

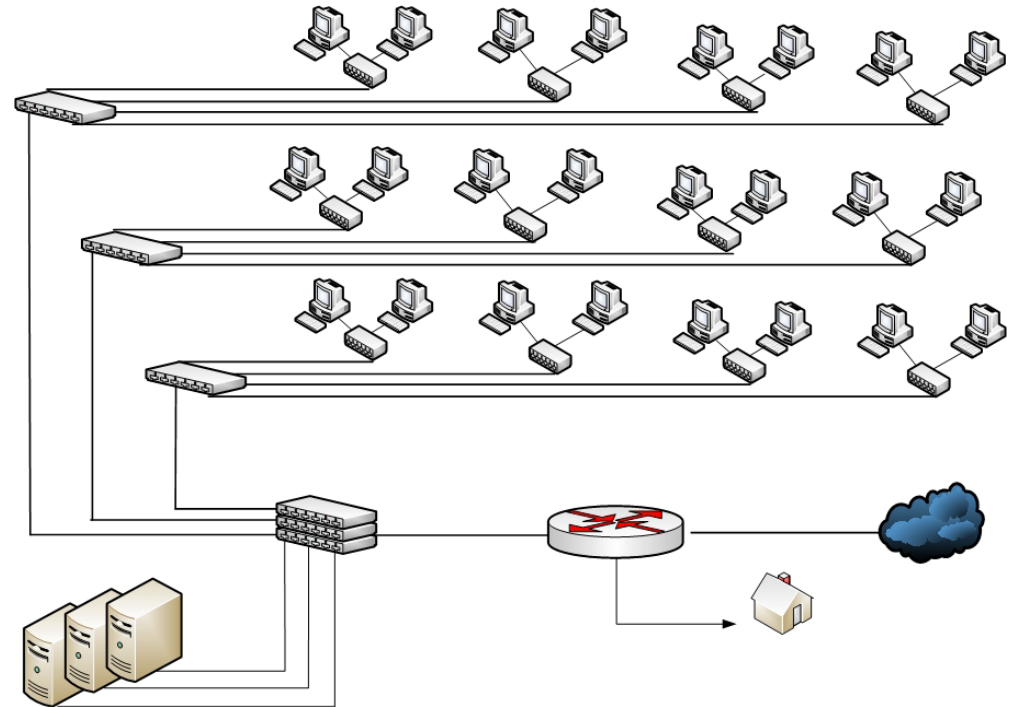
Computer Netzwerk-Technik

Teil 1: Netzwerk-Design

- Verkabelungen
- Topologien
- Geräte im Netz
- Protokolle
- TCP/IP
- Routing
- OSI-Modell

Autor: Rainer Egewardt

Copyright © by PCT-Solutions



Kompaktes Netzwerk-Wissen rund um Netzwerk-Hardware und TCP/IP

Unsere Bücher „Das PC-Wissen für IT-Berufe“ als Print-Medien, sind zu Bestsellern im IT-Buchmarkt geworden.
Hier nun auch kompaktes IT-Wissen als ebook.

Powered by



Inhaltsverzeichnis

Copyright © 2010
für Text, Illustrationen
und grafische Gestaltung
by PCT-Solutions
Rainer Egwardt

Dieses ebook wurde auf der Basis von fundierten Ausbildungen, Weiterbildungen und umfangreichen Praxiserfahrungen erstellt. Für Schäden aus unvollständigen oder fehlerhaften Informationen übernehmen wir jedoch keinerlei Haftung.

PCT-Solutions

info@pct-solutions.de
www.pct-solutions.de

Überblick über die einzelnen Kapitel

Netzwerk-Arten.....	04
Ausdehnungen.....	06
Übertragungsmedien.....	07
Topologien.....	12
Bandbreiten.....	16
Backbones.....	17
Zugriffsverfahren.....	18
Bezeichnungen Netzwerke.....	21
Geräte im Netzwerk.....	29
Strukturierte Verkabelung.....	37
Übertragungs-Protokolle.....	41
Multiprotokoll-Umgebung.....	43
TCP/IP.....	44
Hilfsprotokolle zu TCP/IP.....	53
TCP/IP-Routing.....	55
WAN-Technologien.....	60
OSI-Schichten-Modell.....	65

Tipp: Für ein detailliertes Inhaltsverzeichnis mit allen Unterpunkten benutzen Sie bitte die Lesezeichen links im AcrobatReader. Hier kann schnell und direkt zu den einzelnen Punkten und Kapiteln gesprungen werden.

*Unsere top-aktuellen
Neuveröffentlichungen
als EBooks zum Download
von unserer Web-Site*

**Copyright © 2010
für Text, Illustrationen
und grafische Gestaltung
by PCT-Solutions
Rainer Egwardt**

PCT-Solutions

**info@pct-solutions.de
www.pct-solutions.de**

- Computer-Netzwerke Teil 1
 - Computer-Netzwerke Teil 2
 - Computer-Netzwerke Teil 3
 - Computer-Netzwerke Teil 4
 - Computer-Netzwerke Teil 5
 - Computer-Netzwerke Teil 6
 - Computer-Netzwerke Teil 7
 - Datenbank Teil 1
 - Datenbank Teil 2
 - Datenbank Teil 3
 - Mailing Teil 1
 - Mailing Teil 2
 - Internet Teil 1
 - Internet Teil 2
 - Internet Teil 3
 - Web-Programmierung Teil 1
 - Web-Programmierung Teil 1
 - Web-Programmierung Teil 1
 - Web-Programmierung Teil 1
 - Web-Programmierung Teil 1
 - Web-Programmierung Teil 1
 - Software Teil 1
 - Software Teil 2
 - Software Teil 3
- Netzwerk-Design (Netzwerk-Hardware)
Konfiguration eines Windows-Server basierten Netzwerkes
DNS-, WINS-, DHCP-Konfiguration
Optimieren von Windows-Netzwerken
Netzwerkanbindung von Windows-Clients
Scripting-Host in IT-Netzwerken
Projekt-Management in IT-Netzwerken
MS-SQL-Server als Datenbank-Backend
MS-Access als Datenbank-Frontend
SQL-Programmierung (Transact-SQL)
MS-Exchange-Server als Mail-Server
Outlook als Mail-Client
Internet-Information-Server als HTML-Server
MS-Frontpage zum Erstellen eines HTML-Pools
Internet-Browser
HTML
DHTML
CSS
PHP
JavaScript
XML
Professionelle Bildbearbeitung Corel PhotoPaint
Professionelle Layouts mit Adobe Illustrator
Grafisches Allerlei mit MS-Visio

und viele weitere EBooks zum Download auf unserer Internetseite

Computer-Netzwerk-Technik (Netzwerk-Design)

Unter einem Netzwerk wird die Verbindung von mindestens zwei Rechnern verstanden, die gemeinsam Ressourcen nutzen, Informationen gegenseitig austauschen und mit einem einheitlichen Datenbestand arbeiten können.

Netzwerk-Arten

Peer-To-Peer-Netzwerk

(alle Rechner sind gleichberechtigt)

Die Peer-Rechner benutzen gemeinsam Ressourcen (Drucker, Daten), die auf allen Rechnern verteilt liegen können (schlechte Übersicht, wo Daten liegen). Jeder Peer muss für die Sicherheit seiner Ressourcen selber sorgen.

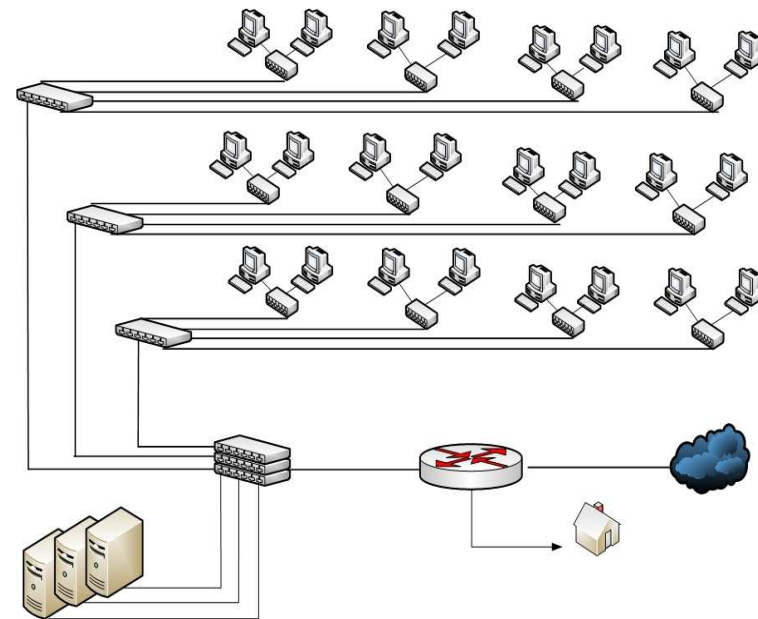
Ein Peer kann Client sein (wenn er Ressourcen anfordert) oder Server (wenn er Ressourcen verteilt).

- Datenaustausch auf Freigabeebene
- wenn benutzerabhängig, muss jeder Benutzer auf jeder Workstation (WS) bekannt sein
- hoher Verwaltungsaufwand
- keine Datenkonsistenz
- Zugriffskontrolle schwierig
- Datensicherung schwierig
- nur für kleinere Netzwerke oder als Home-Netzwerk zu empfehlen

Server basiertes Netzwerk (Client/Server-Prinzip)

In einem serverbasierten Netzwerk gibt es Server, die Dienste und Ressourcen anbieten (starke, leistungsfähige Rechner, die nur für diesen Zweck optimiert sind) und Clients (benutzerorientierte Rechner), die die Ressourcen der Server nutzen.

- zentrale Verwaltung der Freigaben der Benutzerdatenbank des Servers
- zentrale Verwaltung der Daten
- Nutzer müssen nur auf dem Server bekannt sein
- Datenkonsistenz ist gewährleistet
- Zugriffskontrolle möglich
- Datensicherung einfach

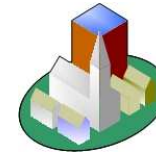
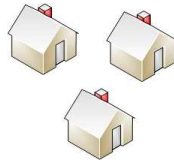


PC-Netzwerk mit zentralisierten Servern

Ausdehnungen

LAN (Local-Area-Network)

- Lokales Einsatzgebiet (Gebäude)
- hohe Übertragungsraten
- Übertragungsmedium = Kabel
- und/oder = Funk (WLAN)



WAN (Wide-Area-Network)

- Einsatzgebiet weltweit
- geringe – mittlere Übertragungsraten
- Übertragungsmedium = öffentliche Kabel, Satelliten, Richtfunk

MAN (Metropolitan-Area-Network)

- Einsatzgebiet im Stadtbereich und bis zu 50 km Umkreis
- noch hohe Übertragungsraten
- Übertragungsmedium = besonderes Kabel



Kabel-Übertragungsmedien

Koaxial-Kabel (10BASE-2) (nur noch vereinzelt zu finden)

- wird im BUS-Netz verwendet (siehe auch Topologien)
- Axialer Innenleiter, geflochtener Außenleiter
- die Netzkarte muss einen BNC-Anschluss haben
- das Kabel wird über T-Stücke direkt mit der Karte verbunden
- die Enden des BUSses müssen mit Terminatoren (Widerständen) abgeschlossen werden

Kupferkabel (Coaxial)		
Kabeltyp	Impedanz	Einsatzgebiete
RG-58/U	53,5 OHM	teilweise für Ethernet eingesetzt
RG-58A/U	50 OHM	Thinwire-Ethernet, 10Base2
RG-58C/U	50 OHM	Thinwire-Ethernet, 10Base2
RG-59	75 OHM	Kabelfernsehen
RG-62	93 OHM	SNA (3270), ARCnet

Twisted-Pair (10/100BASE-T)

- wird überwiegend mit der Stern- oder Baum-Topologie verwendet (siehe auch Topologien)
- verdrehtes Paar (können auch mehrere sein, können abgeschirmt (STP) oder nicht abgeschirmt (UTP) sein)
- die Netzkarte muss einen UTP-Anschluss (RJ 45) haben
- die PC's werden mit dem Kabel über HUB's oder Switches (siehe auch Geräte im Netz) an das Netzwerk angeschlossen

Kupferkabel (Twisted Pair)				
Kabeltyp	Spezifikat.	spezifiziert	Impedanz	Einsatzgebiet
STP	IBM Typ 1/9	20 MHz	150 OHM	4/16-MBit-Token-Ring
UTP-1 Kat 1	EIA/TIA-568	–	100 OHM	Analoge Sprachübertragung, Alarmsysteme
UTP-2 Kat 2	EIA/TIA-568	–	100 OHM	IBM-Verkabelung Typ3 (Sprache)
UTP-3 Kat 3	EIA/TIA-568	16 MHz	100 OHM	10BaseT, 100BaseT4, 100-VG-Anylan, 4-MBit-Token-Ring, ISDN
UTP-4 Kat 4	EIA/TIA-568	20 MHz	100 OHM	16-MBit-Token-Ring
UTP-5 Kat 5	EIA/TIA-568	100 MHz	100 OHM	100BaseTx, ATM

Fiber-Optic-Kabel (Glasfaser, 10/100/1000BASE-F)

Lichtwellenleiter

Glasfaser-Kabel			
Kabeltyp	Durchmesser (Kern/Gesamt)	Bandbreite (Länge 1 km)	Einsatzgebiet
Multimode mit Stufenprofil	100 bis 400 µm / 200 bis 500 µm	100 MHz	unter 1 km
Multimode mit Gradientenprofil	50 µm / 125 µm	1 GHzLAN	Backbone, ATM
Multimode mit Gradientenprofil	62,5 µm / 125 µm	1 GHzLAN	Backbone, ATM
Monomode Single- mode mit Stufenprofil	8 µm/125 µm	100 GHz	Netzwerke mit mehr als 1 GBit pro Sekunde

Zusammenfassung von Daten der wichtigsten Übertragungsmedien

10Base2 oder Thin-Ethernet	
Mindestabstand zwischen 2 Clients	0.5 m
Einzelnes Kabelsegment	185 m
Gesamtes Netz darf nicht länger sein als	925 m
Max. Anzahl von Knoten pro Segment (Inc. Clients und Verstärker)	30

Im gesamten Netz darf es nicht mehr als 5 Segmente geben, die über max. 4 Verstärker verbunden werden können, und nur in 3 der 5 Segmente dürfen Knoten enthalten sein.

