

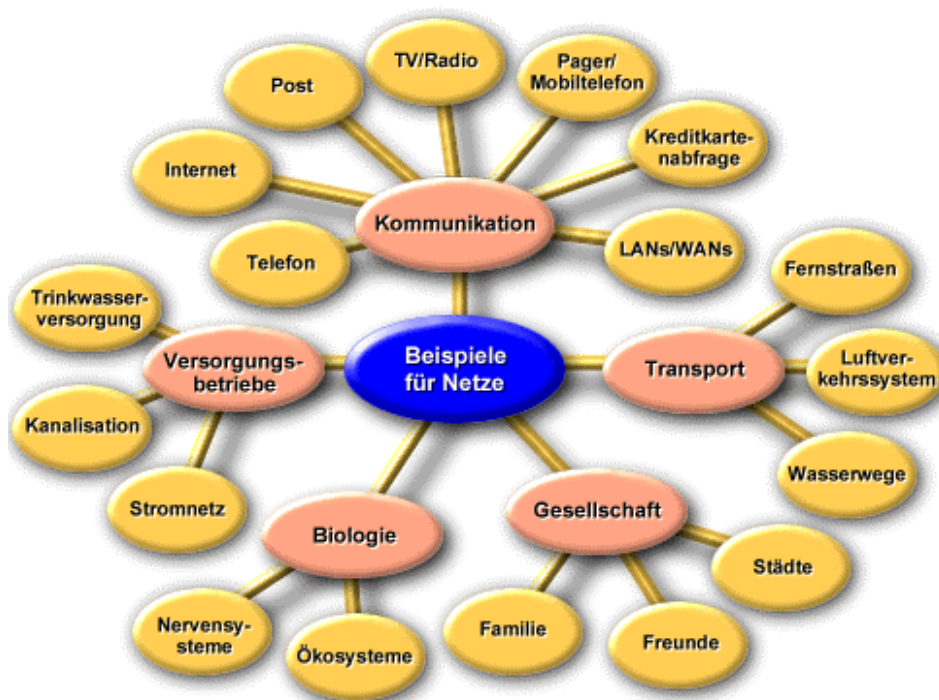
Einführung in die Netzwerktechnik

Grundlagen, Technik, Protokolle

03/2003-Georg N. Strauss

Inhalt:

1. Historische Entwicklung
2. Netzwerkdienste
3. Grundlagen der Netzwerktechnologie
4. Netzwerktopologien
5. Netzwerktechnologien im LAN Bereich
6. IP Adressierung
7. Netzwerkbegriffe



1. Historische Entwicklung

Terminalarbeitsplätze an Großrechnern:

- als Ersatz für offline-Eingaben über Lochkarten,
- Einzelanbindung von Terminals an je einen Anschlusspunkt am Zielrechner,
- später Terminalemulation auf Arbeitsplatzrechner mit der Möglichkeit des Datentransfers.

Netze zum (lokalen) Datenaustausch:

- schnellere Kommunikationsmedien,
- von mehreren Rechnern gleichzeitig benutzte Medien,
- Kopieren von Daten über das Netz,
- Terminalemulation.

Aufbau nationaler und internationaler Datennetze:

- Elektronische Post,
- Dateitransfer über weite Entfernungen.

Netzwerkbetriebssysteme:

- Einführung virtueller Netzwerkdienste (Drucker, Speicherkapazitäten),
- Client-Server-Konzepte,
-
- „Das Netzwerk als System“ (statt des Großrechners).

Verteilte Systeme

Multi-Media-Dienste und –Netze

| Art des Netzes | Was fließt? | Verschiedene Formen? | Regeln? | Transportmittel |
|----------------|---------------|---|---|--|
| Wasser | Wasser | Heiß, kalt, Trinkwasser, Abwasser | Zuflussregulierung (Betätigung von Hähnen), Spülen, Verbot bestimmter Substanzen in Abflüssen | Rohre |
| Straße | Fahrzeuge | LKWs, PKWs, Zweiräder | Verkehrs- und Höflichkeitsregeln | Straßen und Autobahnen |
| Post | Objekte | Briefe (schriftliche Informationen), Pakete | Regeln für Verpackungen und festgelegte Porti | Briefkästen, Postämter, LKWs, Flugzeuge, Zusteller |
| Telefon | Informationen | Gesprochene Sprache | Regeln für den Zugang zum Netz und Benimmregeln | Telefonleitungen, Funkwellen usw. |

Abb.1.1: Vergleich von verschiedenen allgemeinen Netzen

2. Netzwerkdienste

Angebote und Möglichkeiten, die dem Nutzer durch das Netz eröffnet werden.

2.1. Kommunikationsmodelle

2.1.1. Client-Server-Modell

- Server: Ein oder mehrere Netzwerkknoten stellen Dienste zur Verfügung
- Client: Andere Rechner nutzen diese Dienste, ohne selbst Dienste anzubieten
- Gängiges Modell für größere Netze
- Die Trennung in Clienten und Server wird nicht bezüglich jeder Funktion immer 100%ig eingehalten.
- Hintergrund: Ablösung von Großrechnersystemen durch Client-Server-Konzepte

2.1.2. Peer-To-Peer-Netze

- Netzwerk aus gleichberechtigten Rechnern
- Alle Rechner bieten Dienste an, alle nutzen Dienste
- Für kleine Netze geeignet
- Preiswert, da keine dedizierten Server
- Leistungsgrenzen
- Problem Betriebssicherheit

2.1.3. Verteilte Systeme

- Stärkere Verteilung der Aufgaben auf mehrere Server mit spezielleren Aufgaben,
- Mischung von Client-Server-Rollen
- Mit der Ausdehnung der Netze bieten sich die Möglichkeiten zu weitergehender Vermaschung
- Grenzen zu Client-Server-Modell fließend

2.2. Arten von Netzwerkdiensten

- Netze als EDV-Hilfsmittel mit dem Ziel einer effizienten Nutzung von EDV-Ressourcen:
 - Gemeinsame Nutzung von Druckern und anderen Peripheriegeräten
 - Gemeinsame Datenhaltung
 - Nutzung zentraler Archivierungs- und Sicherungssysteme
 - Zugriff auf entfernte Rechner und deren Kapazitäten
 - Hilfsmittel zum Datenaustausch (lokal)
- Netze als Hilfsmittel für Kommunikation und Informationsaustausch:
 - Funktion
 - Austausch von Daten (insbesondere über weitere Entfernungen)
 - Austausch von persönlichen Informationen
 - Allgemeine Informationsdienste
 - Diskussionsforen
 - Typische Anwendungen
 - Email
 - Diskussionslisten (News, Listserver)
 - Verteilte Informationssysteme (Gopher und World Wide Web)
- Zukünftige Ziele:
 - Multi-Media-Systeme: Integration aller Kommunikations- und Mediensysteme (Sprache, Bilder und Daten, Unterhaltung und Geschäftsleben)
- Unterteilungsmöglichkeit der Dienste nach typischen LAN- oder WAN-Diensten

2.3. Beispiele

2.3.1. Mehrfachnutzung von Ressourcen

- Massenspeichernutzung
 - File-Server
 - Benutzerdaten (Vorteil: gleiche Daten für alle, gleiche Daten überall, zentrale Sicherung)
 - Anonymous FTP
 - Typische Protokolle: IP/NFS, IPX, SMB, AppleTalk/AFP
 - Archiv-Server
 - Backup-Server
- Software-Nutzung
 - Nutzung zentral gehaltener und gepflegter Software (bei Nutzung der eigenen CPU)
 - Zentrale Pflege
 - Sicherheit (z.B. discless Workstations)
 - Effiziente Nutzung von Lizenzen
 - Zugriff auf Software und CPU entfernter Rechner
- CPU-Nutzung
- Peripherie-Nutzung
 - Drucker
 - Plotter
 - Spezialausgabe-Geräte
 - Eingabegeräte (Bänder, Kassetten)
- Verteilte Datenbanken
- Spezielle Kombination von Speicher-, Software- und CPU-Nutzung
- Datenbankabfragesprache (SQL)
- Achtung: Unterschied zwischen SQL-Servern und Zugriff auf Datenbankdateien über File-Server!

2.3.2. Verteilte Systeme

- Verteilte Dateisysteme
 - NFS bei starker Verschachtelung der Server-Dienste
 - AFS
 - Vom Konzept her ein weltweites Dateisystem
- Verteilte Fenstertechnik
 - X-Window
 - Achtung bei den Begriffen: der Server ist der lokale Rechner (der den Bildschirm zur Verfügung stellt)
- Verteilte Datenbanken
 - Aufteilung von Datenbanken auf mehrere Server
- Verteilte Anwendungen / Parallelverarbeitung
 - nur mit Hochgeschwindigkeitsnetzen
- Verteilte Informationssysteme

2.3.3. Kommunikationsdienste

- Dateitransfer
- E-Mail
- Verteilung von Nachrichten (Broadcasts)
- Diskussionslisten
 - Per E-Mail (Listserver)
 - Als Diskussionsforum
 - Client-Server-Struktur
 - z.B. NetNews
- Informationsdienste
 - Gopher
 - World-Wide-Web

- Multimedia-Dienste

2.3.4. Mehrfachzugang zu Telekommunikationsdiensten

Übergang in andere Netze

- Gateways
 - Übergang LAN-Backbone
 - Übergang zu Weitverkehrsnetzen
- Telekom-Dienste
 - Datex-P/X.25
 - ISDN
 - DSL
 - Telex/Teletex
 - FAX
 - Btx

3. Grundbegriffe der Netzwerktechnologie

Eine mögliche Einteilung der Datennetze ist nach deren geografischer Ausdehnung. Hier kann man zwischen LAN (Local Area Network), MAN (Metropolitan Area Network), WAN (Wide Area Network) und GAN (Global Area Network) unterschieden werden. In vielen Fällen wird nur zwischen lokalen Netzen (LAN) und Weitverkehrsnetzen (WAN) unterschieden.

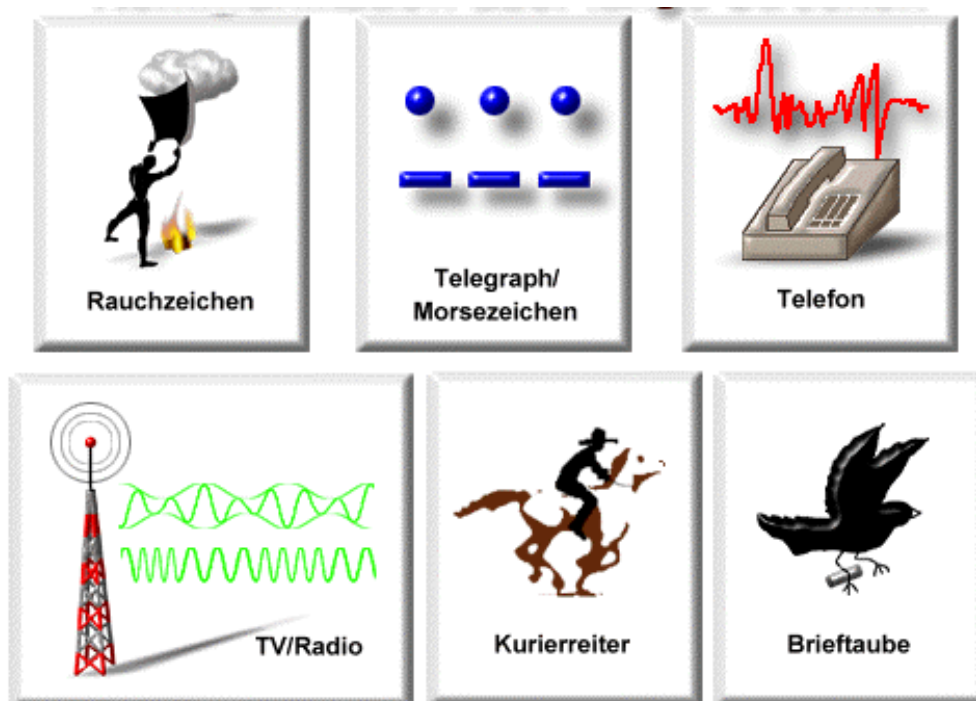


Abb.3.1: Kommunikation über lange Strecken

Als Unterscheidungsmerkmale zwischen LAN und WAN können folgende Kriterien dienen:

| Kriterium | LAN | WAN |
|---------------------------------|--|--|
| Geographische Ausdehnung | Geographisch auf einzelne Gebäude oder Gebäudekomplexe beschränkt (z.B.: Firma, Campus). | Verbindung weitentfernter LANs (oder MANs) miteinander. |
| Übertragungskapazitäten | Hohe Übertragungskapazität (10 0 MBit/s oder mehr). | Meist vergleichsweise geringe Übertragungskapazitäten (meist von ca. 10 kbit/s bis 2 MBit/s, erst neuere Techniken (ATM - Asynchronous Transfer Modus) bieten 34 MBit/s und mehr). |
| Dienstangebote | LANs dienen meist der Nutzung verteilter Ressourcen wie Datei- und Druckerserver. | WANs dienen meist dem Zugriff auf entfernte Rechner (Terminalemulation), der Datenübertragung oder dem Informationsaustausch (email, Diskussionslisten, WWW , usw.). |
| Vermittlungsfunktion | keine Vermittlungsfunktion | keine Vermittlungsfunktion vorhanden |
| Eigentumsverhältnisse | Privates Netz | Meist öffentliche Netze |
| Nutzungsgebühren | Meist keine | Anschlussgebühren und/oder Nutzungsgebühren |
| Struktur | Shared Media | Peer to Peer (Punkt-zu-Punkt) |

Als eine Zwischenstufe zwischen LAN und WAN wird auch der Begriff des Metropolitan Area Network (MAN) benutzt. Darunter versteht man dann ein Netz mit LAN-Technologie (Zugriffsverfahren und Adressierung) und LAN-Geschwindigkeiten aber WAN-Ausdehnungen und Vermittlungsfunktionen. Zusätzlich werden hier z.T. auch virtuelle private Netze (VPN) implementiert.

Bei WANs wird zwischen Leitungs- und Paketvermittlung unterschieden:

Leitungsvermittlung:

- Schaltung einer dedizierten Leitung (eventuell mit Benutzung von Multiplexverfahren). Insofern ähnlich den ersten Terminalnetzen, bei denen dedizierte Leitungen von jedem Terminal zu einem dedizierten Anschluss am Großrechner gezogen wurden oder dem Telefonnetz, bei dem Leitungen vorübergehend geschaltet werden, die dann für eine Verbindung dediziert benutzt werden.
- Nachteil, dass ihre Übertragungskapazität wegen anwendungsbedingter Übertragungspausen nicht vollständig ausgenutzt werden kann.
- Vorteil einer garantierten Übertragungskapazität.
- Flexibilität bei Kommunikationsprotokollen.

Paketvermittlung:

- Daten werden in kleinen Blöcke geteilt (Pakete), die dann unabhängig von einander zwischen den Kommunikationspartnern übertragen werden.
- Nachteil, dass bei jedem Paket die Adressierungsinformation mitübertragen werden muss („Verschwendung“ von Übertragungskapazität).
- Die Übertragungswege können von mehreren Kommunikationen quasi zeit-gleich genutzt werden.
- Eine verfügbare Übertragungskapazität kann einzelnen Kommunikationen nicht garantiert werden.

- In Vermittlungssystemen müssen Daten zwischengespeichert werden (Verzögerung, aufwendigere Vermittlungssysteme, Möglichkeit von Datenverlusten bei Stauungen auf Teilstrecken).

In LANs wird das Betriebsmittel zur Datenübertragung (physikalisches Medium) bzw. die Übertragungskapazität typischerweise von allen Stationen gemeinsam genutzt (Shared-LAN). Daher müssen in LANs Verfahren für die Erteilung einer Sendeberechtigung auf dem gemeinsam genutzten Medium definiert werden (Mediumzugriffsverfahren - Medium Access Control - MAC).

Dabei tritt bei Shared-LANs das Problem der Verteilung von Übertragungskapazitäten auf, die einerseits „gerecht“ sein, andererseits aber mit möglichst wenig Aufwand realisiert werden soll. Zudem kann das Problem auftreten, dass einzelnen Anwendungen im Netz wegen ihrer Wichtigkeit Prioritäten eingeräumt werden sollen.

