

TCP/IP

Eine kleine Einführung

A-Net GmbH, Zumikon
www.anetgmbh.ch



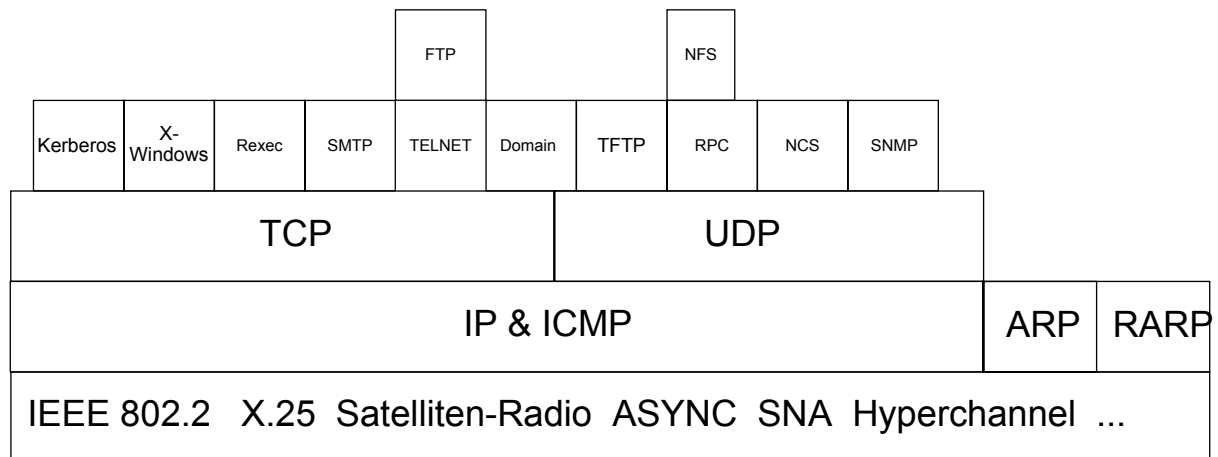
Entwicklung

- DARPA (Defense Advanced Research Project Agency)
- vor 1971 ARPANET basierend auf NCP
- TCP/IP 1978 eingeführt
- ARPANET auf TCP/IP umgestellt 1983
- Berkeley University of California: Gratis Programm-Code für Unix Systeme
- bei fast allen UNIX-Systemen mitgeliefert
- Geschwindigkeiten:
 - ursprünglich 56 kbps Leitungen
 - T1 mit 1.544 Mbps 1989
 - 44.736 Mbps erste Hälfte 90-er Jahre
- RFC Request for Comment (für Normierung)