10Base5 oder Thick-Ethernet	
Mindestabstand zwischen 2 Transceivern	2.5 m
Einzelnes Kabelsegment	500 m
Gesamtes Netz darf nicht länger sein als	2500 m

Max. Anzahl von Knoten pro Segment (Inc. Clients und Verstärker)	100
max. Länge des Kabels vom Transceiver → Computer	50 m

10/100Base-T Thin-Ethernet (Twisted-Pair)	
Mindestabstand zwischen 2 Clients	2.5 m
Max. Wegstrecke vom Verteiler zum Computer	100 m
Gesamtes Netz darf nicht länger sein als	925 m
Max. Anzahl von Knoten innerhalb eines LANs	1024

Bezeichnungen der Übertragungsmedien

- 10BASE-2
- 10BASE-5
- 100BASE-T
- 10BASE-F
- 10BROAD36
- 1BASE5

Die erste Zahl gibt die Übertragungsrate in MBit/s (Megabit pro Sekunde) an.

BASE bzw. BROAD steht für Basis- bzw. Breitband.

Die letzte Zahl/Buchstabe steht für die max. Ausdehnung pro Segment in Hundert Meter, bzw. für das Medium.

T für Twisted-Pair, F für Fiber-Optic, 2 für 200 m, 5 für 500 m, wobei aus der 2 ersehen werden kann, dass hier Thin-

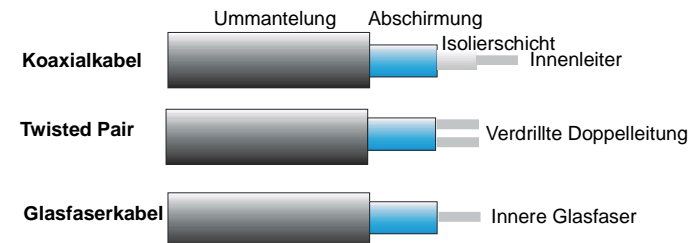
Ethernet (meist Twisted-Pair) und aus der 5 Thick-Ethernet (Yellow Cable), benutzt wird.

Die 100BASE-T unterscheiden sich noch in

100BASE-T4: 100 MBit/s über vierpaariges Kategorie-3-Kabel

100BASE-FX: 100 MBit/s über zwei Glasfaserleitungen

100BASE-TX: 100 MBit/s über zweipaariges Kategorie-5-Kabel (STP oder UTP)



Topologien

Unter einer Netzwerk-Topologie wird die physikalische Auslegung der Verkabelung eines Netzes verstanden. Sie beschreibt nicht nur die elektrische Verbindung, sondern auch die Richtung des Datenflusses im Netz zwischen den Stationen.

BUS-Topologie

Beim Bussystem sind alle Rechner an einem gemeinsamen, passiven Medium, dem Bus, angeschlossen. Jede Station kann frei, unabhängig von einem Host, kommunizieren. Die BUS-Enden müssen durch Terminatoren abgeschlossen werden. Ein Bussystem hat den geringsten Kabelbedarf.

Informationen fließen in allen Richtungen.

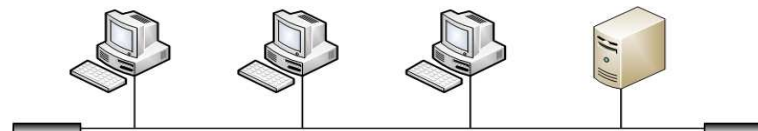
Der Server sollte in der Mitte sein (muss aber nicht).

Der Ausfall eines Knotens führt nicht zum Ausfall des Netzes, wenn es nicht gerade der Server ist. Kabelbruch führt zum Ausfall des Netzes, weil kein Abschluss mehr gegeben ist.

Bekannt geworden ist das Bussystem mit Ethernet.

Die BUS-Topologie wird kaum noch verwendet und eignet sich nur für kleinere Netzwerke.

BUS-Topologie



Ring-Topologie

Es wird ebenfalls ein gemeinsames Übertragungsmedium verwendet, nur dass dieses, im Gegensatz zum Bussystem, zu einem Ring zusammen geschlossen ist. Jede Station hat einen Vorgänger und einen Nachfolger. Die Informationen werden von Station zu Station weitergereicht, wobei jede Station prüft, ob die Nachricht für sie bestimmt ist.

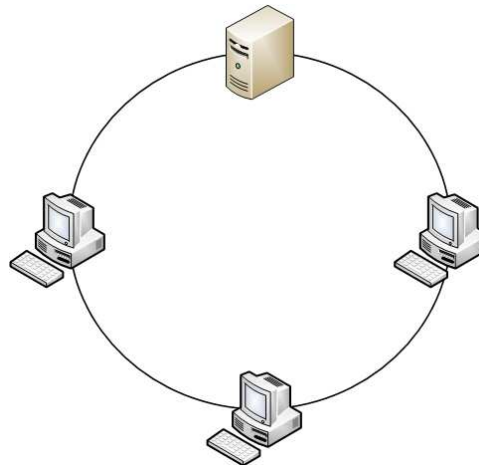
Informationen fließen in einer Richtung.

Die Ring-Topologie hat die absolut geringste Kabelmenge bei kleineren Netzen.

Der Ausfall eines Knotens oder Kabelbruch führt zum Ausfall des Netzes.

Bekannt geworden ist das System durch Token-Ring, welches auch nur noch vereinzelt zu finden ist.

Ring-Topologie



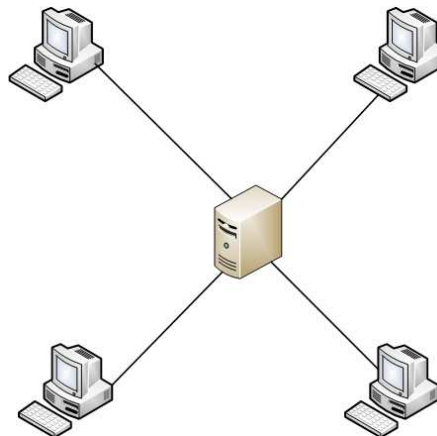
Stern-Topologie

Die Sterntopologie ist eine klassische Auslegung, die im Großrechnerbereich verwendet wird. In der Mitte befindet sich der Host und sternförmig daran angeschlossen sind die I/O-Systeme.

Informationen fließen in beiden Richtungen.

Knotenausfall oder Kabelbruch führt nicht zum Ausfall des Netzes.

Stern-Topologie



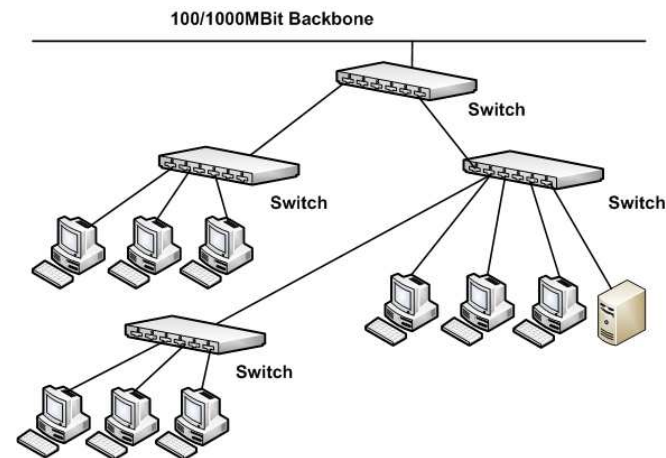
Baum-Topologie

Die Baum-Topologie stellt eigentlich keine eigene Topologie dar, da sich trotz logischem Stern alle Workstations in einer Collosions-Domain befinden (bei Verwendung von HUBs) und sich die Bandbreite des Netzes teilen müssen, wie im normalen Bus-Netz. Nur die Knoten, die

direkt an einem Switch angeschlossen sind, bekommen bis zum Switch die volle Bandbreite (siehe auch Netzwerk-Geräte).

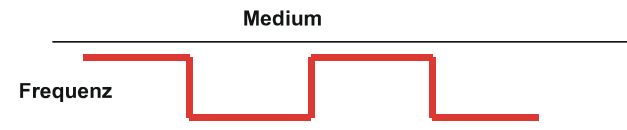
Dieser Aufbau eines Netzes wird heute am meisten verwendet.

Baum- (logischer Stern) Topologie



Bandbreiten

Unter der Bandbreite eines Netzwerkes wird die Fähigkeit eines Mediums, Daten zu übertragen, verstanden. Da Datenübertragungsraten in Mega-Bit pro Sekunde angegeben werden, spricht man z.B. von einer Bandbreite von 100 MBit/s.



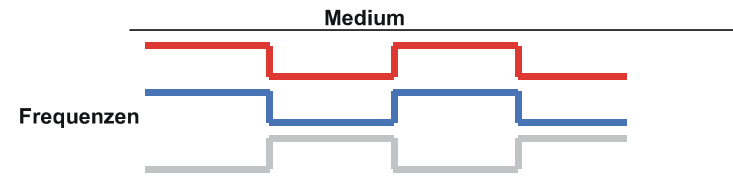
Breitband

Beim Breitband teilen sich mehrere Kommunikationskanäle die Bandbreite.

Übertragene Frequenzen

Basisband

Beim Basisband wird die gesamte Kapazität einem Kommunikationskanal zugeordnet.

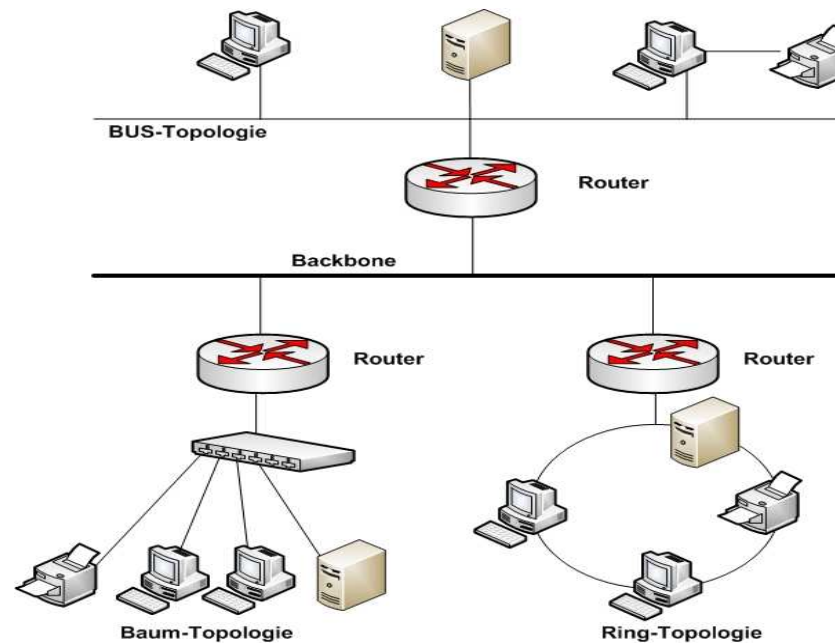


Backbones

Backbones verbinden nur Topologien und stellen keine eigene Topologie dar. Sie sind sehr schnell und laufen an den SUB-LANs vorbei. Mit ihnen werden Übergänge zu anderen Netzen geschaffen, die auch eine andere Topologie aufweisen können.

Bei großen Netzwerken sollte im Backbonebereich mit 1000MBit-Strecken und Switches gearbeitet werden, da hier der größte Netzwerkverkehr zu erwarten ist und so Engpässe vermieden werden können (siehe auch Strukturierte Verkabelung).

Backbone



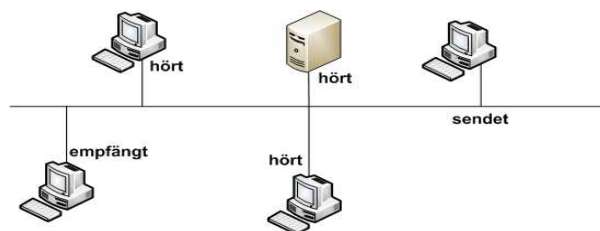
Zugriffsverfahren

Kollosionsverfahren (CSMD/CD)

Damit wird das Zugriffsprotokoll bezeichnet, mit dem Ethernet arbeitet. Das Verfahren regelt hierbei, wie sich die Netzwerkknoten beim gemeinsamen Zugriff auf das Netz verhalten sollen. Es wird im Ethernet angewendet. Es ist nicht beeinflussbar und gehört zur Topologie des Netzes.

Alle Knoten können gleichzeitig senden.