Bei den Zugriffsverfahren, gibt es deterministische (z.B. Token-Ring, FDDI) und statistische Ansätze (z.B. Ethernet). Neuere LAN-Techniken versuchen über zentrale Knoten kurzzeitig zwischen Kommunikationspartnern dedizierte Verbindungen zu schalten (Switching). Solche LANs werden dann als Switched-LANs bezeichnet. Beispiele sind Switched-Ethernet, Switched-Token-Ring, Switched-FDDI oder ATM (letzteres nicht nur als LAN-Technik).













| Entfernung zwischen CPUs | CPUs befinden sich im selben bzw. in der selben | Symbol | Name |
|--------------------------------|--|---|---|
| 0,1 m | Gedruckte Leiterplatte PDA oder Palmtop-Rechner |  | Motherboard Personal Area Network (PAN) |
| 1,0 m | Meter Mainframe-Rechner |  | Computer-Systemnetzwerk |
| 10 m | Raum |  | Local Area Network (LAN) Ihr Klassenzimmer |
| 100 m | Gebäude |  | Local Area Network (LAN) Ihre Schule |
| 1000 m = 1 km | Campus |  | Local Area Network (LAN) Stanford University |
| 10.000 m = 10 km | Stadt |  | Metropolitan Area Network (MAN) San Francisco |
| 100.000 m = 100 km | Land |  | Wide Area Network (WAN) Cisco Systems, Inc. |
| 1.000.000 m = 1.000 km | Kontinent |  | Wide Area Network (WAN) Afrika |
| 10.000.000 m = 10.000 km | Planet |  | Wide Area Network (WAN) Das Internet |
| 100.000.000 m = 100.000 km | Erde-Mond-System |  | Wide Area Network (WAN) Erde & künstliche Satelliten |
| 1.000.000.000 m = 1.000.000 km | Satelliten |  | Solar Area Network (SAN) |
| 71.000.000 km | Sonnensystem |  | Star Trek Area Network (STAN) |

Abb.3.2: Beispiele für Datennetze unterschiedlicher Ausdehnung

4. Netzwerktopologien

Netzwerktopologie: Art und Weise wie die Stationen im Netz miteinander verbunden werden. Dabei kann die physikalische Struktur von der logischen Struktur (Softwarekonzeptionen oder Protokoll) abweichen.

Bei WANs werden typischerweise Knotenrechner in einer baumförmigen oder vermaschten Struktur miteinander über dedizierte Leitungen verbunden (die dann von den Knotenrechnern mit Paketen beschickt werden oder im Multiplexverfahren in Kanäle aufgeteilt werden).

Im LAN treten folgende Topologien auf:

4.1. Physikalische Topologie

Bustopologie

- Anschluss aller Stationen an ein gemeinsames Kabel
- Senden von Daten in alle Richtungen.
- Keine Verteilerfunktionen nötig.
- Geringer Platzbedarf für die Verkabelung, wenige Kabel
- Jede Störung an Kabeln oder Endgeräten kann zu einem Totalausfall des Netzes führen.
- Meist Abschlusswiderstände notwendig

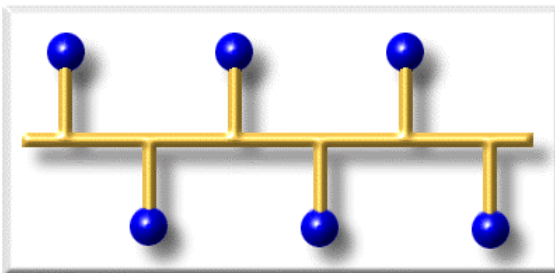


Abb.4.1: Bustopologie

Sterntopologie

- Dedizierte Kabel von jeder Station zu einem zentralen Verteiler (der aber anders als bei Terminalvernetzungen oder WANs keine Endgeräte oder Vermittlungsfunktion hat).
- Notwendigkeit von (mehr oder weniger intelligenten) Verteilern.
- Hoher Aufwand bei Verkabelung
- Flexibilität in der Konfiguration.
- Geringe Anfälligkeit bei Störungen seitens der Verkabelung oder durch die Endgeräte, da ein Defekt jeweils nur eine Station stören.
- Netzwerk-Managementfunktionen im bzw. mit Hilfe des Verteilers möglich.

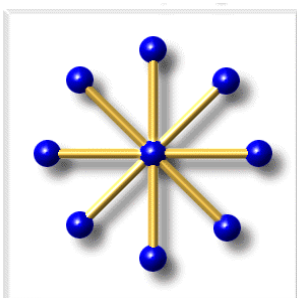


Abb.4.2: Sterntopologie

Baumtopologie

- Erweiterung der Sterntopologie durch Zusammenschaltung mehrerer Sterne mittels Leitungen zwischen den Verteilern
- Vor- und Nachteile wie bei Sterntopologie.

Ringtopologie

- Verbindung aller Stationen in Form eines Ringes.
- Jede Station überträgt empfangene Daten an die nächste Station im Ring weiter.
- Geringere Kabelmengen als bei Sterntopologie und kaum mehr als bei Bustopologie.
- Ausfall einer Kabelstrecke oder einer Station kann zu einem Totalausfall führen.
- Häufig Ausführung als Doppelring, um den Ausfall einer Verbindung oder einer Station kompensieren zu können.

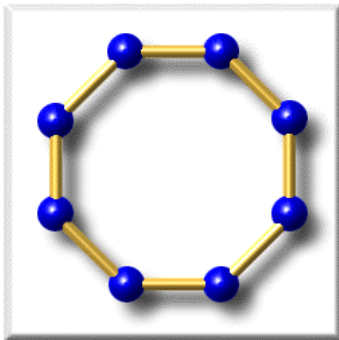


Abb.4.3: Ringtopologie

4.2. Logische Topologie

- Bustopologie
- Ringtopologie
- Physikalische Stern- oder Baumtopologien werden durch entsprechende Verschaltung der Leitungen zu logischen Bussen oder Ringen verwandelt (anders bei WAN-Verbindungen, bei denen die Baumstruktur explizit berücksichtigt wird).

Beim Entwurf einer Netzwerkarchitektur sind zwei Grundregeln zu berücksichtigen:

- Es ist davon auszugehen, dass Daten verfälscht werden können.
- Es ist davon auszugehen, dass Daten verloren gehen können.

4.2. Arten von Netzwerkkomponenten

Hardware

- **Passive Komponenten:** Komponenten die über keine Stromversorgung verfügen
 - Kabel
 - Stecker
 - Passive Ringleitungsverteiler (im Token Ring)
- **Aktive Komponenten:** Komponenten, die eine Stromversorgung benötigen
 - Rechner
 - Internetworking Komponenten (Repeater, Brücken, Router usw.)
- **Architekturen und Normen**
 - Modelle für Netzwerkverfahren
 - Normierungen von Netzwerktechnologien und Komponenten
- **Software**
 - Netzwerkbetriebssysteme
 - Netzerkwendungen

5. Netzwerktechnologien im LAN Bereich

5.1. Überblick

Gängige Vernetzungstechnologien im LAN-Bereich sind:

Terminalvernetzung

- Im wesentlichen veraltet, aber zum Teil noch vorhanden.
- Statt einer direkten Verkabelung Terminal-Rechner erfolgt meist der Anschluss von Terminals an Terminalserver, die dann über ein LAN mit Rechnern kommunizieren.
- Wird im weiteren nicht behandelt.

Ethernet

- In LANs die am weitesten verbreitete Technologie.
- Durch Bustopologie und weite Verbreitung sehr kostengünstig zu realisieren.
- Mit einer Übertragungskapazität von 10 MBit/s ein LAN mittlerer Geschwindigkeit. (Realistische ist eine Auslastung von 30% die oberste Grenze.)
- Ursprüngliche Entwicklung durch Digital, Intel und Xerox.
- Statistische Zugriffskontrollverfahren.
- Weiterentwicklungen zu Fast Ethernet mit 100MBit/s Übertragungskapazität.

Token-Ring

- Von IBM entwickeltes Vernetzungssystem mit (logischer) Ringtopologie und in der Praxis physikalischer Sterntopologie als Konkurrenz zu Ethernet.
- Durch Anforderungen an die Verkabelung, Netzwerkadapter und geringere Verbreitung teurer als Ethernet.
- Mit einer Übertragungskapazität von 4 oder 16 MBit/s ein LAN mittlerer Geschwindigkeit.
- Deterministisches Zugriffskontrollverfahren.

FDDI

- Hochgeschwindigkeitsnetz für LAN und MAN (100 MBit/s)
- Physikalische Doppelring und/oder Baumstruktur.
- Logische Ringstruktur.
- Deterministisches Zugriffskontrollverfahren.

ATM

- Hochgeschwindigkeitsnetz für LAN und WAN.
- Eignung für Multi-Media-Anwendungen.
- Cell-Switching-Technologie.

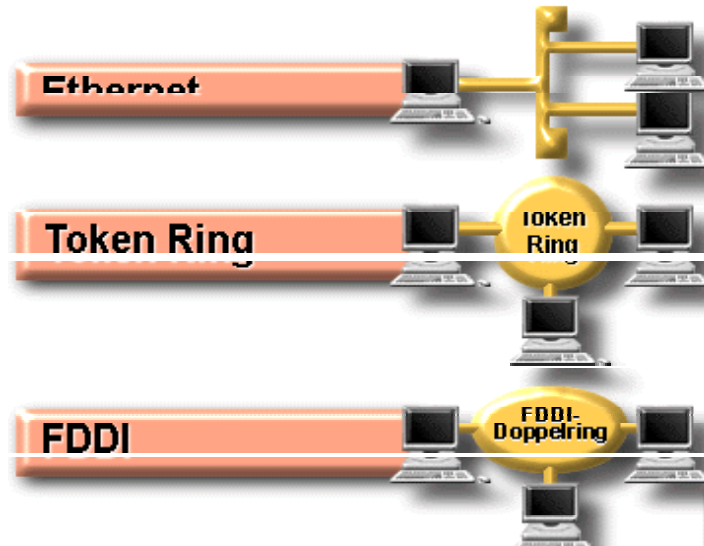


Abb.5.1: Beispiele für LAN Technologien

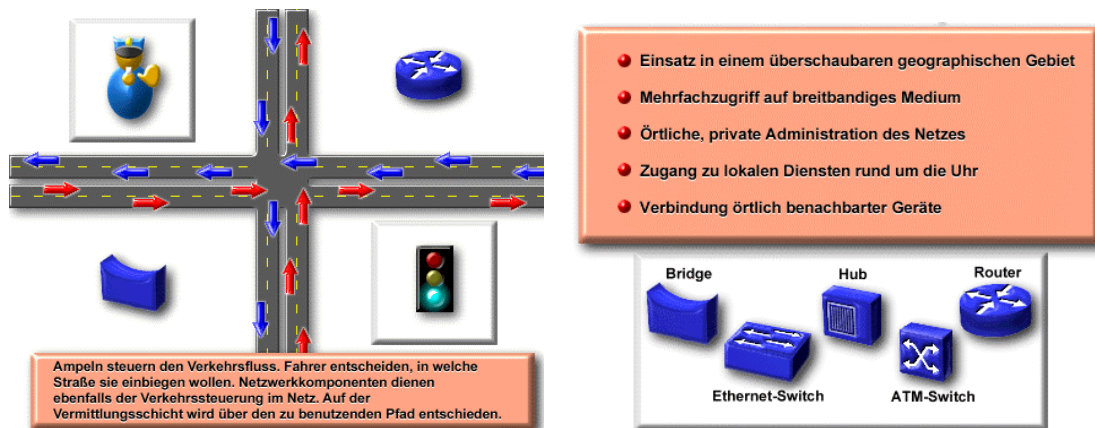


Abb.5.2: Beispiele für Netzwerkkomponenten

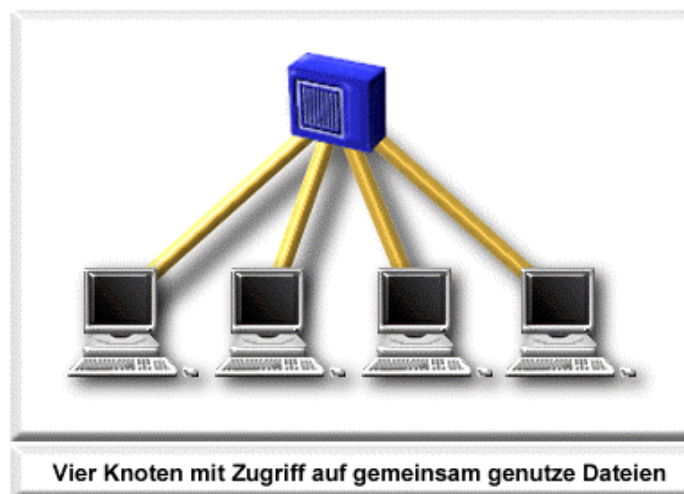


Abb.5.3: Netzwerk mit Hub

5.2. Physikalische Medien



Abb.5.4: Beispiele für physikalische Übertragungsmedien

10 Base 2 oder Thinwire-Ethernet

- Historisch die zweite Variante von Ethernet-Verkabelung
- Billigere und flexiblere Alternative zu 10 Base 5 (Thicknet)
- Maximale Länge eines Segments: 185 m
- Koaxialkabel mit
 - 50 Ω Wellenwiderstand
 - Signalausbreitungsgeschwindigkeit (ca.) 0,65c
 - Kabeldurchmesser ca. 0,5 cm
 - Minimaler Biegeradius bei Verlegung 5 cm
 - Leicht voneinander abweichende Kabeltypen (zusätzliche Schirmung, abweichende Signalausbreitungsgeschwindigkeiten)
 - Achtung: unterschiedliche Kabel sollten möglichst nicht vermischt werden!
- Maximale Anzahl Anschlüsse pro Segment: 30 Anschlussmöglichkeiten:
 - BNC-Steckverbinder
 - Unterbrechungsfreie Steckverbindungen / Dosen
- Mindestabstand zwischen zwei Anschlussstellen: 0,5 m

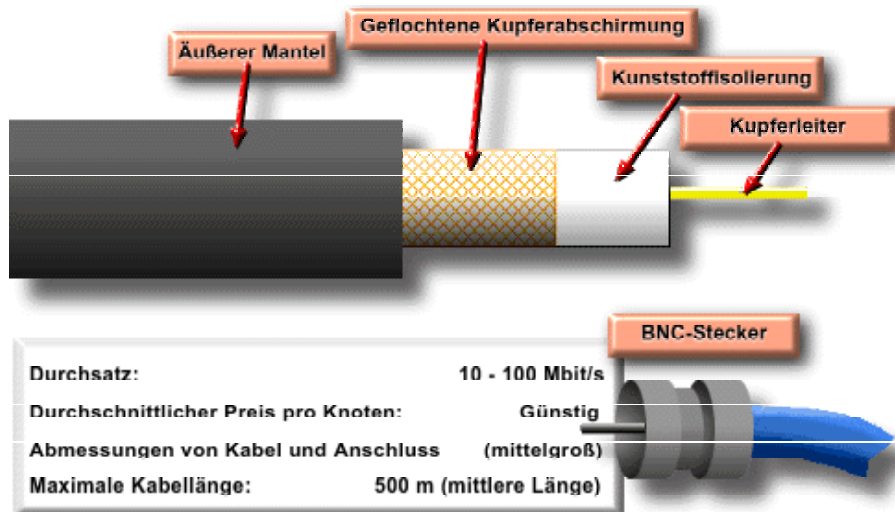


Abb.5.5: Koaxialkabel - 10Base2

10 Base 5 oder Thickwire-Ethernet

- Ursprüngliche Ethernet-Verkabelung
- Heute veraltet (höchstens noch in lokalen Backbones zu finden).
- 500 m maximale Segmentlänge
- Koaxialkabel mit
 - 50 Ω Wellenwiderstand
 - 0,77c Signalausbreitungsgeschwindigkeit (c=Lichtgeschwindigkeit=300.000 m/s)
 - ca. 1 cm Durchmesser
 - 25 cm Biegeradius (beim Verlegen einzuhaltender minimaler Radius einer Biegung des Kabels)
- Maximale Anzahl Anschlüsse pro Segment: 100 MAUs (MAU=Media Access Unit, auch Transceiver genannt)
- Maximale Stationsanzahl im Netz (genauer: innerhalb einer Kollisionsdomäne): 1024
- Anschlüsse von Stationen durch
 - „Vampirklemmen“ (Taps) ohne Unterbrechung des Kabels oder
 - Steckverbinder (Installation nach Auftrennung des Kabels)
- Mindestabstand zwischen zwei Anschlüssen: 2,5 m
- Anschluss von Stationen an MAUs über Dropkabel mit
 - Maximaler Kabellänge von 50 m
 - Signalausbreitungsgeschwindigkeit 0,65c
 - Maximale Signallaufzeit von 0,257 μ s