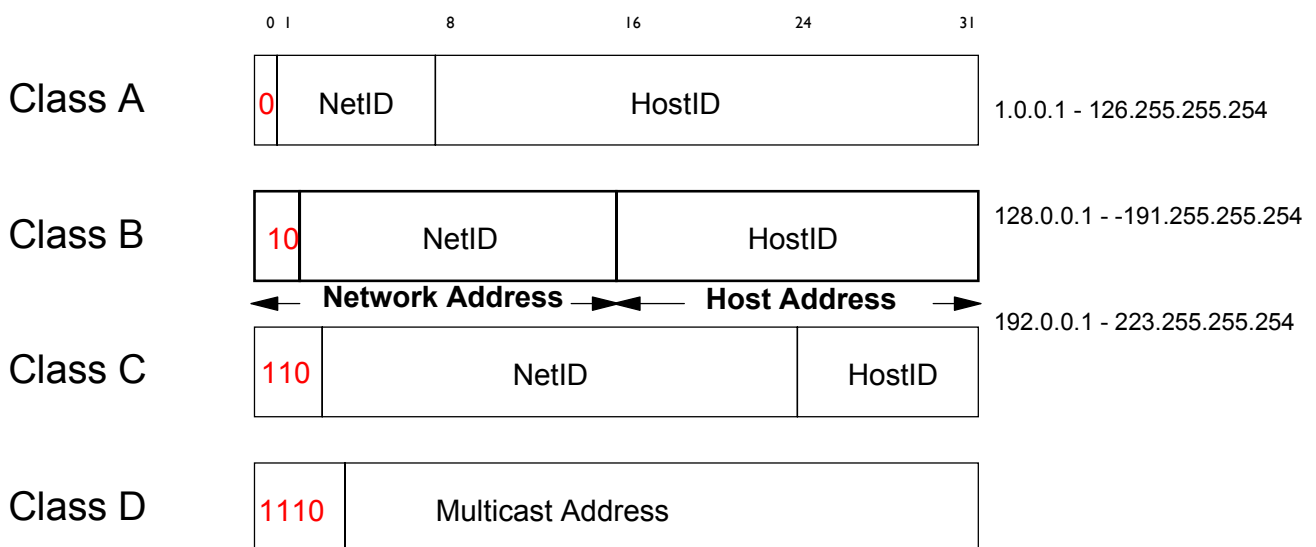
TCP/IP Architektur

Eine Sammlung von einzelnen Applikationen

- normalerweise je ein Client und Server-Modul (=Daemon)
z.B. **TELNET** auf dem Client, **TELNETD** auf dem Server
- Umfang je nach TCP/IP Implementation stark unterschiedlich



TCP/IP Adresstypen



Beispiel einer IP-Adresse: 128.4.78.15

NetID wurde vergeben vom Network Information Center (NIC) in Kalifornien
Heute: ICANN (Internet Corporation for Assigned Names and Numbers),
.ch und .li-Domänen reservieren bei www.switch.ch für die Schweiz

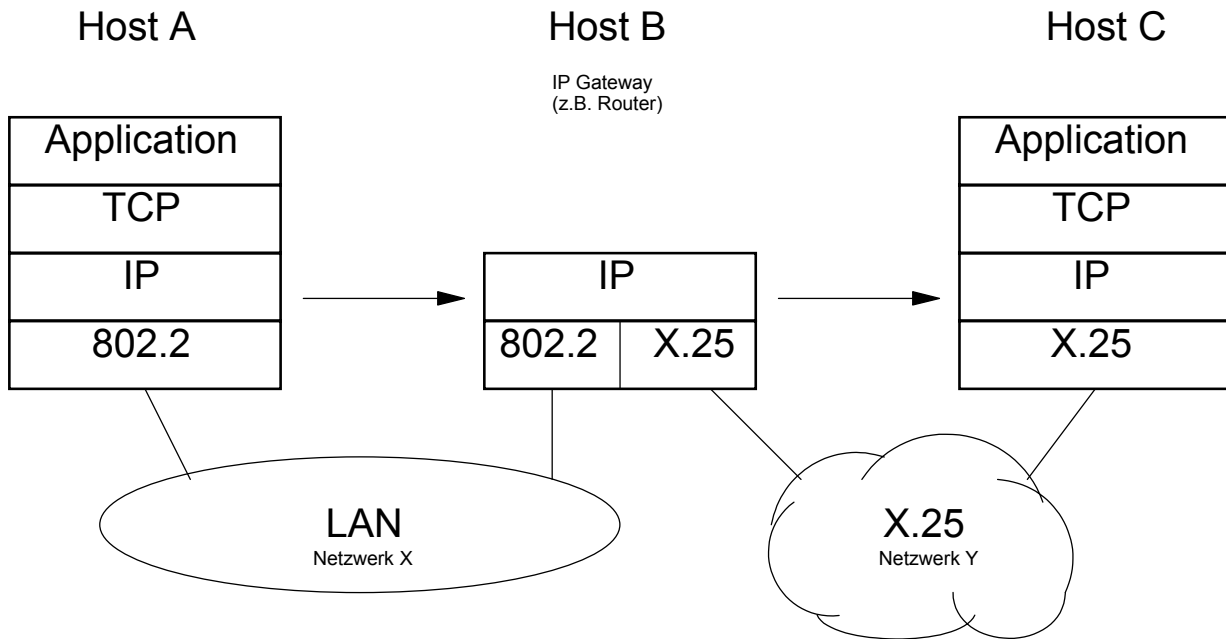
IP Routing und Gateways

- NetID-Teil der Internetadresse bestimmt Zielnetz des Hosts (--> Adressänderung bei Netzwechsel zwingend)
- Core Gateways müssen alle IP Netze kennen.
 - Core Gateways werden vom Internet Network Operations Center verwaltet
 - Gateway-to-Gateway Protocol (GGP)und Exterior Gateway Protocol (EGP)
- Non-Core Gateways kennen einen Teil des Netzes
 - verwaltet von individuellen Gruppen
 - Datenaustausch mit EGP
- Routenauflösung mit
 - Routing Information Protocol (Berkeley)
 - OSPF (Open Shortest Path First)
 - Hello
 - Exterior Gateway Protocol (EGP)