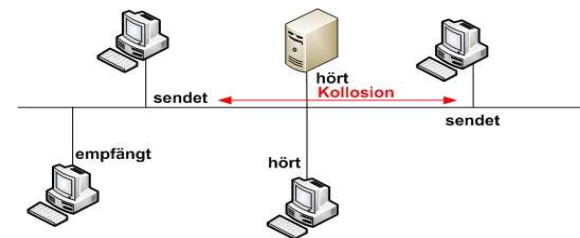
Kollosions-Verfahren



Vorher wird abgefragt, ob die Leitung frei ist. Wenn sie frei ist, dann wird gesendet. Andere Knoten werden nicht gesperrt und können auch senden.

Es entsteht eine Kollision.

Der Knoten, der sendet, muss nach dem Senden wieder abfragen, ob eine Kollision vorliegt (senden eines anderen Knotens gleichzeitig). Stellt er fest, dass eine Kollision vorgelegen hat, sendet er seine Nachricht nach einer gewissen Zeitspanne nochmal. Dieser Vorgang wird solange wiederholt, bis die Nachricht gesendet und empfangen worden ist.



Token(Zeichen)-Verfahren

Das Token-Verfahren wird im Ringnetz verwendet. Es wird ein Zeichen von einem Knoten zum nächsten weitergegeben. Dabei gibt es Belegt- und Freitoken. Die Workstation muss abfragen, ob ein Freitoken vorhanden ist. Dann kann sie die Leitung belegen und senden. Jeder Knoten prüft, ob die Nachricht für ihn bestimmt ist. Wenn nicht, wird das Datenpaket weitergegeben. Ist das Datenpaket beim Empfänger angekommen, nimmt dieser die Daten entgegen und gibt ein Freitoken aus.

FDDI

Als besonderes Zugriffsverfahren zählt FDDI. Es ist ein Zugriffsverfahren, dass 100-MBit/s-Übertragungsraten garantiert.

FDDI wurde als 100-MBit-Token-Ring für hohe Bandbreiten konzipiert und wird überwiegend im Backbonebereich mit Glasfaserkabel eingesetzt (lässt sich aber auch mit Koax- bzw. Twisted-Pair realisieren).

FDDI kennzeichnet ein Zugriffsverfahren, aber auch ein Verbindungskonzept und eine Netzwerktypisierung.

Als Übertragungsmedium wird FDDI im Doppel-Token-Ring eingesetzt.

Das Zugriffsverfahren FDDI basiert auf Token-Passing.

ARC-Net

Das ArcNet wird vorzugsweise im Sternnetz verwendet – unter bestimmten Voraussetzungen aber auch im BUS-Netz oder im logischen Ring.

Eckdaten Arc-Net

- ArcNet Netzwerkkarte
- Kollisionsfreies Token-Bus-Zugriffsverfahren (bei BUS und Stern)
- wird über Knotenadressen organisiert
- 2 1/2 MBit/s Übertragungsgeschwindigkeit
- verwendet das RG-62-Koaxial-Kabel mit 93 Ohm Widerstand
- Anschluss an BNC-Stecker
- Topologie ist stern- oder busförmig
- als Verteiler werden HUB's genommen (aktiv, passiv)

Längen:

Rechner → akt. Hub = 600 m

akt. Hub → akt. Hub = 600 m

Rechner → pass. Hub = 30 m

akt. Hub → pass. Hub = 30 m

Es können bis zu 255 Rechner in ein ArcNet eingebunden werden.

Die gesamte Ausdehnung des Netzes kann 6500 m betragen.

Bei Busvernetzung werden alle Rechner mit einem T-Stück verbunden, dass sich auf der Netz-Karte befinden muss. Das Buskabel darf bis zu 300 m lang sein, wobei bis zu 8 Rechner angeschlossen werden dürfen. Dafür müssen spezielle Netzwerkkarten verwendet werden (HZ-Karten). Die beiden Enden des Busses sind mit Terminatoren zu versehen.

Bezeichnungen Netzwerke

Ethernet

Beim Ethernet wird unterschieden in:

- *Thick-Ethernet* (alte Technologie)
- *Thin-Ethernet* (heute verwendet)

Thick-Ethernet

- Übertragungsgeschwindigkeit 10MBit/s (fällt bei Belastung schnell)
- Kollisionsverfahren
- dickes, gelbes Koaxialkabel mit 50 Ohm, relativ starr, schwer zu verlegen, relativ hohe Kosten
- unempfindlich gegen Störeinflüsse und ein Segment kann sehr lang sein
- wird für die Bus-Topologie verwendet
- der Kabelstrang darf 500 m lang sein und muss terminiert werden
- der Anschluss an die Rechner geschieht über Transceiver, das Trans-

ceiverkabel wird mit der Netzwerkkarte verbunden, das aber nicht länger als 50 m sein darf

- manche Ethernetkarten bieten einen DIX- und einen Thin-Ethernet-Anschluss. Die Anschlussart muss auf der Karte eingestellt werden
- minimalste Distanz zwischen 2 Transceiver = 2.5 m oder ein Vielfaches davon
- in einem Segment dürfen 100 Transceiver vorhanden sein. Bei mehreren Rechnern auf engem Raum wird ein Multitransceiver benutzt, der an einen normalen Transceiver angeschlossen wird und 8 Ausgänge besitzt. Mehrere Segmente werden mit Transceivern verbunden. Auf diese Weise kann der BUS über 500 m hinaus verlängert werden

Thin-Ethernet (Cheapernet)

- nur noch vereinzelt zu finden
- Übertragungsgeschwindigkeit 10MBit/s (fällt bei Belastung schnell)
- Kollisionsverfahren
- verwendet RG-58-A/U-Koaxial-Kabel, welches flexibel ist
- verursacht geringe Kosten, ist allerdings störanfälliger wegen der geringeren Abschirmung. Cheapernet wird vor allem bei kleineren Netzen (Büro-umgebung) eingesetzt und wird bus-förmig aufgebaut
- die Segmentlänge kann 185 m betragen und muss terminiert werden
- der Rechner wird über ein T-Stück mit dem BUS verbunden.
- der Abstand zwischen 2 Rechnern darf min. 0.5 m betragen
- an einem Segment können 30 Rechner angeschlossen werden. Zur Kopp-

lung mehrerer Segmente werden die gleichen Elemente, wie beim Thick-Ethernet benutzt

- über spez. Adapter kann Thick- und Thin-Ethernet verbunden werden
- bei mehreren Segmenten muss ein Repeater benutzt werden

Thin-Ethernet (Twisted Pair)

- Übertragungsgeschwindigkeit 10–100 MBit/s (fällt bei Belastung schnell)
- Kollisionsverfahren. Nur bei Einsatz von Switches können die vollen Bandbreiten teilweise erhalten werden
- es verwendet STP oder UTP-Kabel der Kategorie 1–5 (siehe auch Übertragungsmedien) und verursacht auch noch geringe Kosten
- es ist logisch sternförmig aufgebaut. Bei Verwendung mit HUB's allerdings physk. busförmig, da sich alle Rechner, die an einen HUB angeschlossen sind, die Bandbreite teilen müssen

- Die Rechner werden über HUB's oder Switches verbunden, die Repeaterfunktionen beinhalten.

Der Abstand zwischen 2 Rechnern darf min. 2.5 m betragen.

Token-Ring

- Nur noch vereinzelt zu finden
- Übertragungsgeschwindigkeit 4–16 MBit/s
- Token-Zugriffsverfahren
- es verwendet 7 verschiedene Kabeltypen

Token-Ring ist eine Reihe ringförmig gekoppelter Sterne, die einen geschlossenen Ring ergeben. Wichtigster Bestandteil ist dabei die MAU (Multistation Access Unit). Diese hat 2–16 Anschlüsse für die Rechner und RING-IN- / RING-OUT-Anschlüsse, um mehrere MAUs zu verbinden.

Um einen Rechner an den Ring anzuschließen, wird eine Hin- und eine Rückleitung benötigt. Jeder Rechneranschluss in der MAU ist mit einem Relais versehen. Durch die Einbindung eines Rechners wird der Ring erweitert.

Fällt ein Rechner aus oder wird er vom Netz genommen, wird das Relais geschlossen, sodass der Ring nicht unterbrochen wird. Auch die Verbindung zu anderen MAUs hat 2 Leitungen, sodass ein Ausfall immer abgefangen werden kann.

Die Distanzen zwischen MAUs und Rechnern ist vom verwendeten Kabel abhängig.

Faustregeln

Rechner → MAU = 50 m

MAU → MAU = 50 m

Mit entsprechenden Einheiten können die Distanzen erhöht werden.

Gigabit-Ethernet

Gigabit-Ethernet ist eine Technologie, die sich in heutigen Netzwerken immer mehr durchsetzt, da immer höhere Anforderungen an Geschwindigkeiten im Netzwerk gestellt werden. Neuere Betriebssysteme und Anwendungen benötigen auch immer größere Bandbreiten, die die aufkommenden Datenmengen noch bewältigen. In sehr großen Netzwerken ist ein reibungsloser Betrieb des Netzwerkes ohne eine entsprechende Backbone auch fast nicht mehr möglich. In diesem Zusammenhang macht Gigabit-Ethernet und ATM immer mehr von sich reden und ist in großen Netzwerken schon zum Standard geworden.

- Übertragungsgeschwindigkeit 1250 Mbit/s
- verwendet 3 verschiedene Kabeltypen wie, Twinax, Glasfaser, Twisted-Pair

- Der Kabeltyp bedingt bestimmte Segmentlängen
- kann für alle Ethernet-Technologien verwendet werden
- kann das herkömmliche Zugriffsverfahren des Ethernets (CSMA/CD) verwenden, welches in „geschwitchten Umgebungen“ allerdings nicht mehr nötig ist
- kann 10, 100 oder 1000 Mbit verwenden
- verursacht hohe Kosten
- wird hauptsächlich im Backbone-Bereich verwendet
- aber auch für schnelle Verbindungen von Switches zu Switches und Switches zu Servern
- kann im Vollduplex-Mode betrieben werden

Halfduplex = Senden und empfangen nacheinander

Vollduplex = Senden und empfangen gleichzeitig

Kupferkabel (billiger, aber eher in Serverschränken und Serverräumen zu finden, wegen der geringen Längen)

Typ	Reichweite	Impedanz	Kabeltyp	Stecker
1000BaseCX	25 m	150 Ohm	Twinax	STP (DB9, Style 1)
1000BaseCX	25 m	150 Ohm	Twinax	IEC61076 (Style 2)

Glasfaserkabel (für die Backbone-Verkabelung)

Typ, Faser	Bandbreite [MHz / km]	Segmentlänge	Kabeltyp	Stecker
1000BaseSX, 62,5µm	160	2-220 m	Multimode	Duplex SC
1000BaseSX ,62,5µm	200	2-275 m	Multimode	Duplex SC
1000BaseSX , 50µm	400	2-500 m	Multimode	Duplex SC
1000BaseSX, 50 µm	500	2-550 m	Multimode	Duplex SC
1000BaseLX, 62,5 µm	500	2-550 m	Multimode	Duplex SC
1000BaseLX, 50 µm	400	2-550 m	Multimode	Duplex SC
1000BaseLX, 50 µm	500	2-550 m	Multimode	Duplex SC
1000BaseLX, 10 µm		2-5000 m	Monomode	Duplex SC

ATM

(Asynchronous Transfer Mode)

ATM ist für hohe Bandbreiten konzipiert und ist eine Technologie, die mit speziellen Geräten im Netzwerk verwendet wird. Während andere Technologien mit Zellen (Frames) von unterschiedlichen Längen arbeiten, baut ATM auf Zellen fester Länge (53 Byte) auf.

