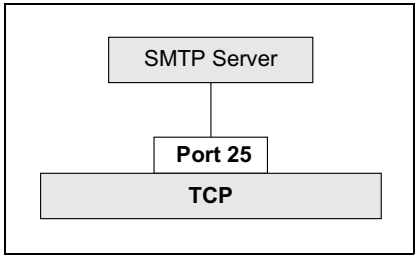


Abbildung 4.78: SMTP Socket

Nach einer Mailanforderung des Benutzers stellt der SMTP-Sender eine Verbindung zum SMTP-Empfänger her, wobei der SMTP-Empfänger entweder der Zielrechner selbst oder eine Zwischenstation sein kann.

Funktionsweise von SMTP

Im Folgenden wird beispielhaft eine typische SMTP-Mail-Sitzung beschrieben. Sie besteht im Wesentlichen aus drei Phasen:

- ✔ Verbindungsaufbau
- ✔ Senden der Daten
- ✔ Verbindungsabbau

An der Übertragung ist immer ein Client und ein E-Mail-Server beteiligt. Der Server ist permanent online und verwaltet seine lokalen User. Ist der Adressat einer empfangenen Mail nicht lokal, dann wird der Server die Mail via Internet an den nächsten ihm bekannten Server weiterleiten.

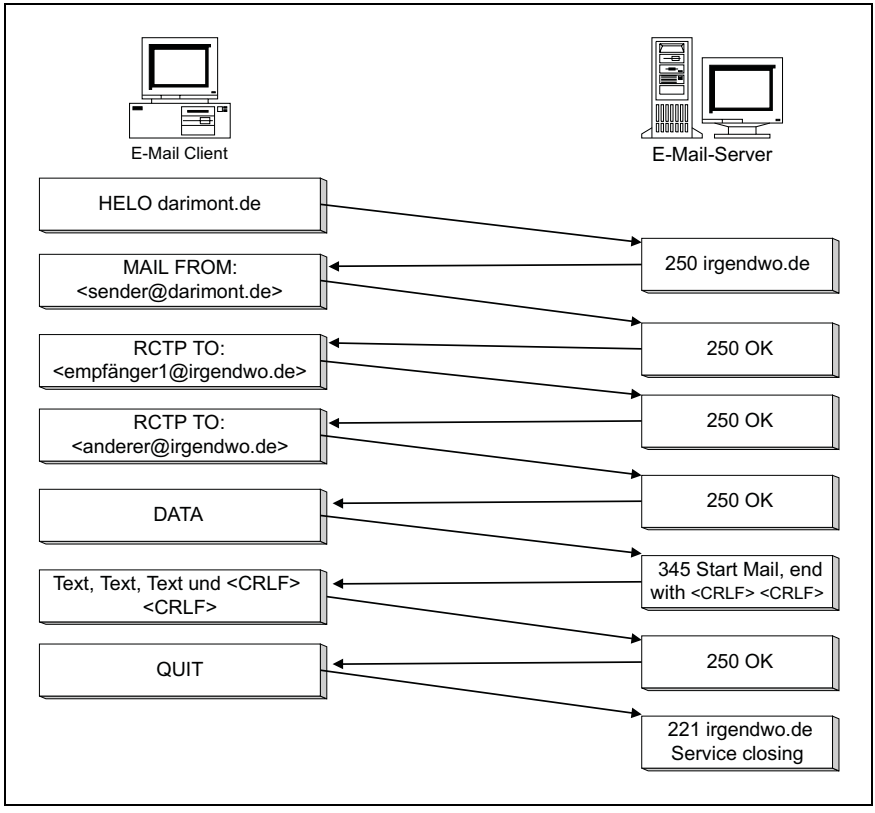


Abbildung 4.79: Ablauf einer SMTP-Sitzung

Details einer SMTP-Sitzung:

1. Der Quell-Host baut eine Verbindung zum Ziel-Host auf.
2. Der Quell-Host empfängt vom Ziel-Host eine Service-Ready- oder eine Service-Not-Available-Meldung.
3. Der Quell-Host antwortet mit HELO und identifiziert sich mit seiner Domäne.
4. Der Quell-Host setzt einen MAIL-Befehl ab, womit der eigentliche Mail-Prozess beginnt. Der Ziel-Host antwortet mit OK.
5. Der RCPT-Befehl sendet dem Ziel-Host die Adresse des Empfängers. Der Ziel-Host antwortet entweder mit OK oder Mailbox Unavailable.

6. Mit dem DATA-Befehl startet der Quell-Host die Datenübertragung. Der Ziel-Host reagiert mit Start Mail Input; End With <CRLF>.<CRLF>. Die beiden letzten Zeichen stehen für Carriage Return, Zeilenumbruch, mit anschließendem Zeilenvorschub, Line Feed.
7. Wenn die Übertragung beendet werden soll, signalisiert der Quell-Host dies mit <CRLF>.<CRLF>.
8. Der Quell-Host beendet die Session mit dem QUIT-Befehl. Der Ziel-Host beantwortet dieses mit Service Closing Transmission Channel.

Befehle des Quell-Hosts

Kommando	Syntax	Bedeutung
Hello	HELO <sendender-rechner>	Identifikation des Quell-Hosts
From	MAIL FROM:<sender-adresse>	Adresse des Quell-Hosts
Recipient	RCPT TO:<empfänger-adresse>	Adresse des Ziel-Hosts
Data	DATA	Datentransfer, Beenden mit <crlf>.<crlf>
Reset	RSET	Abbruch
Verify	VRFY <string>	Benutzer-Id wird bestätigt
Expand	EXPN <string>	Expandieren einer Mailingliste
NOOP	NOOP	Erwartet Bestätigung
Help	HELP <string>	Online-Hilfe
Quit	QUIT	Normaler Verbindungsabbau

Tabelle 4.25: SMTP-Befehlsübersicht

SMTP definiert für die Rückmeldungen des E-Mail-Servers einen dreiziffrigen Zahlencode. Die erste Ziffer gibt dabei einen Hinweis auf die Art der Antwort, Replay genannt. Beginnt der Code mit der Ziffer »2«, dann handelt es sich um eine positive Rückmeldung, Positive Completion Replay. Der Server reagiert auf die Anforderungen des Clients mit der entsprechenden Befehlsausführung.

Codes, die mit der Ziffer »5« beginnen, deuten auf Fehler hin, Permanent Negative Completion Replay.

Auszugsweise Reaktionen des Ziel-Hosts

Meldung	Bedeutung
220	Service Ready
221	Service schließt den Übertragungskanal
250	OK
251	Empfänger nicht lokal, wird weitergegeben an <forward-path>

Tabelle 4.26: SMTP-Error-Codes

Meldung	Bedeutung
354	Start der Mail-Eingabe, Ende mit <crlf>.<crlf>
500	Syntax-Fehler
550	Negative Antwort, wenn Operation nicht möglich
551	Empfänger ist nicht lokal, Rückmeldung der richtigen Adresse
553	Empfänger kann nicht eindeutig identifiziert werden

Tabelle 4.26: SMTP-Error-Codes

Eine komplette Übersicht über die Reaktionen des Ziel-Hosts sind in dem RFC 821, Page 34 »Replay Codes by Function Groups« beschrieben.

Das folgende Beispiel zeigt Auszüge einer Nachricht, die aufgrund eines Fehlers an den Sender einer Mail geschickt wurde. In Zeile eins sehen Sie, wer die ursprüngliche Nachricht abgesetzt hat. Der Empfänger wird in der Zeile fünf genannt. In Zeile sieben sehen Sie den Fehlercode 550. Die Fehlerursache liegt darin, dass die IP-Adresse des Ziel-Hosts, in unserem Beispiel **irgendwo**, vom DNS-Server nicht ermittelt werden konnte.

BEISPIEL

```
1  -POP3-Rcpt: a.darimont@hit.handshake.de
2  The original message was received at Sun, 24 Oct 1999 10:30:38 +0200
3  from hs2-243.handshake.de [194.77.98.243]
4   ----- The following addresses had permanent fatal errors -----
5  <irgendwer@irgendwo>
6   ----- Transcript of session follows -----
7  550 <irgendwer@irgendwo>... Host unknown (Name server: irgendwo: host not
   found)
```

Im weiteren Beispiel wurde eine gültige Hostadresse verwendet. Allerdings gibt es den Empfänger nicht. Die daraus resultierende Fehlermeldung sehen Sie in Zeile sechs.

BEISPIEL

```
1  The original message was received at (unknown)
2  from unknown@hs-gate
3   ----- The following addresses had delivery problems -----
4  willibald.schmalspur@hit.handshake.de (Empfänger unbekannt)
5   ----- Transcript of session follows -----
6  550 willibald.schmalspur@hit.handshake.de... User willibald.schmalspur
   unbekannt
7   ----- Original message follows -----
8  U-Received: from K6 (hs1-246.handshake.de [194.77.97.246])
               by hs-gate.handshake.de (8.9.3/8.9.3) with SMTP id RAA18413
               for <willibald.schmalspur@hit.handshake.de>;
               Sun, 24 Oct 1999 17:52:53 +0200
9  MID:        000801bf1e38          $a29467e0     $c864640a@darimont.net
```

Alle SMTP-Informationen werden direkt im Datenbereich der E-Mail transportiert. Moderne E-Mail-Clients blenden diesen jedoch aus, so dass der Empfänger lediglich die eigentliche Nachricht sieht.

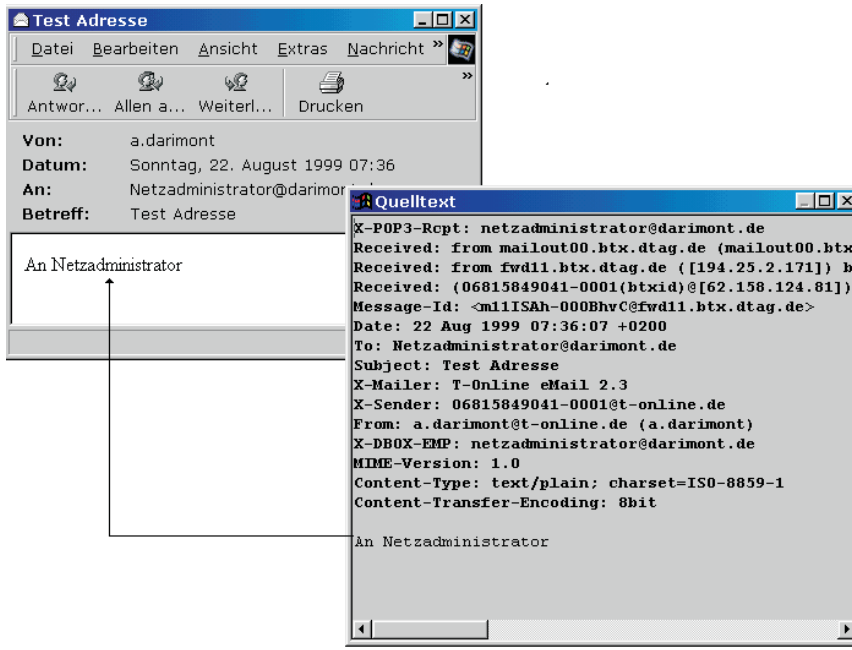


Abbildung 4.80: SMTP-Quelltext

Administratoren müssen aber auch die SMTP-Informationen lesen können. Deshalb besteht die Möglichkeit, diese bei Bedarf einzublenden. Abbildung 4.80 zeigt im linken Fenster, wie der E-Mail-Client dem Empfänger eine Nachricht darstellt. Der Empfänger sieht den so genannten Body, dessen Inhalt die vom Sender eingegebene Nachricht ist. Im rechten Fenster sind die SMPT-Informationen vollständig aufgeführt. Alle Informationen von SMTP und die eigentliche Nachricht werden angezeigt.

Spooling

Eine zu versendende E-Mail wird nicht direkt von der Mail-Anwendung über das Netz zum Ziel-Host gesendet, sondern vielmehr mit allen relevanten Informationen in eine Warteschlange, den Spoolbereich, gestellt. Der Spoolbereich wird dann in festgelegten Zeitabständen nach nicht zugestellten Mails durchsucht. Dieser Hintergrundtask versucht anschließend, eine TCP/IP-Verbindung zum Ziel-Host oder zum Mail-Server herzustellen.

Besteht die Verbindung, wird die E-Mail übertragen und im Spoolbereich des Ziel-Hosts abgelegt. Dort bleibt die E-Mail bis sie dem Empfänger zugestellt werden kann oder von ihm abgeholt wird. Nach erfolgreicher Übertragung wird die E-Mail aus dem Spoolbereich gelöscht.

Konnte die E-Mail nicht übertragen werden, bleibt die E-Mail im Spoolbereich, wobei nach einer gewissen Wartezeit erneut eine Übertragung versucht wird. Ist eine Zustellung auch nach mehrmaligen Versuchen nicht möglich, wird eine Fehlermeldung an den Quell-Host geschickt.

Reverse und Forward Path – Details zur SMTP Message

Beim Übertragen von E-Mails via SMTP wird die Adresse des Senders als Reverse Path bezeichnet. Die Adresse des Empfängers ist entsprechend der Forward Path. Der Forward Path wird mit dem Kommando RCPT übermittelt. Da dieser Befehl beliebig oft mit jeweils einem anderen Empfänger gesendet werden kann, muss die eigentliche Mail selbst bei Hunderten von Empfängern nur einmal vom Sender an seinen Server übertragen werden.

Beide Pfadangaben beinhalten nicht nur die Adresse einer Mailbox, sondern je nach Situation eine Routingliste, die aus mehreren Hosts bestehen kann, die beim Senden der Nachricht durchlaufen wurden. Dadurch wird der Weg, den eine Nachricht genommen hat, nachvollziehbar. Ohne diesen Mechanismus könnte ein Absender beim Auftreten von Fehlern nicht informiert werden. Ein typischer Fehlerfall besteht darin, dass der Sender eine ungültige E-Mail-Adresse angegeben hat, dies jedoch vom ersten Mail-Server nicht erkannt werden konnte. Erst spätere Server erkennen diesen Fehler und müssen nun in der Lage sein, eine entsprechende Meldung an den Sender abzugeben.

Beim Transfer einer Nachricht werden Reverse- und Forward-Path nach dem folgenden Verfahren geschrieben:

- ✔ Der empfangende Host entfernt seinen am Anfang des Forward Paths stehenden Namen und stellt ihn dem bisherigen Reverse Path voran.

Das unten abgebildete Beispiel zeigt einen typischen Reverse Path:

1. Server: @onlinehome.de (Zeile 5)
2. Server: pd4b886f0.dip0.t-ipconnect.de (Zeile 4)
3. Server: mx01.kundenserver.de (Zeile 3)
4. Server: mout00.kundenserver.de (Zeile 2)
5. Empfänger: info@darimont.de (Zeile 1)

Beispiel

```
1  X-POP3-Rcpt: info@darimont.de
2  Received: from mout00.kundenserver.de (mout00.kundenserver.de
   [195.20.224.69]) by hs-gate.handshake.de (8.9.3/8.9.3) with ESMTP id
   HAA32407 for <info@darimont.de>; Sat, 2 Oct 1999 07:00:55 +0200
3  Received: from [195.20.224.236] (helo=mx01.kundenserver.de) by
   mout00.kundenserver.de with esmtp (Exim 2.12 #2) id 11XHIe-0005p6-00 for
   info@darimont.de; Sat, 2 Oct 1999 07:01:36 +0200
4  Received: from pd4b886f0.dip0.t-ipconnect.de ([212.184.134.240]
   helo=onlinehome.de) by mx01.kundenserver.de with esmtp (Exim 2.12 #2) id
   11XHIM-0004Ga-00 for info@darimont.de; Sat, 2 Oct 1999 07:01:18 +0200
5  Message-Id: <37F59199.FDAE4FAC@onlinehome.de>
6  Date: 02 Oct 1999 06:01:13 +0200
7  From: 1145-53@onlinehome.de (1145-53)
8  X-Mailer: Mozilla 4.6 [de]C-CCK-MCD QXW0321n (Win95; I)
9  X-Accept-Language: de,en
10 To: info@darimont.de
11 Subject: Imagemap
12 X-DBOX-EMP: info@darimont.de
13 MIME-Version: 1.0
14 Content-Type: multipart/mixed; boundary=«------------
   F5A9BC314C54952F1F9E3012«
15 Content-Transfer-Encoding: 8bit
```

Der Empfänger steht in diesem Beispiel in Zeile 1 und hat den Account-Namen: **info** in der Domäne **@darimont.de**. Der verwaltende E-Mail-Server hat die Adresse **hs-gate.handshake.de**. Sollte hier ein Fehler auftreten, dann wird der Server die Fehlermeldung an **onlinehome.de** senden und dabei den unten gezeigten Reverse Path benutzen.

1. Server: mout00.kundenserver.de (Zeile 2)
2. Server: mx01.kundenserver.de (Zeile 3)
3. Server: pd4b886f0.dip0.t-ipconnect.de (Zeile 4)
4. Server: @onlinehome.de (Zeile 5)

SMTP und Datenobjekte – MIME

SMPT erlaubt nach dem RFC 822 »Standard for the Format of ARPA Internet Text Messages« nur das Versenden von reinem Text. Da dies nicht mehr zeitgemäß war, wurde 1991 mit dem RFC 1521 der Standard erweitert: Er enthält nun **MIME**, Multipurpose Internet Mail Extentions, als eine Technik zur Spezifizierung und Beschreibung von Dateiformaten in einer E-Mail-Nachricht, »Mechanisms for Specifying and Describing the Format of Internet Message Bodies«. Dadurch ist der Benutzer beim Versenden von Nachrichten nicht mehr nur auf reinen Text beschränkt. 1996 wurden RFC 1521 und 1522 durch die überarbeiteten RFCs 2045 bis 2049 ersetzt. Vielfach wird aber noch auf den alten Standard verwiesen.

MIME stellt somit die »multimediale« Erweiterung von SMTP dar, wodurch auch das Versenden von Objekten wie Sound- und Videodateien ermöglicht wird. Diese werden als Anhang oder Attachment an die im Textformat vorliegende Nachricht angehängt.

Im unten abgebildeten Beispiel können Sie in den Zeilen drei und vier sehen, dass die eigentliche Nachricht als ASCII-Text mit 8-Bit Zeichensatz übertragen wird. Das Schlüsselwort ist hier Content-Type. Der Zeichensatz entspricht der ISO-Norm 8859-1. Damit ist der Zeichensatz der Nachricht definiert, und der Anwender kann nationale Sonderzeichen wie z.B. Umlaute verwenden. Die ISO-Norm ist wie folgt zu interpretieren:

- ✔ ISO 8859-x entspricht einem Zeichensatz mit nationalen Sonderzeichen
- ✔ x ist die Angabe, zu welchem Gültigkeitsbereich der Zeichensatz gehört. Die folgende Tabelle zeigt eine Auswahl:

ISO-Norm	Zeichensatz
8859 – 1	Lateinisch Nr. 1 Westeuropa
8859 – 2	Lateinisch Nr. 2 Osteuropa
8859 – 3	Lateinisch Nr. 3 Südeuropa
8859 – 4	Lateinisch Nr. 4 Nordeuropa
8859 – 5	Kyrillisch
8859 – 6	Arabisch

Tabelle 4.27: Nach ISO standardisierte Zeichensätze

Ab der Zeile zehn beginnen die Information zum MIME-Format des Anhangs. Es handelt sich hier um eine Datei, die zu einer Anwendung gehört, application/xxx. Der Datentyp ist x-zip-compressed. Das bedeutet, dass die angehängte Datei gepackt ist und die Erweiterung, den Suffix, zip, besitzt.

BEISPIEL

```
1  Dies ist eine mehrteilige Nachricht im MIME-Format.
2  --------------F5A9BC314C54952F1F9E3012
3  Content-Type: text/plain; charset=iso-8859-1
4  Content-Transfer-Encoding: 8bit
5  Hallo Herr Darimont, hab grad 'ne Imagemap beim Surfen gefunden, aber
6  warum Imagemap + Tabelle
7  Sende die HTML Seite mit den Bildern als zip
8  Gruß xxxx
9  --------------F5A9BC314C54952F1F9E3012
10 Content-Type: application/x-zip-compressed;
11  name="imap.zip"
12 Content-Transfer-Encoding: base64
13 Content-Disposition: inline;
14 filename="imap.zip«
```

Die folgende Tabelle zeigt weitere Beispiele zum Thema MIME-Formate. Es handelt sich hier um eine Auswahl, die nochmals das Prinzip verdeutlicht. Sie sehen den MIME-Typ für Audio- und Videodateien, video/xx bzw. audio/xx und einen MIME-Typ, der das Ausführen von Befehlen auf dem Empfängersystem ermöglicht.

MIME-Content-Typ	Beschreibung	Suffix
video/x-msvideo	Video for Windows	Avi
audio/basic	Audio-Datei	Au
audio/x-aiff	Audio-Format MacIntosh	aif, aiff
audio/x-wav	Audio-Format	Wav
application/x-director	Shockwave Movie	dir, dxr, dcr

Tabelle 4.28: MIME-Formate

In der letzten Zeile finden Sie Datenformate einer Anwendung, application/xx, die Director heißt.

Die Eigenschaft Content-Type unterscheidet zwischen Top-Level-Media-Types wie video, audio, application oder text, und Sub-Types wie msvideo oder x-director.

MIME-Formate spielen insbesondere auch bei der Erweiterung des WWW um multimediale Elemente eine entscheidende Rolle. So können z.B. in einem Browser die oben aufgeführten Dateiformate dargestellt bzw. abgespielt werden. Dazu muss dann ein so genannter Viewer eingebunden werden, der in der Lage ist, das angegebene Datenformat anzuzeigen. Viewer werden in der Regel als so genannte Plug-Ins installiert.

MIME-Formate stellen ein potentielles Risiko dar. Details hierzu finden Sie bei Kyas, Sicherheit im Internet, DATACOM 1996.

4.7.5 POP3 (Post Office Protocol Version 3)

SMTP ist für Systeme ohne Direktanbindung nicht geeignet. Das Post Office Protocol POP beseitigt diese Einschränkung. Es ermöglicht eine zentrale Verwaltung und Speicherung von Nachrichten. Das hierfür eingesetzte System wird als Post Office bezeichnet. Hier befinden sich die elektronischen Postfächer der eingerichteten User.

Die Spezifikationen des Post Office Protocols in der Version 3 sind in den RFCs 1081 und 1225 veröffentlicht und seit 1994 etabliert.

Der Empfänger von POP-Nachrichten muss dazu auf einem POP3-Server als Benutzer eingetragen sein und dort ein Postfach, Konto, besitzen. Im DNS-Eintrag des E-Mail-Clients wird der E-Mail-Server vermerkt, weil alle per SMTP eingehenden Mails zunächst dort landen. Das Mail-Programm des Empfängers kann dann bei Bedarf mit POP3 über den TCP/IP-Port 110 das Postfach auf dem Mail-Host leeren.

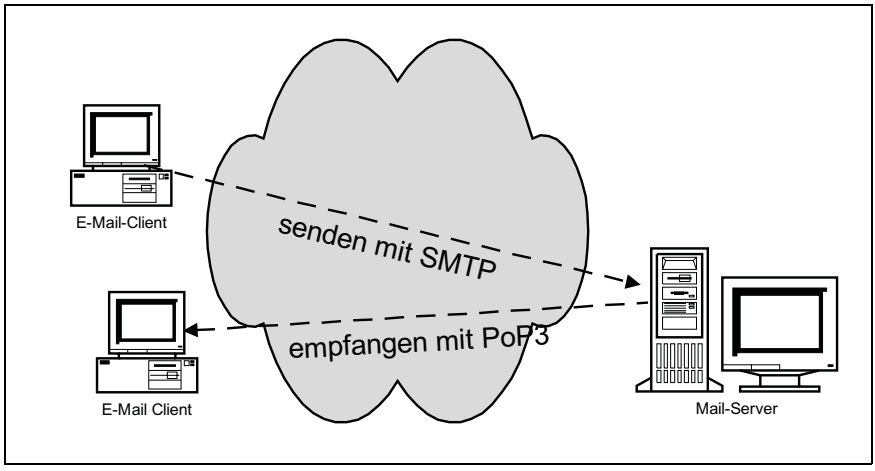


Abbildung 4.81: SMTP und POP3 im Zusammenhang

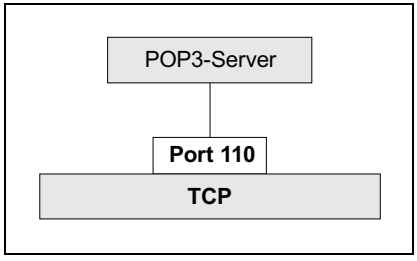


Abbildung 4.82: POP3-Socket

Da auf nahezu jedem Mailsystem sowohl ein POP- als auch ein SMTP-Server eingerichtet ist, ergänzen sich heute die beiden Protokolle. Der Netzadministrator wird also in der Regel für seine Anwender jeweils einen SMTP- und einen POP3-Server konfigurieren. Konfigurationsparameter sind dann:

- ✔ Adresse des POP3-Servers, als DNS Name oder IP-Adresse
- ✔ Adresse des SMTP-Servers, als DNS-Name oder IP Adresse
- ✔ Benutzername
- ✔ Passwort

Als Erweiterung von POP2, welches zwingend auf das SMTP-Protokoll angewiesen war, kann POP3 aber auch ohne Verwendung von SMTP eingesetzt werden. POP3 ist also ein spezielles Client/Server-Protokoll, das der Kommunikation zwischen einem E-Mail-Programm auf dem PC eines Anwenders und einem Mail-Server mit dem Postfach dieses Anwenders dient.

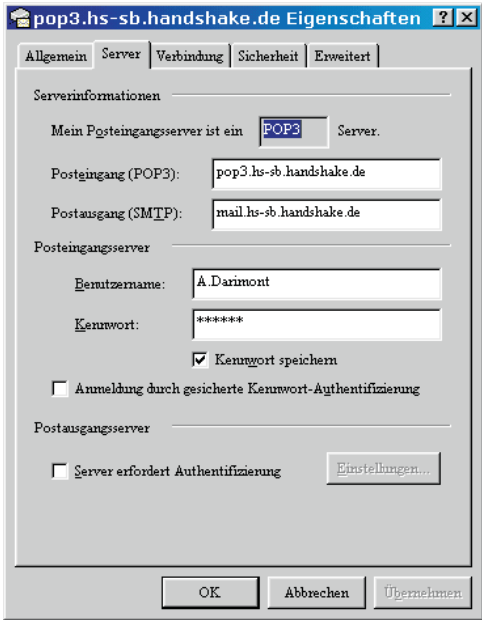


Abbildung 4.83: SMTP- und POP3-Konfiguration

Befehlsübersicht POP 3

POP3 definiert auf der einen Seite eine Reihe von Kommandos, die der Client absetzt, und auf der anderen Seite mögliche Antworten des Servers. Die folgende Tabelle gibt einen Überblick.

Befehl	Parameter	Bedeutung
USER	<name>	Meldet den Benutzer beim Server an
PASS	<passwort>	Überträgt das Passwort des Benutzers
APOP	<name> <zahlencode>	Ersetzt die Kommandos USER und PASS. Die Daten werden verschlüsselt.
STAT	Keine	Gibt Anzahl und Gesamtgröße der vorhandenen Nachrichten aus
LIST	Keine <nummer>	Wird kein Parameter angegeben, dann werden alle Nachrichten mit ihrer Nummer und der Größe angegeben. Mit Parameter werden die Daten der Nachricht mit der entsprechenden Nummer gesendet.
RETR	<nummer>	Ruft die angegebene Nachricht ab
DELE	<nummer>	Löscht die angegebene Nachricht
NOOP	Keine	Keine Operation, wird vom Server mit OK bestätigt
LAST	Keine	Sendet die Nummer der Nachricht, auf die zuletzt zugegriffen wurde

Tabelle 4.29: Befehlsübersicht POP3

Befehl	Parameter	Bedeutung
RSET	Keine	Zähler auf die aktuelle Nachrichtennummer bei Start der Session zurücksetzen. Löschmarken werden dabei entfernt.
QUIT	Keine	Server leitet das Beenden der Verbindung ein. Dabei werden alle als zu löschend markierten Nachrichten gelöscht.

Tabelle 4.29: Befehlsübersicht POP3

Reaktionen des Servers

Meldung	Bedeutung
+ OK	Positive Bestätigung, es kann ein beliebiger einzeiliger Text folgen oder aber der Server wiederholt den vorangegangenen Befehl.
- Error	Negative Bestätigung, es kann ein beliebiger einzeiliger Text folgen oder aber der Server wiederholt den vorangegangenen Befehl.

Tabelle 4.30: Rückmeldungen eines POP3-Servers

Ablauf einer POP3-Session

Die folgende Grafik zeigt den typischen Ablauf einer POP3-Session. Die Verbindung wird in diesem Beispiel über das Kommando APOP aufgebaut. Dies bewirkt, dass Benutzername und Passwort verschlüsselt übertragen werden. Die Befehle USER und PASS übertragen im Gegensatz dazu die Daten als Klartext.

Auch eine POP3-Session besteht aus den drei Phasen:

- ✔ Verbindungsaufbau
- ✔ Senden der Daten
- ✔ Verbindungsabbau.

Dabei wartet der Server am Port 110 auf eine Verbindung, die vom Client initiiert wird. Die folgende Grafik zeigt die auf den Verbindungsaufbau folgenden Phasen.

Adressformat

Der erste Teil einer E-Mail-Adresse ist, sofern noch nicht vergeben, von Ihnen frei wählbar. Der zweite Teil nach dem @-Zeichen wird jedoch fest vorgegeben und entspricht der Domain, in der der Server liegt.

IhrName@IhrServer.Top-Level-Domain

z.B. niklas.steffen@t-online.de oder auch vincent.steffen@t-online.de

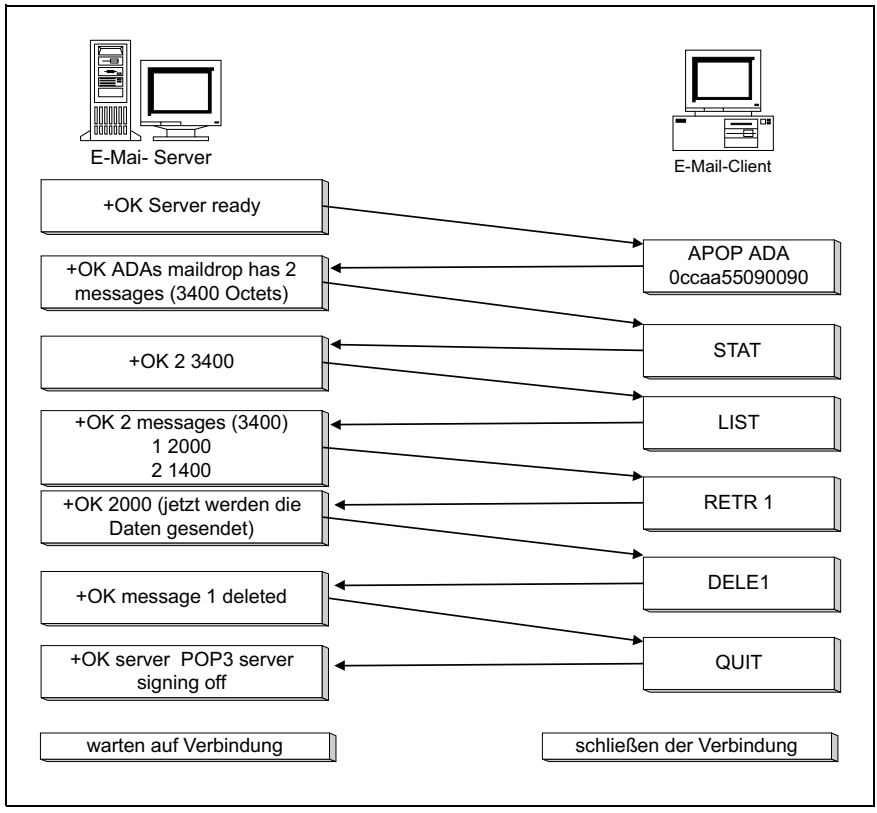


Abbildung 4.84: Ablauf einer POP3-Sitzung

4.7.6 HTTP – Hypertext Transfer Protocol

Das Hypertext Transfer Protocol ist das Anwendungsprotokoll des World Wide Web. Seine Hauptaufgabe auf Serverseite besteht darin, über Hyperlinks verknüpfte Dokumente für den Abruf durch HTTP-Clients zur Verfügung zu stellen. Die aktuelle Version HTTP 1.1 ist im RFC 2068 veröffentlicht und abwärtskompatibel zu HTTP 1.0, dokumentiert in RFC 1945.