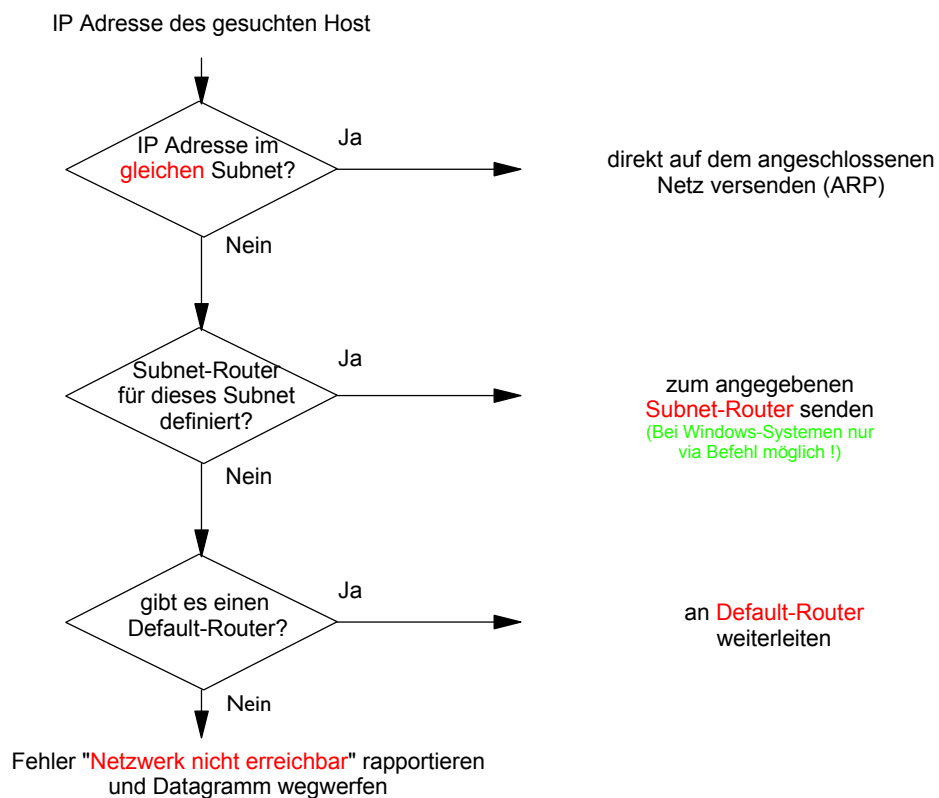
Internet-Gateways (= Router)

- Grundsätzlich gilt:
 - alle Systeme, die TCP/IP auf mehr als einem Interface unterstützen, können auch Routen
 - dazu gehören:
 - ▶ OS/2 ab Warp
 - ▶ Windows NT 4, Windows 2000, Windows XP
 - ▶ alle Unix-Versionen: Linux, AIX, HP-UIX etc.
 - ▶ OS/400 etc.
- Ausnahme: keine Routing-Funktion enthalten
 - Windows 95, Windows98, Windows ME
- Es gibt reservierte Adressebereiche für Test-/interne Zwecke. Diese werden im Internet **nicht** geroutet
 - 10.0.0.0 bis 10.255.255.255 (Class A)
 - 172.16.0.0 bis 172.31.255.255 (Class B)
 - 192.168.0.0 bis 192.168.255.255 (Class C)

Internet Gateway (=Router)