- Übertragungsraten zwischen 155 und 622 Mbit/s
- wird vornehmlich im Backbone-Bereich oder zur Übertragung von Sprache und Video eingesetzt, wobei der Übertragung von Audio/Video Vorrang im Netz eingeräumt wird
- die Kommunikation in ATM-Netzen verläuft über virtuelle Pfade
- Bandbreiten können in beliebiger Höhe an WS's zugewiesen werden (Quality of Service, QoS)
- bedingen ATM-kompatible Geräte im Netz wie ATM-Router, ATM-Switches, etc
- übertragen Daten nicht nach Ip- oder MAC-Adressen, sondern über spezielle 3 Byte große Identifikationen (Gerät-zu-Gerät-Verbindung)
- kann im LAN sowie für WAN-Verbindungen eingesetzt werden

Fazit zu den voran gegangenen Erläuterungen

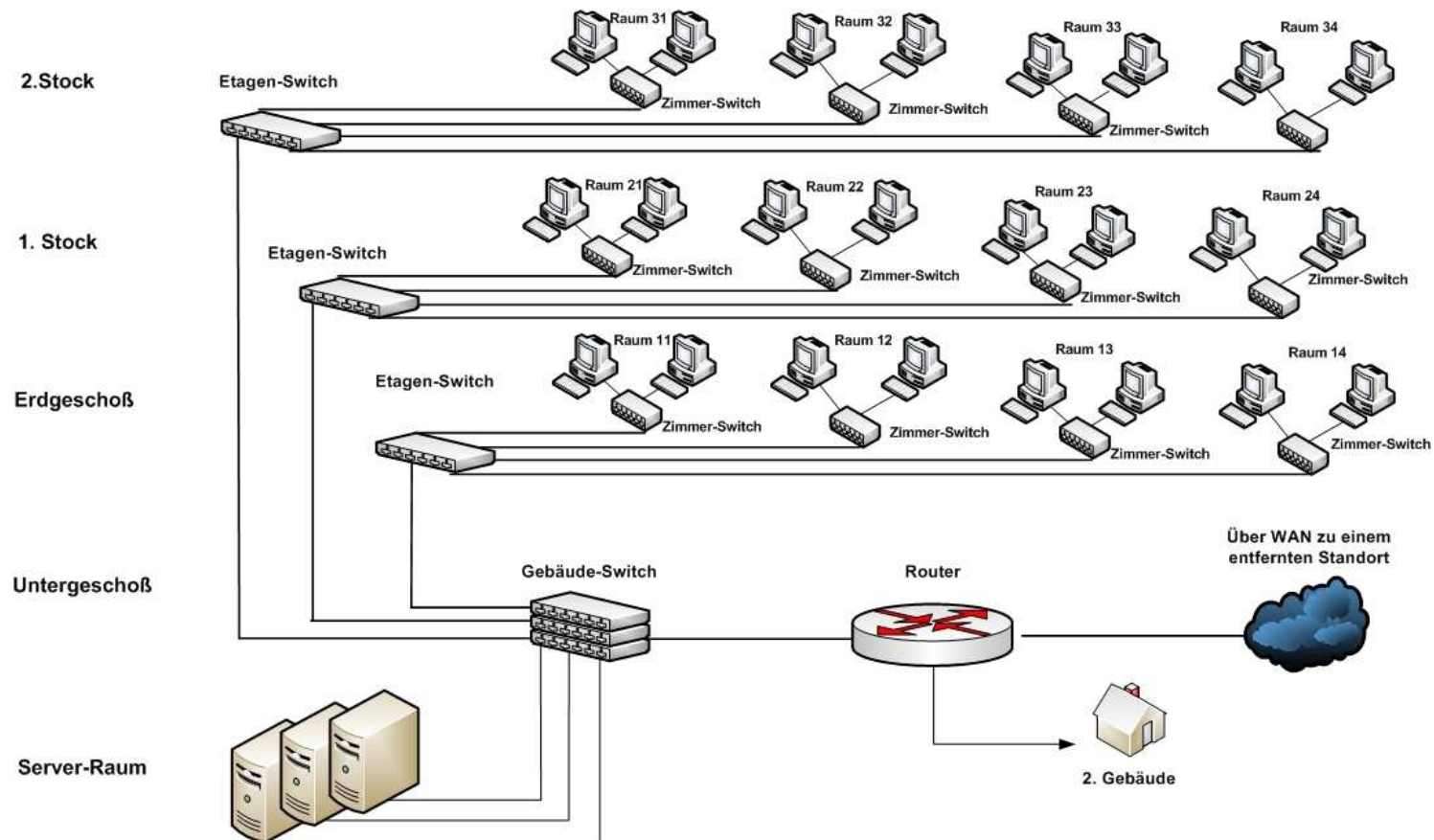
Insgesamt ist festzuhalten, dass sich in heutigen Netzwerken die Baum-Struktur durchgesetzt hat. BUS-, und Ring-Topologien sowie die dazugehörigen Zugriffsverfahren sind sicher nur noch vereinzelt in älteren Netzwerken vorzufinden (aber es gibt sie noch).

Wenn heute von Ethernet gesprochen wird, dann heißt dies Thin-Ethernet (100MBit/s), also Twisted Pair Kabel (STP oder UTP) der Kategorie 5. Hier herrscht das Zugriffsverfahren CSMD/CD (Kollisionsverfahren) vor. In kleineren und mittleren Netzwerken reicht diese Verkabelung auch für den Backbone-Bereich. In größeren Netzwerken sollte

hier aber mit Glasfaser und 1GBit Strecken gearbeitet werden.

Wie auch im nächsten Abschnitt „Geräte im Netzwerk“ beschrieben, wird in LANs mit diversen Netzwerk-Geräten hantiert, je nach Notwendigkeit für das gewünschte Design und die gewünschten Effekte. Ein in der Vergangenheit gewachsenes Netzwerk, welches nicht unter den Vorzeichen der Skalierbarkeit erstellt wurde, enthält sicher auch noch heute eine ganze Reihe der nachfolgend vorgestellten Geräte. Vorherrschend sind in modernen Netzwerken aber Switches und Router, mit denen man ein Netzwerk perfekt designen kann (siehe auch unser EBook Netzwerk-Technik Teil 3, Optimieren von Netzwerken).

Beispiel für ein modernes Netzwerk



Geräte im Netzwerk

Server

Ein in das Netz eingebundener Rechner, der mit der Ausführung spezieller Aufgaben betraut ist. Unterscheidung in DEDICATED (Rechner, der nur dafür abgestellt ist) und NON DEDICATED (Rechner, der auch weiterhin im Normalbetrieb arbeitet).

Server können als File-, Print-, Fax- oder Datenbank-Server arbeiten. Mehrere Aufgaben in einem Server sind möglich.

File-, Print-, Datenbank- etc. Server (Zentral-Rechner)

Rechner, der die Daten / Ressourcen des Netzwerks zentral speichert und verwaltet.

Er sorgt für die kontrollierte Bereitstellung von gemeinsam benutzten Daten.

Weiterhin wickelt er die Kommunikation zwischen den Benutzern im Netz ab.

Netzwerkdienste können auch auf mehrere Server verteilt sein.

Als Server muss ein Rechner eingesetzt werden, der von seiner Konfiguration auch die Aufgaben eines Servers erfüllen kann.

Netzwerk-Betriebssystem

Als Herz des Netzwerkes arbeitet der Server mit einem speziellen Netzwerkbetriebssystem (Novell, Unix, Windows)

Workstations (Client)

Rechner, der in das Netz eingebunden ist, einem Benutzer an seinem Arbeitsplatz zur Verfügung steht und vom Server Dienste beanspruchen kann.

Hardware-Verbindung

Alle Server und Workstations müssen unter einer bestimmten Topologie miteinander verbunden sein. In jedem Rechner muss eine Netzwerkkarte vorhanden sein, die durch die Übertragungsmedien und Verteiler miteinander verbunden sind.

Repeater (OSI 1, phys. Layer)

- Signalformer (Verstärker), um Signale, auf Grund der Ausdehnungsbeschränkung von Segmenten (Thin-Ethernet 185 m, Thick 500 m) zu überbrücken
- aktives Element
- protokoll-transparent
- erhöht nicht die Bandbreite eines Segments
- auch Sternverteiler (HUB's) und Ringverteiler gehören hierzu
- unterschiedliche Netzsegmente können damit zu einem Netz zusammengefügt werden

- mit Repeatern sind baumartig gestaltete Netzwerke von beachtlicher Ausdehnung realisierbar
- filtert keine Adressen, reicht also Pakete in alle Segmente weiter
- werden immer weniger eingesetzt und mehr und mehr von Bridges und Routern abgelöst

Transceiver

Wandlungs- (D/A-Wandlung) und Steuerungsaufgaben beim Senden und Empfangen.

Bridge (OSI 2, Data Link Layer)

Dient einerseits der phys. Entkopplung großer Netze, andererseits der Verbindung gleicher lokaler Netze oder Netzsegmente über Stationsadressen, die in einer Bridge-Tabelle gespeichert sind.

Diese Tabellen können bei „Learning Bridges“ selbstständig von der Brücke aufgebaut werden (Brücke konfiguriert sich selber, Plug and Play).

- Mittels Bridges lassen sich LANs praktisch unbegrenzt ausdehnen
- aktives Element
- protokoll-transparent, wenn Bauform „Transparente Brücke“ ist
- verstärkt auch Signale
- kann verschiedene Zugriffsverfahren koppeln
- kann verschiedene physikalische Medien (Koax-UTP) verbinden
- unterschiedliche Segmente werden zu einem Netz zusammengefasst
- je nach Bauform werden Adressen gefiltert und interpretiert oder nicht. Werden Adressen in Datenpaketen interpretiert, werden diese Pakete nur in das entsprechende Segment verschickt (Routingfunktion) und dadurch eine Lasttrennung (kein Datenverkehr in den anderen Segmenten durch dieses Paket) des Netzes erreicht.
- kann nur MAC Hardware-Adressen (Knotenadressen) verarbeiten, mit denen die Bridge-Tabellen aufgebaut werden (jedes Netz separate Tabelle), wodurch Bridges in der Lage sind, zwischen dem Verkehr innerhalb eines Netzes und eines anderen Netzes zu unterscheiden
- erhöhen die Gesamtbandbreite des gesamten LANs
- eingehende Pakete werden aufbereitet
- es gibt Source-Routing-Bridges (werden oft schon zu den Routern gezählt), die auf Grund der im Paket enthaltenen Informationen ein begrenztes Routing durchführen können
- Bridges und Backbones gehören zusammen
- kann Remote (Remote-Bridge) eingesetzt werden (also über Stand-Telefonleitung ein weit entferntes LAN verbinden) oder lokal (Local-Bridge)

Router (OSI 3, Network Layer)

- verbindet gleiche oder unterschiedliche Netzwerk-Topologien miteinander (mit gleichen Protokollen)
- verbindet auch unterschiedliche Zugriffsverfahren
- sucht den besten oder schnellsten Weg durchs Netz in andere Subnets, da sie Routing-Tabellen unterhalten und austauschen
- kann bei Ausfall oder starker Belastung einer Strecke selbstständig eine andere Route durch ein Maschennetz aussuchen
- ist von dem eingesetzten Protokoll auf Ebene 3 abhängig (also entweder Multiprotokoll-Router verwenden oder gezielt den Router für ein bestimmtes Protokoll (muss das Protokoll kennen))
- besteht aus Hard- und Software-Anteil
- übersetzt keine Protokolle
- verstärkt auch Signale
- interpretiert im Gegensatz zur Bridge die Pakete (jedes IP-Paket wird ausgepackt und die im Header enthaltene IP-Adresse interpretiert). Nachteil: Bei viel Netzwerkverkehr schnelle Überlastung des Routers
- arbeitet nicht mit MAC-Adressen (IP-Adresse genügt), übermittelt aber auch über MAC, wenn sie das Paket nicht interpretieren kann, wobei allerdings die Routing-Funktion verloren geht
- filtert Adressen und leitet Pakete nur in Segmente (Subnets) mit den entsprechenden Adressen, wobei nicht die Adressen der Endgeräte wie bei der Bridge, sondern nur die Adressen der beteiligten Netzwerke (Routing-Tabellen) angelegt werden
- die Filterfunktion erlaubt erhöhte Sicherheit, da sich Router so konfigurieren lassen, dass ein Zugriff auf ein Teil-LAN nur bestimmten IP-Adressen erlaubt werden kann (Firewall)

Gateway (OSI 7, Application Layer)

- kann völlig verschiedene Kommunikationssysteme verbinden
- ermöglicht die Entkopplung von LANs mit unterschiedlicher Adressierung
- lassen sich auch über Software realisieren (IPX-IP Gateway auf Novell-Servern)
- setzen Protokolle real in andere Protokolle um
- sie werden auch für den Übergang auf Großrechenanlagen benutzt

Segment

Zusammenhängendes Kabelstück innerhalb eines LANs. LANs können wiederum aus mehreren Segmenten bestehen, die über Repeater, Bridges oder Router verbunden sind.

HUB (OSI 1, phys. Layer)

- zentraler Verteiler, an den sternförmig PC's angeschlossen werden
- aktiv (Kabellänge bis 600 m), verstärkt auch Signale

- passiv (Kabellänge bis 30 m)
- wird in Baum-Topologien verwendet
- bedingt UTP-Kabel
- die Buchsen eines HUB's sind so belegt, dass immer ein Endgerät angeschlossen werden kann
- 2 HUB's miteinander verbinden (kaskadieren) = gekreuztes Kabel (crossover) verwenden (oder der Anschluss am HUB hat einen Schalter zum Kreuzen (Transmit → Receive, meistens Anschluss 1)

Switch (OSI2, Data Link Layer)

- Sollte heute anstatt HUB's (bei Ethernet-Switch) benutzt werden
- insbesondere bei größerem Datenaufkommen
- erhöht die Bandbreite in einzelnen Segmenten
- Verbindungen werden direkt geschaltet (nach MAC-Adressen), Interpretation der IP-Adresse entfällt
- trennt Netze physikalisch

Fazit zu Netzwerkgeräten (Routing und Switching)

Umso mehr Computer in einem Netzsegment vorhanden sind, desto geringer wird die Bandbreite, da sich damit das Datenaufkommen erhöht. Computer, die viel miteinander kommunizieren, sollten deswegen im selben Segment liegen, um den Netzwerkverkehr gering zu halten.

Über Bridges ist es unmöglich, Datenkommunikation zu Segmenten zu betreiben, die nicht direkt an die Bridge angeschlossen sind, sondern durch mehrere Netze getrennt sind. Dafür gibt es Router, die diese Aufgabe erfüllen können. Reine auf Router basierende Netzwerke können heutige Anforderungen an Datendurchsatzraten für neuere Anwendungen aber nicht mehr gänzlich allein erfüllen. Multi-Protokoll über ATM oder IP-Switching sind in einem modernen LAN deswegen mehr und mehr unausweichlich.