10 Base T oder Twisted-Pair-Ethernet

- Twisted Pair: Moderne Variante der Ethernet-Verkabelung
- Strukturierte Verkabelung
- Sternförmige Kabelführung zu jedem Anschluss
- Verkabelung mit Standardkabeln, die auch für andere Netzwerktechniken nutzbar sind.
- Eigener Anschlusspunkt für jeden einzelnen Anschluss an einem Verteiler mit Repeaterfunktion nötig
- Maximale Kabellänge für einen Anschluss: 100 m
- Paarweise verdrehte Kabel mit
 - 100 Ω Wellenwiderstand
 - Signalausbreitungsgeschwindigkeit 0,585c bei ungeschirmten (UTP-) Kabeln
 - Signalausbreitungsgeschwindigkeit 0,75c bei geschirmten Kabeln des Typs „Kategorie 5“
 - Zweipaarige Kabel

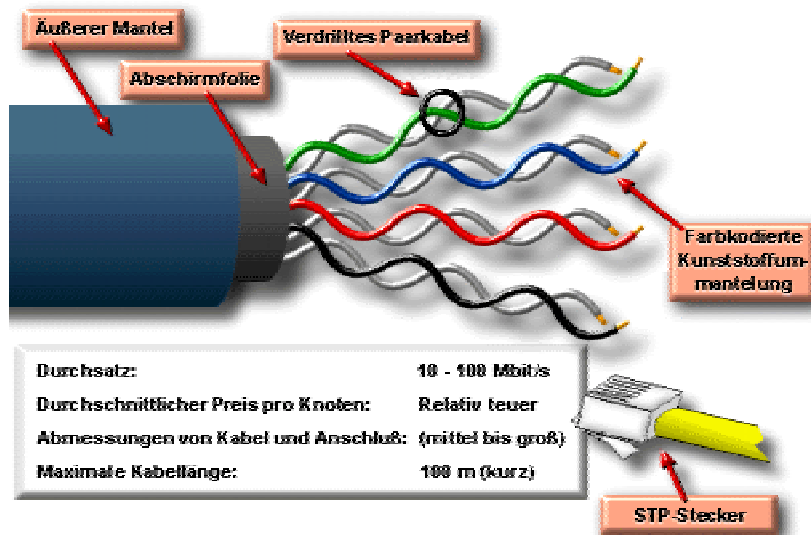


Abb.5.6: Verdrehtes Paarkabel – Twisted Pair (TP)

10 Base F oder Glasfaser-Ethernet

- Strukturierte Verkabelung
- Sternförmige Kabelführung zu jedem Anschluss
- Auch für andere Netzwerktechniken nutzbar
- Eigener Anschlusspunkt für jeden einzelnen Anschluss an einem Sternkoppler
- Maximale Kabellänge für einen Anschluss:
 - 2000 m bei aktiven Sternkopplern
 - 500m bei passiven Sternkopplern (unüblich)
- Glasfaserkabel
 - In der Regel Gradientenkabel 62,5/125 μ (in Europa abweichend oft 50/125 μ)
 - Selten Monomodekabel 9/125 μ
 - Zwei Fasern pro Verbindung
 - Signalausbreitungsgeschwindigkeit 0,68c
- Maximale Anschlüsse pro Kabelsegment: 1 Station
- Anschluss technik: ST-Steckerverbinder
- Kostenintensive aber zukunfts sichere Verkabelungsvariante
- Besser Abhörsicherheit als Kupferkabel
- Keine elektromagnetischen Beeinflussungen

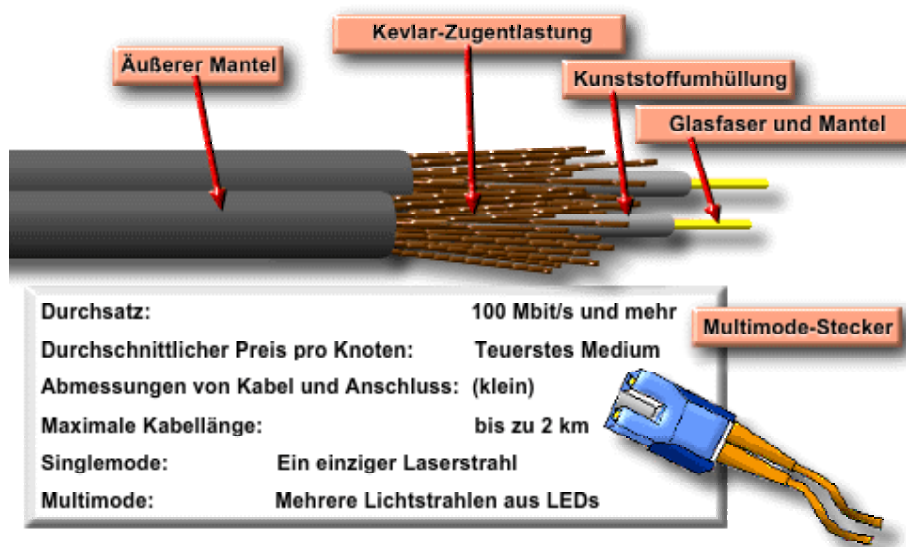


Abb.5.7: Glasfaserkabel

100 Base TX

- Ethernet-Variante mit 100 MBit/s Übertragungsrage
- Strukturierte Verkabelung
- Sternförmige Kabelführung zu jedem Anschluss
- Verkabelung mit Standardkabeln, die auch für andere Netzwerktechniken nutzbar sind.
- Eigener Anschlusspunkt für jeden einzelnen Anschluss an einem Verteiler mit Repeaterfunktion nötig
- Maximale Kabellänge für einen Anschluss: 100 m
- Paarweise verdrehte Kabel (wie bei 10 Base T) mit
 - 100 Ω Wellenwiderstand
 - Signalausbreitungsgeschwindigkeit 0,75c bei geschirmten Kabeln des Typs „Kategorie 5“
 - Zweipaarige Kabel der Kategorie 5 bzw. 7
- Maximale Anschlüsse pro Kabelsegment: 1 Station
- Anschlusstechnik: RJ45-Steckerverbinder

100 Base FX

- Ethernet-Variante mit 100 MBit/s Übertragungsrage
- Strukturierte Verkabelung
- Sternförmige Kabelführung zu jedem Anschluss
- Verkabelung mit Standardkabeln, die auch für andere Netzwerktechniken nutzbar sind.
- Eigener Anschlusspunkt für jeden einzelnen Anschluß an einem Verteiler mit Repeaterfunktion nötig
- Maximale Kabellänge für einen Anschluss: 450 m (bei Duplex-Übertragung bis 2000m)
- Glasfaserkabel
 - In der Regel Gradientenkabel 62,5/125 μ (in Europa abweichend oft 50/125 μ)
 - Selten Monomodekabel 9/125 μ
 - Zwei Fasern pro Verbindung
 - Signalausbreitungsgeschwindigkeit 0,68c

VG-AnyLAN

- Konkurrierende Entwicklung zu 100BaseXY-Standards
- Eigentlich kein Ethernet, da nicht CSMA/CD-Algorithmus
- Demand Priority Verfahren:
 - Vergabe der Zugriffsberechtigung durch den zentralen Verteiler
 - auf Anforderung
 - mit Möglichkeit von Prioritätenvergabe
 - in festgelegter Reihenfolge der Ports
- Standardisiert als IEEE 802.12 (nicht 802.3 wie alle Ethernet-Varianten)

Beispiele für typische Medien

| Beispiele für typische Medien | Maximale theoretische Bandbreite | Maximaler Abstand |
|---|----------------------------------|-------------------|
| 50-Ohm-Koaxialkabel (Ethernet 10Base2, ThinNet) | 10-100 Mbit/s | 185 m |
| 50-Ohm-Koaxialkabel (Ethernet 10Base5, ThickNet) | 10-100 Mbit/s | 500 m |
| Unabgeschirmte verdrehte Paarkabel (UTP) der Kategorie 5 (Ethernet 10BaseT, 100Base-TX) | 10 Mbit/s | 100 m |
| Unabgeschirmte verdrehte Paarkabel (UTP) der Kategorie 5 (Ethernet 100Base-TX)(Fast Ethernet) | 100 Mbit/s | 100 m |
| Multimode (50/125 µm) Glasfaserkabel 100Base-FX | 100 Mbit/s | 2000 m |
| Singlemode (10 µm Kern) Glasfaserkabel 1000Base-LX | 1000 Mbit/s (1.000 Gbit/s) | 3000 m |
| Andere Technologien, an denen geforscht wird | 2400 Mbit/s (2.400 Gbit/s) | 40 km = 40.000 m |
| Drahtlos | 2.0 Mbit/s | 100 m |

Abb.5.8: Typische kennwerte von physikalischen Medien

5.3. Ethernet

5.3.1. Medienzugriffsverfahren

Ethernet ist ursprünglich unter diesem Namen von Digital, Intel und Xerox als Ethernet Version 1 und Ethernet Version 2 „standardisiert“ worden. An manchen Stellen findet man daher das Kürzel DIX für die drei Entwicklerfirmen. Ethernet V.1 hat heute keinerlei Bedeutung mehr.

Später erfolgte eine Standardisierung durch internationale Gremien (IEEE und ISO), die allgemein unter der Bezeichnung 802.3 bekannt ist. Diese weicht geringfügig von Ethernet V.2 ab ist aber damit kompatibel. Der Begriff Ethernet wird meist für beide Standards benutzt.

Das wesentliche Charakteristikum des Ethernet ist das Verfahren der Mediumzugriffskontrolle.

Das Verfahren nennt sich CSMA/CD (Carrier Sense, Multiple Access with Collision Detection) und entspricht den Prinzipien einer Gesprächsrunde ohne Diskussionsleiter.

Bei einer solchen Diskussionsrunde gelten folgende Regeln:

- Jeder Teilnehmer kann anfangen zu reden, wenn nicht schon ein anderer redet.
- Sollten mehrere Teilnehmer zufällig gleichzeitig in einer Gesprächspause anfangen zu reden, so haben sie alle sofort ihren Beitrag abzubrechen.
- Durch zufällige Verzögerungen (oder Gesten) ergibt sich dann, wer als nächster reden darf.

Vorgehen bei Ethernet

- Sendewillige Stationen hören das Medium ab und warten bis es frei ist (Carrier Sense).
- Ist das Medium frei, so kann jede sendewillige Station nach einer Pause von 96 Bit (9,6µs, 12 Byte, Interframe Gap) einen Sendevorgang beginnen (Multiple Access).
- Während des Sendens überprüft jede Station ob andere Stationen gleichzeitig senden, es also zu einer Kollision kommt (Collision Detection). Kollisionen werden an der Überlagerung von Signalen (überhöhte Signalpegel, Phasenverschiebung der Signale) erkannt.

- Nach dem Erkennen einer Kollision werden noch 4-6 weitere Byte (meist als 01-Bitmuster) gesendet, damit alle Stationen genügend Zeit haben, die Kollision zu erkennen (Jam Signal).
- Nach dem Ende aller Übertragungen während eines Kollisionsvorgangs warten alle Stationen $9,6\mu\text{s}$ (Interframe Gap).
- Die kollisionserzeugenden Stationen warten zusätzlich ein Vielfaches i der Slot time (512 Bit , 64 Byte , $51,2\mu\text{s}$), wobei i eine Zufallszahl zwischen 0 und 2^k ist und k die Nummer des Übertragungsversuchs für ein bestimmtes Paket (maximal 10) ist. (Backoff-Algorithmus)
- Nach Ablauf der Wartezeit beginnt der Algorithmus von vorn.

Sollte bei dem Versuch ein bestimmtes Paket zu senden 16mal eine Kollision auftreten, so wird ein Fehler (Excessive Collision) gemeldet und der Übertragungsversuch abgebrochen.

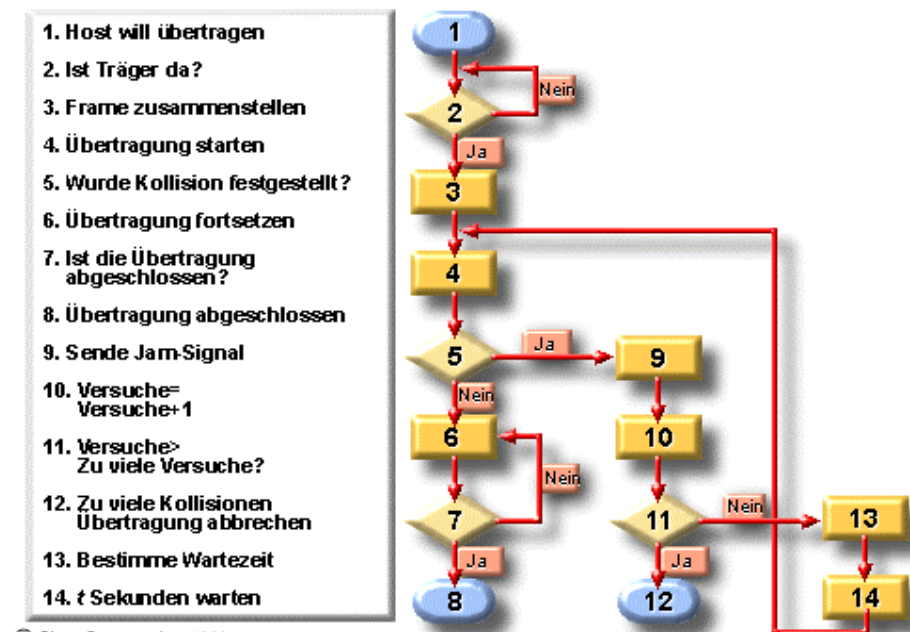


Abb.5.6: Ablauf einer CSMA/CD Kommunikation

5.3.2. Konsequenzen des CSMA/CD-Verfahrens

Aus der Notwendigkeit der Kollisionserkennung ergeben sich Konsequenzen:

- Die sendenden Stationen müssen eine Kollision vor dem Ende des jeweiligen Sendevorgangs erkennen. Beispiel:
- Station A beginnt zu senden (Zeitpunkt 0).
- Station B beginnt unmittelbar bevor sie das Signal von A erreicht zu senden (Zeitpunkt t).
- Station B erkennt praktisch sofort die Kollision (Zeitpunkt t)
- Station A erkennt die Kollision erst, wenn das Signal von B bei A angekommen ist (Zeitpunkt $2t$).
- Hätte Station A den Sendevorgang zum Zeitpunkt $2t$ schon beendet, so hätte A die Kollision nicht erkannt, wodurch das Verfahren zusammenbrechen würde (CD!).
- Folgerung: Die maximale Signallaufzeit zwischen zwei Stationen im Netz und die minimale Paketlänge müssen unter Berücksichtigung der Übertragungsrateso aufeinander abgestimmt sein, dass das Senden eines Pakets minimaler Größe länger als die doppelte maximale Signallaufzeit im Netz dauert. Im Ethernet müssen folgende Werte eingehalten werden:
 - Maximale Signallaufzeit: $25,6\mu\text{s}$
 - Minimale Paketlänge: 64 Byte (512 Bit , $51,2\mu\text{s}$)

5.3.3. Adressierung

Jede Station im Ethernet muss eine eindeutige Adresse (**MAC-Adresse**) besitzen, um angesprochen werden zu können. Der Standard legt fest, dass die MAC-Adressen **48 Bit** lang sein müssen.

In der Praxis werden die Adressen von den Herstellern von Netzwerkadaptern fest-gelegt und bestehen aus einem 24 Bit langem Code des Herstellers und einer ebenso langen Seriennummer (**Hardware-Adressen**).

Die MAC-Adressen weisen daher keine besondere Systematik bezogen auf die Netztopologie auf.

Neben Adressen für die einzelnen Stationen gibt es auch **Gruppenadressen**, mit denen mehrere Stationen in Form eines Rundrufs angesprochen werden können. Solche Adressen sind dadurch erkennbar, dass das erste Bit der Adresse eine 1 ist.

Die bekannteste Gruppenadresse ist die Broadcast-Adresse (an alle). Sie besteht an allen Positionen aus Einsen (hexadezimal geschrieben FFFFFFFF). Die anderen Funktionsadressen werden als Multicast-Adressen bezeichnet (an viele). Manche Software-Hersteller (z.B. Digital bei DECnet) benutzen nicht die vordefinierten, aber unsystematischen Hardware-Adressen, sondern definieren per Software andere MAC-Adressen, um eine Systematik der Adressen zu erhalten und in der Netzwerksoftware zu nutzen. Solche Adressen werden dadurch gekennzeichnet, dass das zweite Bit der Adresse den Wert 1 hat. Solche Adressen heißen dann lokale Adressen im Gegensatz zu den universalen Adressen mit einer 0 an Bitposition 2.