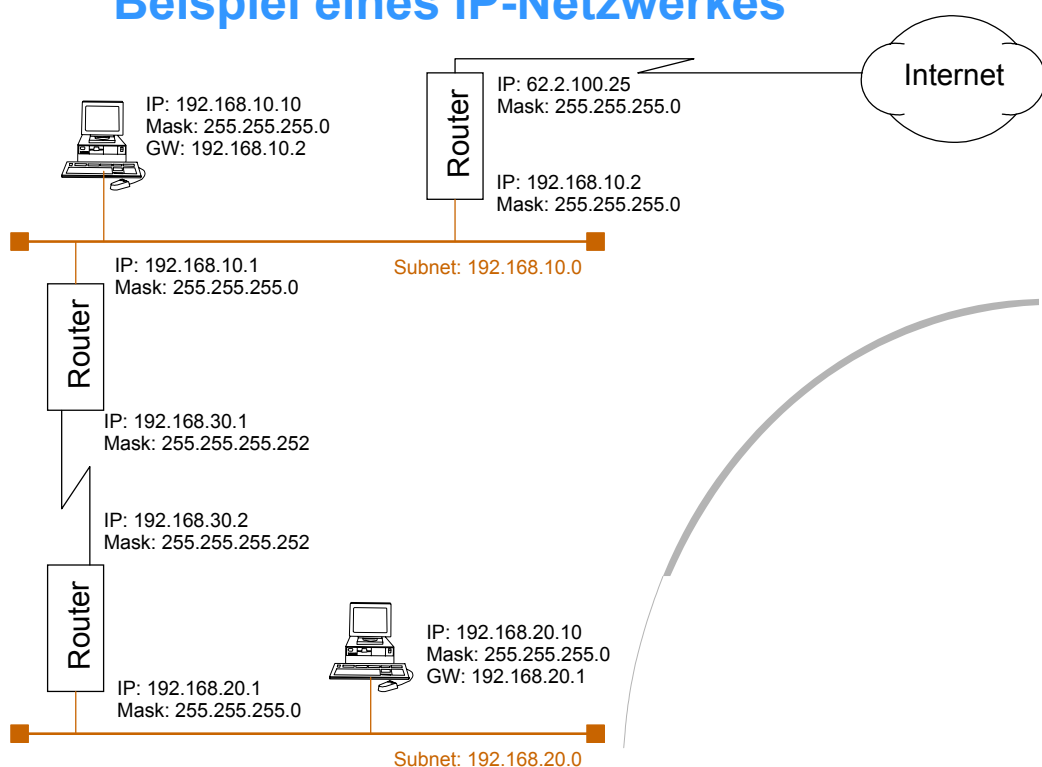
Routingschema



Adressauflösung im LAN

- Address Resolution Protocol (ARP)
 - setzt IP-Adresse in MAC-Adresse um (im LAN)
 - Broadcast zum Auffinden unbekannter Adressen (ARP Request)
 - Lookup Tabelle für bekannte Adressen (=ARP Cache)
- Reverse Address Resolution Protocol (RARP) für Diskless Arbeitsstationen
 - erfragt beim RARP-Server seine IP-Adresse aufgrund seiner MAC-Adresse
 - RARP-Server mit Tabelle der Adressen notwendig

Beispiel eines IP-Netzwerkes



Ethernet Frame

Preamble	Destination Address	Source Address	Typ	Daten	CRC
64 bit	48 bit	48 bit	16 bit	variabel	32 bit

- maximale Länge des Datenfelds: 1500 Bytes
- Typ-Nummer grösser als 1500
 - Typ 2048 (x 0800): IP Datagram
 - Typ 2054 (x 0806): ARP Datagram
 - Typ 24579 (x 6003): DECnet Phase IV
 - Typ 24580 (x 6004): DEC LAT
 - Typ 32923 (x 809B): Appletalk

RFC894

802.3 Frame

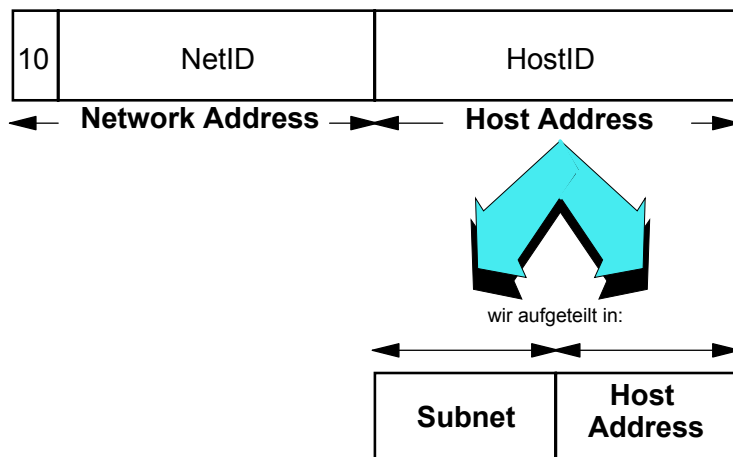
Preamble	Destination Address	Source Address	Daten Länge	Daten	CRC
64 bit	48 bit	48 bit	16 bit	variabel	32 bit