HTTP setzt standardmäßig auf dem Port 80 auf. Die aktuellen Server lassen aber die Konfiguration beliebiger Ports zu.

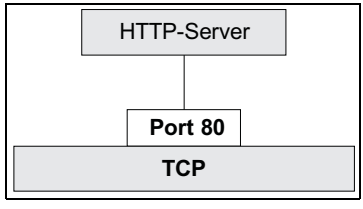


Abbildung 4.85: HTTP-Socket

HTTP als Client/Server-Protokoll

HTTP funktioniert nur zwischen einem HTTP-Client und einem HTTP-Server. Programme, die den Client implementieren, werden Browser genannt, die Server heißen Webserver. HTTP-Clients fordern Dokumente an, in der Regel Webseiten, die der Server sendet.

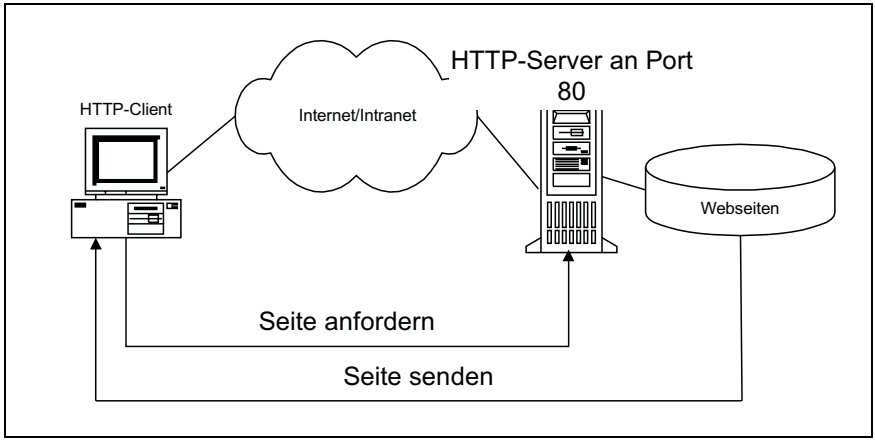


Abbildung 4.86: HTTP-Client und HTTP-Server

Die Kommunikation zwischen Client und Server wird über HTTP-Befehle gesteuert. HTTP-Kommandos werden in Textdateien transportiert, die zwischen Client und Server ausgetauscht werden. Die hier transportierten Nachrichten können aus bis zu drei Bereichen bestehen.

- ✔ Anforderungszeile mit HTTP-Befehlen
- ✔ Header mit Informationen zum Transportieren von Dokumenten
- ✔ Body mit dem Inhalt des Dokuments, der dann z.B. von einem Browser dargestellt wird

Die folgenden Zeilen demonstrieren den Inhalt von Anforderungszeilen und von Headern. Als erstes sehen Sie eine Client-Anforderung, die von einem Browser via HTTP gesendet wird. Das zweite Beispiel zeigt Headerinformationen, die vom Server kommen.

HTTP-Anfrage durch einen Client

BEISPIEL

```
GET /webshare/myWeb/index.html HTTP/1.1
Accecpt: text/html
Accept: image/gif
```

Die erste Zeile fordert die Datei **index.html**. Dabei wird über den Befehl GET der Pfad auf dem Web-Server angegeben. Der Client signalisiert in der gleichen Zeile, dass er die HTTP-Version 1.1 unterstützt. In den folgenden Zeilen, die mit dem Schlüsselwort Accept beginnen, teilt der Client dem Server mit, dass er HTML-Dokumente und Dateien im GIF-Grafikformat darstellen kann.

HTTP-Antwort eine Webservers

Aus der ersten Zeile der Antwort ist zu erkennen, dass der Datenaustausch ohne Fehler durchgeführt werden konnte. In den weiteren Zeilen werden Statistiken, wie Zeit-/Datumsangaben, Format und Länge des gesendeten Dokuments, aufgeführt.

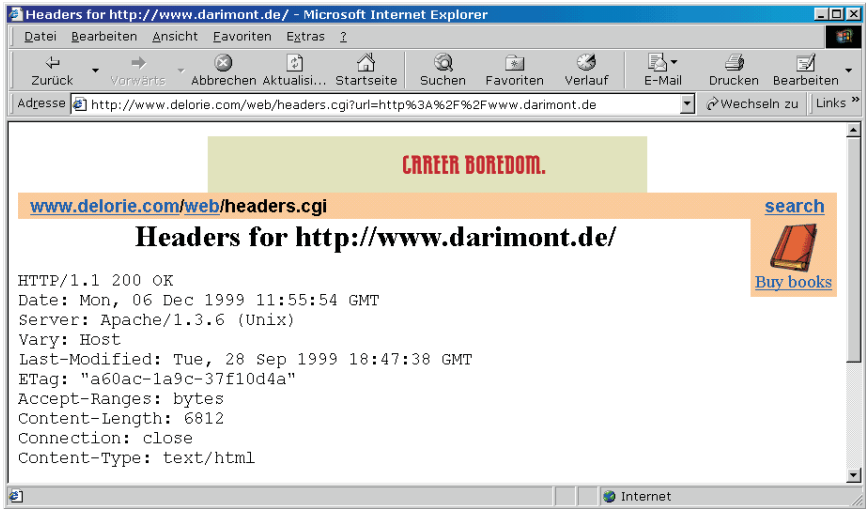


Abbildung 4.87: Header-Informationen zu einer HTML-Seite

Hat ein Client nicht nur den Header, sondern das komplette Dokument angefordert, dann wird in einem zweiten Schritt der Body des Dokuments übertragen. Erkennt ein Client, dass in das empfangene Dokument Grafikdateien eingebunden werden müssen, dann fordert er diese im weiteren Verlauf ebenfalls via HTTP vom Server an. Dies führte bei HTTP 1.0 dazu, dass unter Umständen für die Darstellung einer mit vielen Grafiken versehenen Seite viele Verbindungen aufgebaut und auch wieder abgebaut werden müssen. Ab der Version 1.1 kann schon der HTTP-Server erkennen, welche Grafikdateien mit einem angeforderten Dokument mitgeliefert werden müssen. Der Server wird dies dann selbständig tun. HTTP 1.1-Server erzielen damit einen erheblichen Geschwindigkeitsvorteil.

Aufbau und Darstellung der via HTTP transportierten Dateien werden durch die Seitenbeschreibungssprache HTML, Hypertext Markup Language, definiert. Abbildung 4.88 zeigt ein Beispiel. Hier sind die Zeilen markiert, die den Bereichen Header und Body unter HTTP entsprechen.

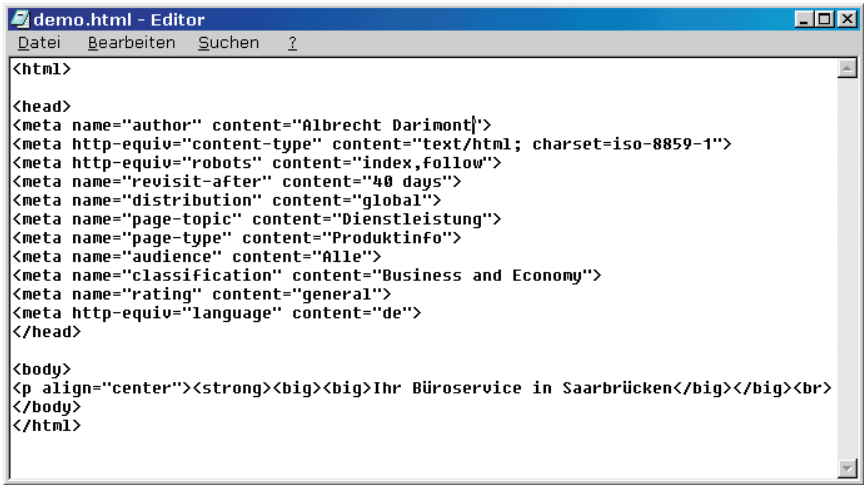


Abbildung 4.88: Header und Body einer HTML-Seite

Die folgende Tabelle gibt einen Überblick über den HTTP-Befehlssatz.

Befehl	Funktion/Bedeutung
GET	Der Befehl GET fordert vom adressierten Server ein in der URL angegebenes Dokument an. Dieser Befehl wird für den Anwender transparent gesendet, wenn dieser in der Adresszeile seines Browsers eine Internetadresse, die o.g. URL eingibt. Die Dokumentation zur URL finden Sie im RFC 1738.
HEAD	Analog zum GET-Befehl ist HEAD ebenfalls ein Kommando, das von einem Client abgesetzt wird. HEAD fordert allerdings nicht ein Dokument an, sondern die Informationen zum referierenden Dokument. Diese Informationen werden Meta-Informationen genannt und enthalten unter anderem Daten wie das Dateiformat, die Länge des Dokuments und das letzte Änderungsdatum.
PUT	Mit Hilfe des PUT-Befehls kann der Client Informationen an den Server senden. Mit PUT können auch vollständige Dokumente auf den HTTP-Server kopiert werden.
POST	POST dient zum Übertragen von kurzen Informationen, wie sie z.B. vom Anwender in ein Formular eingegeben werden. Die Eingabedaten werden an die Internetadresse des Servers angehängt.
DELETE	Mit DELETE können Dateien auf dem Server gelöscht werden. Dies setzt allerdings entsprechende Zugriffsrechte des Clients bzw. des Users voraus, der die Verbindung zum Server aufgebaut hat.
LINK	Der Link-Befehl erzeugt eine oder mehrere Verbindungen.
UNLINK	UNLINK hebt die mit Link angeforderten Verbindungen wieder auf.

Tabelle 4.31: HTTP-Befehle

HTTP-Befehle werden auch Methoden genannt. Die folgende HTML-Seite demonstriert, wie HTTP-Befehle in eine HTML-Seite integriert werden. Es handelt sich in diesem Beispiel um ein Web-Formular, dessen Inhalt über die Methode POST an den in **action** angegebenen Server gesendet wird.

<form action="http://www.darimont.de/mailsl/« method="POST« name="form1">

Client und Server tauschen mit dem HTTP-Protokoll Fehlermeldungen aus. Diese Error Codes liegen im Wertebereich zwischen 100 und 599. Je höher der Wert ist, desto schwerwiegender ist der aufgetretene Fehler. Tabelle 4.32 gibt einen Überblick. Eine detaillierte Auflistung aller Fehler sowie umfassende Informationen zu HTTP und HTML finden Sie in Heindl, Der Webmaster.

Error Code	Bedeutung
100-199	Statusmeldungen
200-299	Client-Anfrage erfolgreich
300-399	Client-Anfrage umgeleitet, ohne dass der Benutzer eingreifen muss
400-499	Fehler im Dokument oder ungenügende Rechte zum Lesen eines Dokuments. Am häufigsten wird hier der Anwender mit 404 konfrontiert. Dieser Fehler wird im Browser angezeigt und bedeutet, dass das angeforderte Dokument nicht gefunden werden konnte.
500-599	Serverfehler deuten auf Probleme im Webserver hin.

Tabelle 4.32: HTTP-Fehlermeldungen

HTTP-Proxy

Über HTTP können Zwischenspeicher, Cache-Speicher, implementiert werden. Aufgabe des Cache-Speichers ist in diesem Fall das Zwischenspeichern angeforderter Dokumente, die dann nicht mehr über das Internet übertragen werden müssen. Dadurch können Zugriffszeiten reduziert werden.

HTTP verwendet für die Konfigurationen eines HTTP-Proxy spezielle Befehle. So kann über den HEADER-Befehl der Status eines Quelldokuments abgefragt werden. Meldet der Server auf eine HEADER-Anfrage zum Beispiel Error Code 304, dann wurde das Dokument auf dem Ursprungsserver nicht verändert. Der Error Code gibt also Aufschluss darüber, ob das Dokument im Cache-Speicher veraltet ist oder nicht.

Die Funktionalität von HTTP-Proxy-Servern kann durch eine hierarchische Struktur optimiert werden. In der Praxis werden dazu mehrere Proxys hintereinander »geschaltet«. Dabei fragt der lokale Proxy bei einem nicht vorhandenen Dokument zuerst seinen übergeordneten Server. Die folgende Abbildung, die dem oben genannten Buch, Der Webmaster, Seite 31, entlehnt ist, demonstriert das hier beschriebene Prinzip.

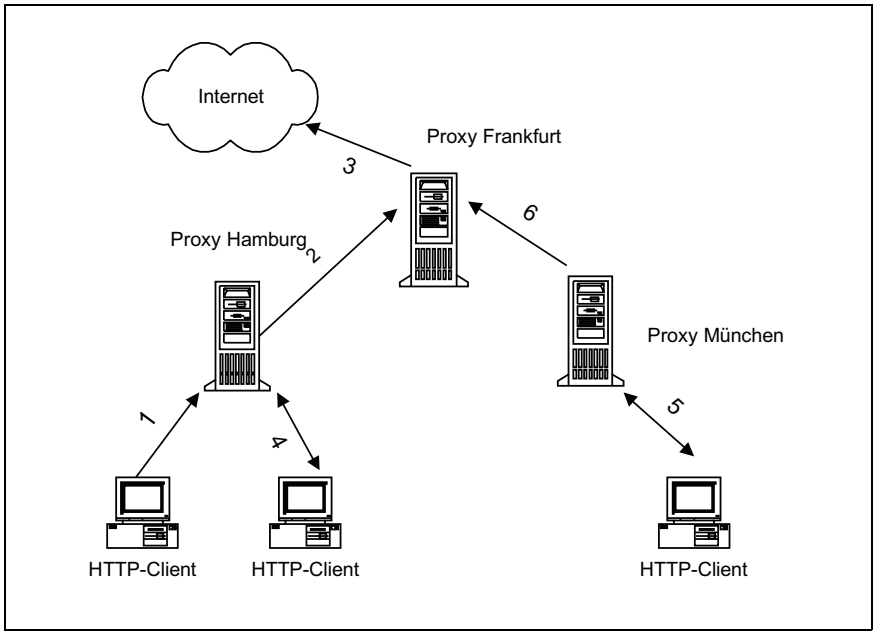


Abbildung 4.89: Hierarchisches Caching durch Proxy-Server

In der Phase eins fordert ein Client eine Webseite an. Die Anfrage wird in Phase zwei an den übergeordneten Proxy in Frankfurt weitergeleitet, der die Seite in Phase drei aus dem Internet lädt. Auf dem Rückweg wird das Dokument in Frankfurt und in Hamburg gespeichert. In Phase vier wird eine Anforderung direkt vom lokalen Server beantwortet. In Phase fünf fragt ein Client in München nach der gleichen Seite. Der lokale Server leitet die Anfrage weiter, erhält aus dem Cache in Frankfurt die entsprechende Seite, speichert diese und antwortet seinem Client. Die nächste Anfrage wird dann direkt aus dem Cache beantwortet.

Proxy-Befehle finden Sie im Header eines HTML-Dokuments. Dazu werden die Befehle in das Meta-Tag HTTP-EQUIV eingefügt. Der Webentwickler kann also das Verhalten der installierten Proxy-Server steuern. Auch hier möchten wir auf Details aus Heindl, Der Webmaster, verweisen.

Proxy-Befehl	Bedeutung
Public	Das so gekennzeichnete Dokument kann gecachet und von anderen benutzt werden. Ein Proxy-Server wird dieses Dokument zwischenspeichern.
Private	Der Inhalt darf nur einem bestimmten Benutzer aus dem Cache zur Verfügung gestellt werden.
No-cache	Die Seite wird nicht gecachet.
No-store	Diese Seite darf nicht auf externe Daten, z. B. Backup-Bänder gespeichert werden.

Tabelle 4.33: Proxy-Befehle

Werden Dateien auf dem Proxy gespeichert, dann stellt sich die Frage, für wie lange dies geschehen soll. Hierzu dient der Befehl EXSPIRES, der angibt, zu welchem Datum und zu welcher Uhrzeit die gecachete Seite »veraltet« ist und deshalb vom Ursprungsserver neu angefordert werden muss. Liegen keine Angaben vor, dann entscheidet der Proxy selbst über die Ablaufzeit. Dazu kann der Administrator einen TTL-Wert setzen, Time to Live.

SSL Socket Secure Layer

Socket Secure Layer ist eine Spezifikation für die sichere, d. h. verschlüsselte Übertragung von Daten im Internet. SSL setzt auf TCP/IP auf und ist in der Lage, alle TCP/IP-Anwendungsprotokolle sicher zu übertragen. Das Haupteinsatzgebiet liegt im World Wide Web. Mit SSL werden sensible Daten wie Adresse oder Kreditkartennummern über HTML-Formulare verschlüsselt gesendet.

Sie können eine mittels SSL abgesicherte Seite an der Adresse HTTPS://... erkennen. Anbieter von SSL-gesicherten Webservern benötigen einen SSL-fähigen Server und eine Zertifizierung des eigenen Servers durch eine hierzu berechtigte Zertifizierungsstelle. Während der Zertifizierung erzeugt der Server einen öffentlichen und einen geheimen Schlüssel. Die Zertifizierungsstelle generiert anschließend ein Zertifikat mit einer einmaligen Kennung, die als digitale Unterschrift gilt. Mit Hilfe der gültigen Sicherheitszertifikate können abschließend die SSL-Funktionen des Servers aktiviert werden. Jetzt ist die Identität des Betreibers des SSL-Servers für jeden Client überprüfbar.

Öffentlicher und geheimer Schlüssel dienen dazu, vor dem Austausch der HTML-Seiten mit Hilfe der beiden Schlüssel die Daten in beide Richtungen zu verschlüsseln und nur für den Client bzw. den Server lesbar zu machen.

Die folgende Abbildung zeigt ein Beispiel für den Einsatz von SSL. Sie sehen hier eine mit SSL gesicherte Seite. Die Adresse ist:

https://www.amazon.de/exec/obidos/account-access-login2/028-6455000-9563457

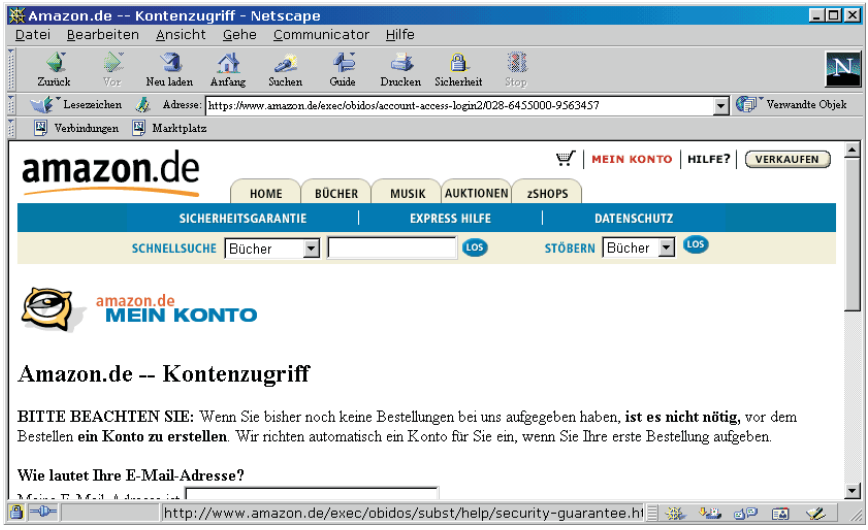


Abbildung 4.90: Eine mit SSL gesicherte HTML-Seite

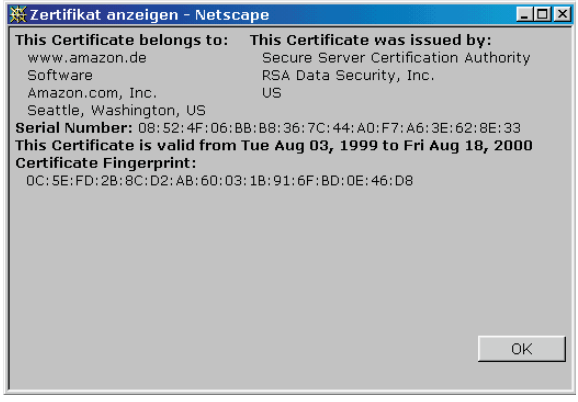


Abbildung 4.91: SSL-Zertifizierungsinformationen

4.7.7 SNMP (Simple Network Management Protocol)

Bedingt durch immer breitbandigere Anwendungen, Umzüge von Anwendern, vermaschte Netze und andere Faktoren, treten immer wieder schwer zu lokalisierende Fehler in einem Netzwerk auf. Um diese Fehler zu lokalisieren und zu beheben, sind leistungsfähige Netzwerk-Management-Programme notwendig. Die für diese Zwecke im TCP/IP-Netzwerk verwendete Software basiert auf dem Simple Network Management Protocol. Denn im Gegensatz zu den anderen Diensten und Protokollen ist das Simple Network Management Protocol ausschließlich für den Transport von Kontrolldaten zuständig. Diese Kontrolldaten beinhalten Daten über Managementinformationen, Status- und Statistikinformationen, die ein effizientes Netzwerkmanagement ermöglichen.

Die Spezifikationen des Simple Network Management Protocols sind in den RFCs 1052, 1065, 1066 und 1157 veröffentlicht.

SNMP-Architektur

SNMP kann keiner Schicht des OSI-Referenzmodells zugeordnet werden. Vielmehr zieht es sich durch alle sieben Schichten, wobei in jeder Schicht dem Netzwerk Management Informationen durch die Management Information Base, MIB, zur Verfügung gestellt werden.

SNMP arbeitet verbindungslos über den UDP Port 161 und erlaubt eine einfache Implementierung mit einem relativ geringen Einsatz von Ressourcen, »trap directed polling«.

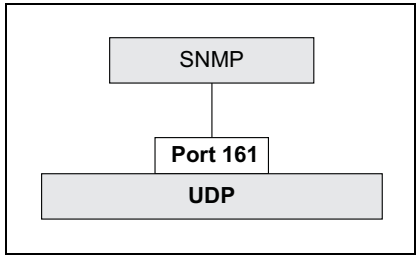


Abbildung 4.92: HTTP-Socket

SNMP ist prinzipiell für Einsatz in lokalen Netzwerken konzipiert. Die Kontrolldaten werden entsprechend der SMI, Structure of Management Information for TCP/IP-based Internets, dargestellt. Informationen, die von der MIB für jede Schicht generiert werden, übernimmt SNMP, um diese anschließend weiterzuleiten.

Funktion von SNMP

In der SNMP Terminologie wird das zu verwaltende Gerät als MNE, Managed Network Entity, bezeichnet. Auf dem MNE läuft die Agent-Software als Server und überwacht den Status des Gerätes. Auf der zentralen NMS, Network-Management-Station, läuft die Manager-Software als Client, der die Statusinformationen aller zu verwaltenden MNEs sammelt und bearbeitet.

Server und Agents müssen einer gemeinsamen Community angehören. Diese Community bezeichnet eine Gruppe von Hosts, die zu einer Management Station gehören. Der Standardname für Community heißt public. Selbstverständlich können für die Community auch andere Namen vergeben werden. Eine Community kann sehr heterogen zusammengesetzt sein, d.h. die Agents laufen unter unterschiedlichen Betriebssystemen bzw. auf spezifischen Hardwareplattformen.

Wie bereits oben erwähnt, benutzt SNMP das UDP mit dem Port 161. UDP als unzuverlässiges Protokoll kann deshalb verwendet werden, weil der Manager einen Request an den Agenten schickt, der wiederum mit einem Replay antwortet. Sollte ein Request nicht beantwortet werden, wird einfach eine neue Anfrage gesendet.

Die Anfrage- und Antwortnachrichten, die SNMP als Datagramme verschickt, werden als PDUs, Protocol Data Units, bezeichnet.

PDU	Anwendungen
GetRequest	Manager fordert Aktualisierung eines Tabelleneintrags an
GetNextRequest	Manager fordert den nächsten Tabelleneintrag an
GetResponse	Agent antwortet auf Anfrage des Managers
SetRequest	Manager verändert Daten auf dem zu verwaltenden Gerät
Trap	Agent informiert Manager über ungewöhnliche Ereignisse

Tabelle 4.34: SNMP-Protokollpakete

Die NMS fragt mit GetRequest in regelmäßigen Abständen, so genanntes Polling, den Status der verwalteten MNEs ab. Diese antworten mit einem GetResponse auf die Anfrage.

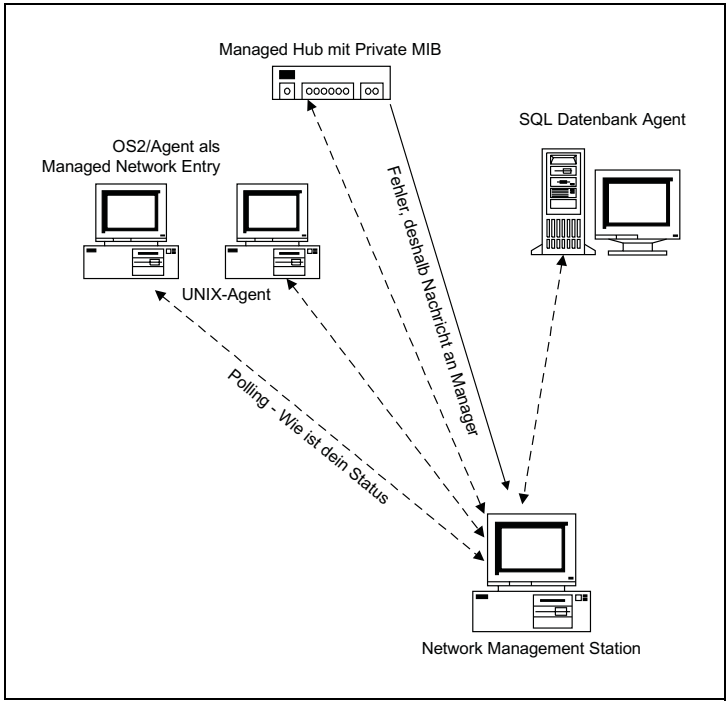


Abbildung 4.93: SNMP-Architektur

Da ein auftretender Fehler erst bei der nächsten Abfrage bekannt wird, muss zusätzlich ein modifiziertes Polling von SNMP eingesetzt werden. Dies bezeichnet man als trap-directed-polling, und es wird durch Interrupts gesteuert.

Ein Trap ist eine Unterbrechung, welche durch ein vorher festgelegtes Ereignis ausgelöst wird. Tritt ein solches Ereignis auf, wird vom Agenten sofort eine Nachricht zum Manager gesendet, ohne die nächste Abfrage abzuwarten. Diese Traps werden dann über den UDP-Port 162 gesendet.

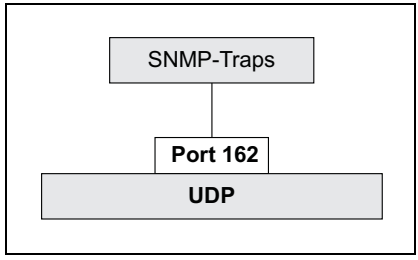


Abbildung 4.94: SNMP-Traps über Port 162

Die folgende Tabelle listet die im RFC definierten Trap-Ereignisse auf.

Trap	Bedeutung
ColdStart	Ein Agent wurde neu gestartet, möglicherweise mit geänderter Konfiguration
WarmStart	Ein Agent wurde neu initialisiert ohne Änderung der Konfiguration
EnterpriceSpecific	Ein für dieses Gerät oder diese Software spezifisches Ereignis
AuthenticationFailure	Ein Agent empfängt eine nicht-bestätigte Nachricht
LinkDown	Ein Agent hat eine Netzwerk-Unterbrechung festgestellt
LinkUp	Ein Agent stellt behobene Netzwerk-Unterbrechung fest
EgpNeighborLoss	Der EGP-Nachbar des Geräts ist außer Betrieb

Tabelle 4.35: Trap-Ereignisse

MIB (Management Information Base)

Die Management Information Base, MIB, stellt die konkrete Beschreibung der Objekte, auf die der SNMP-Agent zugreifen kann, zur Verfügung. Des Weiteren stellt sie Strukturen, Pointer, zur Verfügung, die einen direkten Zugriff auf die spezifischen Informationen der Objekte erlauben.

Man unterscheidet dabei konzeptionelle Informationen aus der Standard-MIB und den nicht standardisierten Objekten. Beide müssen jedoch mit SMI kommunizieren. Die Standard-MIB entwickelte sich aus der MIB-I, definiert im RFC 1156, die aber mittlerweile von der MIB-II, definiert im RFC 1213, abgelöst wurde.

Darüber hinaus gibt es herstellerspezifische MIBs, Private MIBs, die immer mit dem Objekt Idenitifer 1.3.6.1.4 beginnen. Viele Unternehmen haben unter diesen Private MIBs eigene Objekte definiert. Die einzelnen Objekte einer jeden MIB sind wiederum in Gruppen angeordnet. Diese Gruppen beziehen sich zum einen auf das Gesamtsystem und zum anderen auf die einzelnen Protokolle in den verschiedenen Netzwerkschichten. Dabei sind nur die für das jeweilige System relevanten Gruppen wichtig. In der Praxis bedeutet dies, dass nicht alle Gruppen implementiert werden müssen. Die Anzahl der Objekte innerhalb einer Gruppe ist nicht teilbar.

Die folgende Tabelle gibt einen Überblick über die Gruppen der MIB I nach RFC 1156.

Gruppe	Beschreibung	Anzahl der Objekte
system	Informationen über das eigene System	03
interface	Informationen über das (die) Interface(s)	22
at	Informationen über das Adress-Mapping	03
ip	Internet-Protocol	33 (Zähler, Adressen, Routing usw.)
icmp	ICMP Informationen	26
tcp	TCP Informationen	17
udp	UDP Informationen	4
egp	EGP Informationen	6

Tabelle 4.36: Objektgruppen der MIB I

Die folgende Tabelle gibt einen Überblick über die Gruppen der MIB II nach RFC 1213.