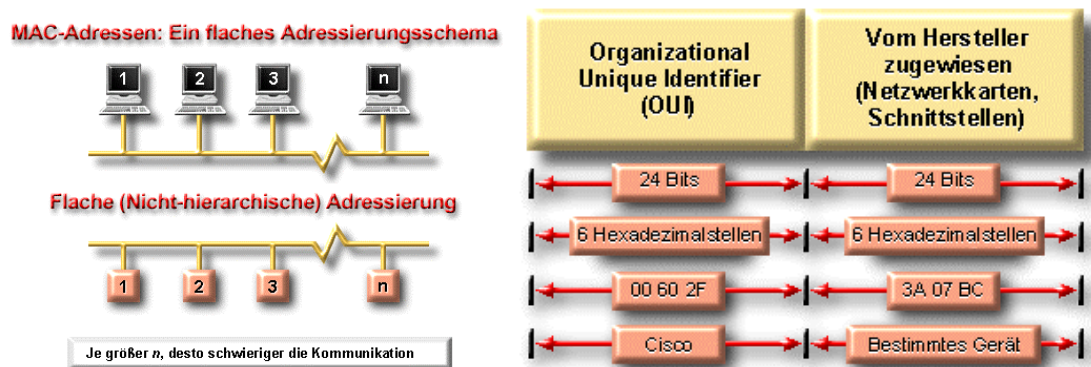


Abb.5.8: MAC Adressen - Physikalische Adresse eines bestimmten Host (NIC)

5.3.4. Arten fehlerhafter Pakete im Ethernet

- CRC-Fehler: Die Prüfsumme ist falsch.
- Alignment-Fehler: Die Anzahl der Bits ist nicht durch 8 teilbar.
- Runt-Pakete: Pakete, die kürzer sind als die minimale Länge.
- Jabber- oder Giant-Pakete: Pakete mit Überlänge
- Late Collisions: Kollisionen, die nach mehr als 51,2 μ s nach Beginn des Pakets auftreten.
- Excessive Collisions: 16 Kollisionen beim Versuch ein Paket zu senden.

5.3.5. Übertragungsverfahren

Signalisierung mit Pegel zwischen 450 mV und 1315 mV

- Idle-Level: 0 mV \pm 40 mV
- Gleichstromfreie Signalisierung
- Binäre Kodierung (nur 0 und 1)
- Signalisierung durch Spannungswechsel (nicht durch Spannungspegel)
- Selbstsynchronisation der Empfänger aus den Signalen

- Manchester-Codierung:
 - 1 ist Übergang von negativem zu positivem Pegel und 0 ist Übergang von positivem zu negativem Pegel
- Datenrate 10 MBit/s bei einer
- Bitrate (aus dem Kehrwert der Dauer eines Bits berechnet) von 10 MBit/s, einer
- Fundamentalfrequenz (Kehrwert aus der Dauer des kürzesten Signalzyklus) von 10 MHz und einer
- Baudrate oder Datentaktrate (Kehrwert der Dauer des kürzesten Impulses) von 20 Mbaud.
- Frequenz muß innerhalb minimaler Schwankungen bleiben
- Flankensteilheit muß innerhalb bestimmter Toleranzen liegen
- Für Fast Ethernet andere Kodierung (4B/5B Kodierung und Übertragung im MLT-3-Kode, s. FDDI)

5.4. Token Ring

5.4.1: Überblick

- Logische Ringtopologie
- Physikalisch meist als Stern aufgebaut
- Durch physikalische Sternstruktur bessere Ausfallsicherheit
- Kopplung im Verteilerstandort durch passive oder aktive MAUs oder RLV (Medium Access Unit bzw. Ringleitungsverteiler)
- Deterministische Zugriffskontrollverfahren (Token-Prinzip)
- Zwei Varianten
 - 4 MBit/s Übertragungskapazität (ursprünglicher Standard)
 - 16 MBit/s Übertragungskapazität (spätere Erweiterung)
- Von IBM entwickelt
- Als IEEE-Standard 802.5 normiert (bzw. ISO 8802.5)
- LLC-Protokoll 802.2 in Ebene 2 (wie bei Ethernet 802.3)

5.4.2. Medien

- Typisches Kabel: Geschirmte paarweise verdrehte Kabel vom IBM-Typ 1 oder 1M
- Andere Kabel: LWL und andere TP-Kabel
 - Bei IBM-Typ-1-Verkabelung: geschirmte paarweise verdrehte Vierdrahtkabel mit - 150 W Wellenwiderstand, 0,64 cm Durchmesser
- Maximale Kabellänge zum Verteiler (Lobe-Kabel) 100 - 375 m abhängig von der Anzahl der Verteilerstandorte und Ringleitungsverteiler
- Maximal 260 Geräte in einem Ring
- Anschlusstechnik
 - Am Verteiler und an Anschlußdosen: hermaphroditischer IBM-Datenstecker (Würfel, Stecker und Buchse gleichzeitig)
 - Am Endgeräte: DB9-Buchse
- Ein Bit entspricht ca. 50m (bei 4 MBit/s) oder 12,5m (bei 16 MBit/s).

5.4.3. Übertragungsverfahren

- Jede Station regeneriert das Signal
- Differential-Manchester-Kodierung
 - Abgeleitet vom Manchester-Code
 - Kodierung abhängig vom letzten Signal
 - Für 1: keine Umkehrung der Polarität am Signalanfang
 - Für 0: Umkehrung der Polarität am Signalanfang
 - In der Signalmitte bei 0 und 1 Polaritätsumkehrung
 - Zusätzliche Signale „J“ und „K“ ohne Polaritätsumkehr in der Signalmitte
 - „J“: keine Polaritätsumkehr am Anfang
 - „K“: Polaritätsumkehr am Anfang
- Datenrate 4 bzw. 16 MBit/s bei einer Bitrate von 4 bzw. 16 MBit/s, einer Fundamentalfrequenz von 4 bzw. 16 MHz und einer Baudrate von 8 bzw. 32 Mbaud.

5.4.4. Ringleitungsverteiler

- Zweck: Zusammenschluss der sternförmigen Verkabelung zu einem logischen Ring
- **Überbrückungsfunktion** bei nicht belegten Anschlüssen oder ausgeschalteten Endgeräten
- Aktive oder passive RLV
 - Passive RLV arbeiten ohne Spannungsversorgung und schalten über elektromechanische Relais (bei Anlegen einer „Phantomspannung“ durch das Endgerät)
 - Aktive RLV regenerieren die Signale wie eine Endstation, benötigen aber dafür eine Stromversorgung
- Anschlusszahl pro RLV 8-20 (Original-IBM 8)
- RLV können über zwei zusätzliche spezielle Ports (Ring-In [RI] und Ring-Out [RO]) miteinander verbunden werden (jeweils RI mit RO).
- Bei Ausfall einer RI-RO-Verbindung wird eine Umleitung geschaltet (der zweite Ausfall teilt den Ring in zwei isolierte Ringe)

5.4.5. Token-Prinzip

- Auf dem Ring wird ein spezielle Paket erzeugt: das **Token**
- Auf jedem Ring darf zu jedem Zeitpunkt nur ein Token vorhanden sein
- Länge des Token-Pakets: 3 Byte
- Spezielles Format des Token
- Senden darf nur die Station, bei der sich das Token befindet.
- Die sendende Station überträgt statt des Tokens einen Datenrahmen.
- Jeder Rahmen wird von allen Station unverändert weitergegeben (nur der Empfänger setzt ein Bit, um anzugeben, dass er den Rahmen erhalten hat, und der Monitor setzt ein Bit, um Rahmen, die nicht von der sendenden Station entfernt wurden, erkennen zu können).
- Die sendende Station nimmt den Rahmen vom Ring und sendet das Token wieder aus. (Es ist nicht erlaubt, sofort einen weiteren Rahmen zu senden.)
- Eine einzige Station im Ring hat das Recht ein Token zu erzeugen und seine Existenz zu überwachen (aktiver Monitor)
- Zu einer Zeit darf nur eine Station aktiver Monitor sein.
- Jede Station kann aktiver Monitor sein.
- Bei der Initialisierungen oder beim Ausfall des aktuellen aktiven Monitors muss (über eine relativ aufwendigen Algorithmus) ein neuer aktiver Monitor bestimmt werden.
- Maximale Rahmenlänge im Token Ring: 10 ms (also 5.000 Byte bei 4 MBit/s und 20.000 Byte bei 16 MBit/s)

5.4.6. Adressierung

- MAC-Adressen wie bei Ethernet, nur mit umgekehrter Bit-Reihenfolge in den Bytes (msb, most significant bit, höchstwertigstes Bit)

6.3.7. Management-Protokoll

- Komplexität des Token-Ring durch verschiedene Management-Funktionen, die von jeder Station aus ausführbar sein müssen:
 - Jede Station muß die Funktion des aktiven Monitors übernehmen können.
 - Aufgaben des Management-Protokolls:
- Sicherstellen, dass genau ein aktiver Monitor vorhanden ist.
- Der aktive Monitor überwacht anhand von speziellen Bits in den Datenrahmen und über Management-Rahmen die Funktionsfähigkeit des Rings.
- Mehrfachumkreisung von Rahmen im Ring verhindern (durch spezielles Bit im Rahmen).
- Signalisierung von Fehlern durch den aktiven Monitor.
- Feststellung des Nachbarn im Ring (MAC-Adresse)

- Minimale Speicherkapazität von 24 Bit (Token-Länge) im Ring (entspricht bei 4 MBit/s ca. 1.200m bzw. Bei 16 MBit/s 300m) bei Bedarf durch Pufferung durch aktiven Monitor
- Takt wird vom Monitor vorgegeben (keine Präambel zur Synchronisation), gegebenenfalls Aussenden von Idle-Signalen.

5.5. FDDI

5.5.1: Überblick

- FDDI = Fiber Distributed Data Interface
- Ursprünglich nur für Glasfasern definiert.
- Hochgeschwindigkeitsnetz (100 MBit/s Datenrate)
- Normiert durch ANSI (X3T9.5)
- Token-Prinzip
- Topologien
 - Doppelring oder
 - Baum oder
 - Kombination (Dual Ring of Trees)
- Maximale Ausdehnung des Gesamtrings (als Doppelring) 100 km bzw. 200 km bei Fehlerfällen (Rekonfiguration des Rings)
- Bis zu 500 Stationen im Ring
- Für lokale Nutzung neue Norm TPDDI (FDDI über TP-Kabel)
 - FDDI über Kupferkabel
 - Mit 100 MBit/s
 - Über Kategorie-5-Kabel

5.5.2. Übertragungstechnik

- 4B/5B-Kodierung:
 - Je 4 Bit werden in 5 Bit umgewandelt.
 - Dadurch 32 Bitkombinationen (oder Symbole) möglich, von denen
 - 16 zur Datendarstellung und
 - 16 als Steuersignale genutzt werden können.
 - Auswahl der genutzten Kombinationen, so daß 0 und 1 möglichst gleichmäßig in den Symbolen vorkommen (Bei Licht: heißt das an/aus!)
- Brutto 125 MBit/s bei Netto 100 MBit/s
- NRZI-Kodierung bei Übertragung über LWL
 - Non Return to Zero Inverted
 - (NRZ wäre:
 - 0 = Negativ (Licht aus)
 - 1 = Positiv (Licht an))
 - 1 durch Polaritätswechsel am Anfang dargestellt.
 - 0 durch keinen Polaritätswechsel dargestellt
 - Datenrate 100 MBit/s bei einer Bitrate von 125 MBit/s, einer Fundamentalfrequenz von 62,5 MHz und einer Baudrate von 125 Mbaud.
- MLT-3-Kodierung bei Übertragung über Kupferkabel
 - Dreistufige Kodierung (+,0,-)
 - Keine Änderung bedeutet 0
 - Jede Zustandsänderung (bei Beginn des Taktzyklus) bedeutet 1
 - Zustandsänderungen dürfen immer nur in eine vorgeschriebene Richtung erfolgen (0 → - → 0 → + → 0 → - → 0 usw.).
 - Datenrate 100 MBit/s bei einer Bitrate von 125 MBit/s, einer Fundamentalfrequenz von 31,25 MHz und einer Baudrate von 125 Mbaud.

5.5.3. Der Doppelring

- Ringtopologie ist bezüglich der Ausfallsicherheit ungünstig

- Um wenigstens einen Ausfall zu kompensieren, Doppelring aus
 - aktiven Ring (Primärring) und
 - Backup-Ring (Sekundärring, im Normalfall ungenutzt [keine Datenübertragung])
- Im Fehlerfall Umleitung über Backup-Ring

5.5.4. Typisierung aktiver Komponenten

- Unterscheidung: Ring-Anschluss oder Baum-Anschluss
 - Ring:
 - Zwei Ports pro Station für Primär und Sekundärring
 - Bezeichnung: Dual Attached
 - Baum:
 - Ein Port zum Anschluss an einen Konzentrator
 - Bezeichnung: Single Attached
- Unterscheidung: Station oder Konzentrator
 - Station: nur ein Anschluss an das Netz
 - Konzentrator: Mehrfacher Anschluss an das Netz
 - Mehrere Anschlüsse zum Anschluss weitere Geräte (nur Single Attached)
 - Ein Anschluss zur Anbindung an das übergeordnete Netz (Ring oder Baum)
 - Netzelement zum Aufbau von Baumstrukturen
- Vier Typen
 - DAS Dual Attached Station
 - SAS Single Attached Station
 - DAC Dual Attached Concentrator
 - SAC Single Attached Concentrator

5.5.5. Port-Typen

- A-Port
 - Zum Anschluss an Doppelring
 - Empfang im Primärring
 - Senden (ggf) im Sekundärring
- B-Port
 - Zum Anschluss an Doppelring
 - Empfang (ggf) im Sekundärring
 - Senden im Primärring
- M-Port (Master)
 - Port eines Konzentrators zum Anschluss eines SAC oder einer SAS
- S-Port (Slave)
 - Port eines SAC oder einer SAS zum Anschluss an einen Konzentrator
- Kodierung der Porttypen auf der Oberseite des Steckers und des Fasertyps (MMF oder SMF) auf der Unterseite (keine Aussparung bei MMF).

5.5.7. Verkabelungsoptionen

- Multimode Fiber (MMF-PMD)
 - Maximaler Abstand zwischen zwei Stationen: 2 km
 - Faserdurchmesser: 62,5/125µm oder 50/125 µm
 - : 1300 nm
 - Anschluss technik: MIC-Stecker
 - Sender: LED
- Mono- oder Singlemode Fiber (SMF-PMD)
 - Maximaler Abstand zwischen zwei Stationen: 60 km
 - Faserdurchmesser: 9-10/125µm
 - Wellenlänge: 1300 nm
 - Anschluss technik: MIC-Stecker

- Sender: Laserdiode
- Twisted-Pair (TP-PMD)
 - Maximaler Abstand zwischen zwei Stationen: 100 m
 - Paarweise verdrehte Vierdrahtleitung
 - Anschlusstechnik: RJ45-Stecker
 - Belegung der Paare 1,2 und 7,8 im Stecker (Ethernet 1,2 und 3,6, Token-Ring 1,2 und 4,5)
 - Übertragungsverfahren 4B/5B MLT-3
 - MLT-3: Multi Level Transition 3
 - Drei Zustände
 - Reduktion der Frequenz auf 31,5 MHz

6. IP Adressierung

6.1. Einleitung

Mitte der 90er Jahre ist das Internet ein völlig anderes Netzwerk als zu Beginn der 80er Jahre, als es aufgebaut wurde. Heute ist das Internet das größte öffentliche Datennetz der Welt und es verdoppelt seine Größe alle 9 Monate. Dies kommt durch die große Popularität des World Wide Web (WWW) und den Möglichkeiten, die Geschäftsleute sehen, ihre Kunden an einer "virtuellen Theke" bedienen zu können. Es ist klar, dass die sich ausdehnende geschäftliche Nutzung und die soziale Akzeptanz die Nachfrage nach Zugang zum Internet immer weiter steigern wird.

Es gibt eine direkte Beziehung zwischen dem Wert des Internet und der Anzahl der am Internet angeschlossenen Institutionen. Mit dem Wachstum des Internet wächst der Wert jedes Anschlusses, da die Institution immer mehr Benutzer/Kunden über diesen Anschluß erreichen kann.