- maximale Länge des Datenfelds: 1500 Bytes (10 Mbps Netze), sonst grösser
- Sub-Network Access Protocol (SNAP) mit DSAP und SSAP=170, dann gilt
 - Typ 2048 (x 0800): IP Datagram
 - Typ 2054 (x 0806): RP Datagram
 - Typ 32821 (x 8035): RARP Datagram

RFC1010

Subnet

Class B



- Host ID wird aufgeteilt in Subnet Address und Host ID
- Subnet-Bits müssen *nicht* zusammenhängend sein (z.B. Bit 1,3,5,7)
- bitweise AND der ganzen Host ID mit Subnetmask ergibt Subnet Address
- keine Registrierung der Subnets bei Network Information Center (NIC) notwendig
- alle Hosts müssen Subnets unterstützen (implementiert in allen IBM TCP/IP)
- Beispiel : erstes Byte = Subnet, zweites Byte = Host:
 - Subnet Mask 255.255.255.0, Internet Address: 128.3.45.27
 - erstes Host-Byte = Subnet Address = 45
 - zweites Host-Byte = neue Host ID = 27

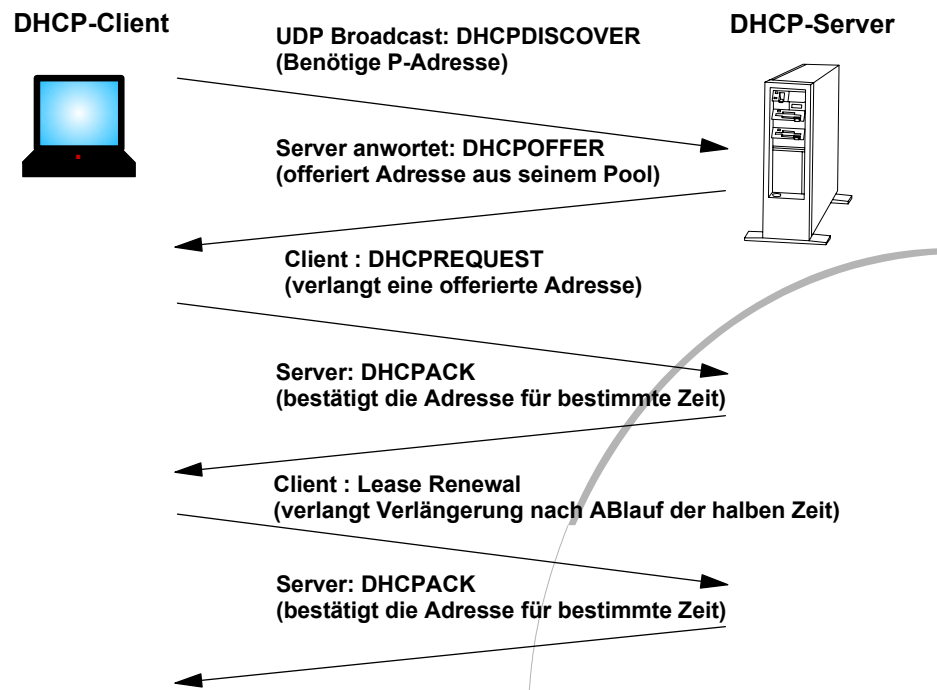
Subnetmask

- bestimmt, wie viele Bits (von links) zum Subnetzteil gehören, der Rest sind Host-Bits
- die Adresse mit allen Host-Bits=0 ist die Adresse des ganzen Subnetzes, diese Adresse *nicht* für Stationen verwenden
- Die Adresse mit allen Host-Bits=1 ist die Broadcast-Adresse, auch diese Adresse *nicht* für Stationen verwenden
- Beispiele:
 - 255.255.255.252 4 Adressen, davon 2 frei
 - 255.255.255.248 8 Adressen, davon 6 frei
 - 255.255.255.240 16 Adressen, davon 14 frei
 - 255.255.255.224 32 Adressen, davon 30 frei
 - 255.255.255.192 64 Adressen, davon 62 frei
 - 255.255.255.128 128 Adressen, davon 126 frei
 - 255.255.255.0 256 Adressen, davon 254 frei
 - 255.255.254.0 512 Adressen, davon 510 frei