Gruppe	Beschreibung	Anzahl der Objekte
system	Informationen über das eigene System	07
interfaces	Informationen über das (die) Interface(s)	23
at	Informationen über das Adress-Mapping	03
ip	Internet-Protocol	38 (Zähler, Adressen, Routing usw.)
icmp	ICMP Informationen	26
tcp	TCP Informationen	19
udp	UDP Informationen	07
egp	EGP Informationen	18
snmp	Informationen über SNMP-Netzwerkdaten	30

Tabelle 4.37: Objektgruppen der MIB II

Objektbeispiele für die in der MIB-II aufgeführten Gruppen:

(1) sys	
sysDescr	Vollständige Systembeschreibung
sysObjectID	Herstellerspezifische Objektidentifikation
sysUpTime	Zeit, die seit dem letzten Systemstart vergangen ist
sysContact	Name der Kontaktperson dieses Systems
sysServices	Dienste, die von diesem System angeboten werden
interfaces ifIndex	Interface-Nummer
(2) if	
ifDescr	Beschreibung des Interfaces
ifType	Beschreibung des Interface-Typs
ifMTU	Größe der MTU (Maximum Transfer Unit)
ifAdminStatus	Statusinformation des Interfaces
ifLastChange	Zeitpunkt der letzten Statusänderung
ifINErrors	Anzahl der Inbound-Packets mit Fehlern
ifOutDiscards	Anzahl der fehlerhaften und verworfenen Outbound-Packete
(3) at	
atTable	Adress-Tabelle
atEntry	Jede vorhandene Zuordnung
atPhysAdress	Physikalische Netzwerk-Adresse
(4) ip	
ipForwarding	Gibt an, ob dieses Gerät ein IP-Gateway ist
ipInHdrErrors	Anzahl verworfener Input-Datagramme mit fehlerhaften IP-Headern
ipInAddrErrors	Anzahl verworfener Input-Datagramme mit fehlerhaften IP-Adressen
ipInUnknownProtos	Anzahl verworfener Input-Datagramme mit fehlerhaften oder nichtunterstützten Protokollen
ipReasmOKs	Anzahl erfolgreich reassemblierter IP-Datagramme

Objektbeispiele für die in der MIB-II aufgeführten Gruppen:

(5) icmp	
icmpInMsgs	Anzahl der empfangenen ICMP-Messages
icmpInDestUnreachs	Anzahl der empfangenen »destination-unreachable«-Messages
icmpInTimeExcds	Anzahl der empfangenen »time-exceeded«-Messages
icmpInSrcQuenches	Anzahl der empfangenen »source-quench«-Messages
icmpOutErrors	Anzahl der aufgrund protokollinterner Fehler nicht versendeten ICMP-Messages
(6) tcp	
tcpRtoAlgorithm	Angabe des Algorithmus zur Ermittlung der Timeouts für die Re-Transmission unbeständiger Oktette
tcpMaxConn	Grenzwert für maximalrealisierbare TCP-Verbindungen für dieses System
tcpActiveOpens	Anzahl direkter Status-Übergänge von CLOSED nach SYN-SENT
tcpInSegs	Anzahl aller empfangenen Segmente
tcpConnRemAddress	Partner-IP-Adresse der aktuellen Verbindung
tcpInErrs	Anzahl verworfener Segmente aufgrund von Format-Fehlern
tcpOutRsts	Anzahl generierter RESETS
(7) udp	
udpInDatagrams	Anzahl an UDP-User gelieferter UDP-Datagramme
udpNoPorts	Anzahl empfangener UDP-Datagramme, für die es keine Anwendungen am gewünschten Port gibt
udpInErrors	Anzahl der UDP-Datagramme, die aus anderen Gründen nicht zugestellt werden können
udpOutDatagrams	Anzahl versendeter UDP-Datagramme

Objektbeispiele für die in der MIB-II aufgeführten Gruppen:

(8) egp	
egpInMesgs	Anzahl fehlerfreier empfangener EGP-Messages
egpInErros	Anzahl fehlerhafter empfangener EGP-Messages
egpNeighAddr	IP-Adresse des unmittelbaren EGP-Nachbarn
egpNeighState	EGP-Status dieses Systems zu seinem EGP-Nachbarn
(11) snmp	
snmpInPkts	Anzahl empfangener SNMP-Messages
snmpInBadCommunity Names	Anzahl empfangener Requests mit fehlerhafter »community«
snmpInGetRequests	Anzahl empfangener »get-requests«
snmpOutTraps	Anzahl versendeter Traps

SNMP arbeitet mit einem sehr einfachen Sicherheitsmodell ohne Verschlüsselung. Deshalb haben erfahrene Hacker kein Problem, Netzwerke mit Hilfe gefälschter SNMP-Pakete durcheinander zu bringen. Schutz bietet also nur eine gute Abschirmung nach außen mit Hilfe entsprechender Firewalls.

KAPITEL 5

5 Proprietäre LAN-Protokolle und Standards für Netzadapter

Kapitel 4 hat gezeigt, dass die TCP/IP-Protokollgruppe nicht von einem bestimmten Hersteller definiert wird. In der Praxis finden Sie natürlich auch Protokolle, die von einem Hersteller stammen und konsequenterweise auch dort zum Einsatz kommen, wo Produkte des entsprechenden Herstellers eingesetzt werden. Es ist absehbar, dass die in den nun folgenden Kapiteln beschriebenen Protokolle an Bedeutung verlieren werden. Aus diesem Grunde wird auch auf die Beschreibung von DLC, AppleTalk oder DECnet verzichtet.

Tabelle 5.1 gibt einen ersten Überblick.

Protokoll	Anbieter/Hersteller	Kurzbeschreibung
SPX/IPX	Novell	Protokolle Layer 3 und Layer 4, routingfähig und lange Zeit de-facto-Standard, wird von TCP/IP abgelöst
NetBIOS	IBM	API und LAN-Protokoll zugleich, nicht routingfähig, dafür klein und schnell
NetBEUI	Microsoft	Im Kern NetBIOS, aber für größere Netze mit mehr als 200 Rechnern konzipiert, wie NetBIOS nicht routingfähig
AppleTalk	Apple	AppleTalk definiert LAN-Hardware und LAN-Protokolle. Mit Appletalk werden die Layer 3 bis 7 des OSI-Modells abgedeckt
DLC	Microsoft	DLC wird unter Windows NT für den Zugriff auf IBM-Mainframes sowie HP-Drucker eingesetzt
APPC	IBM	APPC ermöglicht die Peer-to-Peer-Kommunikation in Netzwerken, die nach dem SNA-Standard aufgebaut sind
DECnet	DEC	DECnet-Protokolle unterstützen OSI- und proprietäre Komponenten von DEC

Tabelle 5.1: Proprietäre Protokolle im Überblick

5.1 IPX/SPX (Internetwork Packet Exchange/ Sequenced Packet Exchange)

In den vergangenen Jahren war die Firma Novell NetWare der führende Software-Hersteller im Bereich der Netzwerksoftware. Als strategisches Netzwerkprotokoll kommt in Novell-Netzwerken (noch) primär die Protokollgruppe SPX/IPX zum Einsatz.

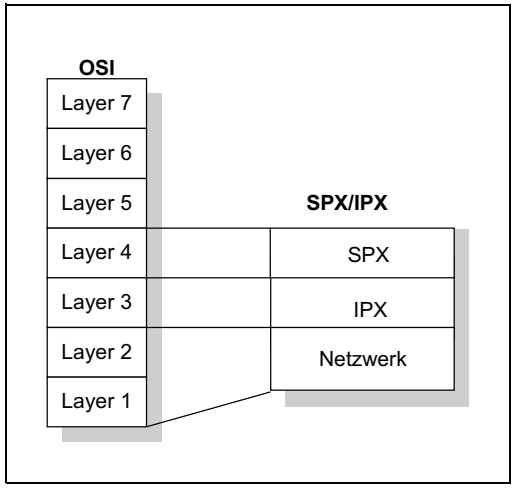


Abbildung 5.1: SPX/IPX-Architektur

IPX erlaubt als Implementierung des Internetwork Datagram Packet Protocols von Xerox den auf den einzelnen Knoten ausgeführten Anwendungen einen direkten Zugriff auf den Treiber der Netzwerkkarte. Somit ermöglicht IPX das direkte Versenden und Empfangen von Datagrammen, deren Strukturen den im XNS, Xerox Network System, festgelegten Konventionen folgt, in das bzw. aus dem Netzwerk.

Die aktuell zur Verfügung stehenden Versionen Novell 4.x und 5.x unterstützen jedoch neben ihrem eigenen Protokoll IPX/SPX auch TCP/IP und andere. Um die Dienste der Protokollfamilie TCP/IP in einem Novell-Netz zu nutzen, gibt es verschiedene Möglichkeiten, die im unteren Abschnitt näher erläutert werden.

5.1.1 IPX (Internetwork Packet Exchange)

IPX ist wie auch IP ein verbindungsloses und unzuverlässiges Datagramm-Protokoll. Damit jeder Knoten im Netzwerk den Weg für ein Datagramm kennt, beinhalten die Datagramme neben anderen Steuerinformationen die Quell- und Zieladresse. Um nun eine gesicherte Datenübertragung zu gewährleisten, kommen Protokolle der höheren Protokollschichten zum Tragen. IPX verwendet dazu für die Adressierung eine hierarchische Struktur, die es ermöglicht Daten über verschiedene physikalische Netzwerke hinweg zu routen. Dazu müssen die eingesetzten Router allerdings IPX-fähig sein.

Eine hierarchische Adresse in einem Novell-Netz ist zehn Byte breit, wobei die ersten vier Byte das Netzwerk bestimmen. Diese Netzwerk-Adresse wird auch Network Number genannt, und wird als achtstellige Hexadezimalzahl dargestellt. Sie wird auf dem Client automatisch generiert und muss auf dem Server konfiguriert werden. Die restlichen sechs Byte definieren den Host als eindeutig innerhalb des Netzes. Diese sechs Byte lange Hostadresse ist die durch die Hardware der Ethernetkarte vorgegebene MAC-Adresse, drei Byte bezeichnen

dabei den Hersteller, drei Byte werden fortlaufend vergeben und repräsentieren weltweit eindeutige MAC-Adressen. Da diese Hostadresse fest vorgegeben ist, muss sie im Umkehrschluss auch nicht vom Administrator vergeben werden.

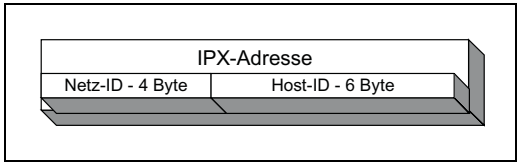


Abbildung 5.2: IPX-Adressformat

Handelt es sich um ein GAN, Global Area Network, wird dem Netzwerk eine feste Novell-Netzwerkadresse über die erhaltene IP-Adresse zugewiesen. Jedes Unternehmen, das vom InterNIC eine registrierte IP-Adresse erhält, bekommt darüber hinaus auch eine eindeutige Novell-Netzwerkadresse.

Beispiel:

Ist die IP-Netzwerkadresse z.B. 196.114, dann heißt die Novell-Netzwerkadresse 00C47200. Um diese Umrechnung durchführen zu können, muss die IP-Adresse um ein Byte nach rechts verschoben werden. Im Anschluss daran wird die IP-Adresse in hexadezimale Zahlen umgerechnet. Sofern es sich um ein A-Klasse- oder B-Klasse-Netz handelt, wird der Hostteil selbst unterdrückt. Dargestellt wird der Hostteil durch die MAC-Adresse. Das erste Byte einer durch diese Methode erzeugten IPX-Adresse, wird immer auf Null gesetzt.

Beispielhafte Einstellungen der Konfigurationsdatei AUTOEXEC.NCF

BEISPIEL
```
LOAD NE2000 FRAME=ETHERNET_II PORT=300 INT=3
NAME=NOVELL
BIND IPX TO NOVELL NET=76B3BC07
```

Interne Netzwerknummer des Servers

BEISPIEL
```
FILE SERVER NAME SERVER01
IPX INTERNAL NET 76B3BC07
```

5.1.2 SPX (Sequenced Packet Exchange)

Eine Ebene über dem IPX-Protokoll ist das SPX-Protokoll implementiert. Analog zu TCP ist auch SPX für den Transport der Datenpakete zuständig. Neben dieser Aufgabe achtet SPX auch auf die richtige Reihenfolge der Datenpakete. Zu diesem Zweck werden mit Hilfe des SPX-Protokolls logische Verbindungen zwischen den kommunizierenden Knoten aufgebaut. Da es sich in diesem Fall um eine formelle Datenübertragung handelt, werden durch SPX die zur Verfü-

gung stehenden Funktionen wie z.B. Verbindungsauf- und -abbau, Abfrage des Verbindungsstatus oder auch Abbruch im Fehlerfall, realisiert. Für jedes übertragene Paket wird eine Bestätigung erwartet. Um diese Aufgaben zu gewährleisten, werden weitere zwölf Byte an den 30 Byte langen Header angehängt.

Von diesen zwölf Byte beinhalten acht Byte die folgenden Informationen:

Feld	Bedeutung
Feld 1-2, Source Connection ID	In diesem Feld wird vom Quell-Host für die Dauer der Verbindung ein eindeutiger Wert zugeordnet. Dieser Wert wird für die Identifikation der virtuellen Verbindung benötigt.
Feld 3-4, Destination Connection ID	Dieses Feld beinhaltet die Identifikation, die vom Ziel-Host der Verbindung zugeordnet wird. Sofern ein Rechner auf ein Paket antwortet, übernimmt er die Source Connection ID und überträgt sie als Destination Connection ID. Dieser Wert wird im ersten Datenpaket mit FFFF angegeben.
Feld 5-6, Sequence Number ID	In diesem Feld wird die Sequenznummer der einzelnen SPX-Pakete eingetragen. Die Sequenznummer repräsentiert eine fortlaufende Nummerierung der übertragenen SPX-Pakete. Bei jeder gelungenen Übertragung wird dieser Wert um eins erhöht.
Feld 7-8, Acknowledgement Number ID	Dieses Feld beinhaltet die Sequenznummer des nächsten Paketes, das der Ziel-Host erwartet. Der Quell-Host überprüft diese Sequenznummer, um zu gewährleisten, dass der Ziel-Host alle bisher gesendeten Pakete empfangen hat.

Da SPX für eine einmal aufgebaute logische Verbindung verantwortlich ist, legt es auch die Anzahl der Wiederholungsversuche bzw. ein Zeitlimit fest, nachdem für ein übertragenes Datagramm eine Quittung erfolgen muss. Sofern diese Zeitvorgaben überschritten werden, erklärt SPX die Verbindung als abgebrochen. Diese Limits werden dabei dynamisch an die jeweilige Netzlast angepasst. So werden die Zeitintervalle zwischen zwei Übertragungsversuchen um jeweils 150 Prozent erhöht, wenn ein einzelnes Datagramm verlorengegangen ist oder wenn keine Positivquittung innerhalb des TimeOut erfolgt. Sobald die Verbindung wieder fehlerfrei arbeitet, werden die Limits auf den ursprünglichen optimalen Wert zurückgesetzt.

5.1.3 SAP (Service Advertising Protocol)

Da es sich bei einem Novell-Netzwerk um ein rein serverorientiertes System handelt, müssen alle Knoten im Netz darüber informiert werden, welche Server zur Verfügung stehen. Darüber hinaus muss mitgeteilt werden, welche Dienste die Server zur Verfügung stellen. Diese Informationen werden in einer Bindery Datenbank auf allen Servern und allen Routern verwaltet und durch das SAP, Service Advertising Protocol, den einzelnen Clients zur Verfügung gestellt.

Die Bindery eines jeden Servers ist eine Datenbank, die alle namentlich definierten Objekte beinhaltet. Mit Hilfe von Bindery-Requests erlangt jeder Client Kenntnis über die zur Verfügung gestellten Dienste. Um nicht jedem Zugang

zu allen Informationen zu erlauben, wird der Zugriff auf die Bindery über verschiedene Berechtigungsstufen gesteuert. Router haben die Aufgabe, diese Informationen an andere angeschlossene Netzwerke weiterzuleiten, so dass diese Informationen sukzessive in jedem Netzwerk zur Verfügung stehen.

5.1.4 NCP (Netware Core Protocol)

Der eigentliche Kern von Novell NetWare ist das NCP, Netware Core Protocol. Dieses Protokoll wird sowohl von den Clients als auch von den Servern verwendet. Die Clients verwenden es zur Anforderung von Diensten, die Server hingegen für die Beantwortung der Anfragen. NCP stellt unter anderem folgende Funktionen zur Verfügung:

- ✔ Dateidienste
  - – Prozessverwaltung, job queue service
- ✔ Druckerdienste
  - – Lokalisieren von Diensten, bindery service
  - – Verzeichnisverwaltung, directory service
  - – Verbindungsaufbau, connection service
  - – Benutzerverwaltung, accounting service

Wie SMTP ist auch NCP ein Request/Response-Protokoll. Durch dieses Merkmal ist die Fehlererkennung und -behandlung besonders einfach. Erfolgt auf die Anfrage eines Client keine Antwort, schickt dieser einen neuen Request. Dadurch wird es möglich, NCP über IPX zu betreiben, ohne jedoch die Zuverlässigkeit von SPX beanspruchen zu müssen.

Von Nachteil ist, dass bei großen Datenmengen diese Art der Datenübertragung nicht effizient ist. Um diesen Nachteil zu kompensieren, bietet NetWare den Burst Mode Transfer an. In diesem Burst Mode werden mehrere Pakete bei nur einer Anfrage übertragen. Theoretisch können bei einer Burst Mode Anfrage bis zu 64 KB Daten übertragen werden. In Ethernet Netzwerken sind mit dieser Technik acht KB problemlos möglich. Integriert ist das NCP in der Workstation-Shell mit der Bezeichnung NETX.COM.

NETX.COM selbst ist ein TSR, Terminate and Stay Resident, ein Programm, dass multifunktional selbstständig die installierte DOS-Variante erkennt. Dieses Programm wertet nun die Requests der Anwendungsprogramme aus und entscheidet darüber, ob sie über das Netzwerk vom Server bearbeitet werden sollen. Diese Nachfrage wird in eine NCP-Nachricht konvertiert und anschließend über das IPX zum Server geschickt.

5.2 NetBIOS (Network Basic Input/Output System)

1983 von Sytek Corporation für IBM entwickelt und von IBM 1984 eingeführt, ist NetBIOS zunächst ein API, Application Programmable Interface, das für eine LAN-Programmierung durch fest definierte Funktionsaufrufe den Programmieraufwand reduziert. Dazu beschreibt NetBIOS die Schnittstelle zwischen einem Betriebssystem und einem beliebigen Transportsystem. Dadurch werden die Funktionen der Schichten 3 bis 5 des OSI-7-Schichten-Referenzmodells abgedeckt, jedoch ohne die Protokolle der Schichten einzeln zu spezifizieren.

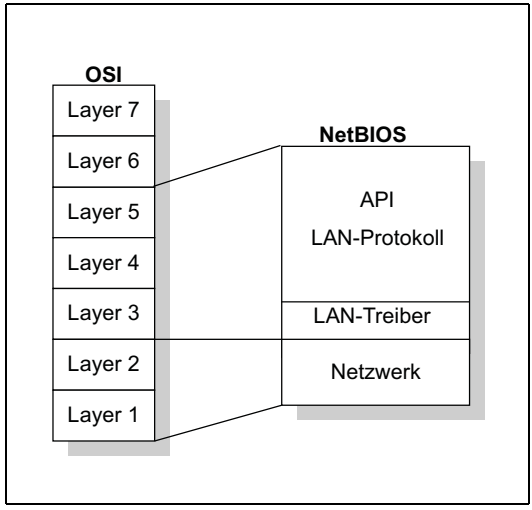


Abbildung 5.3: NetBIOS-Architektur

Darüber hinaus bietet NetBIOS Anwendungsprogrammen die Möglichkeit des Aufbaus virtueller Transportverbindungen und der Verwaltung symbolischer Namen für Endadressen. Ein Beispiel für einen Prozess, bei dem ein NetBlOS-Name verwendet wird, ist, wenn Sie versuchen über den Befehl net use eine Verbindung zu einem anderen Host in Ihrem Netz herzustellen.

z.B. net use lpt1 \\PCHUBELE\HPLJV

Zu diesem Zweck wird mit Hilfe einer NetBIOS-Namensabfrage nach dem NetBIOS-Namen gesucht. Somit erweitert NetBIOS die Möglichkeiten des herkömmlichen BIOS um die Fähigkeit, Informationen über eine Netzwerkkarte ein- und auszugeben. Voraussetzung ist natürlich mindestens eine Verbindung zu einer anderen Netzwerkkarte im LAN. Dieser Zugriff auf NetBIOS-Ressourcen ist jedoch auf 250 gleichzeitige Verbindungen beschränkt. Alle modernen Betriebssysteme verfügen neben ihren eigenen LAN-Treibern auch über Treiber für NetBIOS, da NetBIOS wahlweise als API auf der Anwendungsschicht oder als Transportprotokoll eingesetzt werden kann. Allerdings verfügt NetBIOS

nicht über die in modernen Netzwerken nötige Routingfähigkeit. Dieser eklatante Nachteil kann jedoch durch NetBIOS over TCP/IP kompensiert werden, so dass NetBIOS auch routingfähig wird.

5.2.1 NetBIOS-Name unter Windows NT

Beim Starten von Windows NT wird vom Server-Dienst, vorhanden auf NT Server und NT Workstation, ein eindeutiger, auf dem Computer-Namen basierender NetBIOS-Name registriert. Der NetBIOS-Name selbst setzt sich aus dem bis zu 15 Zeichen umfassenden Computer-Namen und einem 16. hexadezimalen Zeichen zusammen. In der Regel ist dies der Setup-Name, der bei der Installation angegeben wurde. Sie finden den NetBIOS-Namen unter Windows in der Netzwerkkonfiguration. Klicken Sie hier das Register Identifikation. Der hier zu findende Computername ist identisch mit dem Namen, den NetBIOS und alle auf NetBIOS basierenden Anwendungen benutzen.

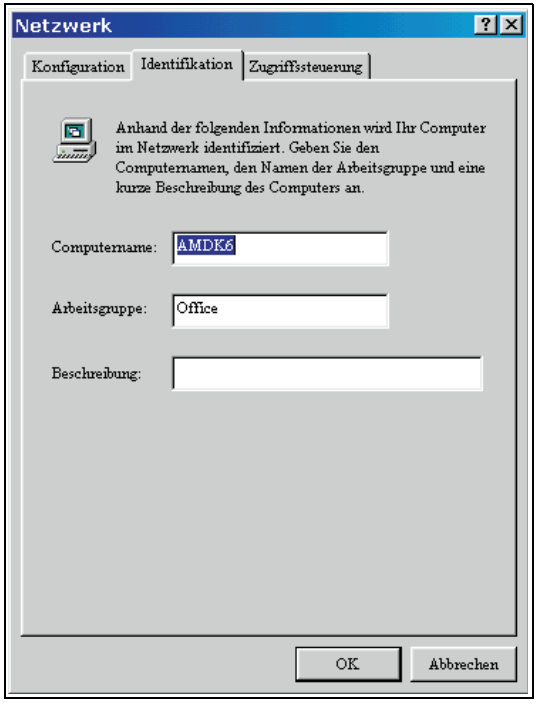


Abbildung 5.4: NetBIOS-Name unter Windows

Ein Computer-Namen wird aber auch von anderen Netzwerkdiensten zum Erstellen der jeweiligen NetBIOS-Namen verwendet. In der Praxis bedeutet dies, dass das 16. Zeichen dazu verwendet wird, um jeden spezifischen Dienst, z.B. den Server- oder den Redirector-Dienst, eindeutig zu identifizieren.

Die folgende Tabelle gibt einen Überblick zu den spezifischen Dienstekennungen.

Name	Suffix(h)	Typ	Art
<computername>	00	U	Workstation Service
<IS~computer_name>	00	U	Internet Information Server
<computername>	01	U	Messenger Service
<computername>	03	U	Messenger Service
<username>	03	U	Messenger Service
<computername>	06	U	RAS Server Service
<domain>	1B	U	Domain Master Browser
<domain>	1D	U	Master Browser
<computername>	1F	U	NetDDE Service
<computername>	20	U	File Server Service
<computername>	21	U	RAS Client Service
<computername>	22	U	Microsoft Exchange Interchange (MSMail Connector)
<computername>	23	U	Microsoft Exchange Store
<computername>	24	U	Microsoft Exchange Directory
<computername>	2B	U	Lotus Notes Server
<computername>	30	U	Modem Sharing Server Service
<computername>	31	U	Modem Sharing Client Service
<computername>	43	U	SMS Clients Remote Control
<computername>	44	U	SMS Administrators Remote Control Tool
<computername>	45	U	SMS Clients Remote Chat
<computername>	46	U	SMS Clients Remote Transfer
<computername>	4C	U	DEC Pathworks TCPIP service on Windows NT
<computername>	52	U	DEC Pathworks TCPIP service on Windows NT
<computername>	6A	U	Microsoft Exchange IMC
<computername>	87	U	Microsoft Exchange MTA
<computername>	BE	U	Network Monitor Agent
<computername>	BF	U	Network Monitor Application
<\\--__MSBROWSE__>	01	G	Master Browser
<domain>	00	G	Domain Name
<domain>	1C	G	Domain Controllers
<domain>	1D	G	Master Browser Name
<domain>	1E	G	Browser Service Elections
<INet~Services>	1C	G	IIS
IRISMULTICAST	2F	G	Lotus Notes
IRISNAMESERVER	33	G	Lotus Notes

Tabelle 5.2: NetBIOS-Dienstekennungen.

Die Benutzung von NetBIOS-Namen ist für ein einzelnes Subnetz, ein lokales Netzwerk oder ein Weitverkehrsnetz geeignet. NetBIOS-Namen müssen zu diesem Zweck in einem Netzwerk angefordert und verteidigt werden. Dazu können prinzipiell zwei Strategien verfolgt werden:

Broadcast NetBIOS

Client-Rechner können auf ihrem broadcast-begrenzten Subnetz per Rundsenden Namen anfordern und auf Basis erfolgreich angeforderter Namen ihre Dienste anbieten. Dazu können in einem LAN oder WAN die Broadcast-Pakete über die TCP/IP-Ports 137, 138 und 139 weitergleitet werden. Das ist aber nicht empfehlenswert. Wenn Sie ein größeres LAN oder WAN haben, werden Sie feststellen, dass einige Hosts bis zu 95 Prozent ihrer Zeit mit der Abarbeitung von Broadcasts verbringen. Ähnliches wird auch für IPX/SPX auf dem LAN berichtet. Ungefähr alle zwölf Minuten ist ein großer Broadcast-Verkehr feststellbar.

NBNS NetBIOS

Der RFC 1001 beschreibt u.a. die Implementierung und Benutzung eines »NetBIOS Name Service«. Unter NT heißt der Dienst »Windows Internet Name Service (WINS)«, der voll RFC 1001/1002 kompatibel ist, aber bei einigen NetBIOS-Namen spezielle Aktionen benutzt. Zum Beispiel wird die Registrierung von <1c> <1d> und <1e> Namen in unterschiedlicher Weise abgewickelt.

Die Benutzung eines WINS-Servers verringert also durch die Punkt-zu-Punkt-Verbindung den Broadcast-Verkehr der durch NetBIOS bei der Namensauflösung erzeugt wird. Alle broadcast-begrenzten Subnetze ihres LAN's oder WAN's werden durch WINS in eine einzige NetBIOS-Umgebung eingebunden, wobei dann auch die TCP/IP-Broadcasts wegfallen. Details zu WINS finden Sie im Kapitel 4.6.

WINS führt damit zu einer effizienteren Nutzung der Bandbreite, weil die Netzlast bei der Namensauflösung und der Suche nach Diensten minimiert werden kann. Welche Strategie hierbei vom Host verfolgt wird, das hängt unter Windows von seinem konfigurierten Typ ab. Microsoft definiert die unten aufgeführten Knotentypen, die durch einen Parameter in der Registry gekennzeichnet werden. Der Knotentyp legt also fest, welche Methode NetBIOS verwendet, um Namen zu registrieren und aufzulösen.

Die folgende Tabelle gibt einen Überblick und führt dabei auch die hexadezimale Kodierung der Knotentypen auf.

Knotentyp und Schlüsselwert	Beschreibung
b-node<0x1>	b-node (broadcast-node); das System löst NetBIOS Namen ausschließlich über Broadcasts im lokalen Segment auf.
p-node <0x2>	p-node (point-to-point-node); das System löst Namen über point-to-point Kommunikation mit einem WINS-Server auf. Broadcasts finden nicht statt, selbst wenn der Name vom WINS nicht aufgelöst wird.
m-node <0x4>	m-node (mixed-node); das System verwendet primär eine Multicast- (Broadcast-) Methode um lokale Systeme aufzulösen. Dabei geht man davon aus, dass die meisten gesuchten Systeme im lokalen Subnetz sind. Für den Fall, dass ein Multicast den NetBIOS-Namen nicht auflösen kann, wird beim WINS-Server nachgefragt.
h-node <0x8>	h-node (hybrid-node); dies ist der Standard-Typ in WINS-Umgebungen. Dabei wird zunächst point-to-point-Kommunikation mit dem konfigurierten WINS-Server verwendet. Sollte der WINS nicht in der Lage sein, den Namen aufzulösen (oder aus irgendwelchen Gründen nicht verfügbar sein), wird die Broadcast-Methode angewandt.

Tabelle 5.3: NetBIOS-Knoten im Überblick.

Beachten Sie, dass p-node und b-node Systeme nicht zusammenarbeiten, auch nicht im selben Subnetz. Alle Systeme, unabhängig vom Knotentyp, prüfen zunächst ihren NetBIOS Name Cache, bevor sie mit einer anderen Auflösungsmethode fortfahren.

5.2.2 NetBIOS-Namen allgemein

Wie bereits am Beispiel von Windows NT 4.0 erwähnt, ist ein NetBIOS-Name eine eindeutige 16-Byte-Adresse, mit deren Hilfe eine NetBIOS-Ressource im Netzwerk identifiziert wird. Bei diesem NetBIOS-Namen handelt es sich entweder um einen exklusiven, eindeutigen Namen oder aber um einen nicht exklusiven Gruppennamen. Eindeutige und somit exklusive Namen, werden in der Regel dazu verwendet, eine Netzwerkkommunikation mit einem bestimmten Prozess auf einem Computer herzustellen. Über Gruppennamen hingegen werden Informationen gleichzeitig an mehrere Computer übertragen.

Hier eine Übersicht:

- ✔ **Unique (U):** Diese Namen haben nur eine IP-Adresse zugewiesen. Bei einem Netzwerkgerät können mehrere Erscheinungen eines einzelnen Namens auftauchen, da das Suffix aber eindeutig ist, macht dies den gesamten Namen eindeutig.
- ✔ **Group (G):** Eine normale Gruppe, ein Name kann mit mehreren IP-Adressen existieren.
- ✔ **Multihomed (M):** Der Name ist eindeutig, da aber mehrere Netzwerkkarten in einem Computer eingebaut sind, ist diese Konfiguration nötig, um die Registrierung zu erlauben. Maximale Anzahl von Adressen: 25.

- ✔ **Internet Group (I):** Eine Sonderkonfiguration des Gruppennamen, der verwendet wird, um WinNT-Domänennamen zu verwalten.
- ✔ **Domain Name (D):** Neu ab NT 4.0

5.2.3 NetBIOS Statusinformationen auslesen

Mit Hilfe des Tools nbtstat können Sie Statusinformationen von NetBIOS auslesen. Die folgende Grafik zeigt als Beispiel das Ergebnis einer Statusabfrage. Hier wurden NetBIOS-Informationen des Remote Rechners amdk6 mit

```
nbtstat -S  amdk6
```

angefordert.

Die Option -S führte dabei zur Ausgabe der so genannten NetBIOS-Verbindungstabelle. Sie können anhand der Eingabespalte z.B. sehen, dass während der zweiten Eingabe eine größere Datenmenge zwischen den beiden Rechnern ausgetauscht wurde. In der zweiten Spalte sind die Namen der Dienste erkennbar. Die erste Spalte zeigt, dass die Namen zweier Computer und eines Users ermittelt wurden.