Größenprobleme des Internet: Während der letzten paar Jahre traten bei dem Versuch des kontinuierlichen und ununterbrochenen Wachstums des Internet zwei Größenprobleme auf:

- der unter Umständen unzureichende Adreßraum von IPv4.
- die Fähigkeit, den Verkehr zwischen der steigenden Anzahl von Netzen (aus denen das Internet besteht) zu routen.

Das erste Problem hängt mit dem Adreßraum von IP zusammen. In der aktuellen Version von IP, IP Version 4 (IPv4) wird die Adresse durch eine 32-Bit-Zahl angegeben. Dies bedeutet, daß es 2^{32} (4.294.967.296) Adressen gibt. Dies ist eine sehr große Zahl. Durch das Öffnen neuer Märkte und dadurch, daß große Teile der Weltbevölkerung Zugang zum Internet erhalten werden, wird der Adreßraum unter Umständen nicht ausreichend sein.

Das Problem der unzureichenden Anzahl von Adressen wurde noch durch die nicht effiziente Verteilung von Adressen verstärkt. Auch wird durch die traditionelle klassenweise Nutzung der Adressen der Adreßraum nicht vollständig genutzt. Die Arbeitsgruppe Address Lifetime Expectancy (ALE) der IETF hat zum Ausdruck gebracht, daß bei der aktuellen Adreßvergabepolitik kurz bis mittelfristig alle Adressen aufgebraucht sein werden. Falls das Problem des Adreßraums nicht gelöst wird, können neue Benutzer in Zukunft nicht mehr an das Internet angeschlossen werden.

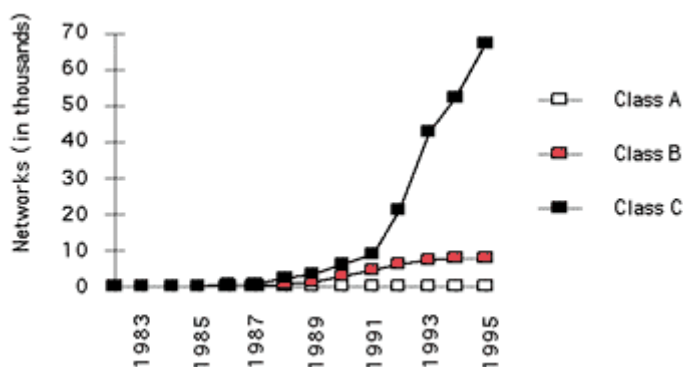


Abb.6.1: Zugewiesene Netzwerknummern

Das zweite Problem wird durch das schnelle Wachstum der Routingtabellen des Internet verursacht. Die Backbone-Router sollten vollständige Routing-Informationen über das Internet besitzen. Mit dem Anschluss vieler Institutionen innerhalb der letzten Jahre sind die Routingtabellen exponentiell gewachsen. Im Dezember 1990 gab es 2.190 Routen, im Dezember 1992 8.500 und im Dezember 1995 mehr als 30.000.

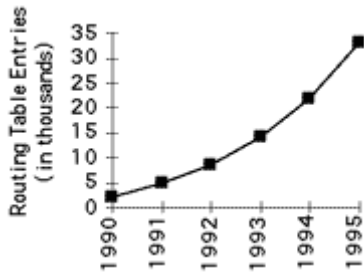


Abb.6.2: Wachstum der Internet Routing Tabellen

Das Routing-Problem kann nicht einfach dadurch gelöst werden, dass mehr Speicher in den Routern installiert wird und die Routingtabellen vergrößert werden. Andere Faktoren sind die notwendige CPU-Leistung, um Änderungen der Tabellen und der Topologie nachzuvollziehen, oder die dynamische Natur des WWW und ihre Einflüsse auf die Cache-Speicher der Router und die schiere Informationsmenge, die von Menschen und Maschinen verarbeitet werden muss. Falls die Routingtabellen in den zentralen Routern beliebig wachsen sollen, werden die Router irgendwann gezwungen sein, Routen zu vergessen. Damit wären Teile des Internet nicht mehr erreichbar.

Die langfristige Lösung dieser Probleme ist in der allgemeinen Verwendung von IP Next Generation (IPng oder IPv6) bis zum Jahrtausendwechsel zu sehen. Während das Internet auf IPv6 wartet, muß IPv4 so geändert werden, dass das Internet die Konnektivität zur Verfügung stellen kann, die von ihm erwartet wird. Dieser Veränderungsprozess kann eine Menge von Schwierigkeiten verursachen und kann fundamentale Konzepte des Internet ändern.

6.2. Klassenweise IP-Adressierung

Als IP 1981 standardisiert wurde, forderte die Spezifikation, daß jedem System, das an das Internet angeschlossen ist, eine eindeutige 32-Bit Internetadresse zugewiesen wird. Einige Systeme, z.B. Router, die Schnittstellen zu mehreren Netzwerken haben, brauchen eine Adresse für jede Netzwerkschnittstelle. Der erste Teil der Internetadresse gibt das Netzwerk an, in dem der Rechner steht. Der zweite Teil gibt den Rechner innerhalb des Netzwerkes an. Dies erzeugt eine zweistufige Adreßhierarchie, die in Abbildung 3 dargestellt ist.

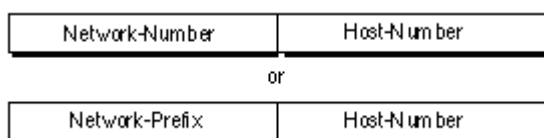


Abb.6.3: Zweistufige Internet-Adresshierarchie

In den letzten Jahren wurde das Feld mit der Netzwerknummer als "Netzwerk-Präfix" bezeichnet, da die Netzwerknummer bei einer IP-Adresse immer vorne steht. Alle Rechner in einem Netzwerk müssen die gleiche Netzwerknummer, aber eine eindeutige Rechnernummer (Hostnummer) haben. Analog müssen zwei Rechner in verschiedenen Netzen unterschiedliche Netzwerk-Präfixe haben, können aber die gleiche Rechnernummer haben.

6.2.1. Primäre Adressklassen

Um unterschiedlich große Netze zu unterstützen, entschieden die Designer, dass der Adressraum von IP in drei Klassen aufgeteilt werden soll - Klasse A, Klasse B und Klasse C. Dies wird als klassenweise Adressierung bezeichnet, da der Adressraum in drei vordefinierte Klassen, Gruppen oder Kategorien aufgeteilt wird. Bei jeder Klasse wird die Grenze zwischen dem Netzwerk-Präfix und der Rechnernummer an einer anderen Stelle innerhalb der 32-Bit gesetzt. Die Formate der fundamentalen Adressklassen werden in Abbildung 6.4 dargestellt.

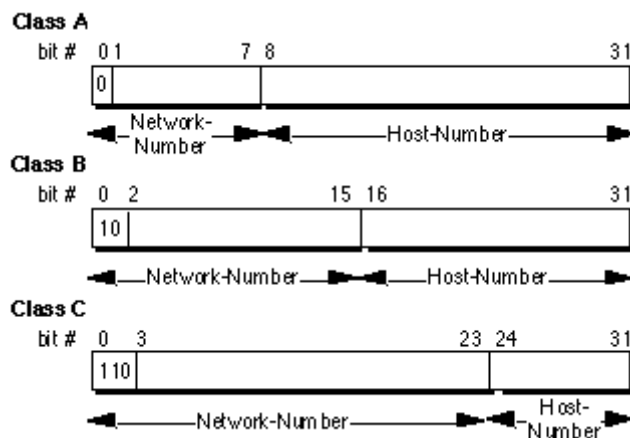


Abb.6.4: Formate der klassenweisen IP-Adressierung

Einer der grundlegenden Eigenschaften der klassenweisen IP-Adressierung ist, daß jede Adresse implizit angibt, welcher Teil der Adresse Netzwerk-Präfix ist und welcher Teil Rechnernummer. Wenn zum Beispiel die ersten beiden Bits einer Adresse 1-0 sind, dann sind die ersten 16 Bit Netzwerk-Präfix und die zweiten 16-Bit sind die Rechnernummer. Dies vereinfachte das Routing-System in den ersten Jahren, da die Routing-Protokolle keine "Maske" oder "Schlüssel" kannten, die mit jeder Route angegeben werden, um die Länge des Netzwerk-Präfixes festzulegen.

6.2.2. Klasse-A-Netzwerke (/8 Präfixe)

Jedes Klasse-A-Netzwerk hat ein Netzwerk-Präfix von 8-Bit, bei dem das erste Bit 0 und die restlichen sieben Bit die Netzwerknummer angeben. Dem folgt dann eine Rechnernummer von 24-Bit Länge. Heutzutage ist es nicht mehr modern, von einem Klasse-A-Netzwerk zu sprechen. Klasse-A-Netzwerke werden heute als "/8" (ausgesprochen "Schrägstrich acht" oder einfach "achter") Netzwerke bezeichnet, da das Netzwerk-Präfix 8 Bit beträgt.

Es können maximal 126 ($2^7 - 2$) /8 Netzwerke definiert werden. Bei der Berechnung der Anzahl müssen zwei abgezogen werden, da das /8 Netzwerk 0.0.0.0 als Standard-Route und das /8 Netzwerk 127.0.0.0 (auch geschrieben als 127/8 oder 127.0.0.0/8) für die "loopback"-Funktion reserviert ist. Jedes /8-Netzwerk unterstützt maximal 16.777.214 ($2^{24} - 2$) Rechner im Netz. Bei dieser Berechnung müssen wieder zwei abgezogen werden, da Rechnernummern, die nur Nullen enthalten ("Netzwerkadresse"), und Rechnernummern, die nur Einsen enthalten ("broadcast" = Rundruf) nicht einem einzelnen Rechner zugewiesen werden können.

Da der /8-Adreßblock 2^{31} (2,147,483,648) individuelle Adressen und der IPv4 Adreßraum maximal 2^{32} (4,294,967,296) umfaßt, belegt der /8-Adreßraum 50 % des IPv4-Adreßraumes.

6.2.3. Klasse-B-Netzwerke (/16 Präfixe)

Jedes Klasse-B-Netzwerk hat ein Netzwerk-Präfix von 16-Bit, bei dem die ersten beiden Bits 1-0 sind und die restlichen 14 Bit die Netzwerknummer angeben. Dem folgt dann eine Rechnernummer von 16 Bit Länge. Klasse-B-Netzwerke werden heute als /16-Netzwerke bezeichnet, da das Netzwerk-Präfix 16 Bit lang ist.

Es können maximal 16,384 (2^{14}) /16-Netzwerke mit bis zu 65,534 ($2^{16} - 2$) Rechnern pro Netzwerk angegeben werden. Der /16-Adreßblock enthält 2^{30} (1.073.741.824) Adressen. Dies sind 25 % des IPv4-Adreßraumes.

6.2.4. Klasse-C-Netzwerke (/24 Präfix)

Jedes Klasse-C-Netzwerk hat ein Netzwerk-Präfix von 24 Bit, bei dem die ersten drei Bits 1-1-0 sind und die restlichen 21 Bit die Netzwerknummer angeben. Dem folgt dann eine Rechnernummer von 8 Bit Länge. Klasse-C-Netzwerke werden heute als /24-Netzwerke bezeichnet, da das Netzwerk-Präfix 24 Bit lang ist.

Es können maximal 2,097,152 (2^{21}) /24-Netzwerke mit bis zu 254 ($2^8 - 2$) Rechnern pro Netzwerk angegeben werden. Der /24-Adreßblock enthält 2^{29} (536,870,912) Adressen. Dies sind 12,5 % (oder 1/8) des IPv4-Adreßraumes.

6.2.5. Andere Klassen

Zusätzlich zu den drei bekannten Klassen gibt es zwei weitere Klassen. Bei der Klasse D sind die obersten vier Bit auf 1-1-1-0 gesetzt. Diese Adressen werden für IP-Multicast verwendet. Bei Klasse-E-Adressen sind die obersten vier Bit auf 1-1-1-1 gesetzt. Dieser Adreßraum ist für experimentelle Anwendungen reserviert.

6.2.6. Dezimalpunkt-Schreibweise

Damit der Mensch Internetadressen leichter lesen und schreiben kann, werden die Adressen als vier Dezimalzahlen, die durch Punkte getrennt sind, geschrieben. Dieses Format bezeichnet man als die "Dezimalpunkt-Schreibweise".

Die Dezimalpunkt-Schreibweise teilt die 32-Bit Internet-Adresse in vier 8 Bit Felder. Diese 8 Bit Werte werden als Dezimalzahl angegeben und die Felder durch Punkte getrennt. Abbildung 5 zeigt wie ein typische /16 (Klasse B) Adresse in Dezimalpunkt-Schreibweise angegeben wird.

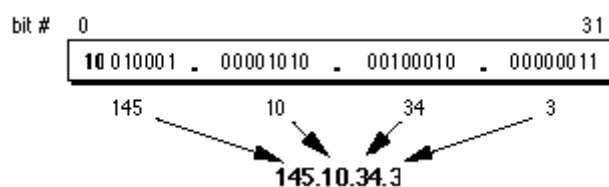


Abb.6.5: Dezimalpunkt-Schreibweise

Tabelle 1 gibt die Bereiche der drei Adressklassen in Dezimalpunkt-Schreibweise an. "xxx" gibt die Rechnernummer an, die von dem Netadministrator zuzuweisen ist.

| Address Class | Dotted-Decimal Notation Ranges |
|------------------|---------------------------------------|
| A (/8 prefixes) | 1.xxx.xxx.xxx through 126.xxx.xxx.xxx |
| B (/16 prefixes) | 128.0.xxx.xxx through 191.255.xxx.xxx |
| C (/24 prefixes) | 192.0.0.xxx through 223.255.255.xxx |

Tabelle 1: Adressbereich jeder Klasse in Dezimaler Punkt Schreibweise

Unvorhersehbare Beschränkungen durch die klassenweise Adressierung Die ursprünglichen Entwickler von IP ahnten niemals, dass sich das Internet zu dem entwickeln würde, was es heute ist. Viele der Probleme, die das Internet heute hat, können auf Entscheidungen zurückgeführt werden, die in den Jahren des Entstehens von IPv4 getroffen wurden.

- IHNO In den frühen Tagen des Internet wurde Organisationen aus dem schier unerschöpflichen Adressraum des Internet Adressen entsprechend den Anforderungen und nicht entsprechend dem tatsächlichen Bedarf zugewiesen. Adressen wurden an die vergeben, die danach fragten, ohne darüber nachzudenken, dass die Adressen ein knappes Gut werden könnten.
- Die Entscheidung, den Adressraum auf 32-Bit zu beschränken, bedeutete, dass nur 2 hoch 32 (4,294,967,296) IPv4-Adressen verfügbar sind. Die Entscheidung, einen etwas größeren Adressraum zu unterstützen, hätte die Anzahl der Adressen exponentiell erhöht und das heutige Problem, dass nicht genügend Adressen zur Verfügung stehen, würde nicht existieren.
- Die Einteilung in die Klassen A, B und C mit ihren Beschränkungen war einfach zu verstehen und zu implementieren. Dies war aber für eine effiziente Belegung des Adressraumes nicht sinnvoll. Probleme entstanden, da eine Netzwerkkategorie fehlte, um mittelgroße Organisationen zu unterstützen. Ein /24-Netz ist mit 254 Rechnern zu klein, während ein /16-Netz mit 65534 Rechnern zu groß ist. In der Vergangenheit wurden Organisationen mit mehreren hundert Rechnern ein /16-Netz anstatt mehrerer /24-Netze zugewiesen. Das Ergebnis war, dass die /16-Adressen schnell knapp wurden. Die einzigen noch verfügbaren Adressen sind die /24-Netze, die den negativen Effekt haben, dass die globalen Routingtabellen schnell wachsen.

Die folgende Geschichte des Internet konzentriert sich auf die Schritte, die unternommen wurden, um die Nachteile der Adressvergabe zu beseitigen und das globale Wachstum des Internet zu fördern.

6.3. Teilnetze

1985 definierte der RFC 950 einen Weg um ein Klasse-A-, B- oder C-Netzwerk in kleinere Netze aufzuteilen. Teilnetze wurden eingeführt, um einen Teil der Probleme zu beseitigen, die sich aus der zweistufigen Adressierungsart ergeben hatten:

- Die Routingtabellen des Internet begannen zu wachsen.
- Lokale Systemverwalter mussten ein neues Netzwerk vom Internet anfordern, um ein weiteres Netz installieren zu können.