Erweiterungen: DHCP und IPng

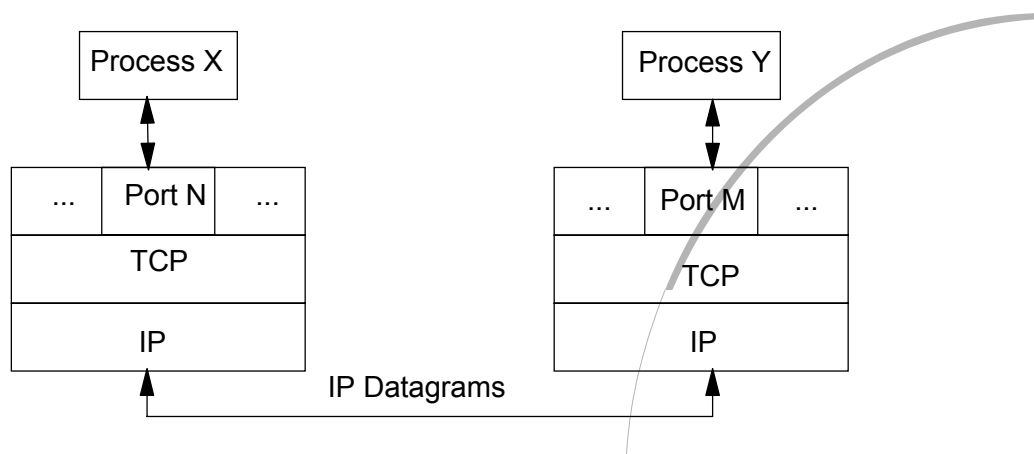
- DHCP: Dynamic Host Configuration Protocol
 - automatische IP-Konfiguration ab DHCP Server
 - verringerter Konfigurationsaufwand
- DDNS: Dynamic Domain Name Server
 - Ergänzung zu DHCP: Host Name wird dynamisch beim Name Server registriert, Name mit Passwort geschützt
 - WINS: NetBios Name Server, Proprietäre Workgrouplösung (die teilweise einem NetBios Name Server entspricht), nur für Windows Systeme, ev. Linux. Name ist nicht geschützt
- Erweiterung von TCP/IP: IPng
 - Adresse 32 Bit --> 128 Bit
 - Quality of Service (QoS) Routing
 - ▶ alle dazwischenliegenden Router müssen mitmachen, sonst geht QoS-Info verloren

DHCP Dynamic Host Configuration Protocol



User Datagram, Ports & Sokets

- Jeder Process identifiziert sich gegenüber TCP/IP mit einem oder mehreren Ports
- IP Soket = (IP Adresse , Port Nummer)
- Ports 0-255 standardisiert, über 255 für Anwendungen frei



Port-Nummern

5	=	RJE	Remote Job Entry
7	=	Echo	ICMP Echo Request (Ping)
20	=	FTP-Data	File Transfer (Daten)
21	=	FTP	File Transfer (Steuerung)
23	=	TELNET	Remote Terminal
25	=	SMTP	Simple Mail Transfer Protocol
37	=	Time	Timeserver
53	=	DNS	Domain Name Server
67	=	BOOTPS	Bootstrap Protocol Server, DHCP
68	=	BOOTPC	Bootstrap Protocol Client, DHCP
69	=	TFTP	Trivial File Transfer Protocol
70	=	Gopher	Suchprogramm im Internet
79	=	Finger	Finger zum Anzeigen von Benutzern auf remote System
80	=	HTTP	Hyper Text Transfer Protocol für WWW
101	=	HOSTNAME	Name Server
103	=	X400	X.400
110	=	POP3	Post Office Protocol 3
137	=	NETBIOS-NS	Netbios Names Service
138	=	NETBIOS-DG	Netbios Datagram Service
139	=	NETBIOS-SSM	Netbios Session Service
161	=	SNMP	Simple Network Management Protocol
162	=	SNMP Trap	SNMP Trap-Meldungen