Über Router kann der Datenverkehr ge-

regelt werden. Router können darüber entscheiden, welcher Datenverkehr von/zu Domänen fließen darf. Unter TCP/IP müssen Daten aus einem Anwenderprogramm in IP-Datagramme und z. B. im Ethernet weiter in Ethernet-Frames zerlegt werden, die dann als Bitstrom in das Kabel gelangen. Wenn sich beide Teilnehmer einer Kommunikation in der gleichen Domäne befinden, wird über die MAC- und IP-Adresse der Datenverkehr vorgenommen. Befinden sich die Teilnehmer in unterschiedlichen Domänen, muss die Kommunikation über Router stattfinden, wobei nur die IP-Adresse für den anderen Teilnehmer verwendet wird. Über die MAC-Adresse wird nur der nächste Router angesprochen, wobei jeder Router die Frames zuerst zwischenspeichern muss, sie zu IP-Datagrammen zusammen setzen muss, um anhand der IP-Zieladresse im Header (sozusagen ein Briefkopf) festzustellen, über welchen seiner Ports er das Zielgerät erreichen kann. Dazu verfügt der Router über

Routing- und Adress-Tabellen, die über Routing-Protokolle aufgebaut wurden.

Sodann werden die IP-Datagramme wieder in MAC-Frames zerlegt, mit einer neuen MAC-Zieladresse versehen und über den entsprechenden Port gesendet. Dies passiert bei allen Routern auf dem Weg zum Zielgerät, was natürlich entsprechend viel Zeit benötigt, bis die Datagramme beim Zielgerät eintreffen. Weiter muss der Router über die Routing-Protokolle (RIP, OSPF, etc.) seine Tabellen aktualisieren, Protokolle konvertieren (z.B. von Ethernet zu Frame-Relay, wenn er auch als WAN-Router arbeitet). All dies benötigt zusätzlich viel Hard- und Software auf einem Router (also teuer).

Switching dagegen hat diese Nachteile nicht. Switches können anstatt HUB's (Port-Switching) oder Routern (Segment-Switching) eingesetzt werden. HUB's senden alle ankommenden Signale grundsätzlich auf allen Ports wieder aus.

D. h., dass wegen dem CSMA/CD-Zugriffsverfahren von Ethernet alle angeschlossenen Geräte in einer Kollisionsdomäne liegen. Switches leiten ankommende Signale nur auf dem Port wieder aus, auf dem das Gerät sich befindet, für das die Nachricht bestimmt ist. Kollisionen auf den anderen Ports entfallen. Switches legen jedes angeschlossene Gerät sozusagen in ein eigenes Segment. Damit wird die Bandbreite des Netzes erhöht.

ATM-Switches z. B. arbeiten mit Zellen (Frames) von festen Längen, wobei nur die Adressinformationen aus dem ATM-Header gelesen werden muss und anhand von Hardwareentscheidungen (MAC-Adresse) der zu verwendende Switch-Port zur Weiterleitung festgestellt werden muss (Cut-Through-Prinzip). Route-Server werden dabei so eingesetzt, dass die Funktion zur Bildung von Domänen im Netzwerk für alle Switches erhalten bleibt. Ein Route-Server bildet

dabei die Intelligenz des Switch-Konzeptes, während die Switches nur Daten weiterleiten, was sie sehr viel schneller in diesem Bereich machen als Router. Ein weiterer Vorteil ist, dass Domänen nicht mehr nach ihren physikalischen Bedingungen (Sub-Netze als Segment) gebildet werden müssen, sondern virtualisiert werden können (sog. virtuelle LANs (VLANs)). ATM bedingt allerdings ATM-fähige Geräte im Netz. Multi-Protocol Over ATM (MPOA) oder Classical IP können aber eine LAN-Emulation herstellen, mittels derer auch herkömmliche LANs über ATM arbeiten können.

ATM-Switches leiten Datagramme also nicht nach IP-Adressen weiter, sondern nach einer völlig inkompatiblen Adressbildung zu IP. Neuere Technologien sollen aber IP-Adressen mit Switches verarbeiten können, um die vielen Vorteile des IP-Protokolls im LAN beibehalten zu können. Dabei wird einem IP-Datenstrom eine Marke zugewiesen, die auf eine Zeile in der Adresstabelle des ATM-Switches verweist. Dadurch kann der IP-Datenstrom nun die Datenpfade der Switches verfolgen, anstatt auf den Routing-Wegen zu bleiben, was das Weiterreichen der IP-Datagramme wesentlich beschleunigt.

Strukturierte Verkabelung in der Netzwerk-Technologie

Jede strukturierte Verkabelung setzt sich aus 3 getrennten Verkabelungsbereichen zusammen:

1. Primär-Verkabelung (gebäude-übergreifende Verkabelung)

Hier hinein fallen alle Kabelwege mit den dazugehörigen Verbindungen, die sich zwischen Gebäuden oder unterschiedlichen Betriebsstätten befindet. Sie endet in der Regel im Keller eines Gebäudes.

Der Primär-Bereich ist das Bindeglied zwischen den einzelnen Sekundär-Bereichen.

Elemente

- Primär-Verkabelung (Campus Backbone Cabling)
- Standortverteiler
- Rangierverteiler im Standortverteiler

2. Sekundär-Verkabelung

Vom Keller hinauf in die einzelnen Eta-

gen erfolgt die Sekundär-Verkabelung. Der Gebäudeverteiler ist der Übergang zum Primärbereich.

Elemente

- Gebäudeverteiler
- Sekundär-Verkabelung
- Rangiereinrichtung im Gebäudeverteiler

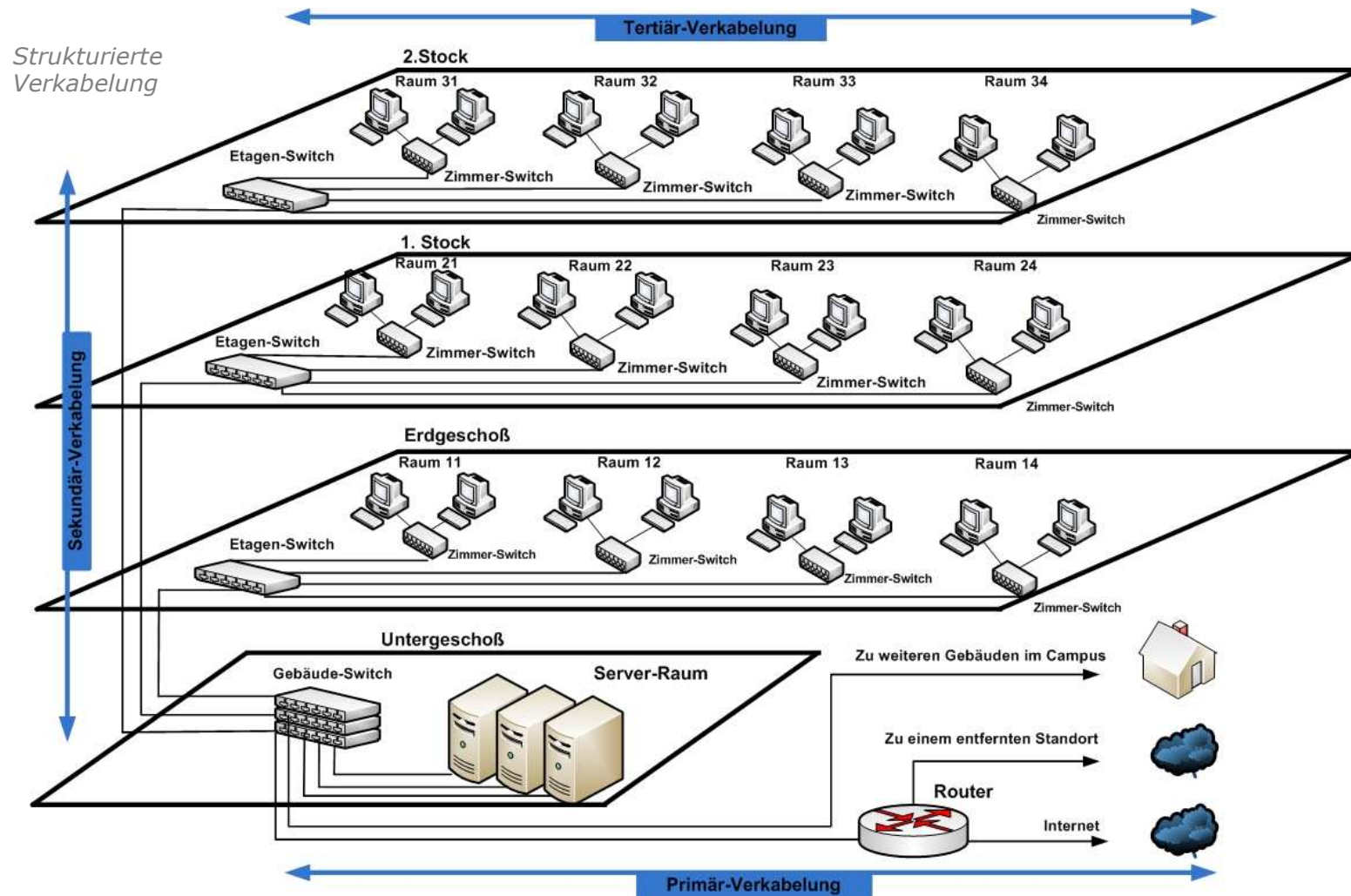
3. Tertiär-Verkabelung

Die Verkabelung auf den einzelnen Etagen wird als Tertiär-Verkabelung bezeichnet.

Der Etagenverteiler ist der Übergang zum Sekundärbereich.

Elemente

- | | |
|-----------------------|-------------------|
| • Etagenverteiler | • Anschluss-Kabel |
| • Tertiär-Verkabelung | • Rangierfeld |
| • Kabelverzweiger | • Rangierkabel |
| • Anschlussdose | |



Backbone-Bereich

Als Besonderheit innerhalb einer strukturierten Verkabelung zählt der Backbone-Bereich.

Mit Backbone-Bereich wird grundsätzlich der Teil der Kabel-Infrastruktur bezeichnet, der als verbindendes Glied der einzelnen Gebäude-Segmente liegt.

Bei großen Netzwerken mit einer gewissen Anzahl von Segmenten innerhalb verschiedener Gebäude werden für die Verbindung der einzelnen Teilbereiche schnelle Verbindungen benötigt (1000 MBit/s).

Der Backbone-Bereich kann einen der folgenden Bereiche der Verkabelung betreffen:

- Primär- und kompletter Sekundär-Bereich
- Primärbereich und einige Sekundär-Bereiche
- ausschließlich Primär-Bereich

Strukturvorgaben

Ein strukturiertes Verkabelungssystem muss folgende Vorgaben enthalten:

1. Standortverteiler SV (Primärbereich)
2. Gebäudeverteiler GV (Sekundärbereich)
3. Etagenverteiler EV (Tertiärbereich)
4. Kabelverzweiger KV
5. Informationstechnische Anschlussdose TA

Primär-Verkabelung

Die Primär-Verkabelung erstreckt sich grundsätzlich vom Standortverteiler bis zum Gebäudeverteiler. Mit ihr erfolgt die Anbindung verschiedener Gebäude. Hier wird im Allgemeinen ein Glasfaserkabel verwendet.

Es sind aber auch Ausnahmen zugelassen, bei denen ein symmetrisches Kupferkabel zum Einsatz kommt.

Sekundär-Verkabelung

Die Sekundär-Verkabelung bezieht sich auf den Bereich der Gebäude- und Etagenverteiler. Grundsätzlich dürfen hier keine Kabelverzweiger verwendet werden. Auch hier kommt ein Glasfaserkabel zum Einsatz, was seine Begründung im hohen Datendurchsatz hat.

Tertiär-Verkabelung

Der Bereich der Tertiär-Verkabelung erstreckt sich auf den Bereich der Etagenverteiler bis hin zu den jeweiligen Anschlussdosen. In der Regel erfolgt hier der Einsatz von symmetrischen Kupferkabeln mit einem Wellenwiderstand von 100 Ohm (UTP1-5, Kategorie 1-5). Alternativ sind auch 150-Ohm-Kabel (STP) zulässig.

Etagenverteiler

Die Empfehlung geht hier zu einem Etagenverteiler pro 1000 qm Bürofläche. Ein solcher Verteiler dient für die Aufnahme von aktiven Elementen (Router, HUB's, etc) und passiven Elementen (Patchfelder). Als Sonderform können in einem Etagenverteiler auch mehrere kleinere Etagen zusammengefasst werden.

Anschlussdose

Pro 10 qm Bürofläche sollten grundsätzlich 2 Anschlussdosen vorgesehen werden. Darüber hinaus müssen pro Arbeitsplatz mindestens 2 Anschlüsse eingeplant werden.

Übertragungs-Protokolle (im LAN-Bereich)

Der Sinn eines Netzwerkes ist der Austausch von Informationen und Daten zwischen verbundenen Computern. Dabei ist wichtig, dass die Computer die gleichen Kommunikationsregeln verwenden, dass sie sozusagen die gleiche Sprache sprechen, um einander zu verstehen.

Diese Kommunikationsregeln werden über die Protokolle definiert.

NetBIOS

- erstes Übertragungsprotokoll im LAN, aber auch BIOS-Erweiterung für das Netzwerk
- wird heute nur noch für spezielle Anwendungen eingesetzt (Windows benutzt NetBIOS over TCP/IP = NBT)
- einige Betriebssysteme, wie DOS, NETWARE beinhalten Emulationsprogramme (Netbios.exe) mit denen

man Software, die auf NetBIOS aufsetzt, aktivieren kann

NetBEUI

- Weiterentwicklung von NetBIOS
- ist ein aus NetBIOS entwickeltes Transport-Protokoll (Standard für alle WINDOWS Betriebssysteme (nicht routingfähiges Protokoll))

Apple Talk

- Protokoll für McIntosh-Rechner
- FRAME unter Netware _SNAP

IPX/SPX

- von Novell entwickelt
- wird grundsätzlich auf alle NETWARE-Anwendungen implementiert
- IPX adressiert und verschickt Datenpakete
- SPX übernimmt die Kontrolle der Übertragung

Zusatzprotokolle zu IPX/SPX (RIP und SAP)

RIP (auch in TCP / IP Netzen verwendet)
Verschickt innerhalb eines LANs Angaben über verfügbare Router, Server und Workstations.