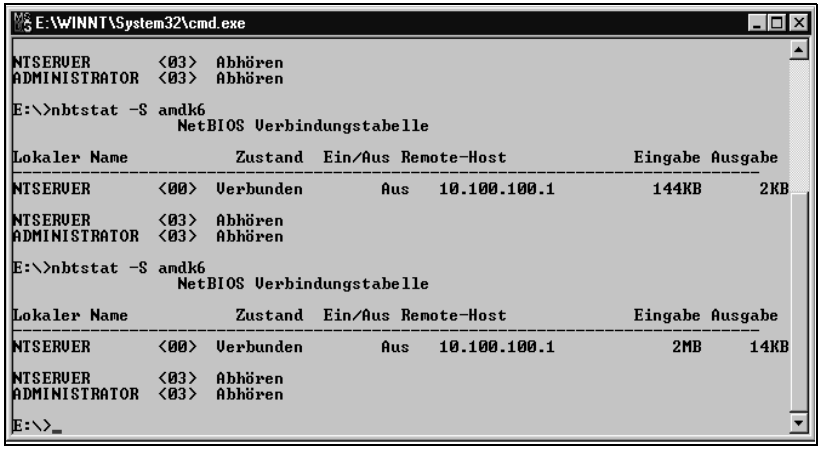


Abbildung 5.5: Statusinformationen von NetBIOS

Die folgende Tabelle gibt einen Überblick zu den Optionen des Programms unter Windows NT.

Option	Bedeutung
-a	Zeigt die Namenstabelle des mit Namen angegebenen Remote-Computers an
-A	Zeigt die Namenstabelle des mit IP-Adresse angegebenen Remote-Computers an
-c	Zeigt den Inhalt des globalen Remote-Namen-Cache mit IP-Adressen an
-C	Zeigt den Inhalt des Remotenamen-Cache mit IP-Adressen pro Gerät an
-n	Zeigt lokale NetBIOS-Namen an
-r	Zeigt mit Rundsendungen und WINS ausgewertete Namen an
-R	Lädt die Remote-Cache-Namenstabelle neu
-S	Zeigt die Sitzungstabelle mit den Ziel-IP-Adressen an
-s	Zeigt die Sitzungstabelle mit den Host-Namen an, die aus den Ziel-IP-Adressen und der Datei HOSTS bestimmt wurden
-RR	Sendet Namensfreigabe-Pakete an WINs und startet die Aktualisierung

Tabelle 5.4: Optionen von nbtstat

Die nächste Grafik zeigt die Ausgabe der Befehlszeile

```
ntbstat -A 10.100.100.254
```

Das Tool wurde auf einem Win98-Rechner ausgeführt, der eine Netzwerkverbindung zu einem IIS-Server aufgebaut hatte. Die Option -A zeigt die Namenstabelle des Remote-Rechners. In der zweiten Zeile sehen Sie z.B. die Dienstekennung <20>. Das bedeutet, dass der NT-Rechner als File-Server fungiert.

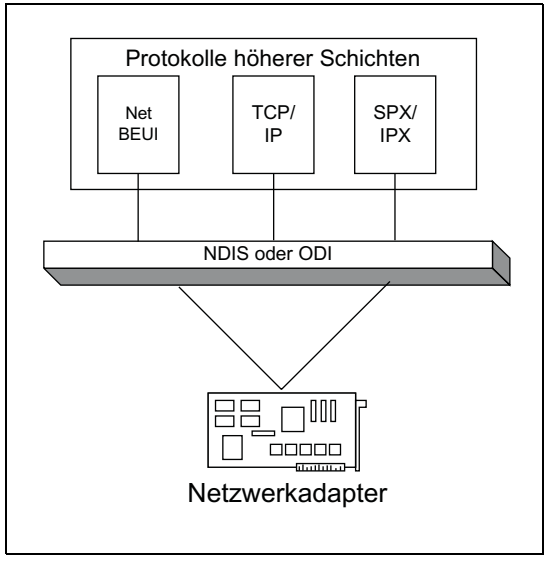


Abbildung 5.6: NetBIOS-Statusinformationen eines entfernten NT-Servers

5.2.4 NetBIOS-Dienste allgemein

Dienste der unteren Ebenen stellen 19 NetBIOS-Befehle bereit. Die folgenden Zeilen geben einen Überblick über die NetBIOS-Befehle. Diese werden in die folgenden Kategorien aufgeteilt:

- ✔ Allgemein
- ✔ Name-Support
- ✔ Datagramm-Support
- ✔ Session Support

Allgemein:

reset, cancel, adapter status, unlink

Name-Support:

add name, add group name, delete name

Datagramm-Support:

send datagram, send broadcast datagram, receive datagram, receive broadcast datagram

Session-Support:

Call, listen, hang up, send, chain send, receive, receive any, session status

Damit stellen die NetBIOS-Befehle eine Unterstützung für die folgenden Dienste bereit:

- ✔ Registrierung und Überprüfung von Netzwerknamen
- ✔ Auf- und Abbau von Sitzungen
- ✔ Zuverlässige, weil verbindungsorientierte Datenübertragung
- ✔ Unzuverlässige und verbindungslose Datagramm-Datenübertragung
- ✔ Netzwerkkartenüberwachung und -verwaltung

5.3 NetBEUI (NetBIOS Extended User Interface)

Das NetBIOS Extended User Interface wurde von der IBM Mitte der achtziger Jahre entwickelt und ist auf LANs mit mehr als 200 Rechnern ausgerichtet. NetBEUI arbeitet auf der Transportschicht und wird vor allem in Microsoft-Netzwerken eingesetzt. Das Protokoll bietet die gleichen Vorteile wie NetBIOS, es ist klein und schnell. Allerdings bedeutet auch hier das Fehlen von Routing-funktionen, dass dieses Protokoll verschwinden wird.

NetBEUI kommuniziert mit höheren Schichten über eine Schnittstelle, die TDI genannt wird, Transport Driver Interface.

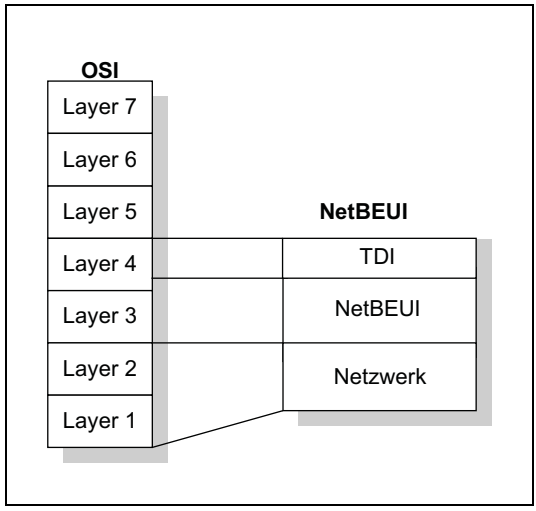


Abbildung 5.7: NetBEUI-Architektur

Die Schnittstelle zum Netzwerk und damit zu den Netzzugriffsmethoden heißt NDIS, Network Driver Interface Specification. NDIS bietet die Möglichkeit, mehrere Protokolle höherer Schichten über eine Netzwerkkarte zu nutzen.

5.4 Standards für Netzwerkkarten

Netzwerkkarten bilden die Schnittstelle zwischen dem Netzrechner und dem Übertragungsmedium. Sie realisieren hardwaremäßig das Netzwerk im OSI-Modell, also die Schichten 1 und 2. Folgerichtig gibt es dann Ethernet, Token Ring, FDDI oder ATM-Karten.

Der Zugriff eines LAN-Protokolls auf das vorhandene physikalische Netzwerk erfolgt über die Software, die die Netzwerkkarte steuert und den Datenaustausch zwischen Betriebssystem und Netzwerkkarte erst ermöglicht. Diese Software wird allgemein als Treiber bezeichnet und gehört zum Lieferumfang der Netzwerkkarte.

Im LAN-Bereich haben sich zwei Treiberstandards durchgesetzt, NDIS von Microsoft/3Com und ODI von Novell/Apple.

Beide Spezifikationen sind unterschiedlich und zueinander inkompatibel. Das bedeutet, dass zum Beispiel für ein Windows-Netzwerk ein Treiber geladen werden muss, der NDIS-kompatibel ist, für ein Novell-Netzwerke wird aber für die gleiche Netzwerkkarte ein ODI-Treiber vorausgesetzt.

Novell und Microsoft bieten allerdings dem Anwender die Möglichkeit, NDIS bzw. ODI dennoch zu benutzen. Novell unterstützt NDIS-Dienste mit einer Software, die ODINSUP, ODI NDIS Support, genannt wird. Die Strategie von Microsoft besteht darin, eine NDIS-verträgliche IPX-Version anzubieten.

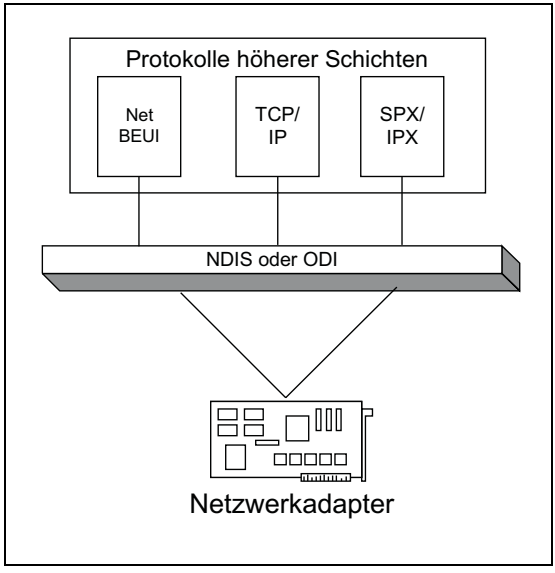


Abbildung 5.8: NDIS und ODI als Multiprotokollschnittstellen

Aus den oben genannten Gründen werden Netzwerkkarten mit Treibern für die jeweilige Standardisierung ausgeliefert. Der Anwender kann dann nach Bedarf den ODI oder den NDIS-Treiber laden. Der Leistungsumfang beider Spezifikationen ist vergleichbar. Von besonderer Bedeutung ist in diesem Zusammenhang die Fähigkeit beider Standards, den parallelen Zugriff mehrerer Protokollstacks auf eine Netzwerkkarte zu ermöglichen.

5.4.1 ODI (Open Data Interface)

Novell-Netzwerke greifen standardmäßig über einen ODI-Treiber, Open Data Interface, auf die Netzwerkkarte zu.

ODI-Treiber erlauben die Konfiguration logischer Netzwerkkarten. Für jede Netzwerkkarte kann ein eigener Rahmen, z.B. IEEE 802.2 oder IEEE 802.3 konfiguriert werden.

Weitere Parameter sind:

- ✔ IRQ
- ✔ Basisadresse
- ✔ DMA

- ✔ Anzahl der gleichzeitig unterstützten Verbindungen
- ✔ Maximale Paketgröße
- ✔ Konfiguration einer logischen MAC-Adresse, die die physikalische überschreibt

Die folgenden Zeilen sind ein Beispiel für die Konfiguration einer Netzwerkkarte, die über einen ODI-Treiber angesteuert wird. Die Parameter werden als ASCII-Text in eine Konfigurationsdatei, die NET.CFG, geschrieben, die beim Booten des Systems ausgelesen wird.

Sie sehen einen Ausschnitt aus der NETCFG zur Konfiguration einer Netzwerkkarte. In unserem Beispiel handelt es sich um einen NE2000-Adapter, dessen vom Standard abweichende Einstellungen in den folgenden Zeilen vorgenommen werden.

```
Link Driver NE2000
PORT 340
IRQ 5
LINK STATIONS 3
MAX FRAME SIZE 1512
```

5.4.2 NDIS (Network Device Specification)

Mit NDIS, Network Device Specification, setzt Microsoft einen eigenen Standard für den Zugriff auf Netzwerkkarten. Was den Leistungsumfang betrifft, ist kein Unterschied zu ODI erkennbar. NDIS-Treiber werden in verschiedene Kategorien eingeteilt. Die Zuordnung ist abhängig vom verwendeten Betriebssystem.

Betriebssystem	Kategorie
Windows 95	NDIS 3
Windows NT	NDIS 3
DOS	NDIS 2
OS/2	NDIS 2

Tabelle 5.5: NDIS-Kategorien

Auch WAN-Karten, wie z. B. eine ISDN-Karte, arbeiten unter Windows mit der NDIS-Spezifikation. Aus der Sicht des Betriebssystems gibt es dann keinen Unterschied zwischen LAN oder WAN. Auf der linken Seite sehen Sie die Treiberinformationen für einen LAN-Adapter unter Windows. Der geladene NDIS-Treiber unterstützt 16-Bit-Anwendungen die unter DOS laufen und 32-Bit-Windowsapplikationen. Im rechten Fenster sehen Sie in der Netzwerkkonfiguration, dass eine ISDN-Karte mit einem NDIS-Treiber eingebunden wurde.

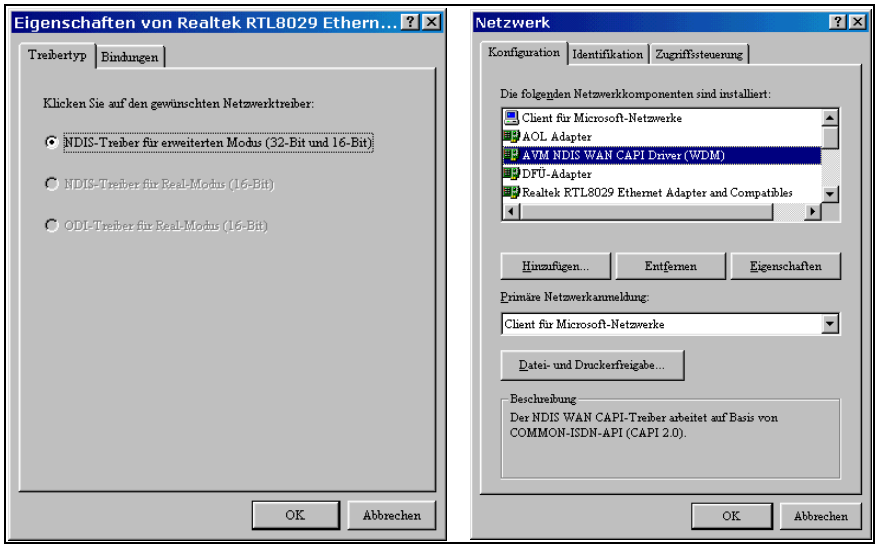


Abbildung 5.9: NDIS unter Windows.

KAPITEL 6

6 Remote Access und Virtual Private Networks

Remote Access beschreibt eine Architektur, die es einem entfernten Rechner ermöglicht, via Telekommunikationsverbindung auf die Ressourcen eines LAN so zuzugreifen, als sei er direkt an das LAN angeschlossen.

Bei der Umsetzung handelt es sich um eine typische Client/Server-Anwendung mit beliebig vielen RAS-Clients und einem RAS-Server. Mittels RAS, Remote Access Services, kann dann eine Verbindung zwischen einem Client und einem entfernt stehenden Netzwerk ohne Einschränkungen hergestellt werden. Ein RAS-Client arbeitet nach Verbindungsaufnahme so, als sei er tatsächlich lokal im Netzwerk über eine direkte Verbindung angeschlossen. Die verwendete Datenübertragungseinrichtung, wie ein Modem oder eine ISDN-Karte arbeitet dann wie eine Netzwerkkarte. Das Grundprinzip verdeutlicht die folgende Abbildung. Im weiteren Verlauf werden Details von Remote Access am Beispiel des entsprechenden Dienstes unter Windows NT besprochen.

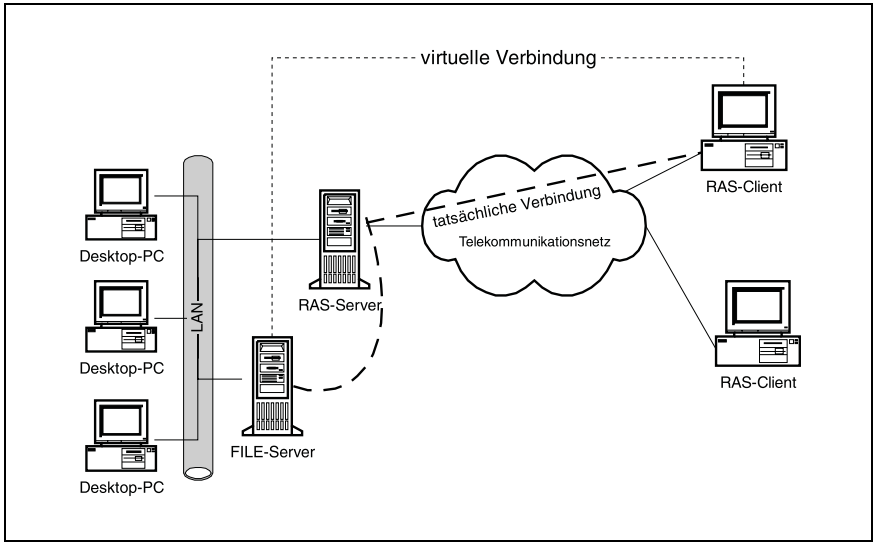


Abbildung 6.1: Remote Access als Client/Server-Anwendung

6.1 Remote Access unter Windows NT

Als Basis für Remote-Anwendungen bietet Windows NT 4.0 den RAS-Dienst, Remote Access Service, sowohl unter der Windows NT Workstation als auch unter dem Windows NT Server an. Wird während des Setups von Windows NT 4.0 die Option Remote-Zugriff auf das Netzwerk ausgewählt, werden der RAS-Dienst und das DFÜ-Netzwerk automatisch installiert.

Die beiden Softwareprodukte NT Server 4.0 und NT Workstation 4.0 unterscheiden sich aber bei diesem Leistungsmerkmal doch erheblich voneinander. So ist die gleichzeitige Verbindung zum RAS-Server bei der Verwendung der Windows NT Workstation 4.0 auf nur eine Verbindung eingeschränkt. Wird als RAS-Server hingegen das Produkt Windows NT Server 4.0 verwendet, können 256 Clients gleichzeitig eine Verbindung zu diesem aufbauen.

Voraussetzung ist natürlich ein entsprechendes technisches Umfeld mit einem leistungsstarken NT-Server. Insbesondere werden hierzu spezielle serielle Schnittstellenkarten oder aber auch ISDN-Karten mit einem eigenen Prozessor benötigt, um die CPU des Servers zu entlasten. Entsprechende ISDN-Karten werden auch als aktive Karten bezeichnet.

Erfolgt der Remote-Zugriff unter NetBIOS ist die Anzahl der gleichzeitigen Verbindungen zudem auf 250 beschränkt, was aber an NetBIOS und nicht an Windows NT liegt. Bedingt durch eine begrenzte Bandbreite unterliegt natürlich auch der RAS-Dienst gerade bei Modem-Verbindungen weiteren Einschränkungen. Durch Verwendung eines ISDN-Anschlusses in Kombination mit Kanalbündelung kann aber eine akzeptable Übertragungsgeschwindigkeit erreicht werden.

Auch die Verwendung von X.25 ist eine weitere Möglichkeit für die Verbindung zwischen den RAS-Clients und einem RAS-Server. Der Zugriff der Clients erfolgt dabei unter Verwendung eines X.25 Adapters oder aber alternativ durch die Anwahl eines PAD. Dieser PAD wandelt seriell zu übertragende Daten in X.25 Pakete um. Andererseits werden empfangene X.25 Pakete von einem PAD in serielle Datenströme umgewandelt. Ein RAS-Server verfügt bei einem X.25-Zugang in der Regel über einen direkten X.25- Hauptanschluss.

Als RAS-Clients können unter anderem verwendet werden:

- ✔ Windows NT Workstation
- ✔ Windows 95/98
- ✔ Windows für Workgroups
- ✔ LAN-Manager-RAS-Clients mit DOS und OS/2
- ✔ UNIX-Clients mit Unterstützung des PPP-Protokoll

Wenn der RAS-Dienst auf der Client-Seite über das DFÜ-Netzwerk eingerichtet wird, dann verfügen die RAS-Clients über eine Benutzeroberfläche, die der von Windows 95 entspricht. Als RAS-Client muss aber nicht notwendigerweise das DFÜ-Netzwerk verwendet werden.

6.1.1 Installieren des Remote Access Service

Im Laufe der Installation des RAS-Dienstes müssen einige Informationen angegeben werden. Diese sollten im Vorfeld bekannt sein, um die Installation ohne Unterbrechung abschließen zu können. Im Einzelnen handelt es sich um folgende Informationen:

- ✔ Typ der Übertragungseinrichtung sowie Modell (Modem, ISDN-Karte u.a.) und die dazugehörigen Kommunikationsparameter
- ✔ Art des DFÜ-Anschlusses
- ✔ Verwendungszweck; wird der Computer als Server oder Client verwendet, wobei eine Verwendung als Server und Client ebenfalls möglich ist
- ✔ Welche Protokolle werden verwendet?
- ✔ Sicherheitseinstellungen und Rückrufoptionen

Der RAS-Dienst als solcher wird auf dem Windows NT Server oder auf der Windows NT Workstation über das Symbol **Netzwerk** und die Befehlsfolge **Eigenschaften, Dienste, Hinzufügen** installiert. Nachdem der Dienst RAS-Dienst aus der Auswahlliste ausgewählt wurde, muss anschließend die Auswahl noch mit »OK« bestätigt werden. Je nach Systemumgebung muss der Dienst von der CD oder Festplatte zum Installieren zur Verfügung gestellt werden. Durch den Button **Fortsetzen** wird der Dienst im System mit eingebunden.

Wird im Anschluss daran keine Datenübertragungseinrichtung gefunden, muss manuell noch ein Modem oder ein anderes RAS-fähiges Gerät installiert werden.

Handelt es sich bei diesem Anschluss um einen seriellen Port, so kann man versuchen über die automatische Erkennung das angeschlossene Modem zu lokalisieren. Unter Verwendung handelsüblicher Modems funktioniert dies auch recht gut.

Welche seriellen Anschlüsse verwendet werden, hängt von der jeweiligen Hardwareausstattung ab. Danach ist die eigentliche Auswahlroutine der Datenübertragungseinrichtung soweit abgeschlossen und wird durch die Schaltfläche **Fertigstellen** noch bestätigt. Später notwendige Einstellungen, wie z.B. Anschluss an einer Nebenstellenanlage, hängen dabei natürlich von der vorhandenen Infrastruktur ab.

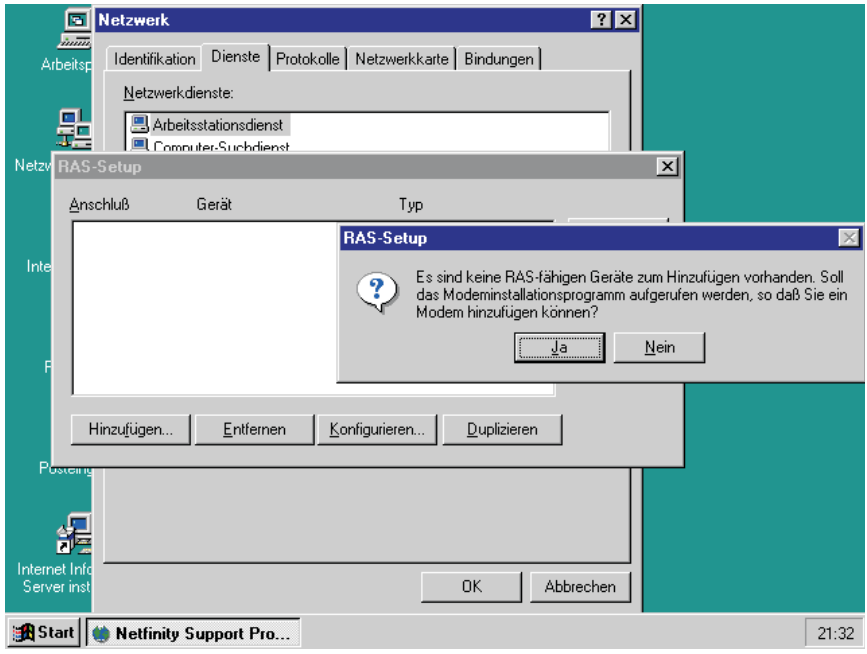


Abbildung 6.2: RAS-Übertragungseinrichtungen installieren

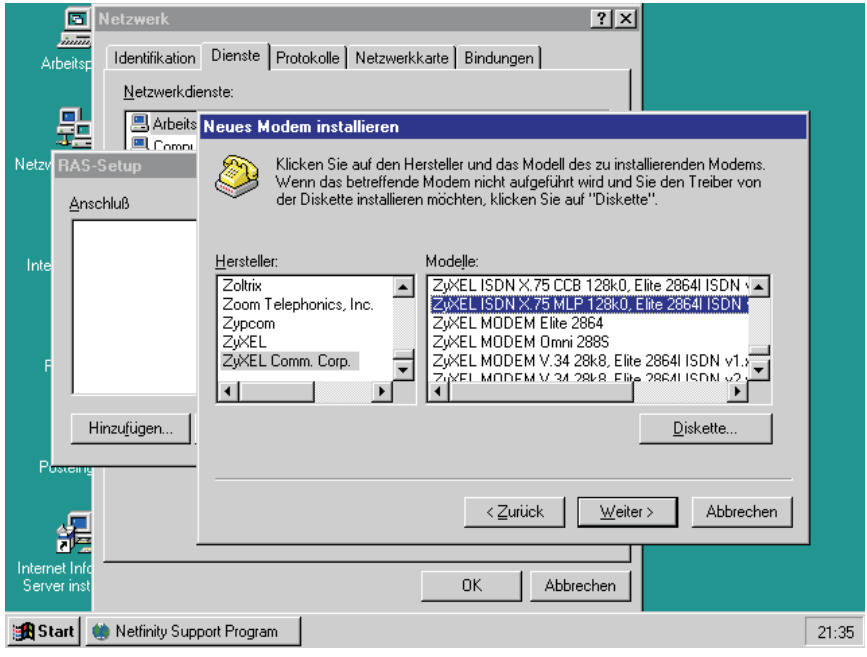


Abbildung 6.3: RAS-Modem auswählen

Auch die Anschlussverwendung wie

- ✔ Nur ausgehende Rufe
- ✔ Nur eingehende Rufe
- ✔ Ein- und ausgehende Rufe

hängen von den örtlichen Gegebenheiten bzw. Bedürfnissen ab.

Über die Schaltfläche **Netzwerk** werden dann weitere notwendige Einstellungen vorgenommen.

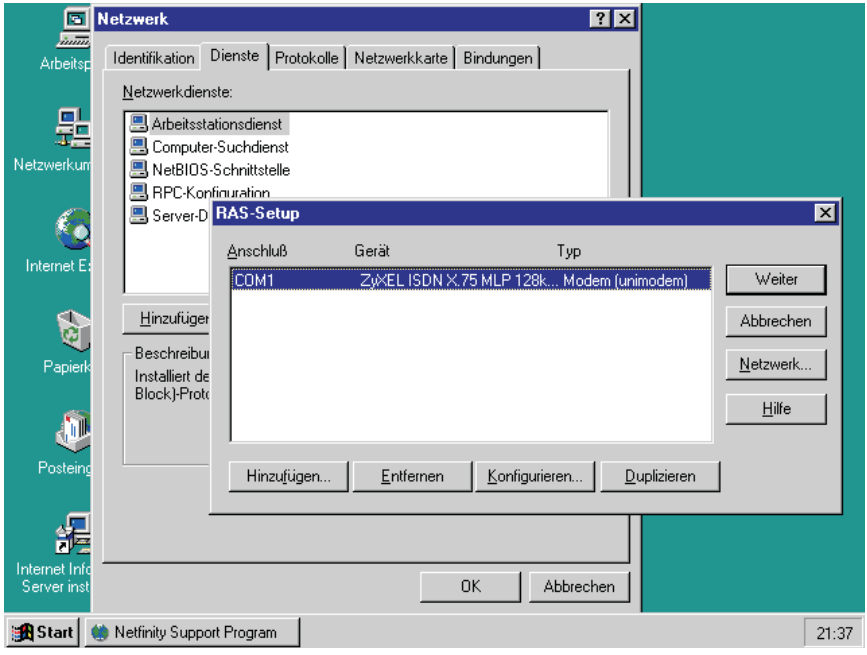


Abbildung 6.4: RAS-Modemkonfiguration

Definiert werden muss hier das verwendete Protokoll mit der Auswahlmöglichkeit zwischen NetBEUI, TCP/IP und IPX.

Soll der RAS-Server für die Verwendung von TCP/IP konfiguriert werden, dann stehen nachfolgende Optionen zur Verfügung:

- ✔ **TCP/IP Clients dürfen zugreifen auf**

  Mit der Einschränkung des Zugangs nur auf den RAS-Server kann verhindert werden, dass der RAS-Client auf das gesamte Netzwerk zugreifen kann. Alternativ dazu kann aber auch der Zugriff auf das gesamte Netzwerk erlaubt werden.

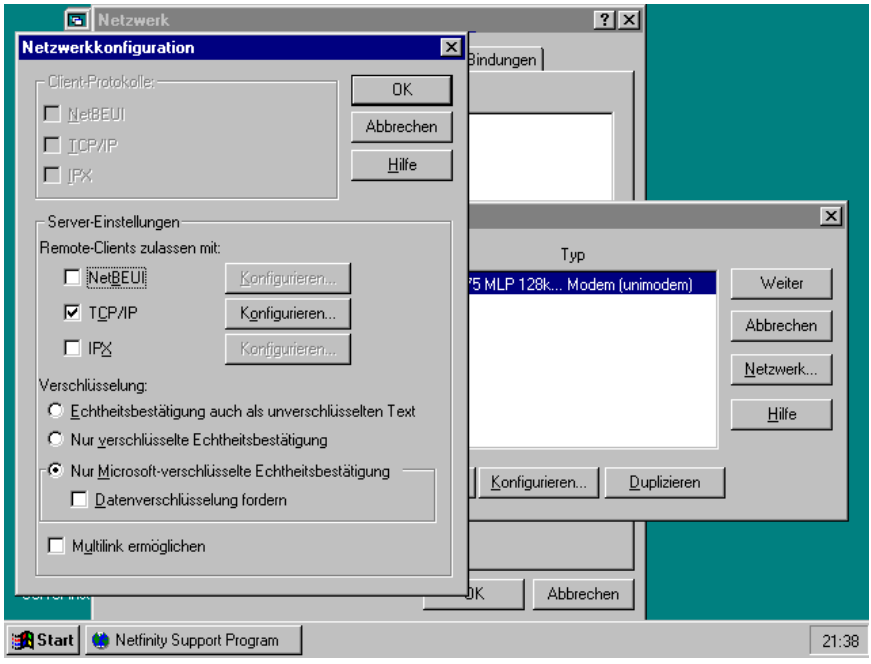


Abbildung 6.5: RAS-Netzwerkkonfiguration unter Windows NT

✔ **DHCP verwenden, um TCP/IP Adressen zuzuweisen**

Sofern diese Option aktiviert wurde, muss sich innerhalb des Netzwerkes ein DHCP-Server befinden, der dem RAS-Client eine gültige IP-Adresse zuweist.

✔ **Statischen Adresspool verwenden**

Mit dieser Option kann einem RAS-Client aus einem Adresspool eine IP-Adresse zugewiesen werden.

✔ **Remote-Clients erlauben, eine vorbestimmte IP-Adresse anzufordern**

Diese Option ermöglicht es den RAS-Clients, eine bestimmte IP-Adresse anzufordern.

Soll der RAS-Server hingegen für die Verwendung unter IPX konfiguriert werden, stehen nachfolgende Optionen zur Verfügung:

✔ **IPX-Clients dürfen zugreifen auf**

Erlaubt den Zugriff auf das Gesamte Netzwerk oder aber nur auf den RAS-Server.