Telnet

- Telnet gestattet, remotes Terminal zu sein (Network Virtual Terminal NVT)
- verschiedene Terminal-Typen (z.B. OS/2):
 - TELNET (zeilenmodus)
 - ANSI Term
 - Telnet VT100 (DEC VT100 Terminal)
 - Telnet VT220 für DEC Systeme und viele andere
 - Telnet 3270 (Full Screen 3270 Terminal für IBM Hosts)
 - Telnet 5250 (Full Screen 5250 Terminal für AS/400)
- **Vorsicht:** Anmeldepasswort geht im Klartext übers Netzwerk!
(sichere Alternative: SSH)



FTP File Tansfer Protocol

- Dient zum Übertragen von Dateien zwischen FTP-Client und FTP-Server
- **put** stellt Datei vom Client auf den Server
- **get** holt Datei vom Server auf den Client
- **ls** zeigt Dateien im aktuellen Verzeichnis an
- **bin** schaltet binäre Übertragung ein (sonst ASCII)
- **cd /xxx** wechselt ins Verzeichnis xxx
- **quit** beendet FTP
- zahlreiche, grafische FTP-Frontends sind erhältlich
- **Vorsicht:** Anmeldepasswort geht im Klartext übers Netzwerk!
(sichere Alternative: SSH)



X-Window

- X-Window ist das Grafik-Fenstersystem für Unix-Systeme
- Client/Server-Modell (auf gleicher Maschine oder via IP-Netzwerk):
 - Grafik-Programm läuft auf dem X-Window Client
 - Anzeige und Steuerung (Tastatur, Maus) erfolgt auf dem X-Window Server
- Verschiedene X-Window Lösungen erhältlich, meist auf Standard X11R6 basierend
- Freie Software Version: xFree86 für fast alle PC-Plattformen
- Programm-Aufruf:
 - **xeyes -display 192.168.112.60:0.0** (oder mit der Variablen \$DISPLAY)
 - (startet das Programm xeyes und leitet die Anzeige zum System mit der IP-Adresse 192.168.112.60 um)

nützlich Befehle (plattformabhängig)

- `ping 192.168.111.15` (alle Plattformen)
 - zum Testen der Verbindung zu dieser Adresse
- `ipconfig /all` (Win98, NT, 2000, XP) `ipconfig` (Win ME) `winipcfg` (Win 95, 98, ME)
 - zeigt aktuelle IP-Konfiguration an, Details auch bei DHCP
- `netstat -a` (OS/2), `ifconfig` (Linux), `netstat *ifc` (AS/400)
 - zeigt aktuelle, eigene Adresse(n) an, unter NT, 2000, XP die aktiven Verbindungen
- `netstat -r` (OS/2, Linux, Win 95, 98, ME, Win NT, 2000) `netstat *rte` (AS/400)
 - zeigt die aktuellen Routen an
- `route add` / `route delete` (OS/2, Win 98, NT, Win 2000, XP) Route hinzufügen/löschen
- `route print` (Win 98, NT, 2000, XP) zeigt aktuelle Routen an
- `arp -a` (fast alle Betriebssysteme)
 - zeigt aktuellen ARP Cache an (IP Adresse - MAC Adresse)
- `dhcpmon` (OS/2)
 - zeigt aktuelle DHCP Konfiguration an
- `ddnscfg` (OS/2)
 - reserviert den Hostnamen beim Name Server
- `tracerte 192.168.111.15` (OS/2, Linux), `tracert 192.168.111.15` (Win9x, ME, NT, 2000, XP)
 - zeigt die benutzten Router für diese Verbindung an
- `nslookup www.anetgmbh.ch` (OS/2, Linux, Win NT, Win 2000, XP)
 - zeigt IP-Adresse eines URL an

Router-Protokolle

- In grösseren Netzwerken ist es sinnvoll, dass die **Router gegenseitig Informationen austauschen**. So können neue Subnetze mit Routern hinzugefügt werden und nach einer gewissen Zeit kennen alle Router im Netzwerk die neuen Subnetze.
- solche internen Router Protokolle (IGP) sind:
 - RIP (Router Information Protocol) Version 1 gemäss RFC 1058
 - RIP Version 2 gemäss RFC 1723
 - OSPF (Open Shortest Path First) Version 2 gemäss RFC 2328
 - EIGRP (Enhanced Interior Gateway Routing Protocol) Standard auf Cisco-Routern