Router gleichen über RIP auch ihre Routing-Tabellen (dem Router bekannte Subnets und Hops (Anzahl der Sprünge über andere Router bis zum Remote-Netzwerk)) ab. Dabei werden nur 16 Hops gespeichert, d.h. Router kennen nur Subnets, die nicht weiter als 16 Hops entfernt sind (im LAN meistens ausreichend, im Internet problematisch, da jeder Router seine Tabellen per Rundsendung verschickt und jeder Router, der diese empfängt, dies genauso tut (schnelle Überlastung der Router)).

SAP

Dient dazu, dass ein Server den anderen Komponenten im Netz seine Dienste (Services) bekannt machen und zur Verfügung stellen kann

TCP/IP

- Standard-Protokoll in LANs (wird am meisten eingesetzt)
- verbindungsorientiertes Protokoll
- TCP übernimmt die Übertragung der Daten zwischen zwei Endgeräten
- vor der Übertragung werden Daten in Datenpaketen zusammengefasst
- IP übernimmt die Adressierung des Versenden und die Überwachung des Transports der einzelnen Datenpakete

Zusatz-Protokolle zu TCP/IP

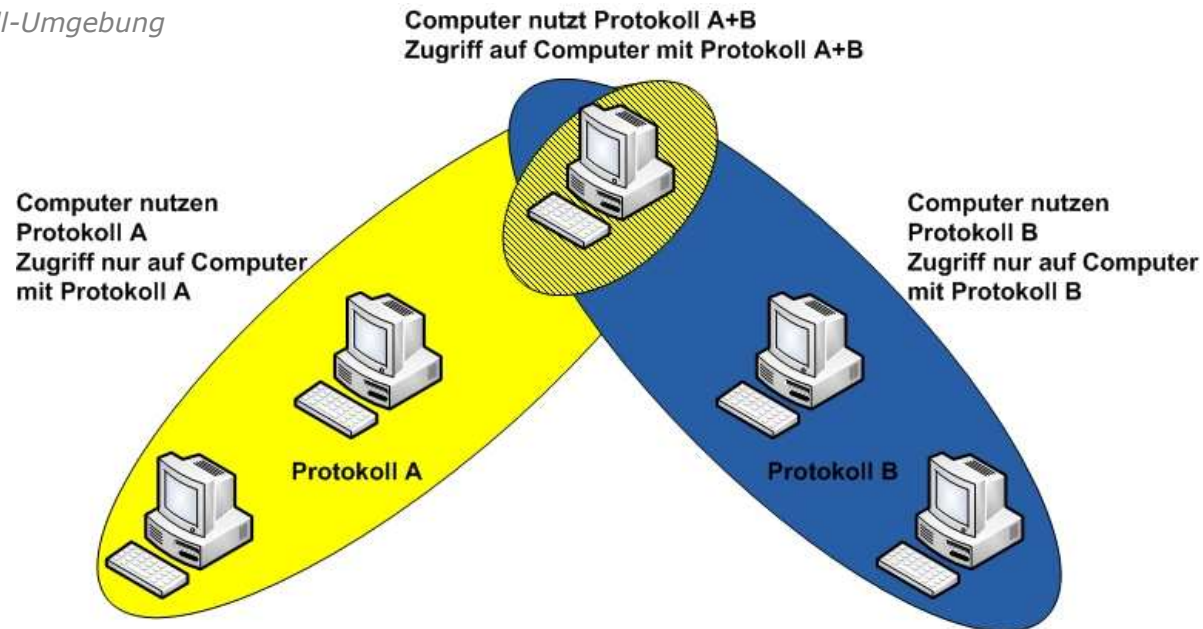
siehe weiter unten bei TCP / IP

Multiprotokoll-Umgebung

Multiprotokoll-Umgebung bedeutet, dass ein Computer auch mehrere Protokolle gleichzeitig nutzen kann. Dies ist dann sinnvoll, wenn es z.B. Novell-Server im

Netzwerk gibt, die mit IPX, und Windows-Server, die mit TCP/IP arbeiten. Der Client bekommt dann TCP/IP und IPX gleichzeitig installiert, und kann so auf beide Server zugreifen.

Multiprotokoll-Umgebung



TCP/IP

TCP/IP hat sich zum absoluten Standard in LANs und im Internet etabliert. Deswegen soll an dieser Stelle auch ganz explizit auf dieses Protokoll eingegangen werden.

- Standard-Protokoll für das Internet
- verbindungsloses Protokoll (Paket wird abgeschickt, ohne Rückmeldung → nur bei udp)
- eindeutige Adresse im Netz (IP-Adresse)
- diverse Hilfsprotokolle (DNS, DHCP, SMTP)

Eindeutige IP-Netzwerk-Adressen sind weltweit Mangelware (können aber angefordert werden) und werden nur benötigt, wenn das eigene Netzwerk direkt mit dem Internet verbunden ist. In ei-

nem privaten / geschäftlichen LAN können IP-Adressen aber wahllos vergeben werden, wenn mit einer Firewall oder einem Proxy-Server zum Internet gearbeitet wird, welcher die eindeutige IP-Adresse zum Internet erhält und das LAN vom Internet abschirmt. Das eigene LAN sollte in seinem IP-Aufbau aber trotzdem den Konventionen entsprechen.

Form und Art von IP-Adressen

IP erfordert, dass jedem Gerät im Netz eine Adresse zugeordnet wird, die IP-Adresse. Sie ist dargestellt durch eine Sequenz von vier Oktetten. Diese Oktetten definieren eine eindeutige Adresse, wobei ein Teil dieser Adresse ein Netzwerk darstellt (und optional ein Teilnetz), ein anderer Teil einen bestimmten Knoten (Rechner) im Netz.

Beispiel (N = Network, H = Host)

NNNNNNNN.HHHHHHHH.HHHHHHHH.HHHHHHHH =
Klasse-A Netz, Subnet-Mask 255.0.0.0

NNNNNNNN.NNNNNNNN.HHHHHHHH.HHHHHHHH =
Klasse-B Netz, Subnet-Mask 255.255.0.0

NNNNNNNN.NNNNNNNN.NNNNNNNN.HHHHHHHH =
Klasse-C Netz, Subnet-Mask 255.255.255.0

Jede Position stellt ein einzelnes Bit aus einem 32-Bit-Adress-Raum dar.

Für die IP-Adresse 160.16.45.3 =

10100000.00010000.00101101.00000011

Es gibt Adressen, die eine bestimmte Bedeutung haben und deswegen nicht benutzt werden dürfen:

Eine Adresse, die mit einer 0 beginnt, bezieht sich auf einen lokalen Knoten:

0.0.0.23 = WS mit Nummer 23 (außerdem im Routing als Defaultroute festgelegt)

127 = Loopback-Adresse (wichtig für Netzdiagnose):

127.0.0.0 ist der lokale Loopback innerhalb der WS

255 = reserviert für Meldungen (Broadcast)

Adressklassen				
Klasse	verfügbare Knoten	Ausgangs-Bits	Start-adresse	Verwendung
A	2E24 = 16777216	1xxx	1-126	sehr große Netze
B	2E16 = 65536	10xx	128-191	256-65536 Knoten
C	2E8 = 256	110x	192-223	bis 256 Knoten
D		1110	224-239	Multicast Nachrichten
E		1111	240-255	zukünftige Entwicklung

Zum besseren Verständnis

Die Subnet-Mask bestimmt, welcher Teil der IP-Adresse Netzwerkanteil und welcher Hostanteil ist. Dabei sind alle Anteile

der IP-Adresse, die Einsen in der Subnet-Mask enthält (Dezimal 255), Netzwerkadresse. Beispiele:

Klasse C	IP-Adresse:	192.168.100.7	andere Schreibweise ist
Klasse C	Subnet-Mask:	255.255.255.0	192.168.100.7 /24
Klasse C	Netz-Adresse:	192.168.100.0	(Subnet-Mask = 3x 8Bit=24)
Klasse B	IP-Adresse:	128.107.100.3	andere Schreibweise ist
Klasse B	Subnet-Mask:	255.255.0.0	128.107.100.3 /16
Klasse B	Netzadresse:	128.107.0.0	(Subnet-Mask = 2x 8Bit=16)
Klasse A	IP-Adresse:	10.194.234.3	(andere Schreibweise ist)
Klasse A	Subnet-Mask:	255.0.0.0	10.194.234.3 /8
Klasse A	Netzadresse:	10.0.0.0	Subnet-Mask = 1x 8Bit=8

Weiter wird vom Computer über die Subnet-Mask ermittelt, ob sich ein Host im gleichen Subnet befindet oder ob dieser in einem anderen Teilnetz untergebracht ist. Am besten wird dies durch die Aufschlüsselung der IP-Adressen in deren Binärwerte klar und durch das Verständnis, welche Rechenoperationen (AND-Verknüpfung) der Computer mit diesen Binärwerten anstellt. Da dieses Buch nicht Gegenstand von binären Rechen-

operationen ist, soll hier nur kurz auf die AND-Verknüpfung eingegangen werden.

Definition: 1=High (an), 0=Low (aus)
AND-Verknüpfung: $1+1=1$, $1+0=0$, $0+1=0$, $0+0=0$

Die IP-Adresse wird in deren Binärwert mit dem Binärwert der Subnet-Mask AND-Verknüpft. Dabei wird die Rechenoperation auf jede Stelle der Binärwerte angewendet.

Zwei Hosts in selben Subnet

1. Host	IP-Adresse	dazugehöriger Binärwert der Oktette				
	198.53.147.45	11000110	00110101	10010011	00101101	Rechenweg
	Subnet-Mask					
	255.255.255.0	11111111	11111111	11111111	00000000	↓
	AND-Verknüpfung Ergebnis	11000110	00110101	10010011	00000000	= 198.53.147.0
2. Host	198.53.147.98	11000110	00110101	10010011	01100010	
	255.255.255.0	11111111	11111111	11111111	00000000	
	AND-Verknüpfung Ergebnis	11000110	00110101	10010011	00000000	= 198.53.147.0

Die Netzwerk-Ids stimmen in beiden Fällen überein, sodass sicher gestellt ist, dass sich beide Hosts im selben Subnet befinden.

Zwei Hosts in unterschiedlichen Subnets

1. Host	IP-Adresse	dazugehöriger Binärwert der Oktette			
	198.53.147.45	11000110	00110101	10010011	00101101
	Subnet-Mask				
	255.255.255.0	11111111	11111111	11111111	00000000
	AND-Verknüpfung Ergebnis	11000110	00110101	10010011	00000000 = 198.53.147.0
2. Host	IP-Adresse	dazugehöriger Binärwert der Oktette			
	131.107.2.200	10000011	01101101	00000010	11001000
	255.255.255.0	11111111	11111111	11111111	00000000
	AND-Verknüpfung Ergebnis	10000011	01101101	00000010	00000000 = 131.107.2.0

Die Netzwerk-Ids stimmen in beiden Fällen nicht überein, sodass sicher gestellt ist, dass sich beide Hosts nicht im selben Subnet befinden.

Teil-Netze

Die Einrichtung einer Teil-Netz-Maske legt fest, wo die Netz-Adresse endet und die Host-Adresse anfängt.

Die Teilnetz-Maske enthält Einsen im Netzwerkfeld und Nullen im Host-Feld.

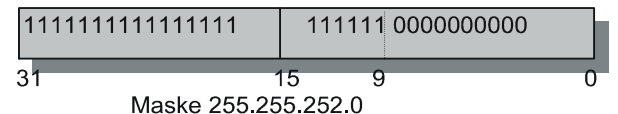
Wird das Klasse-C Netz in vier Klasse-C Netze zerlegt, sieht das so aus:
 NNNNNNNN.NNNNNNNN.NNNNNNNN.NN
 HHHHHH



Anzahl der Teil-Netze = 64

Anzahl der Hosts/Netze = 1024

Teilnetz-Maskierung (Subnet-Mask)



Die Teilnetz-Maske

11111111.11111111.11111111.11000000, in Dezimalschreibweise 255.255.255.192

Wenn aus dem Hostfeld drei Bits entfernt werden, können 8 Netzwerke gebildet werden:
11111111.11111111.11111111.11100000, die Teilnetz-Maske ist 255.255.255.224

Jedes der 8 Netzwerke hätte damit 29 Knoten, weil 5 Adressbits zur Verfügung stehen (es sind eigentlich 32, aber 1, 0 und 127 sind verboten). Dieses Konzept gilt auch für Klasse B-Netze.