Man versuchte, beide Probleme durch Einführung einer weiteren Hierarchie zu lösen. Anstatt der klassenweisen zweistufigen Hierarchie wurde durch Teilnetze eine dreistufige Hierarchie realisiert. In Abbildung 6 wird die Grundidee dargestellt. Die klassenweise Rechnernummer wird in eine Teilnetznummer und eine Rechnernummer in diesem Teilnetz aufgeteilt.

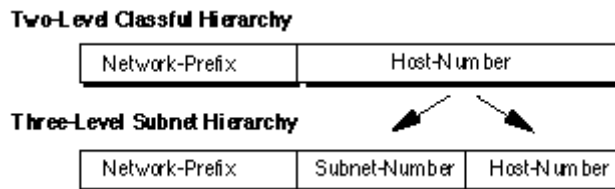


Abb.6.6: Adresshierarchie bei Teilnetzen

Teilnetze verhindern das Routingtabellen-Problem, da die Teilnetzstruktur eines Netzwerkes nie außerhalb der Organisation sichtbar ist. Die Route jeder IP-Adresse zu jedem dieser Teilnetze ist immer die gleiche, unabhängig davon, in welchem Teilnetz der Rechner ist. Alle Teilnetze haben immer das gleiche Netzwerk-Präfix und unterscheiden sich nur in ihrer Teilnetznummer. Die Router innerhalb der Organisation müssen diese verschiedenen Teilnetznummern natürlich unterscheiden. Innerhalb der Internet jedoch werden alle Teilnetze zu einem einzelnen Eintrag zusammengefasst. Damit kann der lokale Systemverwalter beliebig komplexe lokale Netze aufbauen, ohne dass dadurch die Routingtabellen des Internet beeinflusst werden.

Teilnetze verhindern auch den Verbrauch von Netzwerknummern, da einer Organisation eine oder wenige Netzwerknummern des IPv4 Adressraumes zugeteilt werden müssen. Dann kann die Organisation beliebig Teilnetznummern für die internen Netze zuweisen. Insbesondere kann sie später weitere Teilnetz hinzufügen, ohne ein neue Netzwerknummer vom Internet anfordern zu müssen.

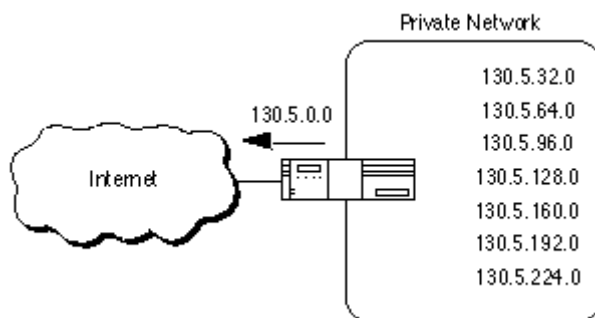


Abb.6.7: Teilnetze reduzieren die Routeranforderungen im Internet

In Abbildung 7 wird ein /16-Adresse (Klasse B) in mehrere logische Teilnetze aufgeteilt. Der Router akzeptiert den gesamten IP-Verkehr, der an das /16-Netz 130.5.0.0 gerichtet ist, und verteilt diesen intern aufgrund des dritten Oktetts in der Adresse. Die Verwendung von Teilnetzen innerhalb eines privaten Netzwerkes hat mehrere Vorteile:

- Die Größe der globalen Internet-Routingtabellen wächst nicht, da der Systemverwalter nicht neue Netzwerknummer für neue Netzwerke braucht. Die Routing-Information für alle Teilnetze kann in einem einzelnen Eintrag zusammengefasst werden.
- Der Systemverwalter hat die Freiheit, neue Teilnetze einzuführen, ohne neue Netzwerknummern vom Internet anfordern zu müssen.
- "Routenflattern" (d.h. häufiges Ändern der Routen) innerhalb eines lokalen Netzes betrifft nicht die Routingtabellen des Internet, da das Internet nicht bezüglich der Teilnetznummer routet, sondern bezüglich des Netzwerk-Präfixes.

Erweiterte Netzwerk-Präfixe

Internet-Router benutzen nur das Netzwerk-Präfix der Zieladresse, um Verkehr in eine Umgebung mit Teilnetzen weiterzuleiten. Router innerhalb der Teilnetzumgebung

benutzen das erweiterte Netzwerk-Präfix, um den Verkehr zwischen den Teilnetzen zu routen. Das erweiterte Netzwerk-Präfix besteht aus dem Netzwerk-Präfix der Klasse und der Teilnetznummer.

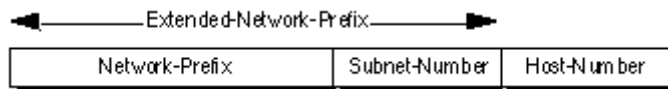


Abb.6.8: Erweitertes Netzwerk-Präfix

Das erweiterte Netzwerk-Präfix wird normalerweise durch die Netzwerkmaske angegeben. Wenn Sie z.B. das /16-Netz 130.5.0.0 haben und das gesamte dritte Oktett als Teilnetzadresse verwenden wollen, müssen Sie folgende Netzwerkmaske angeben: 255.255.255.0. Die Bits der Netzwerkmaske und der Internetadresse werden eins zu eins einander zugeordnet. Ist ein Bit in der Netzwerkmaske eins, so ist das entsprechende Bit in der Internetadresse Teil des Netzwerk-Präfixes. Sollen die Bits in der Internetadresse als Teil der Rechnernummer interpretiert werden, so sind die entsprechenden Bits der Netzwerkmaske auf 0 zu setzen. Abbildung 9 zeigt ein Beispiel.

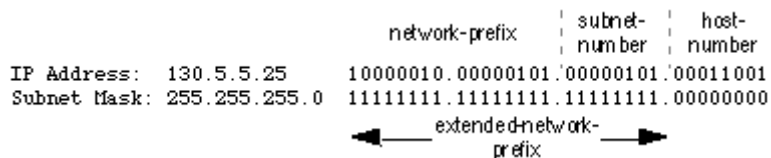


Abb.6.9: Netzwerkmaske

Die heutigen Standards bei Routing-Protokollen geben die Länge des erweiterten Netzwerk-Präfixes statt der Netzwerkmaske an. Die Präfixlänge gibt die ununterbrochene Anzahl Einsen der Netzwerkmaske an. Dies bedeutet, dass eine Netzadresse 130.5.5.25 mit der Netzwerkmaske 255.255.255.0 auch als 130.5.5.25/24 geschrieben werden kann. Die /<Präfix-Längen>-Schreibweise ist kompakter und leichter zu verstehen als das Ausschreiben der Netzwerkmaske in der traditionellen Punkt Schreibweise. Abbildung 10 verdeutlicht dies.

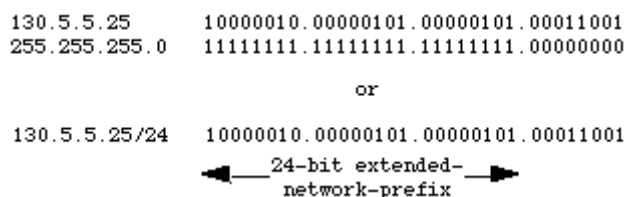


Abb.6.10: Erweiterte Netzwerk-Präfixlänge

Es ist wichtig festzustellen, dass die modernen Routing-Protokolle immer noch die Netzwerkmaske übermitteln. Es gibt kein standardisiertes Internet-Routing-Protokoll, das ein 1-Byte großes Feld im Protokollkopf hat, in dem die Länge des Netzwerk-Präfixes steht. Statt dessen muss immer noch die vier Byte große Netzwerkmaske übermittelt werden.

Bemerkungen zur Teilnetzplanung

Die Erstellung eines Adressplanes erfordert sorgfältige Planung durch den Netzwerk-Systemverwalter. Vier zentrale Fragen müssen beantwortet werden, bevor mit der Planung begonnen werden kann:

- 1) Wie viele Teilnetze braucht die Organisation heute ?
- 2) Wie viele Teilnetze wird die Organisation in der Zukunft brauchen ?
- 3) Wie viele Rechner sind heute in dem größten Teilnetz ?
- 4) Wie viele Rechner werden jemals in dem größten Teilnetz sein ?

Im ersten Planungsschritt muss die Anzahl der benötigten Teilnetze festgestellt werden und auf die nächste Zweierpotenz aufgerundet werden. Wenn eine Organisation 9 Teilnetze benötigt, dann muss auf 2^4 (16) aufgerundet werden. Dabei muss immer genügend Raum für zukünftiges Wachstum gelassen werden. Bei dieser Planung muss der Systemverwalter immer darauf achten, dass genügend Raum für zukünftige Erweiterungen ist. Wenn heute z.B. 14 Teilnetze gebraucht werden, so sollten nicht 16 (2^4) sondern besser 32 (2^5) Teilnetze eingerichtet werden, um Raum für Erweiterungen zu lassen.

Beim zweiten Schritt muss sichergestellt werden, dass im größten Teilnetz der Organisation genügend Rechnernummer verfügbar sind. Wenn im größten Netz 50 Rechnernummern benötigt werden, so muss auf 2^6 (64) aufgerundet werden.

Im letzten Schritt muss festgestellt werden, ob der Adressbereich der Organisation ausreichend ist, um die oben festgestellten Anforderungen zu erfüllen. Hat die Organisation ein einziges /16-Netz, so können problemlos 4 Bit für die Teilnetznummer und 6 Bit für die Hostnummer geplant werden. Hat die Organisation aber mehrere /24-Netze und muss 9 Teilnetze anlegen, so muss jedes der /24-Netze in vier Teilnetze (mittels 2 Bit) aufgeteilt werden. Aus drei in dieser Art aufgeteilten /24-Netzen kann dann das Netz der Organisation gebildet werden. Eine Alternative wäre die Verwendung von Adressen aus dem privaten Bereich (RFC 1918) für interne Verbindungen und die Verwendung eines Network Address Translators (NAT), um externen Internet Zugriff zu ermöglichen.

6.4. Beispiel 1: Subnetting

Voraussetzungen

Einer Organisation wurde die Netzwerknummer 193.1.1.0/24 zugewiesen, und es müssen sechs Teilnetze angelegt werden. Im größten Teilnetz werden 25 Rechnernummern benötigt.

Definieren der Teilnetzmaske / der erweiterten Präfixlänge

Zuerst muss festgestellt werden, wie viel Bit man benötigt, um sechs Teilnetze anzulegen. Da Netzwerkadressen immer an binäre Grenzen gebunden sind, ist die Anzahl der Teilnetze immer eine Zweierpotenz [2 (2^1), 4 (2^2), 8 (2^3), 16 (2^4), usw.]. Es ist daher unmöglich, einen Adressblock zu definieren, der genau sechs Teilnetze enthält. In diesem Beispiel muss der Systemverwalter acht Teilnetze definieren (2^3) und hat damit 2 Teilnetze für zukünftige Erweiterungen übrig. Da 2^3 gleich acht ist, werden genau drei Bits gebraucht um die drei Teilnetze zu definieren. In diesem Beispiel wird ein /24-Netz in Teilnetze aufgeteilt, so dass das erweiterte Netzwerk-Präfix 27 Bit lang ist. Ein Netzwerk-Präfix mit 27 Bit kann als /27 oder 255.255.255.224 geschrieben werden.

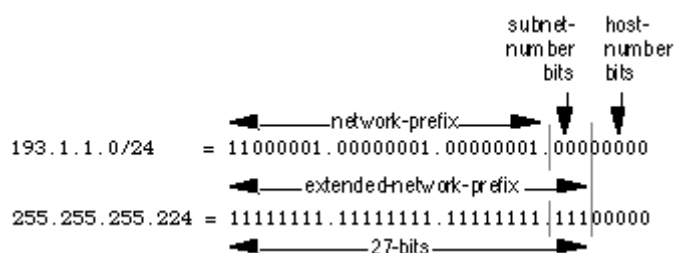


Abb.6.11: Beispiel 1 - Definieren einer Teilnetzmaske/eines erweiterten Netzwerk-Präfixes

Bei einem erweiterten Netzwerk-Präfix von 27 Bit sind noch fünf Bit für die Rechnernummer im Teilnetz übrig. Dies bedeutet, daß bei einem Teilnetz mit einem Präfix von 27 Bit 32 (2^5) fortlaufende IP-Adressen in einem Teilnetz liegen. Da die Rechnernummern, in denen nur Nullen oder nur Einsen stehen, nicht verwendet werden dürfen, bleiben 30 ($2^5 - 2$) benutzbare Adressen in jedem Teilnetz übrig.

Definieren der einzelnen Teilnetznummern

Die acht Teilnetze werden von 0 bis 7 durchnummeriert. Im restlichen Teil dieses Dokumentes gibt die Schreibweise XXX2 die binäre Schreibweise einer Zahl an. Die dreistellige binäre Schreibweise der Zahlen 0 bis 7 sieht dann wie folgt aus: 0 (0002), 1 (0012), 2 (0102), 3 (0112), 4 (1002), 5 (1012), 6 (1102), und 7 (1112).

Um das Teilnetzwerk n zu definieren, muß der Netzwerk-Systemverwalter einfach die binäre Darstellung der Teilnetznummer in das Teilnetznummernfeld eintragen. Um z.B. Teilnetz-Nummer 6 anzugeben, muß der Systemverwalter die binäre Darstellung von 6 (1102) in die drei Bits der Teilnetznummer eintragen.

Unten sind die acht Teilnetznummern für dieses Beispiel angegeben. Die kursiven Zahlen geben das erweiterte Netzwerk-Präfix an, während die **fett** geschriebenen Ziffern das Teilnetznummernfeld angeben.

Basis Netz: *11000001.00000001.00000001.00000000* = 193.1.1.0/24
 Teilnetz #0: *11000001.00000001.00000001.00000000* = 193.1.1.0/27
 Teilnetz #1: *11000001.00000001.00000001.00100000* = 193.1.1.32/27
 Teilnetz #2: *11000001.00000001.00000001.01000000* = 193.1.1.64/27
 Teilnetz #3: *11000001.00000001.00000001.01100000* = 193.1.1.96/27
 Teilnetz #4: *11000001.00000001.00000001.10000000* = 193.1.1.128/27
 Teilnetz #5: *11000001.00000001.00000001.10100000* = 193.1.1.160/27
 Teilnetz #6: *11000001.00000001.00000001.11000000* = 193.1.1.192/27
 Teilnetz #7: *11000001.00000001.00000001.11100000* = 193.1.1.224/27

Um festzustellen, ob alle Teilnetze richtig sind, muß man nur prüfen, ob alle Teilnetznummern ein Vielfaches der Teilnetznummer 1 sind. In diesem Fall müssen es Vielfache von 32 sein. Also 0, 32, 64, 96, ...

Die Teilnetze mit der Nummer 0 und allen gesetzten Bits.

Als Teilnetze in dem RFC 950 definiert wurden, war es verboten, die Teilnetze mit den Nummern 0 und die, bei denen alle Bits auf 1 gesetzt waren, zu benutzen. Mit dieser Beschränkung wollte man Situationen vermeiden, die klassenweise Router verwirren könnten. Heutzutage können die Router klassenweise (z.B. RIP-1) und klassenlose Protokolle (z.B. BGP-4) gleichzeitig verarbeiten.

Unter Berücksichtigung der Teilnetze, die 0 als Nummer haben, muß bei jedem Routingtabellen-Eintrag auch das Paar Route/<Präfix-Länge> angegeben werden, damit zwischen einer Route zum Teilnetz mit der Nummer 0 und einer Route zu einem gesamten Netzwerk unterschieden werden kann. Wenn zum Bekanntgeben der Routen-Information das Protokoll RIP-1 (dieses Protokoll gibt keine Netzwerkmaske oder Präfixlänge an) verwendet wird, dann sind die Routing-Angaben für die Teilnetze 193.1.1.0/24 und 193.1.1.0/27 193.1.1.0 und damit identisch. Ohne Kenntnis der Netzwerkmaske oder der Präfixlänge kann ein Router nicht zwischen der Route zu einem Teilnetz mit der Nummer 0 und dem gesamten Netz unterscheiden. Dies wird in Abbildung 12 verdeutlicht.

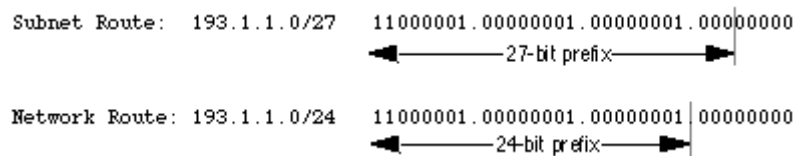


Abb.6.12: Unterscheidung zwischen einer Route zu einem Teilnetz mit der Nummer 0 und dem gesamten Netzwerk.