RIP Version 1

- Ein RIP Router funktioniert so:
 - Jeder RIP-Router baut eine Routingtabelle mit einem Eintrag pro Subnet auf (=Distance Vector)
 - Ein Distance Vector enthält:
 - ▶ Adresse des Subnetzes und Subnetmask
 - ▶ Adresse des nächsten Routers im Pfad (Nachbar)
 - ▶ Hop Count: Anzahl Router zum Netzwerk (=metric)
 - Die Tabelle enthält zu Beginn nur die direkt am Router angeschlossenen Subnetze mit einem Hop Count von 0
 - jeder Router sendet periodisch (ca. alle 30 Sekunden) seine Routing-Tabelle an alle anderen Router in seinen angeschlossenen Subnetzen.
 - Jeder Router lernt so zusätzlich die erreichbaren Netzwerke aus den Meldungen der anderen Router, der Hop Count gibt an, über wieviele Router eine Verbindung geht
 - Hop Count = 16 meldet ein Netzwerk als unerreichbar



Vor- und Nachteile von RIP V1

- Vorteile:
 - RIP ist ein einfaches Routing Protocol, das auf allen grossen und vielen kleinen ISDN Routern (z.B. ZyXel, BinTec, etc.) als auch in Betriebssystemen wie OS/2 (Routed), Linux, Win NT, Win2k etc. anzutreffen ist.
- Nachteile:
 - nur für kleine Netzwerke geeignet (Verbindungen sind über max. 15 Router möglich)
 - nur fixe Subnetmasken möglich
 - keine Sicherheit gegen unbekannte/fremde Router
 - Konvergenzzeit bei ausfallenden Verbindungen teilweise hoch
 - grosser Datenverkehr zwischen den Routern



RIP Version 2

- RIP Version 2 baut auf RIP 1 auf und ist mit diesem kompatibel
- Neue Funktionen:
 - Variable Länge der Subnetmasken möglich(=Supernetting)
 - Multicasting (statt Broadcasting) reduziert die Netzwerkbelastung
 - Authentication möglich, schliesst fremde Router aus
- Vorteile:
 - weniger Daten fließen zwischen den Routern
 - sicherer
- Nachteile:
 - grosse Konvergenzzeit bleibt
 - Authentication ist nicht verschlüsselt (Hacker)



OSPF - Open Shortest Path First

- OSPF baut eine Tabelle mit Verbindungszuständen auf:
 - Status (active/inactive)
 - Cost (günstige/ungünstige Route)
- Updates werden nur mitgeteilt, wenn sich etwas geändert hat
- Grosse Netzwerke werden in Areas aufgeteilt. Jeder Router kennt nur die Details in seiner Area und sonst nur die Verbindungsrouter zu den anderen Areas.
- Die Area 0.0.0.0 ist als Backbone-Area bekannt und muss zusammenhängend sein.
- Authentisierung möglich, unbekannte Router bleiben draussen
- Hello Pakete zum Erkennen neuer Router



OSPF V2

- Vorteile:
 - Stabiles Router Protokoll, auch geeignet für grosse Netzwerke
 - Trotz grosser Netzwerke geringer Datenverkehr
 - Sicher dank Authentisierung der Router
 - Sehr schnelle Konvergenz bei Verbindungsausfällen, da alternative Routen bereits bekannt sind
- Nachteile:
 - in kleinen ISDN-Routern nicht verfügbar
 - bei einigen Herstellern höhere Lizenzgebühren (z.B. Cisco)
 - komplexere Konfiguration



EIGRP

- Enhanced Interior Gateway Routing Protocol wurde von Cisco entwickelt und ist Standard auf diesen Routern.
- Hybrides Protokoll:
 - baut eine Distance Vector Tabelle auf (wie RIP)
 - behält Information von alternativen Verbindungen
 - meldet aber nur Veränderungen (wie OSPF)
- Vorteil:
 - weniger Datenverkehr zwischen den Routern (nur Updates)
 - Konvergenz schneller erreicht (alternative Route bereit)
 - in einem stabilen Netzwerk nur Hello Pakete
- Nachteile:
 - nur auf Cisco-Routern erhältlich
 - kein Area-Konzept