Der Adressbereich eines Klasse-B-Netzes:
NNNNNNNN.NNNNNNNN.HHHHHHHH.HHHHHHHH

Wenn 2 Bits aus dem Hostfeld entfernt werden und dem Netzfeld hinzugefügt werden, wird folgende Teilnetz-Maske verwendet:
11111111.11111111.11000000.00000000, die Maske lautet 255.255.192.0

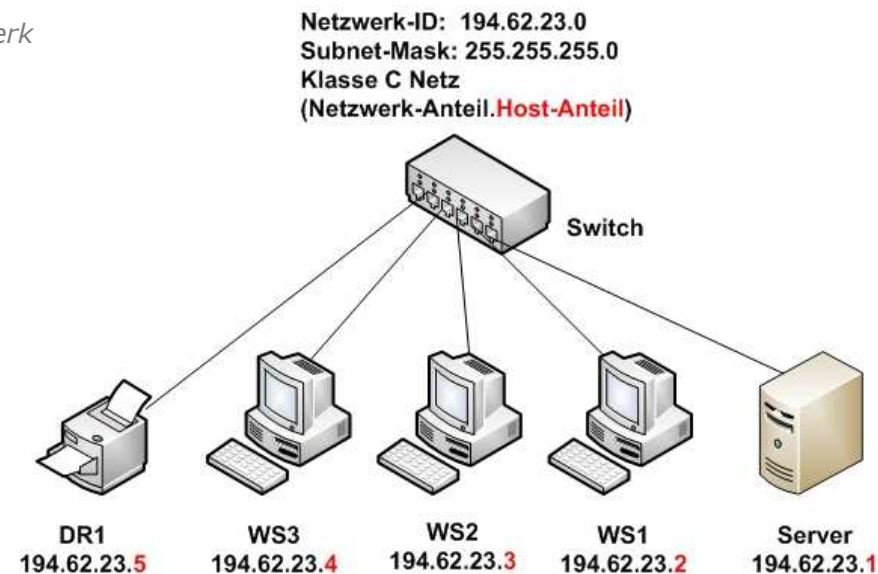
Die IP-Adresse dient nur der eindeutigen Identifizierung eines Gerätes im Netz. IP-Pakete werden aber letztlich immer an die MAC-Adresse der Netzkarte geschickt. Dazu wird ein ARP-Cache (siehe Hilfsprotokolle TCP/IP) verwendet, in

dem schon verwendete Verbindungen von IP-Adressen zu MAC-Adressen aufgelöst werden. Ist die MAC-Adresse der angesprochenen IP-Adresse nicht bekannt, werden Rundsendungen von ARP verschickt, um diese herauszufinden.

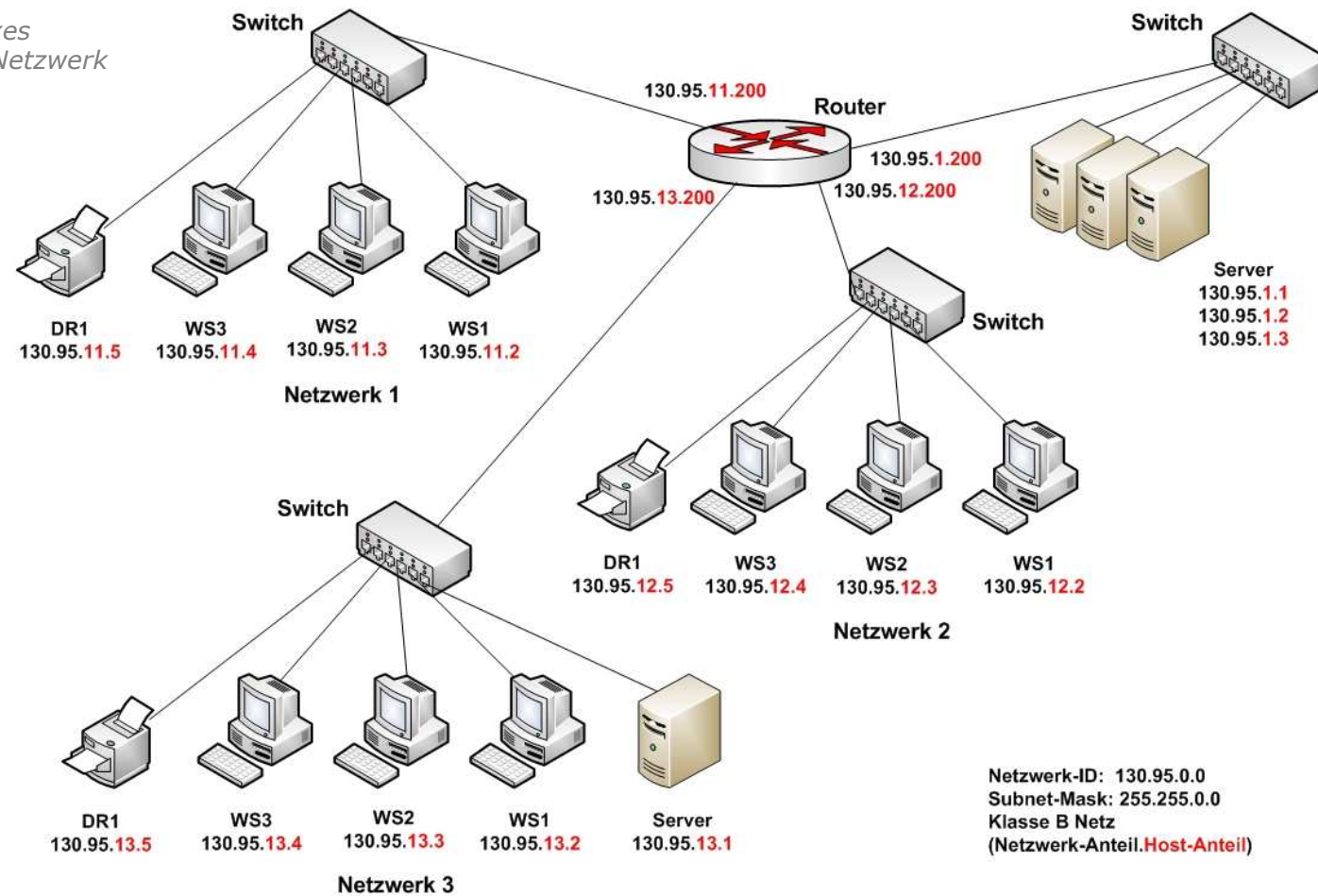
Zum besseren Verständnis:
Jede Netzwerkkarte (NIC) auf der Welt verfügt schon ab Werk über eine weltweit einmalige MAC-Adresse (physikalische Adresse), die nur diese eine Netz-

werkkarte hat, und die nicht veränderbar ist. Einer Netzwerkkarte wird im Netzwerk eine (oder auch mehrere) IP-Adresse(n) zugeordnet.

Einfaches TCP/IP-Netzwerk



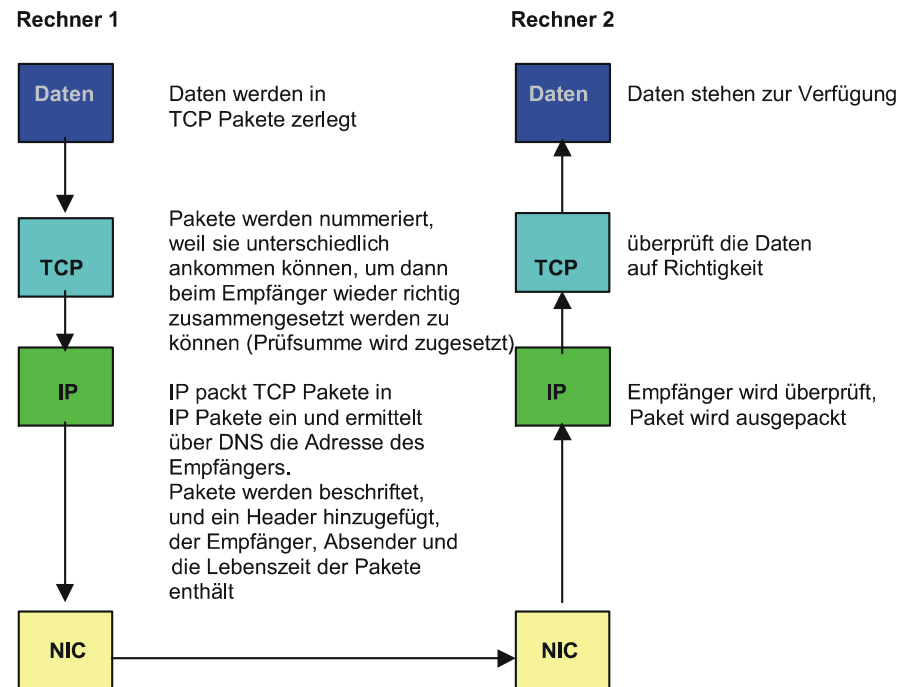
*Komplexes
TCP/IP-Netzwerk*



Sollen Pakete verschickt werden, baut TCP zuerst eine Sitzung vom eigenen Computer zum Remote-Host auf. Der Remote-Host bestätigt die Anfrage und signalisiert, dass er zur Entgegennahme

von Paketen bereit ist (Handshake). IP verpackt nun die TCP-Pakete und schickt sie unter Verwendung des ARP-Caches an die Remote-Adresse.

Übertragung der Daten unter TCP/IP



Hilfsprotokolle zu TCP/IP

DNS (Domain Name System)

Das DNS wandelt IP-Adressen in Domänen-Namen z.B. 192.125.12.5 → PCTWS01.PCT-SOLUTIONS.DE

Für eine Verbindung zu einem anderen Rechner muss nicht mehr die IP-Adresse eingegeben werden, sondern es reicht jetzt auch der Computer-Name (siehe auch unser EBook zu DNS-WINS-DHCP).

SMTP (Simple-Mail-Transfer-Protokoll)

Wird vornehmlich für die Übermittlung elektronischer Post an einzelne Benutzer oder alle benutzt.

POP (Post Office Protokoll)

Wird für eingehende Post aus dem Internet verwendet (Post empfangen).

FTP (File-Transfer-Protokoll)

Wird für die Übertragung von Daten zwischen verschiedenen Rechner-Systemen benutzt, die unterschiedliche Dateiformate benutzen.

Zusätzlich zu den Befehlen für die Dateiübertragung gibt es Befehle zum Anzeigen, Wechseln, Löschen oder Anlegen von Verzeichnissen.

TELNET (Terminal-Emulation)

Stellt eine Verbindung zwischen einem Telnet-Server und Telnet-Client her, wobei auf dem Client ein Terminal des Servers emuliert wird.

NFS (Network File-System)

Verzeichnis eines Rechners kann über das Netz direkt an einen anderen Rechner angeschlossen werden.

RPC (Remote-Procedur-Call)

Erlaubt das Kommunizieren verschiedener Applikationen untereinander.

ARP (Address-Resolution-Protokoll)

Führt die logischen IP-Adressen der Rechner mit ihren physikalischen Adressen (MAC-Adressen) der Netzwerkkarten zusammen (unter Windows ein Befehl, um den ARP-Cache abzufragen).

ICMP (Internet-Controll-Massage-Protokoll)

Protokoll, mit dem Nachrichten über den IP-Zustand verschickt werden.

SNMP (Simple-Network-Management-Protokoll)

Zur Steuerung und Überwachung von Netzwerken.

UDP

Verbindungsloses Übertragungsprotokoll, wenn zuverlässige Datenübertragung nicht nötig ist.

TCP/IP-Routing

Sicher werden in heutigen Netzwerken Router verwendet, die extra für diese Aufgabe hergestellt wurden. Geräte von CISCO, D-LINK oder 3COM, um nur einige zu nennen, werden in den meisten Fällen zur Anwendung kommen. Diese bauen sich ihre Routing-Tabellen dynamisch über Routing-Protokolle selbstständig auf (siehe weiter unten). Aber hat man ein solches Gerät nicht zu Hand, kann auch ein Windows-Server oder Unix-Rechner einen recht leistungsfähigen Router abgeben. Zudem ist zur Erklärung der Routingvorgänge das Verständnis über statisches Routing sinnvoll.

Mit einem Windows-Server können zwei Routing-Typen installiert werden:

1. als statischer Router
2. als dynamischer Router

Statisches Routing

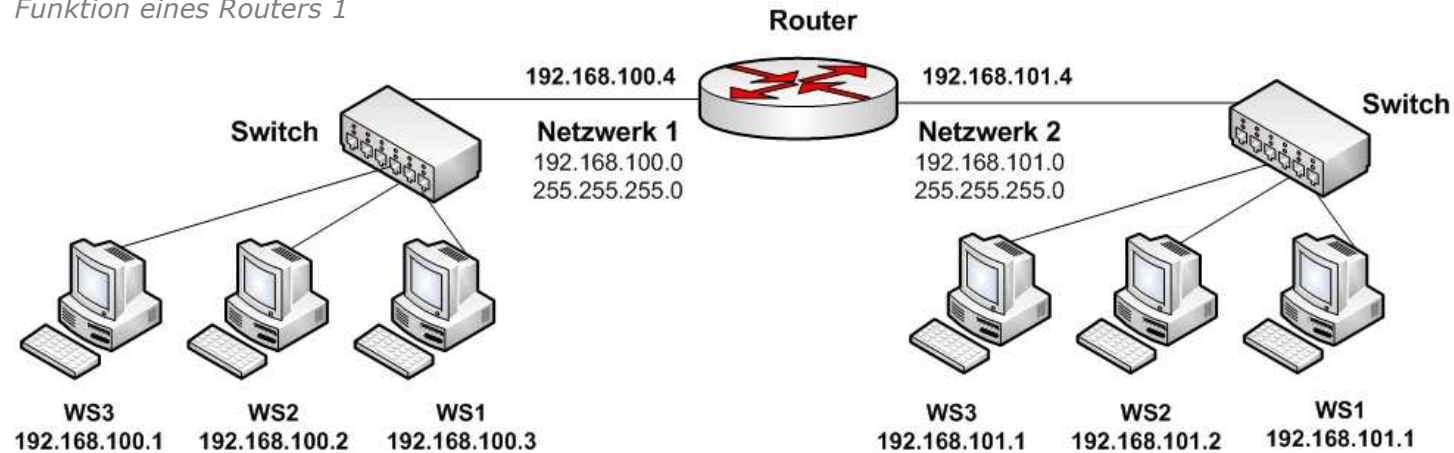
Ein statischer Router weiß nur von entfernten Netzwerken, die ihm in seine Routing-Tabellen eingegeben wurden, oder mit denen er physisch verbunden ist.