Betrachtet man die Teilnetze, in denen die Teilnetzmaske nur aus 1 besteht, so muß bei jedem Tabelleneintrag des Routers die Präfixlänge mit angegeben werden, damit der Router entscheiden kann, ob der Broadcast an das gesamte Netz oder nur an das Teilnetz geschickt werden muß. Es wird beispielsweise für das Netzwerk 193.1.1.0/24 und 193.1.1.224/27 die gleiche Broadcast-Adresse 193.1.1.255 verwendet. Abbildung 6.13 verdeutlicht das Problem.

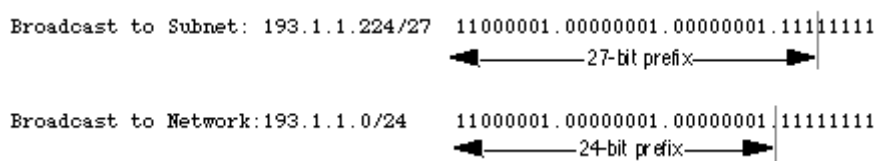


Abb.6.13: Unterscheidung des Broadcasts eines Teilnetzes und eines gesamten Netzwerkes.

Standardmäßig erlaubt die NETBuilder-Software die Weiterleitung an eine Broadcast-Adresse, aber nicht die Weiterleitung an alle Broadcast-Adressen der Teilnetze. Der Netzwerkverwalter kann dieses Verhalten durch die IP CONTROL Parameter FwdSubnetBcast | NoFwdSubnetBcast und FwdAllSubnetBcast | NoFwdAllSubnetBcast ändern.

Mit der Entwicklung von Protokollen, die eine Maske oder eine Präfixlänge mit jeder Route angeben, können die Teilnetze mit nur Nullen oder nur Einsen trotz der Bedenken in RFC 950 wieder verwendet werden. Die Hersteller von Routing-Software haben den Nutzerforderungen nachgegeben und erlauben die Konfiguration von Teilnetzen mit nur Nullen und nur Einsen auf den Router-Schnittstellen. Folgende drei Voraussetzungen müssen erfüllt sein, damit diese Teilnetze mit der NETBuilder Software verwendet werden können:

- Das Interior Gateway Protokoll (IGP) muß laufen
- Der richtige Versionsstand der Netbuilder Software
- Die Fähigkeit der anderen Router im Netzwerk der Organisation

Um die Benutzung von den Teilnetzen mit nur Nullen oder nur Einsen zu unterstützen, muß das IGP erweiterte Netzwerkpräfixe unterstützen oder einen anderen Mechanismus haben, um die Routen den erweiterten Netzwerkpräfixen zuordnen zu können. OSPF und I-IS-IS transportieren erweiterte Netzwerkpräfixe. Sie unterstützen damit die Verwendung der Subnetze in beliebig komplizierten Topologien. RIP-1 transportiert kein erweiterten Netzwerkpräfixe. Der Parameter RcvSubnetMask zusammen mit der Option -RIP CONTROL (..[Aggregate| NoAggregate], [DeAggregate| NoDeAggregate]) unterstützt die Verwendung von Teilnetzen mit nur Nullen oder Einsen bei *einfachen* Topologien.

In die NETBuilder-Software wurde die Unterstützung für Teilnetze mit nur Nullen oder Einsen in mehreren Schritten eingeführt. In Tabelle 2 sehen Sie, ab welcher Software-Version die entsprechenden Teilnetze unterstützt werden.

| Release | Feature Supported |
|------------------|---|
| 6.2 | Permits a router interface to be configured with all-0s in the subnet field |
| 7.0.0.6 | Correctly learns and forwards to routes with all-0s in the subnet field |
| 7.1 | Correctly learns and forwards to routes with all-1s in the subnet field |
| 8.3.0.2 7.2.1 | Permits a router interface to be configured with all-1s in the subnet field |

Abb.6.14: NETBuilder Software-Versionen, ab denen Teilnetze mit nur Nullen und Einsen unterstützt werden.

Schließlich müssen alle Router in dem Netzwerk einer Organisation in der Lage sein, den Datenverkehr zu Teilnetzen mit nur Nullen oder Einsen korrekt zu interpretieren, zu lernen und weiterzuleiten.

Definieren der Rechneradressen für jedes Teilnetz

Entsprechend der Internet-Konventionen kann die Rechnernummer einer Internetadresse nicht nur Nullen oder nur Einsen enthalten. Die Rechnernummer mit nur Nullen gibt die Netzwerknummer an, während die Rechnernummer, in der nur Einsen angegeben sind, die Broadcast-Adresse für dieses Teilnetz oder Netzwerk angibt.

Im aktuellen Beispiel hat die Rechnernummer 5 Bits. Dies bedeutet, daß jedes Teilnetz maximal 30 Rechner ($2^5 - 2 = 30$; die zwei wird abgezogen, da die Rechneradressen, die nur Einsen oder nur Nullen beinhalten, nicht verwendet werden können) beinhalten kann. Die Rechner werden von 1 bis 30 durchnummeriert.

Um im allgemeinen die Adresse des Rechners n in einem bestimmten Teilnetz zu bestimmen, muß man die binäre Darstellung der Rechnernummer in das Rechnerfeld des Teilnetzes eintragen. Um z.B. die Adresse des Rechners 15 im Teilnetz 2 festzustellen, muß man die binäre Darstellung von 15 (011112) in das 5-Bit Rechnerfeld von Teilnetz 2 eintragen.

Die gültige Rechneradresse für Teilnetz 2 aus unserem Beispiel ist unten angegeben. Der Teil in Schrägschrift gibt das erweiterte Netzwerkpräfix an, während der **fett** geschriebene Teil die 5-Bit der Rechnernummer angibt:

Teilnetz #2: *11000001.00000001.00000001.01***000000** = 193.1.1.64/27
 Rechner #1: *11000001.00000001.00000001.01***000001** = 193.1.1.65/27
 Rechner #2: *11000001.00000001.00000001.01***000010** = 193.1.1.66/27
 Rechner #3: *11000001.00000001.00000001.01***000011** = 193.1.1.67/27
 Rechner #4: *11000001.00000001.00000001.01***000100** = 193.1.1.68/27
 Rechner #5: *11000001.00000001.00000001.01***000101** = 193.1.1.69/27
 .
 .
 Rechner #15: *11000001.00000001.00000001.01***001111** = 193.1.1.79/27
 Rechner #16: *11000001.00000001.00000001.01***010000** = 193.1.1.80/27
 .
 .
 Rechner #27: *11000001.00000001.00000001.01***011011** = 193.1.1.91/27
 Rechner #28: *11000001.00000001.00000001.01***011100** = 193.1.1.92/27
 Rechner #29: *11000001.00000001.00000001.01***011101** = 193.1.1.93/27
 Rechner #30: *11000001.00000001.00000001.01***011110** = 193.1.1.94/27

Unten werden die gültigen Rechnernummern für das Teilnetz sechs angegeben. Der kursiv geschriebene Teil gibt den erweiterten Netzwerkpräfix an, während der **fett** geschriebene Teil die aus 5 Bit bestehende Rechnernummer angibt.

Teilnetz 6: $11000001.00000001.00000001.11000000 = 193.1.1.192/27$
 Rechner #1: $11000001.00000001.00000001.11000001 = 193.1.1.193/27$
 Rechner #2: $11000001.00000001.00000001.11000010 = 193.1.1.194/27$
 Rechner #3: $11000001.00000001.00000001.11000011 = 193.1.1.195/27$
 Rechner #4: $11000001.00000001.00000001.11000100 = 193.1.1.196/27$
 Rechner #5: $11000001.00000001.00000001.11000101 = 193.1.1.197/27$
 .
 .
 Rechner #15: $11000001.00000001.00000001.11001111 = 193.1.1.207/27$
 Rechner #16: $11000001.00000001.00000001.11010000 = 193.1.1.208/27$
 .
 .
 Rechner #27: $11000001.00000001.00000001.11011011 = 193.1.1.219/27$
 Rechner #28: $11000001.00000001.00000001.11011100 = 193.1.1.220/27$
 Rechner #29: $11000001.00000001.00000001.11011101 = 193.1.1.221/27$
 Rechner #30: $11000001.00000001.00000001.11011110 = 193.1.1.222/27$

Definieren der Broadcast-Adresse für jedes Teilnetz

In der Broadcast-Adresse für das Teilnetz 2 sind alle Bits der Rechnernummer auf 1 gesetzt:

$11000001.00000001.00000001.01011111 = 193.1.1.95$

Beachten Sie, daß die Broadcast-Adresse für Teilnetz 2 genau eins weniger ist als die Basisadresse für Teilnetz 3. Dies ist eine einfache Eselsbrücke. Die Broadcast-Adresse von Teilnetz n ist die Basisadresse des Teilnetzes n+1 minus 1.

In der Broadcast-Adresse für das Teilnetz 6 sind alle Bits der Rechnernummer auf 1 gesetzt:

$11000001.00000001.00000001.11011111 = 193.1.1.223$

Sie sehen, daß die Broadcast-Adresse von Teilnetz 6 genau eins weniger als die Basisadresse von Teilnetz 7 (193.1.1.224) ist.

7. Netzwerk Begriffe

10BASE-T

Bei 10BASE-T handelt es sich um eine Unterart der Übertragungstechnik Ethernet. Der Namensbestandteil 10 steht für 10 Mbps, BASE steht für Basisband und T für Twisted-Pair-Kabel.

10BASE-T ist die weltweit am meisten eingesetzte Übertragungstechnik.

Adresse

In einem Netzwerk hat jede Station eine physische und eine logische Adresse. Die physische Adresse, das ist eine Zeichenfolge, die vom Hersteller in die Netzwerkkarte eingebraut wurde. Der Aufbau der logischen Adresse hängt demgegenüber vom verwendeten Protokoll ab.

Jedes Paket, das über ein Netzwerk verschickt wird, enthält im Header einen Hinweis auf die Adresse der Zielstation.

Architektur

Der Begriff (Netzwerk-) Architektur wird in der Netzwerk-Literatur uneinheitlich verwendet. Teilweise wird er im Sinne von Topologie verwendet. In der amerikanischen Netzwerk-Welt versteht man unter der Architektur eines Netzwerks dagegen die Übertragungstechnik.

Backbone

Ein Netzwerk-Segment, das dazu dient, andere Netzwerke miteinander zu verbinden. Es handelt sich also um das "Rückgrat" der Netzwerk-Infrastruktur. Für den Backbone-Bereich werden oft Glasfaserkabel eingesetzt.

Bandbreite

1. In technischen Darstellungen ist die Bandbreite die Differenz zwischen der niedrigsten und der höchsten Frequenz bei den Übertragungen auf einem Kanal.
2. In weniger technischen Darstellungen wird mit der Bandbreite die maximale Datenmenge bezeichnet, die über eine Kommunikationsverbindung übertragen werden kann.

Bridge

Bridges sind Geräte, die als Kopplungselemente zwischen Netzwerken eingesetzt werden. Sie sorgen für die Filterung aller eintreffenden Pakete. Die Bridge unterscheidet anhand von Routing-Tabellen zwischen zwei Arten von Paketen: Pakete, die innerhalb des Netzwerks verbleiben, aus dem sie gekommen sind und Pakete, die für das jeweils andere Netzwerk bestimmt sind. Weitergeleitet werden nur die Pakete, die für das andere Netzwerk bestimmt sind. Da nur noch weitergeleitet wird, was weitergeleitet werden muß, sorgen Bridges für eine Entlastung in den angeschlossenen Netzwerken.

Bei Bridges handelt es sich um "lernfähige" Geräte. Eine Bridge betrachtet die Absender-Angaben aller Pakete, und jede Adresse, die bisher nicht in der Routing-Tabelle vorhanden ist, wird notiert. Wenn zukünftig ein Paket eintrifft, das diese Adresse als Zieladresse aufweist, kann die Bridge bestimmen, in welchem Netzwerk sich die Station befindet.

Bus-Topologie

Wenn ein Netzwerk (oder ein Netzwerk-Segment) der Bus-Topologie folgt, dann gibt es ein Hauptkabel, und die Kabel, die zu den PCs führen, sind an das Hauptkabel durch ein Verbindungsstück direkt angeschlossen. (Die Stationen sind gegenüber dem Hauptkabel so positioniert wie es zumeist Häuser zu einer Straße sind.)

Carrier

1. Das akustische Trägersignal bei Modem-Verbindungen. (Ein Modem wandelt dieses Trägersignal ab, und jede Abwandlung repräsentiert ein Bit.)
2. Als "Carrier" werden allerdings auch die Anbieter von Leitungen zur Datenübertragung bezeichnet, also die Telefongesellschaften.

CSMA/CD

CSMA/CD ist neben Token Passing das wichtigste Zugriffsverfahren. Es kommt in Ethernet-Netzwerken zum Einsatz.

Während Token Passing darauf abzielt Kollisionen gänzlich zu vermeiden, sind sie bei CSMA/CD normale Vorkommnisse. Wenn es Kollisionen gegeben hat, legen die sendenden Stationen allerdings eine Pause beliebiger Dauer ein, und starten erst dann den nächsten Versuch, ihre Daten zu übertragen.

CSMA/CD wurde im Standard IEEE 802.3 festgelegt.

Cyclical Redundancy Check (CRC)

Mit dem Cyclical Redundancy Check (deutsch: zyklische Redundanz-Überprüfung) werden Datenübertragungen auf Fehler überprüft. Über die Daten des betreffenden Pakets wird eine Prüfsumme gebildet (nach einem mathematischen Verfahren wird ein Wert ermittelt). Dies geschieht auf dem sendenden Computer ebenso wie auf dem empfangenden. Stimmen die beiden Ergebnisse überein, kann von einer fehlerfreien Übertragung ausgegangen werden. Wenn nicht, dann wurden die Daten während der Übertragung verändert. In diesem Fall fordert die CRC den Quellcomputer auf, die Daten erneut zu übertragen. Die CRC-Daten werden im Trailer eines Pakets übertragen.

Ethernet

Neben Token Ring die am meisten verbreitete Übertragungstechnik. Das Hauptmerkmal von Ethernet ist das verwendete Zugriffsverfahren, CSMA/CD.

Die Regeln für Ethernet wurden von dem Institute of Electrical and Electronics Engineers in der Spezifikation 802.3 festgelegt. Die Spezifikation umfaßt Regeln für die Topologie von Ethernet-LANs, für die Übertragungsmedien, die verwendet werden können, und dafür, wie die Elemente des Netzwerks zusammenarbeiten sollten. Die am meisten verbreitete Variante von Ethernet ist 10BASE-T.

Das Ethernet-Protokoll legt fest, wie die Aufgaben der Schichten 1 und 2 des OSI-Modells erfüllt werden sollen.

Fast Ethernet

Eine Weiterentwicklung von Ethernet. Fast Ethernet kann Daten mit einer Geschwindigkeit von 100 Mbps übertragen.

Fiber Distributed Data Interface (FDDI)

FDDI ist eine Übertragungstechnik, die als Zugriffsverfahren Token Passing verwendet. FDDI wird in erster Linie bei Backbones verwendet.

Filterung

Filterung von Datenpaketen dient dazu, Netzwerke zu entlasten. Geräte, die Filterungsfunktionen übernehmen, sind Bridges und Router. Da diese Geräte nur jene Pakete weiterleiten, die weitergeleitet werden müssen, verringert sich der Datenverkehr.

Gateway

Gateways werden benötigt, wenn zwei Netzwerke miteinander verbunden werden sollen, die unterschiedliche Protokolle verwenden. Üblicherweise wird als Gateway ein dedizierter PC eingesetzt.

Beispiel für die Arbeit eines Gateways: Bei der Anbindung eines LANs an einen Großrechner treffen unterschiedliche Netzwerk-Welten aufeinander. Damit die Kommunikation dennoch klappen kann, muß es Protokollkonvertierungen geben. Mit einem zwischengeschaltetem Gateway kann dafür gesorgt werden, daß dem Großrechner eine LAN-Station wie ein dummes Terminal erscheint. Die LAN-Station wiederum kann durch die Vermittlungsarbeit des Gateways auf den Großrechner zugreifen als wenn es sich um einen normalen Netzwerk-Server handeln würde.