- ✔ **Netzwerknummern automatisch reservieren**

  Weist den RAS-Clients automatisch eine Netzwerknummer zu, wobei allen IPX-Clients dieselbe Netzwerknummer zugewiesen werden kann.

- ✔ **Netzwerknummern reservieren**

  Den RAS-Clients wird manuell eine Netzwerknummer zugewiesen.

- ✔ **Gleiche Netzwerknummer an alle IPX-Clients zuweisen**

  Allen IPX-Clients wird dieselbe Netzwerknummer zugewiesen. Dies bewirkt, dass der Routing Tabelle nur eine Netzwerknummer für alle aktiven RAS-Clients hinzugefügt wird.

- ✔ **Clients dürfen IPX-Knotennummer anfordern**

  Erlaubt den RAS-Clients eine andere als die vom RAS-Server zugewiesene IPX-Knotennummer zu verwenden.

6.1.2 RAS-Sicherheitsfunktionen

Um einen unerlaubten Zugriff auf das Netzwerk zu unterbinden, stehen unter Windows NT unterschiedliche Sicherheitsmechanismen zur Verfügung. Wie für herkömmliche Benutzer unter Windows NT gelten auch für RAS-Clients die gleichen Anmelderoutinen. Der RAS-Server stellt dem Benutzer bei einem Remote-Zugang dieselben Berechtigungen wie am Büroarbeitsplatz zur Verfügung, da bei jeder Anmeldung des RAS-Clients eine Kopie des Benutzerprofils auf dem Client zwischengespeichert wird. In der Praxis bedeutet dies, dass der RAS-Client über ein Benutzerkonto und über die entsprechenden Einwahlberechtigungen verfügen muss.

Sind diese Voraussetzungen gegeben, dann werden bei der Übertragung durch den RAS-Dienst standardmäßig sämtliche Echtheitsbestätigungs- und Anmeldeinformationen verschlüsselt. In diesem Fall müssen die eingesetzten Clients die Verschlüsselung auch unterstützen. Darauf ist besonders bei 16-Bit-Clients zu achten.

Auch eine unverschlüsselte Übertragung ist möglich. Durch eine aktivierte Überwachung können darüber hinaus alle Remote-Verbindungen kontrolliert werden. Abbildung 6.6 zeigt das entsprechende Überwachungsfenster.

Abbildung 6.6: RAS-Anbindungen überwachen

6.1.3 Rückrufsicherheit

Zur Erhöhung der Sicherheit können unterschiedliche Rückrufoptionen eingestellt werden. Sofern diese Rückrufsicherheit ausgewählt wurde, wird der RAS-Server nach Verbindungsaufbau diese wieder trennen, um anschließend wahlweise eine fest vorgegebene Telefonnummer oder aber eine vom RAS-Client angegebene Rufnummer zurückzurufen. Durch diese Sicherheitsoption kann genau gesteuert werden, welchen Anschluss der RAS-Server zurückrufen wird.

Erfolgt das Einwählen der Remote-Station über ISDN, dann kann auch die Rufnummer übermittelt und damit vom Angerufenen identifiziert werden. Damit können unerwünschte Anrufe abgeblockt werden. Nur konfigurierte Rufnummern werden zugelassen. Dieses Verfahren wird CLI, Calling Line Identification, genannt.

Beim automatischen Rückrufverfahren meldet sich der Kommunikationspartner am Kommunikationsserver, dem Router, an. Dieser unterbricht die Verbindung und ruft automatisch zurück. In der Praxis finden sich drei Rückrufvarianten:

- ✔ Rückruf zwingend
- ✔ Rückruf nur an eine definierte Nummer
- ✔ Rückruf an eine beliebige Nummer

Die folgende Abbildung zeigt ein Beispiel unter Windows NT. Hier kann auf dem RAS-Server der Rückrufstatus eines jeden Zugriffsberechtigten eingestellt werden.

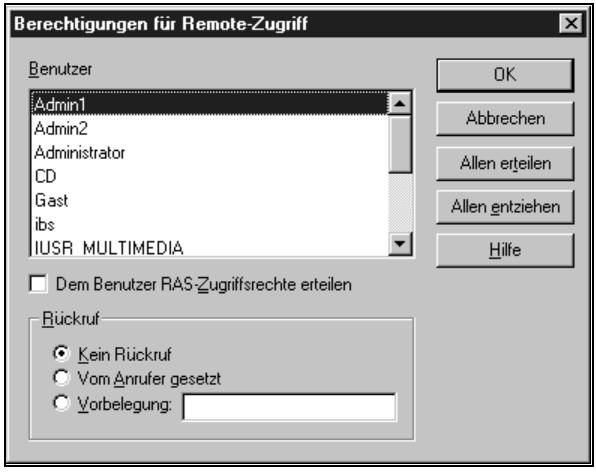


Abbildung 6.7: Rückrufberechtigungen konfigurieren

6.2 RAS-Zugangsprotokolle

Da der entfernte Zugriff auf ein Netzwerk immer über ein WAN erfolgt, müssen für die Strecke zwischen entferntem Rechner und Netzwerk spezielle Protokolle eingesetzt werden, die die Daten über das Verbindungsnetzwerk, z.B. ein Telefonnetz, transportieren. Dies gilt insbesondere dann, wenn die Verbindung über das Internet aufgebaut wird.

RAS-Zugangsprotokolle transportieren LAN-Protokolle und schaffen damit einen transparenten Zugang des Clients zum Netzwerk und zu den sich dort befindenden Servern.

Der Netzadministrator muss bei der Konfiguration des RAS-Clients also mindestens zwei Parameter kennen:

1. Das Zugangsprotokoll
2. Das LAN-Protokoll, das vom Zugangsprotokoll transportiert werden soll

Aktuell kommen drei Protokolle als RAS-Zugangsprotokoll in Frage:

- ✔ PPP, Point-to-Point-Protocol
- ✔ SLIP, Serial Line Internet Protocol
- ✔ CSLIP, Compressed SLIP

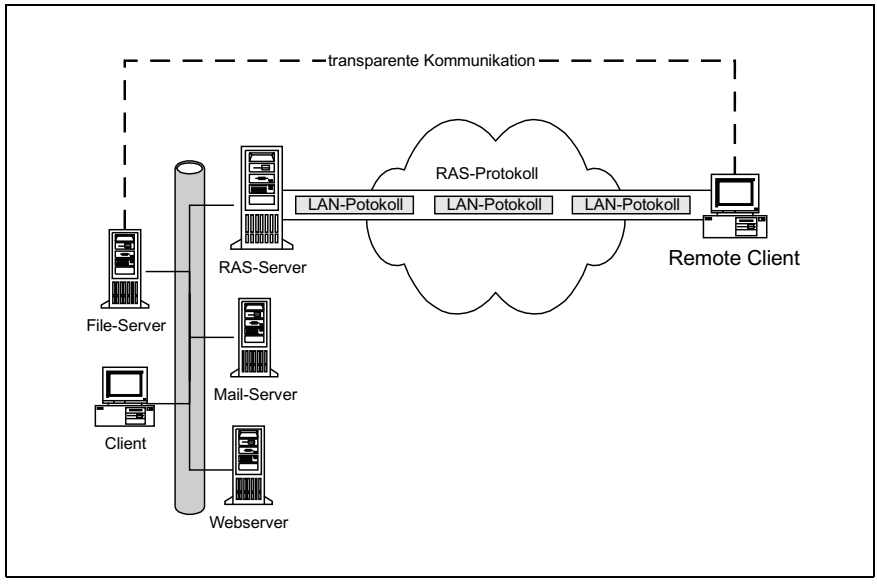


Abbildung 6.8: Remote Access als Client/Server-Anwendung

Die hier aufgeführten Protokolle werden auch serielle Protokolle genannt, weil die Daten seriell und nicht als Pakete übertragen werden.

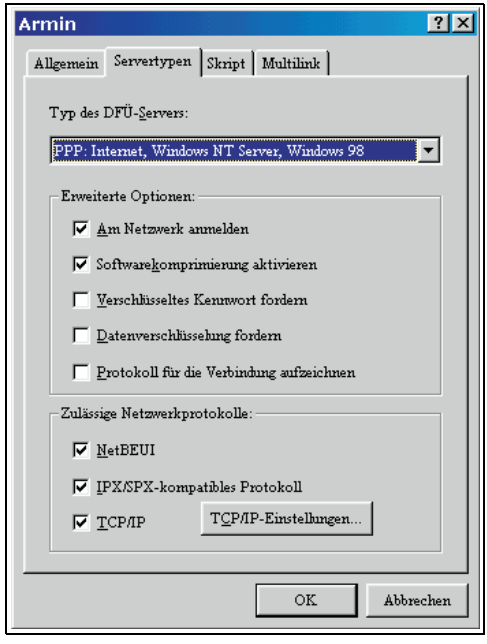


Abbildung 6.9: RAS-Servertypen

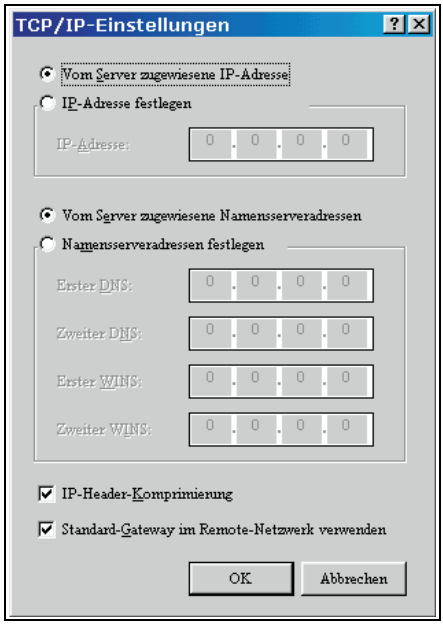


Abbildung 6.10: RAS-Client mit IP-Konfiguration

Abbildung 6.9 zeigt den oben beschriebenen Zusammenhang am Beispiel des DFÜ-Netzwerks unter Windows. Sie sehen hier, dass der Servertyp unter anderem durch das RAS-Protokoll und durch das oder die zulässigen Netzwerkprotokolle bestimmt wird. Ein weiterer Konfigurationsparameter ist die statisch oder dynamisch durch den RAS-Server zuzuweisende IP-Adresse des Clients. Abbildung 6.10 zeigt einen Client, dessen IP-Adresse dynamisch durch den Server zugewiesen wird.

6.2.1 SLIP (Serial Line Internet Protocol)

Das Serial Line Internet Protocol, SLIP, wird in der Regel dazu benutzt, Internet-Protokolle über serielle Wählleitungen zu transportieren. Die Übertragungsgeschwindigkeit liegt dann zwischen 1200 und 19200 Bit/s. In der Regel ist SLIP auf UNIX-Rechnern implementiert.

SLIP ist ein sehr einfaches Protokoll, das mit zwei Steuerzeichen auskommt, dem END-Zeichen und einem Escape-Zeichen. Das END-Byte besitzt das Bitmuster 11000000, ESC wird mit 11011011 codiert.

Wenn IP-Pakete über SLIP übertragen werden, dann werden die Daten ohne SLIP-Header transportiert. Am Ende des IP-Pakets fügt SLIP lediglich das END-Byte an. Anschließend wird das nächste IP-Paket angehängt, wieder ein END-Byte, gefolgt von Daten usw. Sollte zufälligerweise im IP-Datenstrom das gleiche Bitmuster wie für das END-Byte auftauchen, dann werden von SLIP vor

diesem Byte zwei Byte eingefügt. Das erste Byte ist das ESC-Bitmuster und das zweite Byte wird mit dem Bitmuster 11011101 aufgefüllt. Der SLIP-Empfänger entfernt wieder die beiden Steuer-Byte sowie alle END-Byte.

SLIP ist kein offizieller Standard und deshalb gibt es auch keine definierte maximale Paketlänge. Als Richtlinie gilt hier die Berkeley-UNIX-Implementierung mit einer maximalen Paketgröße von 1006 Byte ohne Steuerzeichen.

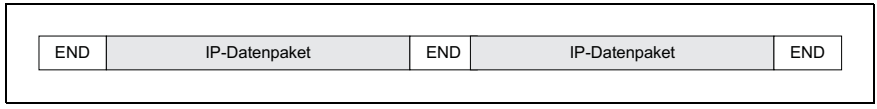


Abbildung 6.11: SLIP-Protokollstruktur

SLIP weist aus heutiger Sicht einige gravierende Nachteile auf. So kennt das Protokoll keinen Mechanismus für die Übertragung von Adressinformationen. Daraus ergibt sich, dass den beteiligten Hosts jeweils die Adresse des Kommunikationspartners bekannt sein muss. Da SLIP keine Protokollinformationen kennt, kann das Protokoll auch jeweils nur für ein Protokoll konfiguriert werden. Der wohl entscheidendste Nachteil ist allerdings das Fehlen jeglicher Sicherungsmechanismen.

CSLIP, Compressed SLIP, ist eine Variante des SLIP-Protokolls, die die Daten komprimiert und dann über die Leitung schickt.

6.2.2 PPP (Point-to-Point-Protocol)

Das Point-to-Point-Protocol ist wesentlich komplexer als SLIP. **PPP** ist so aufgebaut, dass es die simultane Übertragung mehrerer Protokolle über eine serielle Leitung, z.B. analoges Telefonnetz oder ISDN, ermöglicht. PPP ist in den RFCs 1331, 1332 und 1333 veröffentlicht.

Der wesentliche Unterschied zu SLIP liegt darin, dass PPP eine Vielzahl von Sicherungsfunktionen implementiert. Außerdem ist es möglich, Netzwerkadressen via PPP zuzuweisen. Damit besitzt PPP insbesondere bei der Verbindung über das Internet bzw. zum Internet entscheidende Vorteile. Als Administrator wird man in den allermeisten Fällen Remote-Rechner über PPP in das lokale Netzwerk einbinden.

Das PPP-Protokoll besteht aus drei Komponenten:

- ✔ Encapsulation
- ✔ Network Control
- ✔ Link Control

Encapsulation ist die Fähigkeit von PPP, Datenpakete höherer Protokolle zu transportieren. Die zugrunde liegende Technik heißt Kapselung oder Encapsulation. Encapsulation bedeutet, dass Pakete höherer Protokolle von PPP als Nutzdaten transportiert werden.

Für die Netzwerkkontrolle arbeitet PPP mit einem Protokoll, das Network Control Protocol, **NCP**, genannt wird. Das NCP ist für die Konfiguration der Übertragungsparameter eines höheren Protokolls zuständig. Damit hat jedes Protokoll, das von PPP transportiert wird, sein eigenes NCP. So heißt z.B. das NCP, das für Internet-Protokolle zuständig ist, **IPCP**, IP Control Protocol.

Die Link Control ist für den ordnungsgemäßen Auf- und Abbau einer Kommunikation zuständig. Weitere Aufgaben sind die Konfiguration und das Testen einer Verbindung. Das hierfür eingesetzte Protokoll wird Link Control Protocol genannt. Eine mit LCP gesteuerte Verbindung kann in folgende Phasen aufgeteilt werden:

- ✔ Phase 1: Austausch von Konfigurationspaketen
- ✔ Phase 2: Öffnen einer Leitungsverbindung
- ✔ Phase 3: Testen der Qualität der Leitungsverbindung
- ✔ Phase 4: Übertragung von Nutzdaten
- ✔ Phase 5: Verbindungsabbau

LCP sendet zum Testen der Leitungsverbindung so genannte Echo-Requests, die mit Echo-Replay von der Gegenstelle beantwortet werden. Nach der Testphase ruft LCP dann das gewünschte NCP auf.

Die beiden oben beschriebenen Protokolltypen, also NCP und LCP, werden in einem PPP-Paket mit Hilfe unterschiedlicher Kennungen im Protokoll-Typenfeld identifiziert. LCP wird z.B. mit hexC021 codiert, das Internet Control Protocol IPCP mit hex8021. Eine Übersicht zu allen für PPP kodierten Protokollen finden Sie bei Othmar Kyas, Internet. Die folgende Tabelle zeigt eine Auswahl.

Kennung Typenfeld	Protokoll
hex0021	IP
hex0029	AppleTalk
hex002B	Novell IPX
hex0035	Banyan Vines
hex8027	DECNet Phase IV Control Protocol
hexC023	PAP
hexC223	CHAP
hex8021	IPCP
hexC021	LCP

Tabelle 6.1: PPP-Protokolltypen

Die folgende Abbildung zeigt den Protokollaufbau. Sie sehen, dass PPP Anfang und Ende eines Paketes mit einem FLAG kennzeichnet. Das Adressfeld ist immer auf die Broadcast-Adresse 11111111 gesetzt. Das Kontrollfeld besitzt ein Bitmuster, das das Datenpaket als unabhängiges Paket ohne Folgepaket kennzeichnet, Unnumbered Information. Im zwei Byte langen Protokolltypen-Feld wird das von PPP gekapselte Protokoll als hexadezimaler Wert eingetragen. Zur Zeit ist PPP in der Lage, 46 verschiedene Protokolle zu transportieren.

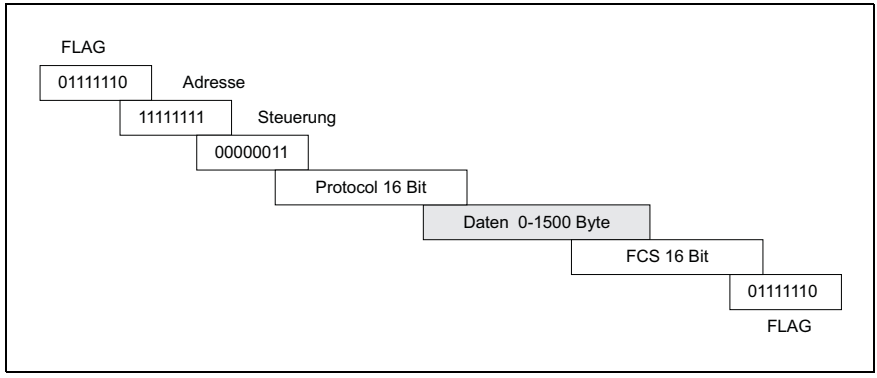


Abbildung 6.12: PPP-Protokollstruktur

Authentifizierungstechniken von PPP

PPP verwendet zwei Authentifizierungstechniken:

- ✔ PAP
- ✔ CHAP

PAP, Password Authenfitication Protocol, ist eine Methode, die den Verbindungsaufbau mit Identitätsprüfung beim ersten Login als gegenseitiges Handshake-Verfahren umsetzt. Problematisch ist dabei, dass die Passwörter unverschlüsselt übertragen werden.

CHAP, Challenge Handshake Authentification Protocol, ist eine aufwändigere Form des PAP. Hier wird ein dreigliedriges Handshake-Verfahren verwendet. Zusätzlich wird die Anruferidentifizierung periodisch auch während einer bestehenden Verbindung überprüft.

Mit Handshake wird ein Verfahren bezeichnet, das nach dem Verbindungswunsch abläuft und mit dessen Hilfe die Legitimität des Clients geprüft wird. Dazu authentifiziert sich der Client. Er sendet einen Benutzernamen, Identification, und ein Passwort zur Autorisierung.

CHAP arbeitet nach dem in der Abbildung 6.13 gezeigten Prinzip.

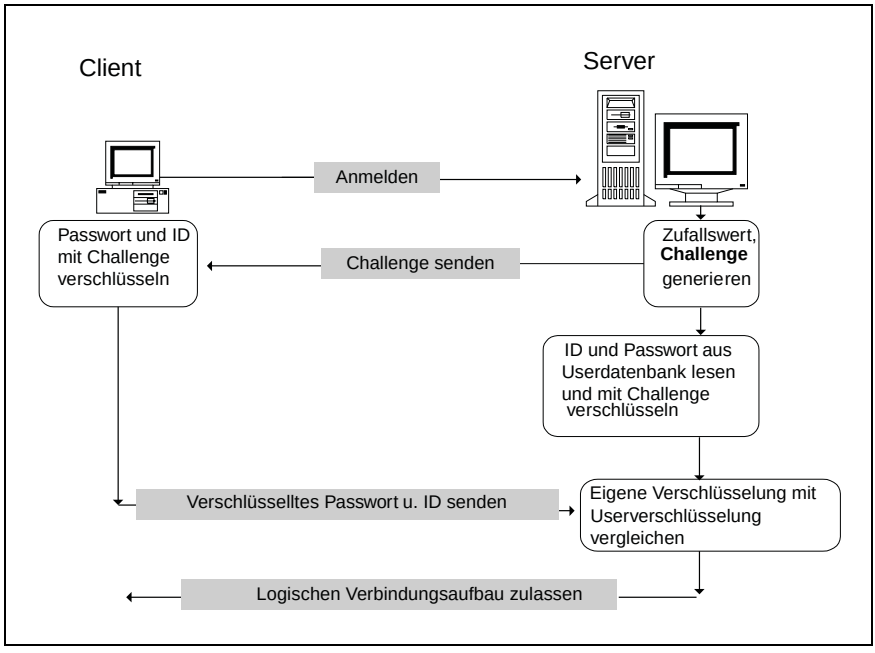


Abbildung 6.13: Das CHAP-Protokoll

Um die Übertragung von Passwörtern und Benutzernamen im Klartext zu vermeiden, arbeitet CHAP mit einem zufällig generierten Schlüssel, der Challenge genannt wird. Der Challenge wird bei einer Verbindungsaufnahme durch den Client generiert und an diesen gesendet. In der zweiten Phase verschlüsselt der Client sein Passwort und seine ID. Das Gleiche tut der Server mit den entsprechenden Eintragungen in seiner User-Datenbank. Der Client sendet in der Phase drei die mit Hilfe des Challenge errechneten Codes an den Server. Der Server vergleicht in der vierten Phase den empfangenen Schlüssel mit dem selbst errechneten Schlüssel. Stimmen beide überein, dann ist der Zugriff berechtigt. Der große Vorteil liegt nun darin, dass für jede Sitzung ein anderer Schlüssel verwendet wird. Darüber hinaus ist es möglich, während der Sitzung weitere Challenges zur Verifizierung zu generieren.

6.3 Virtual Private Networks

Virtual Private Networks, **VPNs**, nutzen das Internet, um lokale Netzwerke gesichert miteinander zu verbinden. VPNs sind eine preiswerte Alternative zu Standleitungen oder Frame Relay, erfordern aber eine Reihe von Sicherheitsmaßnahmen, um Netzwerk und Daten erfolgreich schützen.

VPNs setzen insbesondere die Mitwirkung des Internet Service Providers voraus, ISP. Dieser muss auf seinem Gateway VPN unterstützen, damit die Daten gesichert von Gateway zu Gateway über das öffentliche Internet geroutet werden können.

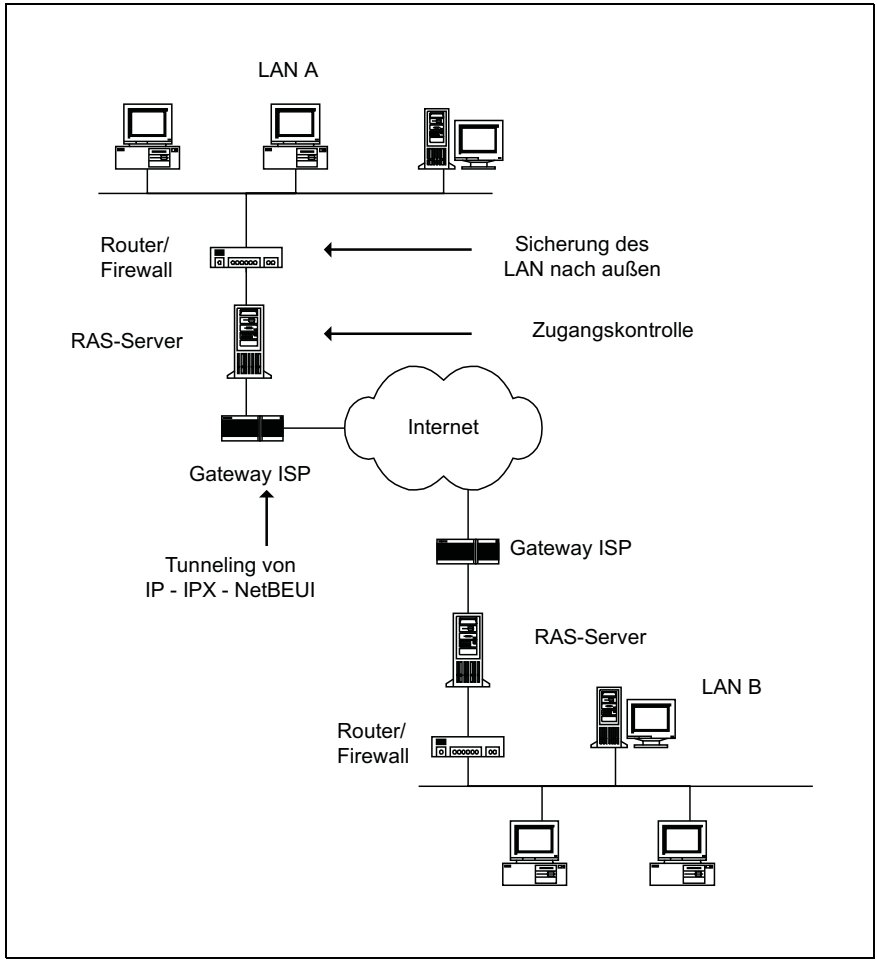


Abbildung 6.14: VPN-Architektur

Für VPNs sind zwei Szenarien denkbar:

- ✔ Verbindung zwischen mehreren Niederlassungen eines Unternehmens
- ✔ Anbindung von Heimarbeitsplätzen bzw. mobilen Mitarbeitern

Die gesicherte Verbindungsstrecke zwischen den Internet-Gateways der entfernten lokalen Netze wird als Tunnel bezeichnet.

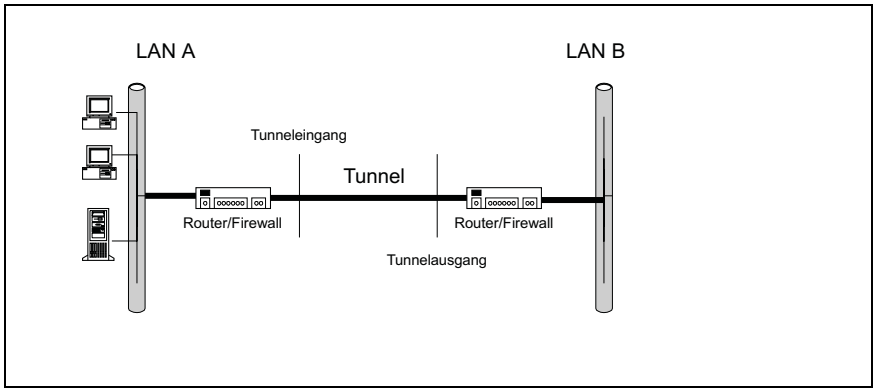


Abbildung 6.15: Architektur eines Tunnels

Der oben gezeigte »Tunnel« besteht aus verschlüsselten Datenpaketen, die zwar über das allgemein zugängliche Internet geroutet werden, aber nur von den Endpunkten des Tunnels »verstanden« werden können. Zum Bild des Tunnels passt auch, dass auch LAN-Protokolle wie IPX oder NetBEUI transparent übertragen werden. Das bedeutet, über VPN verbundene Netze müssen nicht zwangsläufig IP-Netzwerke sein.

Tunnelein- und -ausgang liegen auf den Gateways des ISP. Diese implementieren auch die für die Datenverschlüsselung und das korrekte Routing notwendige Software, die manchmal auch VPN-Server genannt wird.

Tunneling-Protokolle sind:

- ✔ PPTP, Point-to-Point-Tunneling-Protocol
- ✔ L2F, Layer 2 Forwarding
- ✔ L2TP, Layer 2 Tunneling Protocol
- ✔ VTP, Virtual Tunneling Protocol
- ✔ Mobile IP
- ✔ IPSec, Secure IP

Das Layer-2-Forwarding-Protokoll geht auf eine Initiative von Cisco, dem Marktführer von Internet-Routingprodukten, zurück. L2F bietet im Vergleich zu PPTP einen stärkeren Verschlüsselungsalgorithmus und unterstützt neben IP auch Frame Relay sowie ATM.

Das Layer-2-Tunneling-Protocol ist ein Entwurf der IETF und damit ein offizieller Internet-Standard. Als Weiterentwicklung von L2F verwendet L2TP die gleichen Verfahren wie IPSec.

6.3.1 Dial-Up-VPN

Dial-Up-VPNs sind Netzwerke, die den gesicherten entfernten Zugriff auf ein LAN über das Internet ermöglichen. Darin liegt der Unterschied zu einer RAS-Lösung. Hier werden die Remote-Clients direkt über eine geschaltete Telekom-Leitung eingebunden.

Als gesicherte Zugangsprotokolle kommen PPTP, L2F und L2TP zum Einsatz. Damit ergibt sich folgende Architektur:

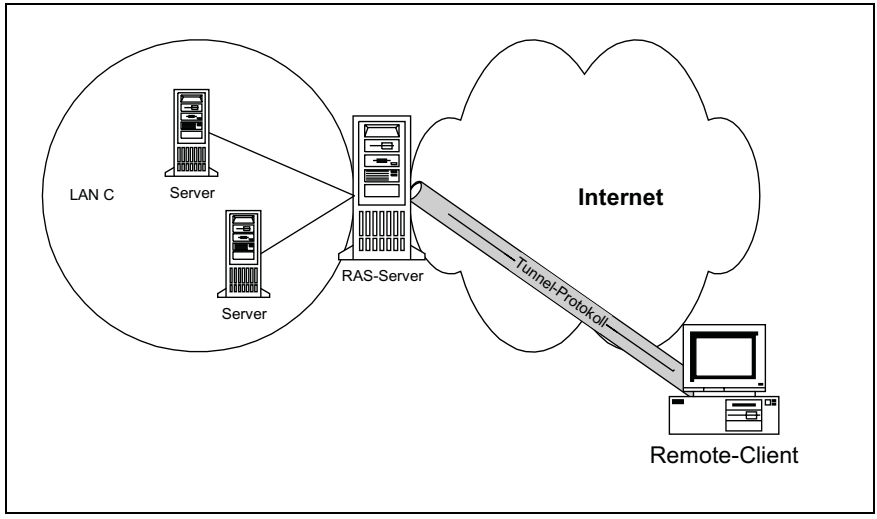


Abbildung 6.16: Dial-Up-VPN

Die Daten werden zwischen RAS-Server und Remote-Client mit Hilfe des PPTP-Protokolls gesichert, weil sie verschlüsselt durch das Internet geroutet werden.

6.3.2 Virtual Private Networks mit IPSec

VPNs werden auch als Extranet bezeichnet. Dieser Begriff verweist auf die Tatsache, dass für das virtuelle Netzwerk öffentliche Internetstrecken verwendet werden, die Daten aber ausschließlich nichtöffentlich sind.

Virtuelle private Netzwerke, die IPSec als Protokoll einsetzen, sind vor allem dort sinnvoll, wo eine gesicherte Anbindung mit unterschiedlichen Partnern, z.B. Lieferanten, benötigt wird. Abbildung 6.17 zeigt das Grundprinzip. Hier bauen VPN-Client und VPN-Server einen durchgehenden ESP-Tunnel auf. Im Internet wird dieser nochmals von einem AH-Tunnel gekapselt.

Damit ist gewährleistet, dass die beteiligten Firewalls immer auch eine Authentifizierung durchführen müssen. Die eigentlichen Daten, die ja direkt zwischen Client und Server ausgetauscht werden, sind zusätzlich durch die Verschlüsselung mit ESP geschützt.