Header

Nachrichten, die über ein Netz verschickt werden sollen, werden in Pakete aufgeteilt. Jedes Paket enthält neben den eigentlichen Daten der Nachricht auch Daten, die für die Kommunikationssteuerung benötigt werden. Diese unterteilen sich in einen Header, der sich vorne am Paket befindet und einen Trailer, der das Ende des Pakets bildet. Im Header befindet sich üblicherweise die Adresse der Ziel-Station.

Hub

Ein Gerät, das dazu dient, den Datenverkehr in einem Netzwerk zu regeln. In einem Stern-Netzwerk ist jede Station durch ein Kabel an einen Hub angeschlossen. An die Ports eines Hubs können aber auch ganze Netzwerke (oder Netzwerk-Segmente) angeschlossen werden.

Die Einsatzmöglichkeiten von Hubs sind vielfältig. Beispiel: Mit einem Hub kann die Bus-Topologie nachgebildet werden. An jeden Port des Hubs ist dann ein Computer oder ein Peripheriegerät angeschlossen. Wenn eine Station ein Ethernet-Paket zum Hub schickt, wird es kopiert und zu allen anderen Ports des Hubs geschickt. Auf diese Weise "sehen" alle Stationen jedes Paket - gerade so wie in einem Bus-Netzwerk. Obwohl jede Station mit einem eigenen Twisted-Pair-Kabel mit dem Hub verbunden ist, handelt es sich doch um ein "Shared Media LAN" (ein LAN mit gemeinsam genutztem Medium).

Hubs sind verwandt mit MAUs (Ringleitungsverteilern). Ein Hub verwendet intern als Zugriffsverfahren CSMA/CD, ein MAU dagegen Token Passing.

IEEE 802.3

Eine Spezifikation für Ethernet, die vom Institute of Electrical and Electronics Engineers (IEEE) festgelegt wurde. Die 802.3-Spezifikation umfaßt Regeln für die Topologie von Ethernet-LANs, für die Arten von Übertragungsmedien, die verwendet werden können und dafür, wie die Elemente des Netzwerks zusammenarbeiten sollen.

IEEE 802.5

Eine Spezifikation für Token Ring, die vom Institute of Electrical and Electronics Engineers (IEEE) festgelegt wurde. Die 802.3-Spezifikation umfaßt Regeln für die Konfiguration von Ethernet-LANs, für die Arten von Übertragungsmedien, die verwendet werden können und dafür, wie die Elemente des Netzwerks zusammenarbeiten sollen.

Intelligente Hubs

Jeder Port eines intelligenten Hubs kann von einer Verwaltungs-Konsole her konfiguriert, überwacht sowie ein- und ausgeschaltet werden. Durch den Einsatz von intelligenten

Hubs wird es möglich, Informationen über eine Vielzahl von Netzwerk-Parametern zu sammeln. Es kann aufgezeichnet werden, wieviele Pakete den Hub und jeden seiner Ports passiert haben, um welche Arten von Paketen es sich gehandelt hat, ob es fehlerhafte Pakete gegeben hat, wieviele Kollisionen aufgetreten sind und anderes.

Die Hersteller von Hubs verkaufen zusammen mit den Geräten Management-Pakete. Diese unterscheiden sich in der Zahl der Informationen, die sie sammeln können, außerdem auch darin, welche Befehle abgesetzt werden können und wie die Informationen dem Netzwerk-Verwalter präsentiert werden.

Internetworking

Der amerikanische Oberbegriff für alles, was mit dem Verbinden von Netzwerken und Netzwerk-Segmenten zu tun hat.

Integrated Services Digital Network (ISDN)

Ein weltweites, digitales Übertragungsnetzwerk, das sich aus dem vorhandenen Telefondienst entwickelt hat. Das Ziel von ISDN ist es, alle vorhandenen Telefonverbindungen durch ein vollständig digital arbeitendes Vermittlungs- und Übertragungssystem zu ersetzen.

Ein Anschluß an das ISDN-Übertragungsnetzwerk erfolgt immer mit zwei sogenannten B-Kanälen, von denen jeder 64 Kbps übertragen kann, und dem D-Kanal für Signalisierungs- Verbindungs- und Steuerinformationen, der eine Übertragungsgeschwindigkeit von 16 Kbps bietet.

Kollision

Kollisionen treten in einem Netzwerk auf, wenn zwei oder mehrere Stationen zur gleichen Zeit Pakete auf das Netzkabel schicken.

Kommunikation

Kommunikation ist in der EDV ein anderer Begriff für Datenübertragung.

Multistation Access Unit (MAU)

Eine MAU (Ringleitungsverteiler) bildet die Verkabelungszentrale in einem Token-Ring-Netzwerk. Die Topologie von Token-Ring-Netzwerke wird als Ring-Topologie beschrieben. Jede Station wird jedoch mit einem separaten Kabel an die MAU angeschlossen (was Hauptmerkmal der Stern-Topologie ist). Der "Ring" befindet sich innerhalb der MAU.

Netzwerk

Verbund mehrerer einzelner Endgeräte (z.B. Computer) zum Zweck des Datenaustauschs und der gemeinsamen Nutzung von Systemkomponenten. Bei der Klassifikation von Netzwerken werden vor allem die folgenden Kriterien angewendet:

1. Netzwerktopologie
(Die Standard-Netzwerktopologien sind: Bus-, Stern- und Ring-Netzwerk)
2. Übertragungsmedium
(Die wichtigsten Übertragungsmedien sind: Koaxial-, Twisted-Pair- und Glasfaserkabel)
3. Übertragungstechnik
(vor allem: Ethernet und Token Ring)
4. Zugriffsverfahren
(vor allem: CSMA/CD und Token Passing)
5. Geographische Erstreckung des Netzwerks
(LAN, MAN oder WAN)
6. Funktionalität (Peer-to-Peer- versus Serverbasiertes Netzwerk)

Netzwerk-Komponenten

Die Hardware-Bestandteile eines Netzwerks. Man unterscheidet zwischen passiven und aktiven Komponenten. Als passive Komponenten werden die Bestandteile im Bereich der Anschlußtechnik bezeichnet. Alle übrigen Netzwerk-Komponenten gehören zu den aktiven Komponenten. Insbesondere sind das Repeater, Bridges, Router, Switches, Transceiver und Hubs.

Netzwerkkarte (Network Interface Card, NIC)

Eine Steckkarte, die in jeden Computer eingesetzt werden muß, der mit einem Netzwerk verbunden werden soll.

Aufgabe der Netzwerkkarte ist es, die Pakete zu "betrachten", die über das Kabel wandern. Pakete, deren Zieladresse mit der Adresse der eigenen Station übereinstimmen, werden kopiert und Computer-intern weitergereicht. Zuvor wandelt die

Netzwerkarte den Bitstrom, den es in Empfang nimmt, so um, daß er sich für die Übertragung auf den parallelen Datenleitungen (den Bus) des Computers eignet.

Netzwerkkarten verfügen über eine vom Hersteller eingeprägte Nummer.

Jede Netzwerkkarte nutzt ein bestimmtes Zugriffsverfahren. Da die Übertragungstechniken Ethernet und Token Ring unterschiedliche Zugriffsverfahren verwenden, gibt es Netzwerkkarten für Ethernet und Netzwerkkarten für Token Ring.

Open Systems Interconnection Reference Model (OSI)

Ein Kommunikations-Modell, das von der International Standards Organization (ISO) entwickelt wurde. Es führt die Aufgaben auf, die von Netzwerk-Komponenten erledigt werden müssen, damit Datenkommunikation funktionieren kann.

Das OSI-Modell beschreibt nur grob, welche Aufgaben von den Komponenten erfüllt werden müssen. Genauere Festlegungen gibt es in Protokollen.

Paket

In Netzwerken werden die Daten einer Nachricht nicht als Gesamtheit übertragen, sondern sie werden zunächst zu Paketen zusammengefaßt und dann als Einzel-Pakete auf die Reise geschickt. Für dieses Vorgehen gibt es vor allem zwei Gründe:

1. Die Übertragungsleitungen werden nicht verstopft. Wartezeiten für die Stationen werden vermieden.

1. Wenn es Fehler bei der Übertragung gegeben hat, muß nicht die gesamte Übertragung wiederholt werden. Lediglich die fehlerhaften Pakete müssen erneut übertragen werden.

Bevor ein Paket auf das Netzwerk geschickt wird, bekommt es allerhand Steuerinformationen zugeteilt, zum Beispiel eine Absender-Adresse und eine Ziel-Adresse.

Protokoll

Protokolle sind Festlegungen für die Zusammenarbeit von Hard- und Software-Produkten. Für alle Abläufe in Netzwerken gibt es Protokolle. Manche dieser Protokolle sind von Standardisierungs-Gremien abgesegnet worden. Daneben gibt es aber auch Protokolle, die im Besitz von einzelnen Firmen sind.

Beispiel: Die Protokolle für Ethernet und Token Ring wurden von dem Institute of Electrical and Electronics Engineers (IEEE) abgesegnet. Jede Firma, die Netzwerkkarten für Ethernet oder Token Ring herstellen will, kann die entsprechenden Spezifikationen kaufen und kann dann die eigenen Produkte auf diese Protokolle ausrichten.

Protokoll-Stack

Bei Protokoll-Stacks handelt es sich um Einzel-Protokolle, die zu Gruppen zusammengefaßt wurden. Häufig eingesetzt werden zum Beispiel die Protokoll-Stacks TCP/IP und IPX/SPX.

Remote Computer

"Remote" bedeutet "entfernt, fern". Bei einem Remote Computer handelt es sich somit immer um einen Computer, den man per Datenfernübertragung erreicht.

Repeater

Repeater sind einfache Geräte für die Verbindung von Netzwerk-Segmenten. Sie erfüllen zwei Funktionen: Sie verstärken die Signale, die sie empfangen und sie leiten diese Signale in ein anderes Netzwerk-Segment weiter.

Da die Preise für die im Netzwerk benötigten Geräte sinken, kann man erwarten, daß die Repeater immer mehr durch die (leistungsfähigeren) Bridges verdrängt werden.

Ring-Topologie

Bei einem Netzwerk mit Ring-Topologie sind die Computer über eine einzige ringförmig verlaufende Leitung miteinander verbunden. Es gibt keine Kabelenden mit Abschlußwiderständen (wie bei der Bus-Topologie)..

Die Signale durchlaufen den Ring in einer Richtung und passieren dabei jeden Computer. Im Gegensatz zur passiven Bus-Topologie funktionieren die einzelnen Computer wie Repeater. Sie senden die Signale, die sie empfangen, verstärkt zum nächsten Computer weiter.

Router

Ein Router [sprich: Rauter] ist ein Gerät, das Netzwerke miteinander verbindet. Router erfüllen komplexere Aufgaben als Bridges. Während eine Bridge Adreßinformationen zu

den direkt angeschlossenen Netzwerken sammelt, können sich Router mit anderen Routern austauschen. Sie sammeln auch Informationen über entferntere Netzwerke und können in Situationen mit mehreren Verbindungs-Möglichkeiten bestimmen, welche die günstigste ist.

Routing-Tabelle

Routing-Tabellen sind kleine Datenbanken, die in Bridges und Routern zum Einsatz kommen. Während Bridges die Adressen von einzelnen Stationen aufzeichnen, werden von Routern nur die Adressen von Netzwerken vermerkt. Bridges merken sich nur Adressen aus den Netzwerken, die sie verbinden. Router dagegen notieren auch Angaben zu entfernteren Netzwerken. Sie sind imstande, ihre Informationen mit anderen Routern auszutauschen.

Segmentierung

Jedes Netzwerk kann nur eine bestimmte Anzahl an Stationen unterstützen. Wenn über die maximale Anzahl hinaus Stationen angeschlossen werden sollen, oder wenn die Übertragungsraten zu wünschen übrig lassen, ist es angebracht, ein Netzwerk in Teil-Netze (Segmente) aufzuteilen. Für die Verbindung der Segmente können Repeater, Bridges, Router und Hubs eingesetzt werden

Station

Als Stationen werden in einem PC-Netzwerk die angeschlossenen PCs bezeichnet. Man spricht auch von Knoten, Arbeitsstationen oder Workstations.

Stern-Topologie

In einem Netzwerk mit Stern-Topologie sind alle Stationen mit einem Hub verbunden. Die Stern-Topologie stammt aus den frühen Tagen der EDV, als die Computerterminals mit einem zentralen Großrechner verbunden waren.

Switch

Ein Gerät, das mehrere separate LANs miteinander verbindet und Paketfilterung durchführt. Ein LAN-Switch ist ein Gerät mit mehreren Ports. Jeder dieser Ports kann eine einfache Station oder aber auch ein gesamtes Ethernet- oder Token-Ring-LAN unterstützen.

Telekommunikation

Ein anderer Ausdruck für "Telekommunikation" ist "Datenfernübertragung". In den Bereich der Telekommunikation fällt jede Form der elektronischen Informationsübermittlung, bei der größere Entfernungen überbrückt werden.

Token

Ein Token ist eine spezielle Abfolge von Bits. Es wird in Token-Ring-Netzwerken benötigt, um Kollisionen zu verhindern. Das Token kreist auf dem Ring, und eine Station, die senden will, muß sich in den Besitz des Tokens bringen und kann dann an das Token die Daten anhängen.

Token Passing

Das Zugriffsverfahren, das in Token-Ring-Netzwerken eingesetzt wird.

Token-Ring-Netzwerk

Token Ring ist nach Ethernet die Übertragungstechnik mit der größten Verbreitung. Das wichtigste Merkmal von Token Ring stellt das Zugriffsverfahren dar, das als Token Passing bezeichnet wird. In einem Token-Ring-Netzwerk sind alle Stationen an eine Multistation Access Unit (MAU) angeschlossen (deutsch: Ringleitungsverteiler). Die MAU enthält einen Ring, auf dem ein Token sich immer in derselben Richtung bewegt und nacheinander alle angeschlossenen Stationen passiert. Sendeberechtigt ist immer nur diejenige Station, die sich im Besitz des Tokens befindet.

Topologie

Wenn man die Topologie eines Netzwerks beschreibt, dann gibt man an, wie die Stationen miteinander verbunden sind. Die Topologie sieht bei jedem Netzwerk anders aus. Es gibt jedoch Standard-Topologien, auf die immer wieder zurückgegriffen wird (siehe Bus-Netzwerk, Ring-Netzwerk, Stern-Netzwerk).

Trailer

Jedes Paket, das über ein Netzwerk verschickt wird, enthält neben den Nutzdaten auch Daten, die für die Kommunikationssteuerung benötigt werden. Diese unterteilen sich in einen Header, der sich vorne am Paket befindet und einen Trailer, der das Ende des

Pakets bildet. In der Regel enthält der Trailer Daten zur Fehlerüberprüfung, die mit Hilfe des Cyclical Redundancy Checks (CRC) berechnet werden.

Transceiver

Einfaches Gerät zum Anschluß von Computern an ein Ethernet.-Netzwerk. Der Transceiver wandelt den parallelen Datenstrom auf dem Prozessorbus in einen seriellen Datenstrom auf dem Anschlußkabel um.

Es gibt interne und externe Transceiver. Ein interner Transceiver befindet sich auf der Netzwerkkarte, ein externer dagegen bildet in einem Bus-Netzwerk das Verbindungsstück zwischen dem Kabel, das zu einer Station führt und dem Hauptkabel.

Twisted-Pair-Kabel

Neben Koaxialkabeln die am häufigsten eingesetzte Kabelart. Es gibt geschirmte und ungeschirmte Twisted-Pair-Kabel, wobei die ungeschirmten die am meisten verbreiteten sind.

Übertragungstechnik

Die bekanntesten Übertragungstechniken sind Ethernet und Token Ring. Der deutlichste Unterschied zwischen den beiden Techniken besteht in dem verwendeten Zugriffsverfahren. (Ethernet verwendet CSMA/CD und Token Ring Token Passing.)

In der amerikanischen Netzwerk-Literatur wird für Übertragungstechnik häufig der Begriff Netzwerk-Architektur (Network Architecture) verwendet.

Verteilerschrank

Ein zumeist mannshohes Metallgestell, das über etliche Einschübe verfügt. Im Verteilerschrank werden Hubs, MAUs und andere Geräte untergebracht.

Zugriffsmethode / Zugriffsverfahren

Die Gesamtheit der Vorschriften, die eine Übergabe von Daten vom Computer an ein Netzkabel regeln. Durch die Anwendung von Zugriffsmethoden wird verhindert daß mehrere Stationen gleichzeitig Pakete auf das Kabel schicken. Die Methoden mit der größten Verbreitung sind CSMA/CD und Token Passing.