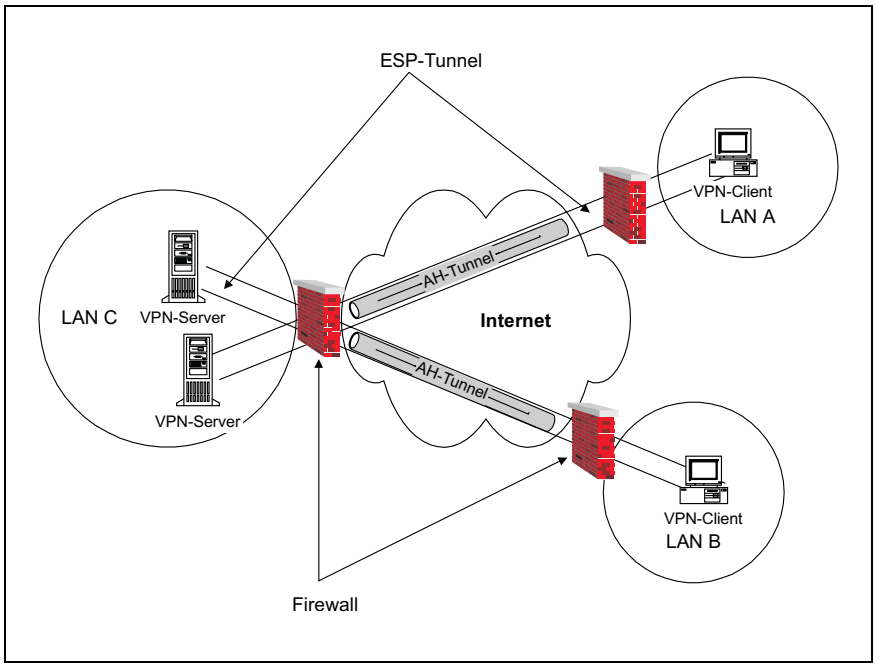


Abbildung 6.17: VPN mit IPSec

6.3.3 Virtual Private Networks mit PPTP

Das Point-to-Point Tunneling Protocol (PPTP) ist ein Netzwerkprotokoll, das ebenfalls einen gesicherten Datentransfer zwischen einem entfernten Client und dem Unternehmensnetzwerk ermöglicht. Das Protokoll ist kein offizieller Standard, sondern geht auf eine Initiative von Ascend, Microsoft, 3COM und US Robotic zurück. Diese Firmen bilden mit anderen das PPTP Forum.

VPNs können also auch über PPTP aufgebaut werden. Für den Einsatz von PPTP sprechen folgende Gründe:

- ✔ **Verfügbarkeit:** Das Protokoll ist in Windows NT4.0 Server, NT Workstation und ohne Aufpreis in RAS-Servern verschiedenster Hersteller enthalten.
- ✔ **Einfache Implementierung**: Auf Remote Access Servern mit PPTP Unterstützung ist das Protokoll einfach zu aktivieren. Möchte sich ein Benutzer über PPTP einwählen, ergänzen Sie im Profil einfach die IP-Adresse des PPTP-Servers.
- ✔ **Tunneling mehrerer Protokolle:** Während manche Tunnel-Software nur das Tunneling von IP-Paketen vorsieht, werden bei PPTP alle gegenwärtigen von RAS unterstützten Protokolle berücksichtigt.

- ✔ **Verwendung firmeninterner und nicht registrierter Adressen:** Wenn VPN Benutzer PPTP-Verbindungen zum RAS-Server herstellen, dann kann ihnen auch eine dynamische IP-Adresse zugewiesen werden.

PPTP unterstützt on-demand und multiprotokoll VPNs über öffentliche Netze wie z.B. das Internet. Die PPTP-Technologie selbst ist eine Weiterentwicklung des Remote Access Point-to-Point Protocol, das in der RFC 1171 beschrieben ist. PPTP kapselt PPP-Pakete in IP-Datagramme, die dann über ein IP-Netz transportiert werden können.

Jede PPTP-Implementierung besteht aus den folgenden drei Computertypen:

- ✔ PPTP Clients
- ✔ Gateways
- ✔ PPTP-Server

PPTP-Implementierungen finden Sie unter Windows NT und UNIX-Derivaten. Weil das Protokoll eine Vielzahl von LAN-Technologien (IP, IPX, NetBEUI) unterstützt, kann damit auf die große Vielfalt existierender LAN-Infrastruktur zugegriffen werden. Dabei sind keine Änderungen in der Adress-Struktur der Netzwerke notwendig.

Sicherheit

Zur Authentifizierung von Nutzern benutzt PPTP die standardisierten Authentifizierungsprotokolle, wie sie auch der Windows NT RAS-Server unterstützt, also PAP und CHAP. MS-CHAP verwendet den MD4-Hash-Algorithmus oder das DES-Verfahren. Eine zusätzliche Authentifizierung kann im Gateway des ISP implementiert werden. Zur Verschlüsselung nutzt PPTP die Möglichkeiten von PPP. Wenn ein User über CHAP beim entsprechenden Netzwerk-Server authentifiziert wurde, so erhält er einen Session-Key mit dem die Daten verschlüsselt werden. Zur Sicherung der Datenübertragung kann das Protokoll einen 40- oder 128-bit großen Schlüssel verwenden.

Die Microsoft-Implementation von CCP (Compression Control Protocol) besitzt ein Bit, das die Verwendung von Verschlüsselung signalisiert. RAS-Clients können deshalb Verbindungsanforderungen nur mit eingeschalteter Verschlüsselung vornehmen. Ob eine Verschlüsselung dann nach der Verbindungsaufnahme weiter benutzt wird bzw. werden soll, das wird im RAS-Server konfiguriert. PPTP-Sessions über das Internet sollten immer mit eingeschalteter Verschlüsselung erfolgen.

Die Netzwerksicherheit kann durch PPTP-Filterung erhöht werden. Bei aktivem Filter akzeptiert und routet der Server nur Pakete autorisierter Benutzer. Dadurch werden alle anderen Pakete nicht in das private Netz weitergeleitet.

Der PPTP-Datenverkehr wird über den Port 1723 abgewickelt, die Transportbenutzer-ID für das IP ist 47 und durch die Internet Assigned Numbers Authority, IANA, zugewiesen. Damit kann PPTP zusammen mit den meisten Firewall- und Routersystemen eingesetzt werden. Die Systeme müssen dazu lediglich den Datentransport über den Port erlauben

Im Folgenden wird ein typisches PPTP-Szenario beschrieben.

Typisches PPTP-Szenario

Ein typisches PPTP-Szenario kann wie folgt beschrieben werden. Wir beginnen mit einem remote oder mobilen PPTP Client, der den Zugriff auf ein privates Unternehmensnetzwerk benötigt. Als Transportnetz dient das Internet, und ein ISP stellt das Gateway für die Einwahl zur Verfügung. Clients unter Windows NT benutzen dazu das DFÜ-Netzwerk mit dem PPP-Protokoll.

Nach Verbindungsaufbau kann der Client Daten in das Internet senden und aus diesem empfangen, wobei das Gateway TCP/IP als Transportprotokoll verwendet. Nach dem ersten Einwählen erfolgt eine zweite Verbindungsaufnahme. Diesmal auf der Basis der bestehenden PPP-Verbindung. Dieser zweite Connect erzeugt eine VPN-Verbindung mit einem PPTP-Server auf der Gegenseite, der dann den Zugriff auf das interne Unternehmensnetzwerk erlaubt. Die jetzt übertragenen Pakete sind IP-Datagramme, in die PPP-Pakete gekapselt sind. Als Ergebnis haben wir also einen Tunnel.

Die folgende Grafik demonstriert das Prinzip.

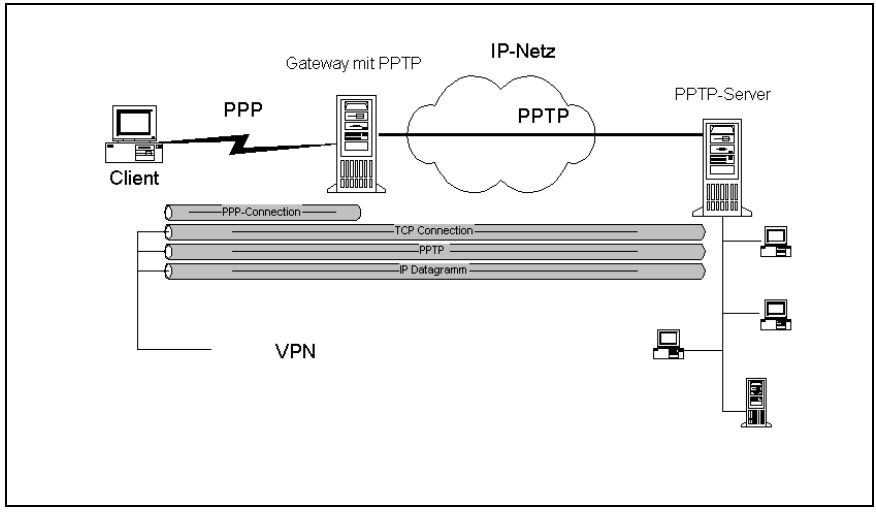


Abbildung 6.18: VPN mit PPTP

Das Szenario macht auch deutlich, dass die gesamte PPTP-Kommunikation zwischen dem Gateway des ISP und dem PPTP-Server stattfindet.

KAPITEL 7

7 Samba – ein SMB Server unter Linux

Dieser Abschnitt soll Ihnen einen kurzen Überblick über die Einsatzmöglichkeiten eines Samba-Servers geben. Natürlich kann aufgrund der Komplexität des Themas dadurch kein komplettes Buch über Samba ersetzt werden. Vielmehr sollen hier die grundlegenden Funktionen sowie deren Verwendung erklärt werden. Zunächst jedoch soll die Frage geklärt werden, was Samba eigentlich ist.

Bei Samba handelt es sich um die Implementierung eines SMB (Server Messages Block) Protokollservers, der geschrieben in C, als Open Source Produkt auf fast jedem UNIX-Derivat wie zum Beispiel

- ✔ SCO
- ✔ OSF1
- ✔ AIX
- ✔ Solaris2.x
- ✔ SunOS 4.x
- ✔ Linux
- ✔ Irix
- ✔ Ultrix
- ✔ HP-UX

ausgeführt werden kann. Unter dem Aspekt einer immer größer werdenden Akzeptanz von Samba, erfolgte auch eine Portierung auf die nachfolgend auszugsweise aufgeführten Betriebssysteme:

- ✔ MVS
- ✔ OS/2
- ✔ VMS
- ✔ Amiga
- ✔ Stratus-VOS
- ✔ MPE/iX

Mit Hilfe eines SMB-Protokollservers können nun Microsoft-Clients Dateien und Drucker benutzen, die sich auf einem UNIX-Server befinden, so als wäre dieser ein Windows-Server. Dabei ist dieser Vorgang so transparent, dass die Windows-Anwender selbst in der Regel nicht wissen, dass ihre Zugriffe auf einem Unix-System ausgeführt und umgesetzt werden.

Darüber hinaus kann Samba auch dazu verwendet werden, die Anmeldeauthentifizierung eines Microsoft-Client entgegenzunehmen. Neben serverbasierten Benutzerprofilen können dabei auch Login-Skripte auf einem Samba-Server verwaltet werden. Dadurch wird in einem heterogenen Netzwerk mit Microsoft Windows-Clients die Verwaltung erheblich vereinfacht.

Zusammenfassend sprechen folgende Punkte für den Einsatz von Samba:

- ✔ Samba ist ein frei erhältliches Open Source Produkt.
- ✔ Samba ermöglicht die Authentifizierung von PC-Logins.
- ✔ Samba erlaubt die Datei- und Druckerfreigabe auf UNIX-Servern zur Verwendung von Microsoft-Clients.
- ✔ Samba ist ein kostengünstiger und leistungsfähiger Ersatz für einige Server- Betriebssysteme.
- ✔ Es zeichnet sich ein wachsender Arbeitsmarkt für Samba-Administratoren ab.

Für das Verständnis von Samba spielt SMB eine entscheidende Rolle, da wir es hier, wie oben schon erwähnt, mit einem SMB-basierten Server zu tun haben. Aus diesem Grunde finden Sie im folgenden Kapitel einen Überblick zu SMB. Weitere Basisinformationen hierzu finden Sie in Kapitel 5.2 NetBIOS.

7.1 Server Message Block – das Protokoll SMB

Erstmals definiert wurde SMB in einem Microsoft/Intel-Dokument namens »Microsoft Networks/OpenNET-FILE SHARING PROTOCOL« im Jahr 1987. Das Server Message Block (SMB) ist ein Client-Server-Protokoll, das wie ein »Umschlag« fungiert über den die eigentliche Netzkommunikation in einem Microsoft- oder OS/2-Netz abläuft. Wenn die Clients sich über ein Netzwerkprotokoll mit dem Server verbunden haben, können sie Kommandos, und das genau sind SMBs, zum Server schicken, die es ihnen erlauben, auf Freigaben zuzugreifen, und diese wie ein eigenes Dateisystem, das auch geschützt sein kann, zu behandeln.

Die aktuelle Version lautet NT LM 0.12 und ist, wie der Name schon andeutet, eine spezielle Version für Windows NT. Es gibt also eine Menge von unterschiedlichen SMB- Dialekten auf dem Markt. Jedoch gilt für alle Dialekte, dass sich der Client beim Server authentifizieren muss, um einen Zugriff aus dessen Ressourcen zu bekommen.

SMB selbst wird dabei auf einem anderen Netzprotokoll, wie TCP/IP, IPX/SPX oder NetBIOS aufgesetzt. Die folgende Grafik zeigt die entsprechende Position von SMB im OSI-Modell.

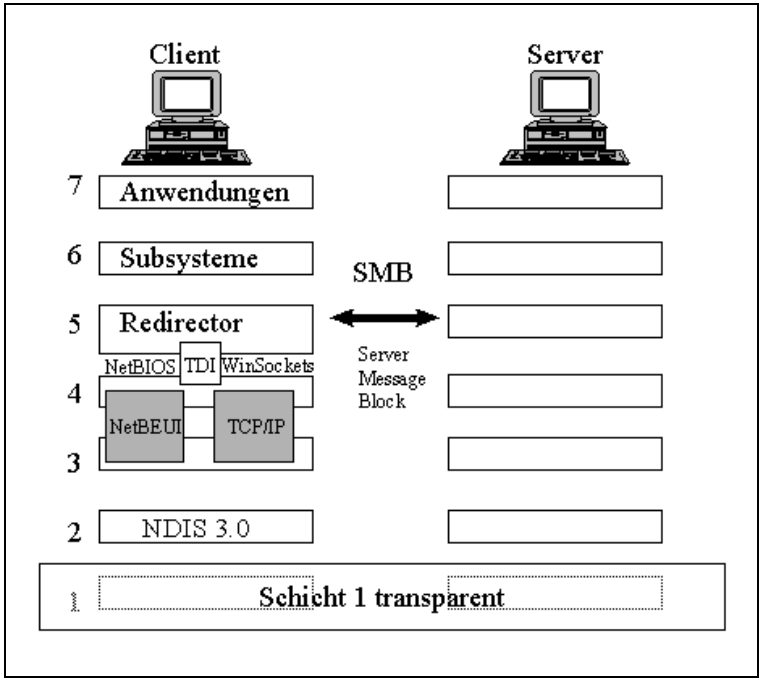


Abbildung 7.1: SMB im OSI-Modell

Eine der wichtigsten Aufgaben von SMB ist es, Dateien, Verzeichnisse, Drucker und andere Ressourcen über ein Netzwerk verfügbar zu machen. Vergleichbar mit Network File System von UNIX oder auch NCP, Netware Core Protocol, arbeitet SMB also damit auf den OSI-Layern 5 bis 7.

Leistungsmerkmale sind:

- ✔ Protokoll für Microsoft und OS/2 Netzwerk-Anwendungen
- ✔ Client-Server-Ptotokoll
- ✔ Entwickelt für DOS (LAN-Manager), für Windows 3, Win9x, NT und 2000 jeweils erweitert
- ✔ Basierend auf NetBIOS
- ✔ OSI-Schichten 5-7

Die wesentlichen Dienste sind:

- ✔ Zugriff auf entfernte Dateien
- ✔ Zugriff auf entfernte Drucker

- ✔ Verzeichnis der Netzwerk-Ressourcen (Browsing-Dienst)
- ✔ Benutzer-Authentifizierung
- ✔ SMB-Core-Dienste
  - TREE CONNECT
  - TREE DISCONNECT
  - OPEN FILE
  - CREATE FILE
  - CLOSE FILE
  - FLUSH FILE
  - READ
  - WRITE
  - SEEK
  - CREATE DIRECTORY
  - DELETE DIRECTORY
  - DELETE FILE
  - RENAME FILE
  - GET FILE ATTRIBUTES
  - SET FILE ATTRIBUTES
  - LOCK RECORD
  - UNLOCK RECORD
  - MAKE NEW FILE
  - CHECK PATH
  - GET SERVER ATTRIBUTES
  - NEGOTIATE PROTOCOL
  - FILE SEARCH
  - CREATE PRINT FILE
  - CLOSE PRINT FILE
  - WRITE PRINT FILE

In der folgenden Tabelle wird der Aufbau des Headers des SMB Protokolls beschrieben. Da es sich bei SMB um ein Protokoll der Layer 5 bis 7 handelt, gibt es eine Vielzahl von Einstellungsmöglichkeiten und Überwachungsfunktionen innerhalb des Headers. Damit sich die Entschlüsselung und Analyse etwas einfacher gestaltet, wurden die Flags in Gruppen aufgeteilt, die so genannten »ParameterWords fields«.

ParameterWords field	Beschreibung / Aufgabe
Command	Enthält den Opcode des jeweiligen SMB Teilnehmers
Status.DosError.Error.Class Status.DosError.Error	Dient zur Übermittlung von Fehlermeldungen
Flags Flags2	Enthalten Bits, die in Abhängigkeit des jeweiligen SMB Dialektes gesetzt werden, um die Leistungsfähigkeit des Clients zu übermitteln
PidHigh	Wird für das NtCreateAndX-Kommando benötigt
Connectionless.Sid Connectionless.SequenceNumber	Für datagrammorientierte Protokolle wie z.B. IPX oder UDP
StreamProtocol.SMBLength	Für Datastream-Protokolle wie TCP/IP
Uid	Wird vom Server gesendet und identifiziert den Client
Tid	Identifiziert das Unterverzeichnis des Servers, auf das der Client zugreifen will
Pid	Wird vom Client erzeugt, um einen Prozess des Clients eindeutig zu identifizieren
Mid	Für Multiplexbetrieb

Tabelle 7.1: Parameter im SMB-Header

7.1.1 Austausch von SMB-Nachrichten

Welches zugrunde liegende Protokoll verwendet werden soll spielt hier eine untergeordnete Rolle, da SMB wahlweise mit TCP/IP, NetBIOS, NetBEUI oder auch mit IPX/SPX arbeiten kann.

Der erste SMB Austausch bei einer Kontaktaufnahme mit dem Server ist immer ein `negprot` SMB, Negogiate Protocoll. In diesem schickt der Client eine Liste der Protokolle welche er unterstützt. Der Server antwortet darauf mit der Nummer des Protokolls das er benutzen möchte, oder jedoch mit einer Ablehnung, wenn kein gemeinsames Protokoll gefunden werden kann. Auch weitere Kommunikationsparameter, wie z.B. Puffergrößen, werden in diesem ersten Schritt ausgetauscht.

Wurde das gemeinsame Protokoll erfolgreich ausgehandelt, kann der Client sich beim Server anmelden. Dies erfolgt über einen `sessetupX` SMB, welcher ein Passwort und ggf. einen Usernamen enthält. Der Server schickt sodann eine Antwort, in der bei gültiger Anmeldung eine UID (User ID) enthalten ist, die bei zukünftigen Zugriffen verwendet wird.

Nach einer erfolgreichen Anmeldung kann der Client nun eine Ressource anfordern. Dazu gibt der Client in einem `tconX` SMB den Namen der Ressource an, auf die er zugreifen möchte. Steht dem Zugriff nichts entgegen, antwortet der Server mit einer TID (Tree ID), welche die Ressource bei zukünftigen Zugriffen eindeutig identifiziert.

Nachdem eine Verbindung mit der Ressource eingerichtet wurde, können nun mit »open SMB's« Dateien geöffnet und mit »read SMB's« und »write SMB's« wahlweise beschrieben oder gelesen werden. Um die Dateien wieder zu schließen, verwendet man »close SMB's«.

Will ein Client auf die Ressourcen des Servers zugreifen, so werden also eine Reihe von Befehlen und Nachrichten, eben die **S**erver **M**essage **B**locks, ausgetauscht. Nachfolgend wird eine typische Kommunikation von einem Client zu einem *user level server* beschrieben. Der Client soll eine Sitzung eröffnen, um auf eine Datei öffnend und lesend zuzugreifen. Danach soll die Datei geschlossen und die Verbindung wieder beendet werden.

Kommando des Clients	Bedeutung und Antwort des Servers
SMB_COM_NEGOTIATE	Erste Nachricht an den Server. Sie enthält eine Liste der vom Client unterstützten Dialekte. Der Server antwortet mit dem SMB Dialekt, der benutzt werden soll.
SMB_COM_SESSION_SETUP_ANDX	Überträgt den Username und das Passwort des Clients. Falls OK, sendet der Server die Uid zurück.
SMB_COM_TREE_CONNECT	Enthält den Namen des Fileshares, auf den der Client zugreifen will. Der Server gibt mit dem Tid den tatsächlichen Ort des Verzeichnisses zurück.
SMB_COM_OPEN	Enthält den Namen der Datei, die der Client öffnen will. Der Server sendet eine fid (File ID) zurück, die der Client zum Zugriff auf die Datei benutzen muss.
SMB_COM_READ	Der Client sendet die Tid, fid, den Datei-Offset und die Anzahl der Bytes, die er lesen will. Der Server sendet daraufhin die angefragten Daten an den Client.
SMB_COM_CLOSE	Der Client schließt die Datei, der Server quittiert dies.
SMB_COM_TREE_DISCONNECT	Client schließt die Verbindung zum Fileshare.

Tabelle 7.2: SMB-Session

7.1.2 Das SMB Sicherheitskonzept

Im SMB-Protokoll sind grundsätzlich zwei verschiedene Sicherheitsmodi definiert, *share-level* und *user-level*. In Samba gibt es zusätzlich noch zwei weitere Modi, die eine Erweiterung des *user-level* Modus darstellen. Im Folgenden finden Sie die Erklärung der verschiedenen Modi, die in dieser Weise auch als Parameter z.B. für die Sambakonfigurationsdatei zu finden sind.

- ✔ **Share:** *share mode* bedeutet, dass jede Freigabe nur durch ein Passwort geschützt ist, also für jeden nutzbar, der das Passwort kennt.
- ✔ **User:** *user mode* bedeutet, dass der Server den Client bei der Anmeldung (beim ersten Zugriff auf irgendeine Ressource) nach einem Namen und Passwort fragt, und daran feststellt, ob ein solches Konto existiert und das zugehörige Passwort stimmt (Authentifizierung). Ist der Benutzer einmal authentifiziert, erhält er eine UID (User ID) und hat nun prinzipiell die Möglichkeit, auf alle Ressourcen zuzugreifen, was in der Praxis jedoch durch die Berechtigungen für die einzelnen Shares verhindert werden kann (Authorisation). Dieser Modus ist dem einfacheren *share mode* vorzuziehen, wenn man unterschiedliche Rechte für unterschiedliche Benutzer festlegen will.
- ✔ **Server:** *server mode* gleicht dem *user mode*, mit der Ausnahme, dass Samba Namen und Passwort an einen anderen Server weiterreicht, der dann den Benutzer authentifiziert. Kann Samba sich erfolgreich am Passwort Server anmelden, lässt es auch die Anmeldung des Clients zu. Dies kann dazu dienen, mehrere SMB-Server mit nur einer Benutzerdatenbank zu betreiben.
- ✔ **Domain:** *domain mode* gleicht ebenfalls dem *user mode* mit der Ausnahme, dass die Authentifizierung an einem Domänencontroller stattfindet, weshalb hier auch der Rechnername überprüft wird, weil ein Computerkonto für diesen Rechner in der Domäne existieren muss.

7.1.3 Zukunft

Das SMB Protokoll soll vom NetBIOS-Protokoll entkoppelt werden und nativ über TCP/IP arbeiten, wobei dann die Namensauflösung über DNS laufen soll. Das neue Protokoll heißt dann *CIFS*, Common Internet File System. Weitere Neuerungen stehen mit Kerberos V, Active Directory und der Änderung des NT-Domänensystems in ein dem DNS angeglichenes Format als hierarchisches Domänensystem an.

7.2 Samba als Fileserver

Die bekannteste Anwendung eines Servers ist der Fileserver. Dieser Servertyp stellt Benutzern Festplatten oder andere Ressourcen in einem Netzwerk zur Verfügung. In der Regel bemerkt ein Anwender bei der Bedienung jedoch keinen Unterschied zwischen seiner eigenen lokalen Festplatte und einem Netzlaufwerk. Die Vorteile eines Netzlaufwerks bzw. Netzverzeichnisses (Share) liegen dabei auf der Hand. So wird unter Verwendung eines Netzlaufwerkes der lokal verfügbare Massenspeicherplatz vergrößert, besser optimiert und ausgenutzt. Des Weiteren wird auf einen zentralen Datenbestand gemeinsam zugegriffen, und es können Daten untereinander ausgetauscht werden. Auch ein

zentrales Backup (Datensicherung) des Fileservers wird somit ermöglicht, so dass die Aufgabe und Verantwortung der Dateisicherung nicht mehr beim Benutzer liegt.

Um einen Datenverlust oder einen unberechtigten Zugriff zu verhindern, erfolgt im einfachsten Falle der Zugriff der einzelnen Anwender in der Regel über ein Kennwort. Bei einer komplexeren Lösung hingegen wird eine zusätzliche Benutzerkennung und ein dazugehöriges Passwort verlangt. Dies stellt einen weitaus höheren Sicherheitslevel dar, da es sich um eine logische UND-Verknüpfung handelt und der Zugriff auf die Ressourcen nur dann erfolgt, wenn beide Informationen korrekt eingegeben werden. Eine komplexe Lösung hat den Vorteil, dass jeder Benutzer über differenziertere Zugriffsrechte verfügen kann.

7.3 Serverbasierte Profile

Für jeden Benutzer unter MS-Windows9.x, MS-Windows NT sowie MS-Windows 2000 wird standardmäßig ein eigenes Benutzerprofil angelegt. Dieses Benutzerprofil beinhaltet die aktuellen Desktop-Einstellungen der einzelnen Anwender. Normalerweise wird ein Benutzerprofil lokal auf dem eigenen Computer abgespeichert und steht somit auch nur dort zur Verfügung. Deshalb muss ein Anwender seine persönlichen Desktop-Einstellungen auf allen Systemen, an denen er arbeitet, beim jeweils ersten Zugriff erneut einstellen.

Dies kann man vermeiden, indem man serverbasierte Benutzerprofile verwendet. Zentral auf einem Server abgespeichert, stehen diese dann in der gesamten Netzwerk-Umgebung zur Verfügung. Der Vorteil liegt auf der Hand. Ein Anwender kann sich nun wechselweise an verschiedenen Clients anmelden und bekommt dennoch immer seine eigene Arbeitsumgebung an jedem Client innerhalb des Netzwerkes zur Verfügung gestellt. Serverbasierte Profile funktionieren aber nur in einer Netzwerkumgebung die mit einem Domain-Controller organisiert ist. Dies kann ein Primary-Domain-Controller unter NT 4.0, ein Domain-Controller unter Windows 2000 oder aber eben auch ein Samba-Server sein.

Momentan ist Samba jedoch noch kein vollwertiger Ersatz für einen NT-Domain- Controller, da man nicht auf alle Funktionen eines PDC zurückgreifen kann. So fehlt z.B. der Benutzer-Manager für Domänen, oder aber auch der Server-Manager. Zum Speichern der Benutzerprofile und zur Authentifizierung der Clients reicht der Funktionsumfang von Samba aber vollständig aus.

7.4 Installation von Samba

Generell stehen Ihnen zwei Möglichkeiten zur Installation von Samba zur Verfügung. Verwenden Sie ein kommerzielles Unix, wie z. B. SCO oder AIX, so müssen Sie sich Samba erst aus dem Internet herunterladen. Eine der aktuell geeigneten Versionen für den Einsatz in einer Produktionsumgebung ist die Version 2.0.6. Durch die rasche Weiterentwicklung von Samba 2.x empfiehlt es sich jedoch, die verfügbaren Releases kontinuierlich zu überprüfen und gegebenenfalls auch neu zu beziehen. Über den Web-Server http://www.samba.org oder aber über den FTP-Server ftp://ftp.samba.org/pub/samba können die aktuellen Quellpakete bezogen werden.

Auf diesen Seiten finden Sie Links zu allen Samba-Mirror-Websites und den FTP-Mirrors. In kurzen und regelmäßigen Abständen werden auf diesen Mirror-Servern (Spiegel-Server) Dateien von den Originalservern gespiegelt. Ein deutscher Mirror-Server ist beispielsweise der FTP-Server der Universität Trier. Unter der Adresse ftp://ftp.uni-trier.de/pub/unix/network/samba finden Sie die jeweils aktuelle Version von Samba.

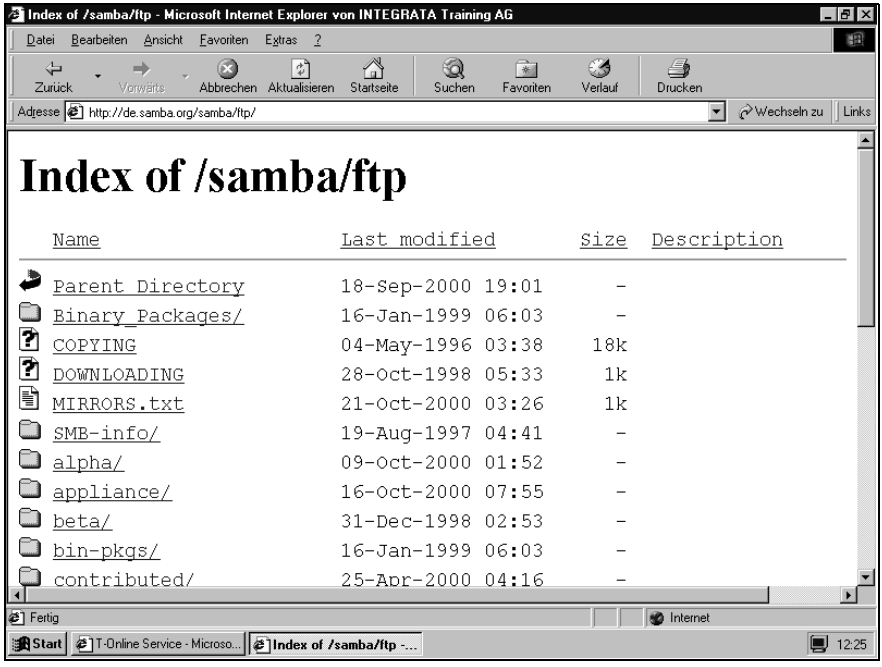


Abbildung 7.2: FTP-Server mit Samba-Quellcode.

Je aktueller die verwendete Version, desto besser und sicherer ist auch die Unterstützung der Domänen-Funktionen. Anders als bei den Versionen 1.x liegt der Schwerpunkt von Samba 2.x, auf der Anbindung an das Serverbetriebssystem Windows NT 4.0 bzw. den Client-Systemen Windows9.x.

7.4.1 Installationsbeispiel unter SuSE-Linux 6.2

Verwenden Sie hingegen eine Linux-Serverinstallation wie z.B. SuSE-Linux 6.2 oder höher ist Samba standardmäßig im Lieferumfang enthalten, wenn auch nicht immer auf dem aktuellsten Stand. Eine bereits installierte Linux-Serverinstallation kann mit dem Kommando

```
rpm -qa grep samba
```

jederzeit überprüft werden. In der Basisversion von SuSE-Linux 6.2 steht wie bereits erwähnt eine übersetzte Version des Samba-Servers zur Verfügung. Anhand der folgenden Schritte werden die benötigten Pakete installiert.

1. Melden Sie sich als root an Ihrem System an. Starten Sie an der Kommandozeile das Programm yast über den Befehl `linux:/root# yast`
2. Über den Menüpunkt **Installation festlegen/starten** gelangen Sie zur Serienauswahl. Markieren Sie das Paket Samba und bestätigen Sie die Auswahl mit der F10 -Taste.
3. Nachdem Sie das Paket Samba ausgewählt und bestätigt haben, gelangen Sie durch ein weiteres Betätigen der F10 -Taste wieder zurück zum Installationsmenü.
4. Gestartet wird die eigentliche Installation dann mit dem Menü-Punkt **Installation starten**. Wurde das Paket erfolgreich installiert, kann die Installationsroutine nun mit Esc wieder verlassen werden.

Nach der hoffentlich erfolgreichen Installation des Paketes steht Ihnen jetzt der Samba-Server zur Verfügung. Innerhalb der SuSE-Linux-Distribution finden Sie dann die einzelnen Dateien im unten aufgeführten Verzeichnisbaum.

Komponente	Pfad
Dienstprogramme	/usr/bin (smbclient.....)
Serverprogramme	/usr/bin (smbd.....)
Konfigurationsdateien	/etc (smb.conf.....)
Dokumentation	/usr/doc/packages/samba
Startup-Programme	/sbin/init.d/smb

7.4.2 Installationsbeispiel von Samba über das Quellpaket

Ein weiteres Beispiel zeigt die grundlegende Vorgehensweise einer Installation von Samba über das Quellpaket. Um eine Installation korrekt und fehlerfrei durchführen zu können, müssen Sie als root an ihrem System angemeldet sein.

1. Laden Sie das zu installierende Paket vom Zielhost. Suchen Sie zu diesem Zweck auf dem Web-Server http://de.samba.org/samba/ftp, eine Datei namens samba-latest.tar.gz. Sollten Sie diese Datei nicht finden, suchen Sie

nach samba-#####.tar.gz mit der höchsten Versionsnummer. In unserem Beispiel handelt es sich um die Datei samba-2.0.6.tar.gz. Dateien mit der Dateierweiterung .tgz und .tar.gz weisen dabei auf komprimierte Archive hin.

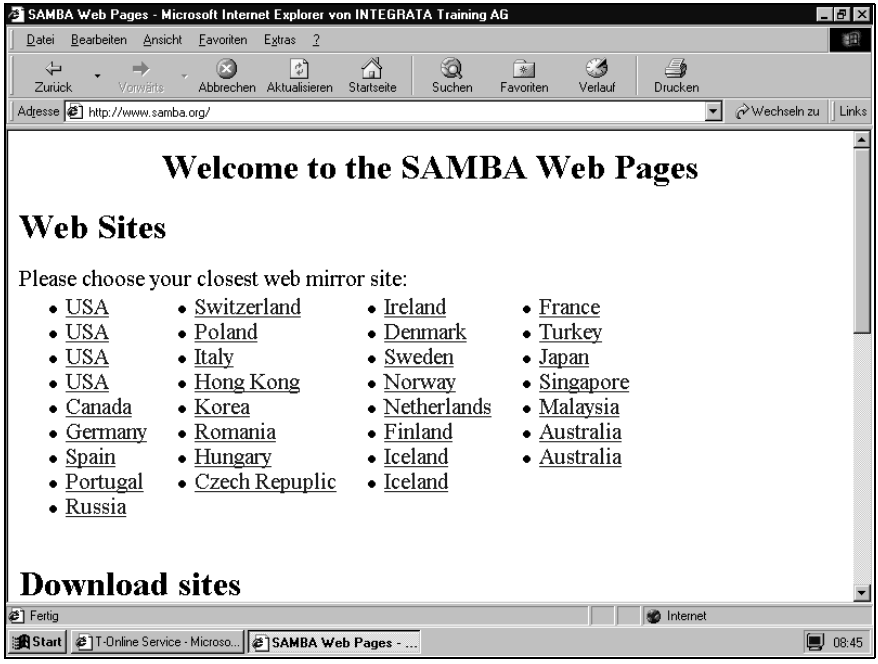


Abbildung 7.3: Samba Web-Sites

2. Kopieren Sie das Tar-Archiv in das Verzeichnis /usr/local/src und wechseln Sie anschließend in dieses Verzeichnis.
3. Starten Sie zum Entpacken des Tar-Archives das Programm tar mit dem Kommando: `linux:/usr/local/src# tar -xvzf ./samba-2.0.6.tar.gz`. Unter dem Verzeichnis samba-2.0.6 steht anschließend der Quellcode zur Verfügung. Wechseln Sie in dieses Verzeichnis.
4. Starten Sie dann die automatische Konfiguration mit `linux:/usr/local/src/samba-2.0.6/source#./configure`.
5. Abgeschlossen wird die Installation durch die Eingabe von `linux:/usr/local/src/samba-2.0.6/source#./make all` und `linux:/usr/local/src/samba-2.0.6/source# ./make install`

Durch diese Kommandos werden die Quelldateien übersetzt und im Binärpfad installiert. Auch nach dieser Installationsart stehen Ihnen die einzelnen Dateien wie in Kapitel 7.5 beschrieben im Verzeichnisbaum zur Verfügung.

7.4.3 Anpassung der Konfigurationsdatei smb.conf

Nachdem der Samba-Server installiert und lauffähig ist, muss noch die Konfigurationsdatei smb.conf für die Verwendung z.B. als Domain-Controller angepasst werden. Zu diesem Zweck steht eine Vielzahl von variablen Parametern zur Verfügung. Diese Parameter finden Sie im globalen sowie in weiteren Abschnitten, die Sections genannt werden. Kommentare in der Datei smb.conf werden dabei mit dem Zeichen Semikolon (;) oder aber auch mit dem Zeichen Raute (#) dargestellt. Die Kommentare enden mit einem Zeilenumbruch.

Der Abschnitt [global]

In der globalen Section der smb.conf befinden sich Parameter, die für die allgemeine Funktionalität des Samba-Servers von großer Bedeutung sind. Typische Parameter in diesem Abschnitt sind Einstellungen, die das Verhalten der

- ✔ Dienste bei Zugriffen,
- ✔ Zugriffsrechte von Diensten,
- ✔ Netzwerksoftware bei Zugriffen,
- ✔ Namen und Kommentare

und andere Funktionen steuern bzw. beeinflussen.

Hier ein kurzer Auszug von [global] mit einigen mögliche Einstellungen:

Einstellung	Bedeutung
[global]	Beginn globaler Bereich
netbios name = snav	Netbios-Name des Servers, Standardwert ist Hostname
workgroup = clk	Arbeitsgruppenname
server string = clk	Text der neben dem Rechnernamen in Browser-Listen angezeigt wird
security = user	Authentifizierung im User-Modus
domain logons = yes	Aktiviert die Funktionen des Domain Controllers
encrypt passwords = no	Verwendung verschlüsselter Passwörter, Standard ist no
name resolve order =	Reihenfolge der Namensauflösung; Standard lmhosts hosts wins bcast
wins support = yes	Verwendung eines WINS-Servers
wins server = 7.4.16.61	IP-Adresse des WINS-Servers

Tabelle 7.3: Globaler Bereich smb.conf

Beispiel: Samba als Domain Controller

Durch das Schlüsselwort domain logons werden z.B die Funktionen des Domain- Controllers aktiviert. Die security Einstellung muss dabei zwingend auf **user** eingestellt werden, da der Server ja selbst die Authentifizierung der Benutzer entgegennimmt. Wird jedoch ein anderer Domain-Controller als Anmeldeserver verwendet, so lautet der Schlüssel für security dann domain.

Der Abschnitt [homes]

Die Section homes als spezielle Freigabe ermöglicht es den Benutzern auf ihre Home-Verzeichnisse zuzugreifen, ohne dass eine besondere Freigabe für jeden einzelnen Benutzer angelegt werden muss. Durch diese automatische Freigabe können viele Anwender mit einem minimalen Konfigurationsaufwand verwaltet werden.

Mögliche Einstellungen aus dem Abschnitt [homes] sind:

Einstellung	Bedeutung
[homes]	Beginn Home-Bereich
comment = Unix	Kommentarzeile
browseable = yes	Freigaben werden im Browser angezeigt.
writeable = yes	Freigabe soll beschreibbar sein.

Tabelle 7.4: Home Bereich smb.conf

Der Abschnitt [printers]

Ähnlich wie *homes* erlaubt auch die Section *printers* den Zugriff auf eine Ressource, jedoch auf eine automatische Freigabe von Druckern. Auch hier ein kurzer Auszug aus einem Abschnitt [printers]:

Einstellung
[printers]
comment = My printers
browseable = no
printable = yes
public = no
read only = yes
Variable-Substitution

Tabelle 7.5: Printer Bereich smb.conf

Die folgenden Variablen werden in der Konfigurationsdatei smb.conf verwendet und während des Ablaufes analysiert und entsprechend der Werte ersetzt.

Variable	Bedeutung
%a	= arcitecture, Betriebssystem-Architektur des Remote Host. Aktuell werden die Betriebssysteme WinNT, Samba, Win95 und WfW erkannt.
%d	= daemon, gibt die Prozessnummer des aktuellen Samba-Servers aus
%g	= group, Name der Gruppe in der %u Mitglied ist
%G	= Group, Name der Gruppe in der %U Mitglied ist
%h	= hostname, Internet-Name des Samba-Servers
%H	= home, Benutzerverzeichnis von %u
%I	= ip-adress, IP-Adresse des Clients
%L	= Netbios-Name des Samba-Servers
%m	= Netbios-Name des Clients
%M	= Internet-Name des Clients
%P	= path, das Root-Verzeichnis des aktuellen Dienstes
%R	= Gibt das verwendete Protokoll aus
%S	= service, Name des aktuellen Freigabedienstes
%T	= time, aktuelles Datum und Zeit
%u	= user, Benutzername der aktuellen Freigabe
%U	= User, Login-Name des Benutzers
%v	= Liefert die Samba-Versionsnummer

Tabelle 7.6: Variablen in smb.conf

BEISPIEL Ein Samba-Server verfügt über die IP-Adresse 7.4.19.61. Deshalb wird die Variable %I auf die IP-Adresse 7.4.19.61 gesetzt.

Die folgende Konfigurationsdatei ist ein Beispiel für den Einsatz von Samba als Fileserver.

```
[global]

        workgroup = TNSO
        netbios name = Andromeda
        netbios aliases = Fileserver
        server string = TNSO Fileserver
        interfaces = 192.168.105.1/255.255.255.0 192.168.105.200/
255.255.255.0

        security = share
        encrypt passwords = Yes
        map to guest = Bad User
        keepalive = 30
        socket options = TCP_NODELAY
        load printers = No
        os level = 2
        guest account = ftp
```

```
[download]
        path = /usr/local/ftp/download
        read only = Yes #<- Ist halt nur zum Runterladen
        guest ok = Yes

[Austausch]
         path = /usr/local/ftp/download
         read only = No
         guest ok = Yes
```

7.5 Verzeichnissystem im Überblick

Der Samba-Server besteht aus verschiedenen Komponenten, die in den folgenden Verzeichnissen abgespeichert werden.

Verzeichnis	Beschreibung
bin	Programmverzeichnis
lib	Konfigurationsverzeichnis von Samba
man	Manuals und Dokumentation make_smb
codepage	make_smbcodepage erstellt Code-Tabellen zur internationalen Anpassung der verwendeten Zeichensätze
netlogon	Verzeichnis für Anmeldeskripte
nmblookup	Abfrage von NetBIOS-Namensinformationen
nmbd	NetBIOS-Nameserver zur Verarbeitung von Anfragen zur Namensregistrierung
private	Besondere Datendateien von Samba
smbclient	Stellt ähnlich FTP Funktionen zum Zugriff auf das Netzwerk zur Verfügung
spool	Verzeichnis zum Spoolen der Druckaufträge
smbstatus	Generiert Ausgaben über den aktuellen Status von Verbindungen und Dateien
smbtar	Ein Shell-Skript, welches Dateien über das Tool smbclient auf UNIX-Bandlaufwerke sichert und auch wiederherstellt
smbd	Stellt Datei- und Druckdienste im Windows Netzwerk zur Verfügung
smbrun	Agierend als Interface können dann über smbd bestimmte Shell-Skripte gestartet werden
smbpasswd	Ermöglicht das Ändern von verschlüsselten Passwörtern für Windows-NT- und Samba-Server
swat	Administratortool zur Verwaltung der smb.conf mit grafischer Benutzeroberfläche
testparm	Lokalisiert fehlerhafte Einstellungen in der Konfigurationsdatei smb.conf
testprns	Überprüft ob ein Druckername auch als Freigabename benutzt werden kann
var	Debug-Dateien der Samba-Server

Tabelle 7.7: Samba-Systemverzeichnisse

7.6 SWAT

Natürlich sollte ein Samba-Server vor einem Einsatz in einer Produktionsumgebung noch ausreichend getestet werden. Auch wenn nicht allen Fehlern vorgebeugt werden kann, so sollten doch grobe Fehler auf jeden Fall im Vorfeld behoben werden. Zu diesem Zweck stehen unter Samba verschiedene Tools zur Verfügung. Eines dieser Administratortools ist SWAT, Samba Web Administration Tool.

SWAT selbst ist eine neue Funktion, die ab den Samba-Versionen 2.x integriert ist. Mit Hilfe von SWAT kann von jedem Rechner im Netzwerk über einen Browser die Samba-Konfiguration eingesehen und bei Bedarf auch verändert werden. Eine Anzeige aller Samba-Man-Pages als HTML-Seiten ist ebenso möglich wie die Anzeige des Server-Status oder aber das Starten und Stoppen des Servers. Eine Passwortänderung kann ebenfalls über SWAT durchgeführt werden.

Über grafische Web-Seiten des Browsers steht somit eine komfortable Benutzeroberfläche zur Verfügung. Nachdem SWAT installiert ist, müssen die folgenden Dateien nur noch modifiziert werden. Unter den neueren SuSE Distributionen sind die gezeigten Einträge schon vorhanden und müssen deshalb lediglich auskommentiert werden:

In der Datei /etc/services steht:

```
#
# swat is the Samba Web Administration Tool
#
swat 901/tcp
```

In der Datei /etc/inetd.conf steht:

```
#
# swat is the Samba Web Administration Tool
swat stream tcp nowait.400 root /usr/sbin/swat swat
```

Um die Dienste dann tatsächlich zu aktivieren, können Sie wahlweise den INETD Dämon neu starten oder auch einen Systemstart durchführen. Nach der Aktivierung von SWAT stehen dem System folgende Adressen zur Verfügung:

http://www/doku/ //sambaDokumentation von Samba

http://www:901 //Adresse von SWAT

Nun muss noch das X-System und ein dazugehöriger Browser aufgerufen werden. Als URL geben Sie die folgende Adresse ein.

http://localhost:901

Erfolgt der Zugriff von einem anderen an das Netzwerk angeschlossenen PC, ändert sich lediglich die URL. Hier lautet die Adresse:

http://[serveradresse]:901

Damit wird das eigentliche Samba-Konfigurationstool aufgerufen. Nach dem Aufruf von SWAT erfolgt noch eine Autorisierung. Während der normale Benutzer lediglich Informationen zu Samba erhält, erlaubt eine Anmeldung als root die Samba-Konfiguration einzusehen und auch zu ändern.

Nach erfolgreicher Autorisierung steht das Konfigurationstool mit den sieben unten beschriebenen Menüs (HOME, GLOBALS, SHARES, PRINTERS, STATUS, VIEW, PASSWORD) zur Verfügung.

HOME

Über das Home-Menü können alle erdenklichen Informationen eingesehen werden. Sobald ein Link angeklickt wird, öffnet sich ein weiteres Browser-Fenster, und in gewohnter Fenstertechnik ergibt sich eine gute Gesamtübersicht.

GLOBALS

Über das Globals-Menü werden generelle Eigenschaften von Samba definiert. Wie oben bereits erwähnt, ist es zum Beispiel möglich einen NT Server über Samba zu realisieren. Über die unterschiedlichen Buttons kann auch die Ansicht für Fortgeschrittene, Advanced View, aktiviert werden. Diese Ansicht listet dann diverse Parameter auf, wobei zu jedem Parameter eine entsprechende Hilfe mit genauen Informationen abgerufen werden kann. Darüber hinaus können hier auch Standardwerte gesetzt werden. Dies ist in sofern nützlich, als nicht immer klar ist, welcher Wert zu welchem Parameter gehört.

SHARES

Ähnlich wie im Globals-Bereich gibt es im Shares-Bereich eine Standard- und eine Fortgeschrittene-Ansicht. Um diese jedoch nutzen zu können, muss der User erst eine Freigabe einrichten, `Create Share`. Sollte eine entsprechende Konfiguration schon vorhanden sein, so kann diese per Pull-Down Menü ausgewählt und über `Choose Share` auch aktiviert werden. Für einzelne Parameter können wie im Globals-Bereich ebenfalls Standard-Werte verwendet werden.

PRINTERS

Vom Aufbau her entspricht das Printers-Menü den Bereichen von Shares und Globals. Bevor aber die eigentliche Konfiguration erfolgen kann, muss zuerst ein Drucker erstellt werden. Dabei sollte der Druckername identisch sein mit dem Eintrag in der Datei etc/printcap. Dies bewirkt, dass nicht alle verfügbaren Drucker in der Netzwerkumgebung angezeigt werden.

STATUS

Über das Status-Menü kann der gesamte Server Status abgefragt werden. Statusinformationen sind Informationen darüber, wer momentan mit dem Server verbunden ist, welche Dateien gerade geöffnet sind oder welche Dämonen gerade ausgeführt werden.

VIEW

Das Menü View zeigt die gesamte Samba-Konfiguration so wie sie sich prinzipiell in der Datei /etc/smb.conf befindet. Auch hier gibt es zwei Bereiche, die Standard- und die Fortgeschrittene-Ansicht. Verwendet man die Standard-Ansicht, so sind die Einträge indentisch mit der Datei /etc/smb.conf. Die Ansicht Fortgeschrittene hingegen zeigt alle Parameter mit den Standardwerten.

PASSWORD

Über das Menü PASSWORD werden User angelegt, die sich vorher schon in der Datei /etc/passwd befinden. Zudem ist es noch möglich, bereits existierende Passwörter von dem Server oder den Clients zu ändern. Ein Aktivieren oder Deaktivieren von Usern kann über diesen Bereich ebenfalls durchgeführt werden.

7.6.1 Samba als NetBIOS Name-Server für Windows-Systeme

Es gibt zwei Arten von Namensauflösung. Die ursprüngliche Methode für einen Client einen Rechnernamen im LAN zu finden ist, dass er einen Broadcast mit der Anfrage ins Netz schickt und der entsprechende Rechner sich dann mit seiner MAC- bzw. IP-Adresse meldet. Die zweite Methode ist die Nutzung eines NetBIOS Name Service Servers, NBNS, bei Microsoft WINS, Windows Internet Name Service, genannt. Hierbei senden die Clients ihren Namen und ihre Adresse an diesen Server bzw. werden diese fest in einer Datenbank eingetragen. Dann können sich die einzelnen Clients bei Namensanfragen an diesen Server wenden, um von ihm die Adressen ihrer Partner zu erfragen. Das funktioniert im Gegensatz zu Broadcasts auch über Subnetze hinweg und verringert außerdem den Netzwerkverkehr durch Reduzierung der Rundsendenachrichten, was sich in größeren Netzen durchaus lohnen kann. Weitere Details zu NetBIOS und Namensauflösung finden Sie in Kapitel 5.

Über SWAT kann ein Samba-Server auch als NetBIOS-Name-Server konfiguriert werden. Dazu muss lediglich die Seite Globals für die globalen Einstellungen von Samba geöffnet werden. Aktivieren Sie die Anzeige für die Darstellung der Eingabemaske mit Hilfe von Advanced View. Soll der Samba-Server neben dem eigentlichen Namensdienst auch als Browser-Server verwendet werden, so müssen folgende Änderungen an der Konfiguration vorgenommen werden:

Die Parameter `os level = 65` und `domain master = yes` erlauben es dem Samba-Server bei den Verhandlungen um die Stellung als Master-Browser den Status des Masters für die Domäne zu gewinnen.

Durch die Einstellungen der Parameter `preferred master =yes` und `local master = yes` übernimmt der Samba-Server für das jeweilige Subnet die Aufgabe des lokalen Browser-Servers.

KAPITEL 8

8 Netzwerksicherheit

Dieses Kapitel hat die Netzwerksicherheit zum Thema. Auch hier handelt es sich um ein sehr komplexes Thema, das im Einzelfall mit Hilfe spezialisierte Literatur vertieft werden muss. Im Folgenden werden deshalb die grundlegenden Aspekte zum Thema Netzwerksicherheit behandelt. Den Schwerpunkt bildet dabei die Analyse der Sicherheitsrisiken der TCP/IP-Protokollfamilie. Wir werden dabei Techniken beschreiben, die Netzangreifer verwenden, damit Sie wissen, welche Gegenmaßnahmen zu treffen sind.

8.1 Firewalls

Jeder Übergang zwischen dem Intranet bzw. LAN und einem öffentlichen Netz bedeutet ein Sicherheitsrisiko, wobei nicht verschwiegen werden darf, dass die meisten Angriffe von innen kommen. Ein externer Angreifer will sich Zugriff auf ein internes Netz verschaffen, während der interne Angreifer sich schon darin befindet. Neben dem Zugriff auf Unternehmensdaten besteht vor allem das Risiko, dass durch Manipulation, Eindringen von Viren usw. das Netz, die Rechner oder die Daten beschädigt werden.

Jeder Zugang von außen, wie beispielsweise eine Modem- oder ISDN-Verbindung an einer Wählleitung, muss folglich durch geeignete Maßnahmen geschützt werden. Neben den verbindungsbezogenen Schutzmechanismen wie Call Back oder der Verschlüsselung von Daten können auch spezielle Zugangsrechner und Software, die so genannten Firewallsysteme, eingesetzt werden.

Die Installation von Firewalls bietet im Wesentlichen folgende Vorteile:

- ✔ Das Sicherheitsmanagement kann auf einen Punkt, nämlich die Firewall, konzentriert werden.
- ✔ Überwachungs- und Kontrollmechanismen müssen lediglich auf der Firewall installiert werden.
- ✔ Alle Verbindungen vom und zum internen Netzwerk müssen über die Firewall laufen und können somit überwacht und kontrolliert werden.

Alle Zugriffe, ob aus dem IT-Netz des Unternehmens nach außen in das WAN bzw. das öffentliche Netz/Internet oder umgekehrt, erfolgen über die Firewall. Zum besseren Verständnis werden die wichtigsten Funktionen im Folgenden beschrieben. Dabei können drei Arten von Firewalls unterschieden werden:

8.1.1 Application Level Gateways

Für jede eingesetzte Anwendung, Applikation, wird ein eigenes Gateway-Programm installiert. Anwendungen, für die kein Gateway installiert wurde, stehen im Internet nicht zur Verfügung. Nach Anmeldung am Gateway übernimmt dieses, bei entsprechender Berechtigung, die Durchführung der Transaktionen im LAN. Der Client hat somit keinen direkten Zugriff in das Netz.

Dieses Verfahren ist das aufwändigste, jedoch auch das sicherste. Nur die Funktionen und Zugriffe, die explizit erlaubt sind, sind nicht verboten. Es lassen sich benutzer- und anwendungsbezogene Zugangs- und Verbindungsprofile definieren.

8.1.2 Circuit Level Gateways

Diese Gateways arbeiten auf der Protokollebene, z.B. TCP oder UDP und prüfen, ob die Verbindung zwischen Client und Server zulässig ist. Erst wenn der Verbindungsaufbau ordnungsgemäß abgeschlossen ist, wird die Übertragung freigegeben. Bis zum Abbau der Verbindung werden alle Daten ungehindert übertragen.

8.1.3 Paketfilter

Diese Firewalltechnologie erlaubt das Herausfiltern von Paketen mit bestimmtem Inhalt, z.B. bestimmten Protokollheadern oder MAC-Adressen. Beim IP-Filtering wird der Datenverkehr aufgrund der Informationen in den einzelnen IP-Paket-Headern geregelt. Dabei werden Quell- und Zieladresse als Hauptkriterium für die Filterung verwendet. So werden z.B. Pakete vom äußeren Netz kommend mit einer Quelladresse aus dem inneren Netz abgelehnt, um Angriffe abzuwehren. Auch die angesprochenen Ports (source und destination) werden blockiert, um einzelne Dienste zu verbieten oder zuzulassen.

Man unterscheidet zwei Arten der Filterung:

- ✔ **Statische Filterung**: Filterung aufgrund genau festgelegter Regeln bezüglich der IP-Header.
- ✔ **Stateful Inspection**: Filterung kann abhängig sein von älteren Paketen, die mit dem aktuellen in Verbindung stehen. Hiermit werden Antwortpakete bei verschiedenen Diensten akzeptiert, welche bei statischer Filterung nicht erlaubt wären.

Trifft auf ein eintreffendes Paket eine Filterregel zu, so wird es entweder einfach fallen gelassen, oder dem Absender signalisiert, dass es abgelehnt wurde. Die Reaktion kann bei jeder Filterregel angegeben werden. Abgelehnte Pakete werden nach der ausgelösten Filterregel sortiert und aufgezeichnet, um später eventuelle Angriffe zu analysieren.

Weitere Funktionen eines Firewallsystems sind im Folgenden aufgelistet und je nach Hersteller unterschiedlich oder nicht realisiert:

- ✔ Filter
  - – Sender/Empfängeradresse bzw. Adressgruppe
  - – Protokolle
  - – Dienste
  - – Uhrzeit
- ✔ Protokollierung von Einbruchsversuchen oder allen Zugriffen
- ✔ Verschlüsselung ist nur möglich, wenn auf der Partnerseite ebenfalls der gleiche Verschlüsselungsalgorithmus verwendet wird.
- ✔ Spezielle Domain Name Services und ähnliche Dienste, die sowohl intern als auch extern eine Pseudowelt darstellen. Das bedeutet, dass außenstehenden Netzteilnehmern bzw. Eindringlingen eine völlig andere Netzumgebung dargestellt wird. Diese Welt wird durch den Netzadministrator aufgebaut und das interne Netz somit nach Bedarf verschleiert.
- ✔ Proxy Services bilden Funktionen nach, die von Rechnern jenseits der Barriere angeboten werden, ohne dass die eigenen Benutzer in Berührung mit diesen Systemen kommen.
- ✔ Vorspiegeln von Schwachstellen zur Ablenkung von »Angreifern« mit Alarmierung bei Einbruchsversuchen. Mit Glück und etwas Geschick des Administrators kann so eventuell sogar der Angreifer aufgespürt werden.

Die folgenden beiden Punkte sind nur für Einwahlstellen und Punkt-zu-Punkt-Verbindungen relevant:

- ✔ Abfrage der Rufnummer der Gegenseite (Caller Identification)
- ✔ Security Call Back, Rückruf der Gegenstelle anhand einer dem Passwort zugeordneten Telefonnummer

8.1.4 Physikalische Komponenten der Netztopologie

Neben den logischen Aspekten einer Firewall muss auch der physikalische Aufbau bestimmt werden. Verschiedene Möglichkeiten, Sicherheit zu realisieren sollen im Folgenden beschrieben werden.

Bastion Host

Einen Rechner, der besonders gesichert ist und als »Bollwerk« gegen Eindringlinge eingesetzt wird, nennt man Bastion-Host. Er dient der Verteidigung des lokalen Netzwerkes und sollte besondere Aufmerksamkeit vom Administrator in der Form von regelmäßigen Audits und Sicherheits-Patches erhalten.

Dual Homed Host/Gateway

Wenn ein Rechner Teil von zwei Netzen ist (mit zwei Netzwerkkarten), spricht man von einem Dual Homed Host. Oft bietet dieser Rechner auch Gateway-Funktionen an. Um hohe Sicherheit zu erlangen wird die Routing-Funktion deaktiviert. Dann können lokale und Internet-Hosts mit dem Gateway kommunizieren, aber der direkte Datenfluss wird unterbunden.

Router mit Firewall-Funktionalitäten

Es gibt viele Hersteller von Routern, die in ihre Geräte Firewall-Funktionalitäten integrieren. Dies sind meistens IP-Filter, die mehr oder weniger detailliert konfiguriert werden können. Manche Geräte aus der höheren Preisklasse bieten weitergehende Funktionen wie IP-Tunneling (VPN) oder Stateful Inspection an.

Solche »Screening Router« werden jedoch sehr oft als Teil einer Firewall eingesetzt.

Der Einsatz eines solchen Routers als alleinige Firewall-Einrichtung ist jedoch nur beschränkt und nur für kleine Netze zu empfehlen. Bei hohen Sicherheitsanforderungen bietet diese Lösung nicht genügend Freiraum zum Konfigurieren und außerdem keine Möglichkeit einer Application Level Firewall.

Firewall-Rechner mit Routerfunktion

Eine Konfiguration dieser Art bietet die gesamte Palette der Möglichkeiten, ist jedoch nicht für Hochsicherheit geeignet. Die Konzentration aller Einrichtungen auf einem Rechner bietet bei einer Fehlkonfiguration zu viele Möglichkeiten für Angreifer. Auch Fehler der verwendeten Programme führen zu Sicherheitslücken, die durch mehrstufige Firewalls geschlossen werden (können).

Firewall-Rechner hinter Router

In den häufigsten Fällen ist der Firewall-Rechner im lokalen Netz und der Router lässt nur Verkehr vom Internet zum Bastion-Host zu. Dieser überprüft die Zulässigkeit der Verbindung und kann sie erlauben oder abblocken. Wenn der Router mit Packet Filtering Rules ausgestattet ist, wird die dahinter liegende Firewall zusätzlich geschützt.

Der Router arbeitet mit seinem eigenen TCP/IP-Stack, welches oft wesentlich stabiler ist als der einer Softwareimplementation. DOS-Angriffe (z.B. Ping of Death, SYN-Flooding) werden somit vom Firewall-Rechner abgehalten und die Down-Zeiten verringert, da ein Router schneller wieder online ist als ein neu zu startender Rechner.

DMZ an Firewall

Bei vielen Anwendungen ist es von Vorteil, ein begrenzt sicheres Netz zu haben. Es entspricht nicht den hohen Sicherheitsanforderungen des LANs, erlaubt aber dennoch eine gewisse Überwachung und Abschirmung. Ein solches Netzwerk nennt man »Demilitarisierte Zone«. Es wird im Allgemeinen dafür benutzt, Dienste für das externe Netz zur Verfügung zu stellen.

Screened Subnet

Ein Screened Subnet ist eine Erweiterung der oben genannten Methoden, da zwischen zwei Firewall-Router ein »Abgeschirmtes Netzwerk« geschaltet wird. Diesem wird nicht völlig vertraut, aber es hat auch nicht mehr einen so feindlichen Charakter wie das externe Netz.

Im Gegensatz zu den obigen Methoden müssen hier zwei Firewall-Systeme überwunden werden, um an das LAN zu gelangen. Sind diese noch von verschiedenen Herstellern und/oder auf verschiedenen Plattformen, erhöht sich der notwendige Aufwand für den potenziellen Eindringling, diese Wand zu durchbrechen.

In dieser DMZ stehen oft Dienste für das externe Netz zur Verfügung und auch das lokale Netz kann auf die DMZ zugreifen. Direkter Verkehr zwischen den beiden Netzen wird jedoch unterbunden. Eine Application Level Firewall auf einem Bastion-Host kann diese Verbindung für spezielle Dienste ermöglichen.

In der folgenden Abbildung ist ein Netz mit mehreren Firewallsystemen exemplarisch dargestellt.

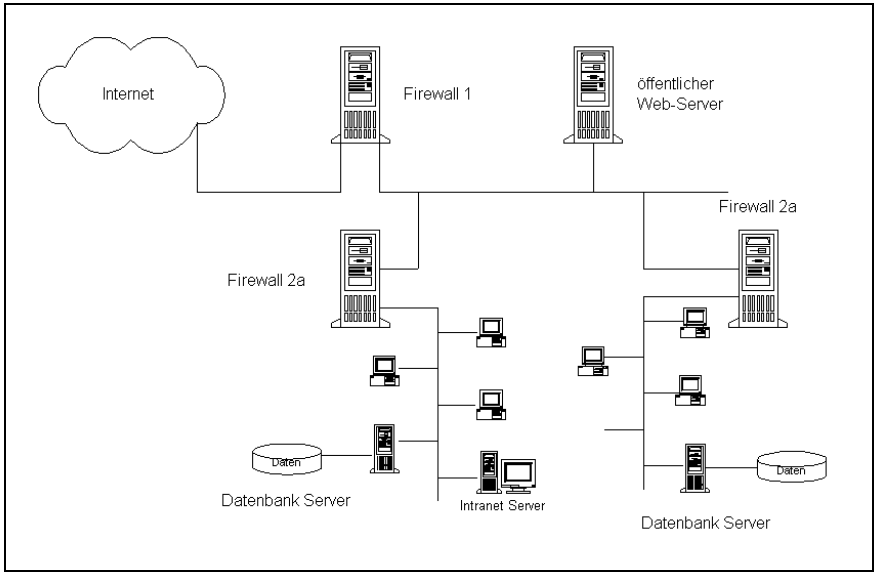


Abbildung 8.1: Firewalls

Das Firewallsystem 1 realisiert die physikalische Anbindung an das Internet. Direkt hinter diesem Firewall sind die öffentlich zugänglichen Server installiert und so gegen Angriffe von außen geschützt.

Die Firewalls 2a/b koppeln die Teilnetze zusammen und schützen die sensiblen Daten der Server. Alle Systeme die sich hinter den Firewallsysteme der Stufe 2 befinden, sind für das öffentliche Internet nicht sichtbar, auch nicht zum Lesen. Durch diese Kaskadierung kann ein optimaler Schutz nach außen und zwischen Teilnetzen realisiert werden. Eine Kommunikation zwischen Teilnetzen ist nur möglich, wenn die entsprechenden Zugriffsrechte in den Firewallsystemen eingetragen sind.

8.1.5 Firewall unter LINUX – ein Praxisbeispiel

Firewalls beinhalten oft ein komplexes Konzept bestehend aus Hard- und Softwarekomponenten. Im Folgenden wird exemplarisch die Firewallfunktionalität von LINUX beschrieben.

LINUX unterscheidet primär zwischen drei Firewall-Betriebsarten:

- ✔ Aktionen für empfangene Pakete, **INPUT,** Option **-I**
- ✔ Aktionen für zu sendende Pakete, **OUTPUT,** Option **-O**
- ✔ Aktionen zwischen zwei Netzwerkkarten in zwei verschiedenen LAN-Segmenten, **FORWARD**

Für jede Betriebsart gibt es drei Regeln:

- ✔ Annehmen, d.h. Pakete durchlassen, **ACCEPT**
- ✔ Ablehnen, d.h. Pakete nicht durchlassen, **DENY**
- ✔ Ablehnen und eine Fehlermeldung an Sender schicken, **REJECT**

Der folgende Abschnitt zeigt die Parameterliste, die Voraussetzung für die Firewallfunktionalität des LINUX-Kernels ist.

```
Config_firewall=y
Config_net_alias=y
Config_inet=y
Config_ip_forward=y
Config_ip_multicast=y
Config_ip_firewall=y
Config_firewall_verbose=y
Config_ip_acct=y
Config_ip_alias=y
```

Die Firewall unter LINUX wird mit dem Programm `ipfwadmin`, **IP F**ire**w**all **Adm**inistration, konfiguriert. Die Regeln, die eine Betriebsart festlegen, werden als **Policy** bezeichnet. Die folgende Zeile definiert für LINUX als Standard die »Input Policy« **DENY**.

```
ipfwadm policy accept -I -p deny
```

Mit dieser Einstellung lehnt die Firewall alle Datenpakete, die von außen kommen, ab. Die oben gezeigte Zeile ist ein Beispiel für die Leistungsfähigkeit von UNIX-Derivaten, die, wie z.B. LINUX, eine komplette Firewall-Funktionalität implementiert haben.

Die folgenden Zeilen sollen das Gesagte nochmals verdeutlichen. Hier wird die Firewall so konfiguriert, dass eine lokale Loopback-Verbindung zugelassen wird. Dies wird über die nachfolgend aufgeführten Optionen gesteuert :

```
ipfwadm -I -a accept -S localhost -D localhost
```

-S Angabe des Hostnamen oder IP-Adresse des sendenden Rechners, der Source

-D Angabe der Zieladresse, der Destination

-a Fügt eine neue Regel hinzu, append

-I Angaben gelten für die Betriebsart Input

Die Standardregeln können individuell geändert werden. Eine Strategie könnte z.B. darin bestehen, generell die Input-Policy auf **DENY** zu setzen. Manuell werden dann die Regeln für einzelne Rechner auf ACCEPT gesetzt. Diese haben dann Zugriff und alle anderen Rechner weiterhin nicht.

Im beschriebenen Beispiel soll ausschließlich der Zugriff für **Telnet, TCP-Port 23,** frei geschaltet werden. Hier wird eine weitere Option aufgeführt:

-P Angabe des Internetnetzwerkprotokolls, Protocol, z.B. tcp

```
ipfwadm -I -a accept -P tcp -S gasthost -D zielhost 23
```

Nach dieser Eingabe kann der Rechner gasthost mit dem Rechner zielhost eine Telnetverbindung aufbauen. Die folgende Eingabe benutzt die Option *-f* für *flash*, um alle Änderungen der Standard-Policy zurückzusetzen.

```
ipfwadm -I -f
```

Um alle Zugriffe über das Internet zu protokollieren genügt es, alle Anweisungen *ipfwadm* mit der Option -o zu ergänzen.

8.2 Techniken zu Netzwerksicherheit

Unter Datenschutz und Datensicherheit wird je nach Blickwinkel etwas anderes verstanden, oder aber die Schwerpunkte sind unterschiedlich gesetzt. Eine mögliche Sichtweise kann mit den Begriffen

- ✔ Datenintegrität
- ✔ Datenverlust
- ✔ Datendiebstahl
- ✔ Viren

umschrieben werden. Hier geht es darum, die Daten vor bewusster oder unbewusster Zerstörung bzw. Verfälschung zu schützen. Datenschutz und Datensicherheit kann aber auch unter dem Gesichtspunkt der Verhinderung von Einbrüchen in das lokale Netzwerk gesehen werden. Dieser Bereich wurde oben mit dem Schlagwort Firewall beschrieben.

Ein dritter Sicherheitsaspekt setzt den Schwerpunkt auf den Schutz des Inhaltes von Nachrichten. Diese sollen nur von autorisierten Personen gelesen werden können. Hier kommen dann die Verschlüsselungstechnologien ins Spiel, die den Schwerpunkt des folgenden Kapitels bildet.

8.2.1 Verschlüsselung

Verschlüsselungstechnologien sind insbesondere für digitale Dokumente und Unterschriften notwendig, da hier vom Original beliebig viele Kopien erstellt werden können. Es muss gewährleistet werden, dass eine solche Kopie:

- ✔ Nicht verwendbar ist, weil man ihren Inhalt nicht lesen kann
- ✔ Als Kopie erkannt werden kann, weil die digitalisierte Unterschrift eindeutig ist

Um die Echtheit eines Dokumentes sicherzustellen, werden so genannte elektronische Unterschriften oder Signaturen verwendet.

Prinzipiell kann zwischen zwei Verfahren unterschieden werden.

Die **Softwareverschlüsselung** erfolgt mit Hilfe eines Programmes, das vom Anwender aktiv genutzt werden muss, wenn er seine Nachricht verschlüsseln oder aber auch entschlüsseln möchte. Eine solche Softwarelösung kann sowohl ein eigenständiges Programm sein oder aber Bestandteil einer Applikation.

Es werden **Chipkarten, Hardwareverschlüsselung,** benutzt, die den gesamten Verschlüsselungsvorgang steuern. Diese Hardwarelösung erscheint insbesondere im Bereich des *Electronic Banking* und *E-Commerce* über das Internet als die wahrscheinlichere zukünftige Lösung.

In der Praxis kommen drei Verschlüsselungstechniken zum Einsatz:

- ✔ Symmetrische Verschlüsselung
- ✔ Asymmetrische Verschlüsselung
- ✔ Einweg-Hash-Funktion

8.2.2 Symmetrische Verschlüsselung

Zwei oder mehr Partner einigen sich bei diesem Verfahren auf ein gemeinsames Kennwort, das auch Schlüssel oder Passwort genannt wird. Alle vertraulichen Nachrichten werden mit einem Verschlüsselungsverfahren chiffriert und beim Empfänger dechriffriert. Dazu muss das zuvor vereinbarte Passwort, das den Schlüssel zur Dechiffrierung liefert, verwendet werden.

DES, Data Encryption Standard, ist das bekannteste symmetrische Verfahren und wurde in den siebziger Jahren von IBM für das NBS, National Bureau of Standards, entwickelt. DES benutzt zur Verschlüsselung einen 64 Bit langen Schlüssel. Das Verfahren nimmt mit dem zu verschlüsselnden Text eine Reihe von Permutationen und Substitutionen vor, die 16-mal mit Varianten des Schlüssels vorgenommen werden, so dass als Ergebnis ein unlesbarer Text entsteht.

Für DES werden Handwarelösungen angeboten. Die folgende Tabelle vermittelt einen Eindruck von der Leistungsfähigkeit. Leistung wird hier als Datendurchsatz gemessen.

Hardware	Durchsatz
DEC VLSI Chip1	1 Gbit/s
PC-Assembler 486/25 MHz	850 Kbits/s
AMD Chip	14 Mbit/s
Smart Cards	2 Kbit/s

Verfahren wie RC2 und RC4 verwenden DES, können aber je nach Sicherheitsanforderungen mit variablen Schlüssellängen arbeiten.

Asymmetrische Verschlüsselung

Dieses Verfahren benutzt einen Schlüssel zum Chiffrieren und einen weiteren Schlüssel, der ausschließlich zum Dechiffrieren von Daten benutzt wird. Der erstere Schlüssel ist öffentlich bekannt und heißt deshalb auch **Public Key**. Der Dechiffrierschlüssel ist nur dem Empfänger einer Nachricht bekannt und heißt deshalb **Private Key**.

BEISPIEL

Anwender A möchte in Zukunft mit Anwender B vertrauliche Nachrichten austauschen. Dazu teilt Anwender B Anwender A seinen öffentlichen Schlüssel mit.

Anwender A verschlüsselt mit dem öffentlichen Schlüssel von B die Nachrichten, die er an B sendet. Nur B ist danach in der Lage, die von A verschlüsselten Daten mit seinem Private Key zu entschlüsseln.

In gleicher Weise kann nun unter ein elektronisches Dokument eine Unterschrift gesetzt werden, die so genannte Digitale Signatur. Dazu wird der umgekehrte Weg beschritten. D.h. mit Hilfe des Private Key verschlüsselt der Sender eines Dokumentes seinen Namen im nicht verschlüsselten Dokument. Im Dokument steht nun eine nicht interpretierbare Zeichenfolge.

Jeder Empfänger, der in Besitz des Public Key des Senders ist, kann nun überprüfen, wessen Name hinter der kryptischen Zeichenfolge steht. Er »verschlüsselt die verschlüsselte Unterschrift« und erhält damit den Absendernamen, der als Unterschrift fungiert, im Klartext.

BEISPIEL

Anwender A möchte ein Dokument für Anwender B unterschreiben. Dazu gibt er seinen Namen als Klartext in einen entsprechenden Bereich ein und verschlüsselt diesen mit seinem geheimen, privaten Schlüssel. Damit wird gewährleistet, dass nur Anwender A die resultierende, verschlüsselte Signatur erzeugt haben kann.

Anwender B erhält das Dokument und findet als Unterschrift eine verschlüsselte Zeichenfolge. Diese entschlüsselt er mit dem öffentlichen Schlüssel von Anwender A. Das Ergebnis muss der Name von Anwender A sein.

Die Schlussfolgerung ist, dass die Unterschrift unter das Dokument nur von A stammen kann, da niemand dessen Private Key kennt bzw. kennen darf. Jeder aber, der über den öffentlichen Schlüssel von Anwender A verfügt, kann seine Unterschrift überprüfen.

Im Falle besonders sensibler Daten kann nach der »Unterschrift« mit Hilfe des Private Key diese vernichtet werden. Damit ist gewährleistet, dass mit großer Sicherheit die Unterschrift nicht mehr reproduziert werden kann.

Die bekanntesten Methoden sind der RSA-Algorithmus und das ElGamal-Verfahren. Das Akronym **RSA** steht für die Namen der Erfinder dieser Methode, Ronald Rivest, Adi Shamir und Leonard Adleman, die das Verfahren 1978 erstmals publizierten. Das Verfahren beruht auf der Tatsache, dass sehr große Zahlen, die das Produkt von Primzahlen sind, nicht mehr in die ursprünglichen Primzahlen zerlegt werden können (Primfaktorenzerlegung). Im Folgenden erhalten Sie eine Kurzbeschreibung der Vorgehensweise.

In einem ersten Schritt werden zwei beliebige, sehr große Primzahlen P und Q gewählt. Als nächstes wird eine Zahl E so bestimmt, dass E und (P-1) * (Q-1) teilerfremd sind, also nicht durch die selbe Zahl ohne Rest teilbar sind. Aus den gegebenen Zahlen E, P und Q wird die Zahl D errechnet, so dass D * E – 1 durch (P-1) * (Q-1) teilbar ist.

Im Folgenden bestimmen die ermittelten Zahlen die Vorgehensweise bei der Verschlüsselung und Entschlüsselung von Klartext. Der Text wird nach folgender Formel verschlüsselt:

$C = (T^E) \bmod n$

Hier ist C der verschlüsselte Text und n berechnet sich aus P * Q. E und n sind der öffentliche Schlüssel. Das Entschlüsseln wird mit Hilfe folgender Formeln erreicht.

$T = (C^D) \bmod n$

Hier ist T der Klartext und n berechnet sich aus P * Q. D ist geheim und n ist öffentlich. Ersetzt man C durch T^E dann ergibt sich die Formel:

$T = (T^{DE}) \bmod n$

Die Zahlen E und D werden auch als öffentlicher bzw. geheimer Exponent bezeichnet. D kann aus den öffentlichen Werten E und n nur dann berechnet werden, wenn es gelingt, n in die Primzahlen P und Q zu zerlegen. Bei einem 512 Bit langen Schlüssel würde ein Rechner mit einer Million Operationen pro Sekunde, ein MIPS, 420.000 Jahre für die Primfaktorenzerlegung benötigen.

Das bekannteste Produkt für die Verschlüsselung mit Hilfe eines asymmetrischen Verfahren ist **Pretty Good Privacy**, PGP, von Phil Zimmermann.

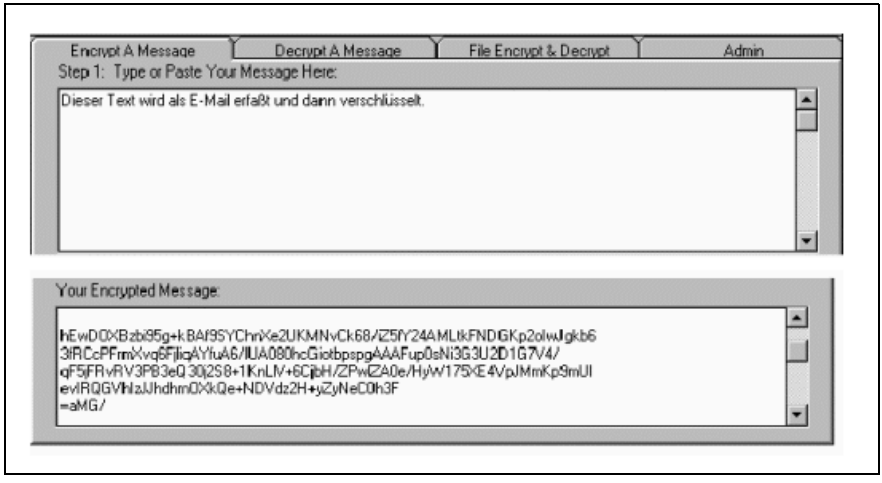


Abbildung 8.2: Klartext und verschlüsselter Text mit PGP

Der Einsatz von öffentlichen und privaten Schlüsseln lässt die Einrichtung anerkannter Zertifizierungsstellen zu. D.h. als Anwender kann man den öffentlichen Schlüssel von einer Zertifizierungsstelle verwalten lassen. Diese kann den Schlüssel verteilen und gewährleistet gegenüber Dritten seine Echtheit. Dazu wird unter anderem auch die Identität des Antragstellers geprüft.

Die wesentliche Aufgabe der Zertifizierungsstelle besteht nun darin, dass diese den öffentlichen Schlüssel eines Antragstellers ihrerseits mit ihrem geheimen Schlüssel signiert. Jeder Interessierte kann nun anhand des öffentlichen Schlüssels der Zertifizierungsstelle die Echtheit der Signatur und damit die Echtheit des öffentlichen Schlüssels des Antragstellers überprüfen.

Zertifizierungsstellen sind hierarchisch organisiert. Die Wurzel wird von der »Internet Society« betrieben und heißt Internet Policy Registration Authority, IPRA. Für die sichere Verwahrung der geheimen Signaturschlüssel werden Hardwaresysteme eingesetzt, die als CSU, Certificate Signing Unit, bezeichnet werden und selbst gegen elektromagnetische Angriffe geschützt sind. Beim Öffnen einer solcher Einheit wird der Inhalt zerstört.

Einweg Hash-Funktion

Dieses Verfahren berechnet aus einer umfangreichen Information eine komprimierte. Dabei erzeugen verschiedene Eingaben, z.B. der Text einer E-Mail, verschiedene Ausgaben, die mit hinreichender Wahrscheinlichkeit sich immer unterscheiden werden. Damit kann die Hash-Funktion auch als Verschlüsselungsmechanismus genutzt werden.

Mit relativ wenig Aufwand kann überprüft werden, ob ein Text verändert wurde. Dazu berechnen Sender und Empfänger jeweils mit Hilfe der Hash-Funktion einen Zahlenwert und vergleichen das Ergebnis, welches wiederum verschlüsselt sein kann, miteinander.

8.3 TCP/IP und Netzwerksicherheit

Den Abschluss dieses Kapitels bildet die Analyse der Sicherheitsrisiken, die beim Einsatz von TCP/IP entstehen. Dazu erhalten Sie einen Überblick zu den Techniken, die potenzielle Angreifer benutzen.

8.3.1 Footprinting

Potenzielle Einbrecher in ein Netzwerk werden in einem ersten Schritt alle relevanten Informationen zu einem Netzwerk sammeln. Das systematische Vorgehen, das es einem Angreifer ermöglicht, ein vollständiges Profil über ein Netzwerk zu erstellen, wird Footprinting genannt. In den folgenden Kapiteln wird eine Auswahl von Techniken beschrieben, die beim Footprinting eingesetzt werden. Den Schwerpunkt bildet hier die Auswertung von Netzwerkdaten.

Hier geht es vor allem darum, IP-Adressen zu ermitteln. Auf der Basis dieser Adressen kann dann versucht werden, auf Server zuzugreifen, um weitere Informationen zu sammeln.

DNS-Abfrage

Die DNS-Abfrage gibt Aufschlüsse über die Organisation eines Netzwerkes und liefert nebenbei weitere Adressen. Folgende Informationen können aus der DNS-Datei ausgelesen werden:

- ✔ IP-Adressen
- ✔ Informationen zu Mail-Servern

- ✔ Informationen zu den verwendeten Betriebssystemen
- ✔ Informationen zu weiteren DNS-Servern, z.B. die Adressen weiterer DNS-Server

Dazu steht mit **nslookup** ein mächtiges Werkzeug zur Verfügung, das es erlaubt, einen Zonentransfer durchzuführen. Das Prinzip ist recht einfach. Wenn die IP-Adresse des DNS-Servers bekannt ist, dann wird er mit nslookup zu einem Zonentransfer veranlasst. Die Informationen können lokal in eine Datei gespeichert und dann in aller Ruhe analysiert werden.

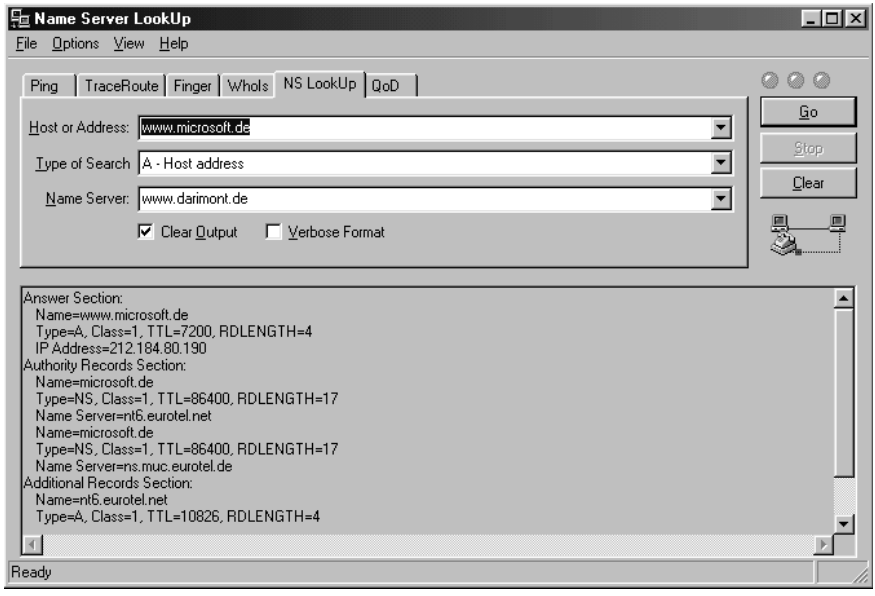


Abbildung 8.3: Footprinting mit nslookup

Das hier mit nslookup gezeigte Sicherheitsloch lässt sich leicht schließen. Dazu müssen Sie in einem ersten Schritt die DNS-Server so konfigurieren, dass sie einen Zonentransfer von nichtautorisierten Benutzern unterbinden. Unter Windows NT verwenden Sie dazu die Option /notify. Netzwerkseitig können Sie eine Firewall oder einen Paketfilter-Router so konfigurieren, dass alle nicht autorisierten Verbindungen über TCP-Port 53 bzw. UDP-Port 53 abgelehnt werden. Ein weiterer Schritt besteht darin, das Eindringlingserkennungssystem, IDS, Intrusion Detection System, so einzustellen, dass Zonentransfers als potenzieller Einbruchsversuch gewertet und protokolliert werden.

Netzwerk auskundschaften

Das Auskundschaften eines Netzwerkes umfasst das Ermitteln der Netzwerktopologie und potenzieller Zugriffspfade. Dazu benutzen Hacker das Programm traceroute, das aus Kompatibilitätsgründen unter Windows tracert heißt, also

nur sieben Buchstaben hat plus Erweiterung. Dieses Programm zeigt den Weg eines Datagramms zum Zielrechner. Als Nebenprodukt werden auch potenzielle Firewalls erkennbar, die man dann zu überwinden versuchen kann.

Zunächst wollen wir uns anschauen, wie tracert funktioniert. In einer einfachen Variante sendet tracert ein Paket an den Zielrechner mit einem TTL-Wert von Eins. Das hat zur Folge, dass der Absender eine Time Exceeded Rückmeldung von ICMP erhält. Als Reaktion darauf erhöht tracert den TTL um eins. Dies wiederholt sich solange, bis der Zielrechner erreicht wurde und es möglich ist, jeden Router, der durchlaufen wurde, aufzulisten.

Was ist aber, wenn der Zielerechner erreicht wurde? Damit dies erkannt werden kann, wird ein Zielport angegeben, an dem kein Server »hört«. Das Ergebnis ist eine Server-not- reachable-Rückmeldung. Jetzt muss das Paket nicht nochmals gesendet werden.

Schauen wir uns auch hier ein Beispiel an.

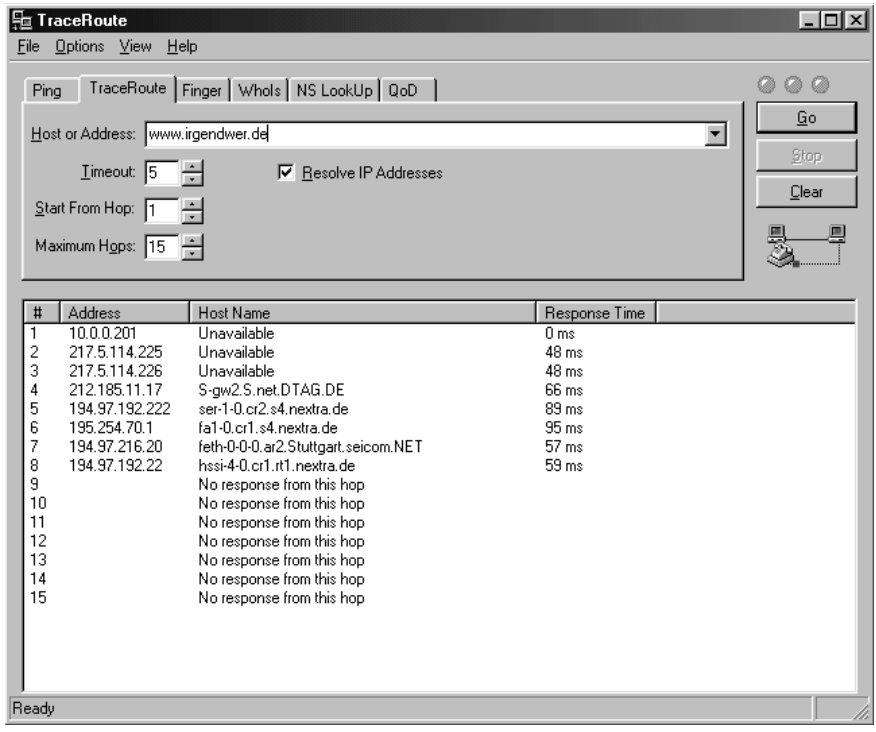


Abbildung 8.4: Footprinting mit tracert

Was fällt auf? Nach dem achten Hob sehen wir nur noch »Sternchen«, d.h. wir bekommen keine Antwort. Das bedeutet, dass der Router traceroute-Abfragen blockiert. Und das kann wiederum ein Hinweis auf eine Firewall sein. Ein Hacker könnte jetzt versuchen, die Nachrichten über den UDP-Port 53 zu sen-

den, der wie Sie wissen, von DNS-Abfragen verwendet wird. Das Ergebnis kann nun sein, dass die Firewall traceroute nicht mehr blockiert, und damit können wir hinter die Firewall sehen. Allerdings sehen wir nicht mehr den Zielrechner, da eine Fehlermeldung wie oben beschrieben ausbleibt.

Wie kann man sich schützen? Eine Möglichkeit besteht darin, Software zu installieren, die zum Beispiel eingehende traceroute-Pakete erkennt und verfälschte Antworten sendet.

8.4 Scanning

Auf das Footprinting folgt das Scanning, das sind Suchläufe nach Rechnern und nach auf diesen Rechnern hörenden Servern, Port Scans.

8.4.1 Ping

Ping ist ein kleines, aber sehr nützliches Tool. Das Programm verwendet ICMP Echo Request Pakete (ICMP Typ 8), auf die die angewählten Hosts mit Echo Replay (ICMP Typ 0) antworten.

Unter Unix können Sie das Tool fping verwenden, das mehrere Pings gleichzeitig absetzen kann und damit zur Generierung einer Adressliste eingesetzt werden kann.

8.4.2 Port Scans

Unter Port Scan versteht man den Vorgang, bei dem eine Verbindung zu den TCP- und UDP-Ports aufgebaut wird, um festzustellen, welche Dienste auf einem Rechner ausgeführt werden.

Die Ziele des Port Scan sind:

- ✔ TCP- und UDP-Ports auf einem System erkennen
- ✔ Das Betriebssystem eines Zielsystems erkennen
- ✔ Spezifische Anwendungen und deren Version erkennen

Man unterscheidet folgende Scan-Typen:

- ✔ TCP-Connect Scan
- ✔ TCP-SYN-Scan
- ✔ TCP-FIN-Scan
- ✔ TCP-Xmas-Tree-Scan
- ✔ TCP-Null-Scan
- ✔ UDP-Scan

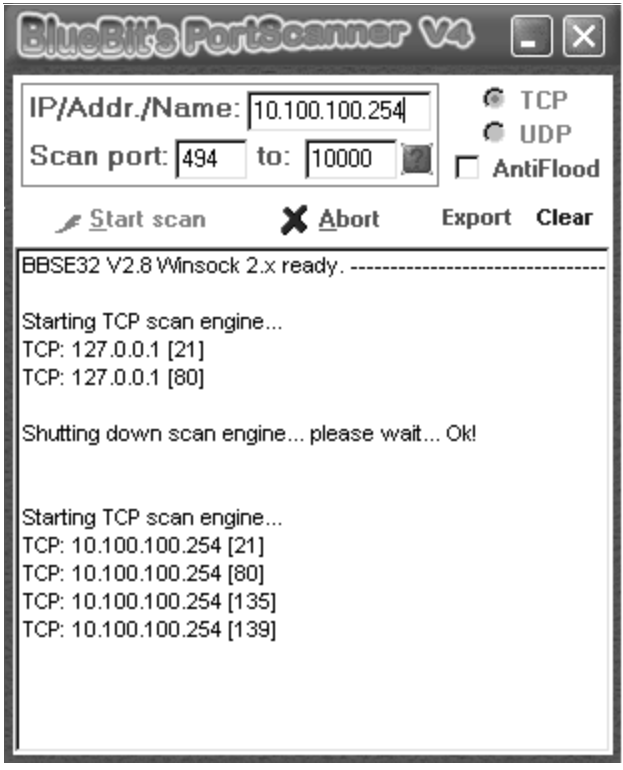


Abbildung 8.5: Port-Scanning

Die oben gezeigte Grafik lässt folgende Schlüsse zu:

Auf dem lokalen Rechner hören ein FTP- und ein HTTP-Server an den Port 21 und 80. Auf dem Remote Rechner des zweiten Scans sind die NetBIOS-Ports 135 und 139 aktiv. Der erste Port wird für den NetBIOS-Suchdienst verwendet, der zweite, also 139, für NetBIOS- Verbindungsdienste.

INDEX