Bei sehr großen Netzwerken ist eine manuelle Pflege der Tabellen eine fast unmögliche Aufgabe.

Um einen Windows-Server als statischen Router zu verwenden, müssen dem Rechner als erstes so viele Netzwerkkarten eingebaut werden, wie er Verbindungen zu Subnets haben soll, in die er hineinrouten soll. Jeder Netzwerkkarte muss eine entsprechende IP-Adresse zugewiesen werden.

Sodann ist unter NETZWERKUMGEBUNG | rechte Maustaste | PROTOKOLLE | TCP/IP selektieren | EIGENSCHAFTEN | Routing | IP-Forwarding zu aktivieren.

Funktion eines Routers 1



In obiger Abbildung weiß der Router selbstständig, dass er mit den Netzen 192.168.100.0 und 192.168.101.0 verbunden ist.

In der DOS-Box kann mit dem Befehl `route print`, die aktuelle Routing-Tabelle abgefragt werden.

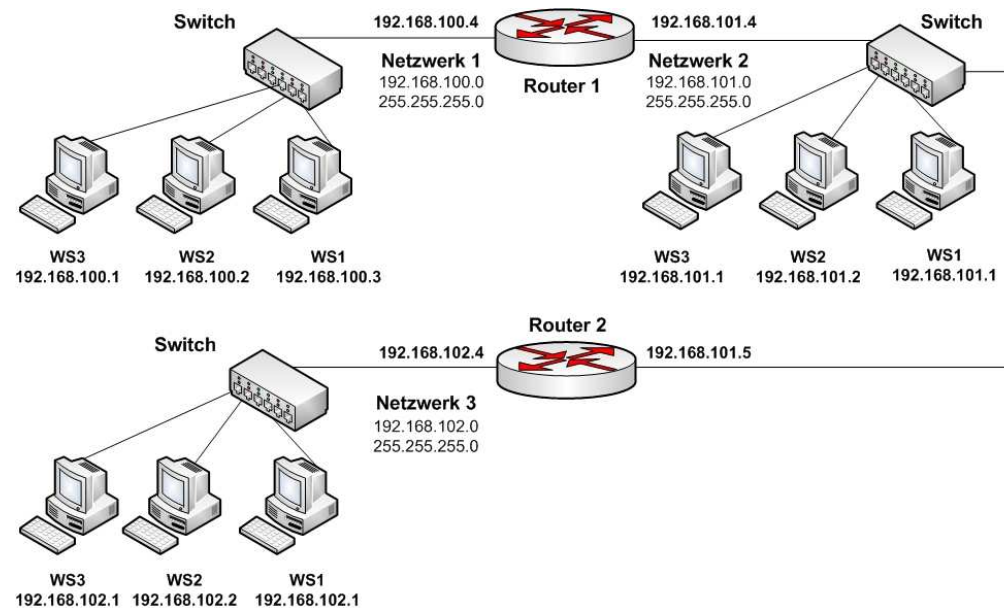
In obigem Fall würde diese so aussehen:

Netzwerk-ID	Subnet-Mask	Gateway
192.168.100.0	255.255.255.0	192.168.100.4
192.168.101.0	255.255.255.0	192.168.101.4

Alle PC's aus dem Netzwerk 192.168.100.0 nutzen das Gateway 192.168.100.4. Soll ein Paket von 192.168.100.1 nach 192.168.101.3 geschickt werden, bekommt der Router das Paket, der im Header des Pakets die Ziel-Adresse analysiert und eine Route in seiner Tabelle findet, sodass er das Paket nach 192.168.101.0 schickt, von wo es an den Adressaten weiter geschickt wird.

Im nächsten Bild ist ein weiteres Netzwerk hinzugefügt. Der erste Router weiß von den Netzwerken 192.169.100.0 und 192.168.101.0, und der zweite Router kennt die Netzwerke 192.168.101.0 und 192.168.102.0. Keiner der Router kennt alle Netzwerke, was bedeutet, dass der PC 192.168.100.2 nicht mit dem PC 192.168.102.3 kommunizieren kann.

Funktion eines Routers 2



Dieses Problem lässt sich durch hinzufügen von statischen Routen in der Routing-Tabellen beider Router lösen. Dazu muß jedem Router mitgeteilt werden, wie er zum anderen Router kommt.

Auf Router 1 ist in der DOS-Box folgender Befehl einzugeben:

```
route -P add 192.168.102.0 mask
255.255.255.0 192.168.101.5
```

Auf Router 2:

```
route -P add 192.169.100.0 mask
255.255.255.0 192.168.101.4
```

Die Routing-Tabelle von Router 1 sieht damit dann so aus:

Netzwerk-ID	Subnet-Mask	Gateway
192.168.100.0	255.255.255.0	192.168.100.4
192.168.101.0	255.255.255.0	192.168.101.4
192.168.102.0	255.255.255.0	192.168.101.5

Es muß dem Router also mitgeteilt werden, hinter welchem Gateway er welches Netz finden kann.

Dabei werden alle Pakete, die nicht für das eigene Subnet adressiert sind an dieses Gateway geschickt.

Die Routing-Tabelle von Router 2 sieht damit dann so aus:

Netzwerk-ID	Subnet-Mask	Gateway
192.168.102.0	255.255.255.0	192.168.102.4
192.168.101.0	255.255.255.0	192.168.101.5
192.168.100.0	255.255.255.0	192.168.101.4

Wie sich aus obigem Vorgang erkennen lässt, ist eine manuelle Pflege von Routing-Tabellen bei noch mehr Netzwerken und Routern sehr, sehr aufwendig.

Dynamisches Routing

Um diese manuelle Pflege zu umgehen, wurde das dynamische Routing entwickelt. Beim dynamischen Routing werden Routing-Protokolle verwendet, um Router in die Lage zu versetzen, Routing-Tabellen, die sie sich selber aufgebaut haben (weil phys. mit den Netzen verbunden sind) gegenseitig auszutauschen.

Routing-Protokolle sind OSPF und RIP.

RIP transportiert nicht nur Informationen von Router zu Router, sondern berechnet auch die Anzahl der Sprünge (Hops) über andere Router zu einem entfernten Netzwerk (werden beim Befehl "route print" unter Anzahl angegeben). RIP funktioniert folgendermaßen: In einem bestimmten Zeitraum versenden der Router ihre Tabellen per Rundspruch im Netz. Dabei ist das max. Maß das ein Router behalten kann 16 Hops. Die anderen Router nehmen die Rundspüche auf und tragen sie in die eigene Tabelle ein. Hinzugefügt werden die Netzwerke und

die IP-Adressen der Router, von denen die Informationen stammen. Die Router, die Informationen empfangen haben, schicken nun ihrerseits Rundsprüche ins Netz, usw. Auf diese Weise erfahren alle Router im LAN bzw. im Internet von vorhandenen Netzwerken und Routern die 16 Hops weit entfernt sind.

Probleme: Da jeder Router weiß, was sein Nachbar weiß, usw. bis 16 Hops erreicht sind, kann die Aufnahmekapazität eines Routers schnell überlastet werden. Deswegen werden Router mit immer mehr RAM und teilweise sogar mit Festplatten ausgestattet, um die Informationen noch speichern zu können. Auch kann durch die Rundsendungen von RIP der Netzwerkverkehr erheblich anwachsen.

RIP kann auch auf Systemen installiert werden, die nicht als Router fungieren. So können Routing-Informationen von anderen Routern eingesehen werden.

WAN-Technologien

Unternehmen sind immer häufiger nicht nur an einem Standort ansässig. Damit der Geschäftsablauf, der die EDV eines Unternehmens betrifft, trotzdem reibungslos funktioniert, müssen Verbindungen der einzelnen Standorte eines Unternehmens über öffentliche Telefonkabel hergestellt werden. Die Verbindung von Netzwerken über öffentliche Telefonkabel sind WAN-Verbindungen. Diese können natürlich auch über Richtfunk oder Satellit eingerichtet werden, was in vielen Firmen auch zum Einsatz kommt. Telefonverbindungen sind jedoch der weitaus gebräuchlichste Teil von WAN-Verbindungen.

WAN-Verbindungen können über das Anwählen einer solchen Verbindung bei Bedarf (Kosten fallen nur an, wenn die Verbindung aktiv ist), oder über sogenannte „Standleitungen“ hergestellt werden. Standleitungen werden von Unter-

nehmen bei einer Telefongesellschaft für den dauernden Einsatz gemietet.

Für WAN-Verbindungen gibt es eine Reihe von verschiedenen Technologien, die sich in ihrer Übertragungsgeschwindigkeit, und damit natürlich auch in den Kosten unterscheiden.

Standleitungen

T1

T1 ist eine digitale Leitungsform, die eine Punkt-zu-Punkt-Verbindung darstellt. Über T1 können 24 Kanäle über 2 Adernpaare übertragen werden, wobei ein Adernpaar für das Senden und das andere Adernpaar für das Empfangen verwendet wird. Die Übertragungsgeschwindigkeit von T1 beträgt 1,544 Mbit/s.

T3

T3 bietet die gleiche Technologie wie T1,

kann aber mit Übertragungsgeschwindigkeiten von 45 Mbit/s arbeiten.

DS-0

Da meistens die 24 Kanäle von T1/T3 nicht benötigt werden, können diese Kanäle auch aufgeteilt werden. Wenn einer dieser Kanäle dazu verwendet wird, 64 kBit/s zu übertragen, spricht man von einer DS-0-Verbindung.

DS-1, DS-1C, DS-2, DS-3

Dies sind weitere Aufteilungen von T1- oder T3-Kanälen.

DDS

DDS ist ebenfalls eine Punkt-zu-Punkt-Verbindung, die mit 2,4 , 4,8 oder 5,6 kBit/s arbeiten kann.

WAN-Protokolle

Da es u. U. für viele Firmen zu teuer sein kann, zu jedem Standort eine Standleitung einzurichten, werden oftmals sog.

Paketvermittlungsdienste eingesetzt, über die Datenpakete zwischen Standorten ausgetauscht werden können. Diese Dienste können über Mietleitungen bei einem Service-Provider bezogen werden. Die Kosten hierfür sind wesentlich geringer als über Standleitungen.

Paketvermittlungsdienste arbeiten oft mit virtuellen Verbindungen. Diese stellen einen ganz bestimmten Weg durch das Netz dar (Pakete suchen sich den Weg nicht selber). Dieser virtuelle Weg wird ganz gezielt für *eine* Übermittlung von Daten hergestellt, der bei der nächsten Übermittlung wieder ein ganz anderer sein kann.

X.25

X.25 ist in WAN-Umgebungen sehr verbreitet und kann dauerhafte oder geschaltete virtuelle Verbindungen benutzen. Diese untersteht einer Ende-zu-Ende-Flusskontrolle für jede virtuelle Verbindung, da X.25 bei seiner Entwicklung unzuverlässige Telefonleitungen

vorhand. Die Übertragungsgeschwindigkeiten von X.25 liegen bei 64 kBit/s. X.25 eignet sich nicht für die Bereitstellung von LAN-Anwendungen in einer WAN-Umgebung und hat viele Einschränkungen.

Frame Relay

Frame Relay bezieht sich auf Glasfaser-Netze, unterstützt B-ISDN und arbeitet mit dauerhaften virtuellen Verbindungen. Die Übertragungsgeschwindigkeiten von Frame Relay liegen zwischen 56 kBit/s und 1,544 Mbit/s (T1). Frame Relay wird an Kunden mit einer gewissen Bandbreite (Übertragungsgeschwindigkeit) verkauft. Es arbeitet nur mit frame-relay-fähigen Netzwerkgeräten (z.B. Frame-Relay-Router).

ISDN

ISDN kann bei Verbindungen mit hohen Bandbreiten mehrere Kanäle verwenden und ist ein Wähldienst, keine dauerhafte Verbindung. Es überträgt digitale Signale

über herkömmliche Telefonleitungen. Dabei kann Basis-ISDN die Kanäle in 2 B-Kanäle (je 64 kBit/s) und 1 D-Kanal (16 kBit/s) auf. Der D-Kanal übermittelt Verbindungs- und Signalisierungsinformationen. Die B-Kanäle übermitteln Daten. Beide B-Kanäle können gleichzeitig zum Übertragen von Daten verwendet werden, wodurch eine Übertragungsgeschwindigkeit von 128 kBit/s entsteht. Primary-Rate-ISDN kann mit 23 B-Kanälen von je 64 kBit/s und 1 D-Kanal mit 64 kBit/s arbeiten.

B-ISDN

Breitband-ISDN ist eine Neuerung von ISDN und ist überwiegend für die Übertragung von Sprach-, Video- und Audio-Daten gedacht. B-ISDN arbeitet eng mit ATM zusammen und hat übliche Übertragungsraten von 51 Mbit/s, 155 Mbit/s und 622 Mbit/s.

DSL (Digital Subscriber Line, digitale Teilnehmeranschlussleitung)

- ADSL (Asymmetric Digital Subscriber Line)
- TDSL (Telekom Digital Subscriber Line, Vermarktung der Telekom AG ihrer ADSL-Anschlusstechnologien)
- DSL Light (langsames ADSL für längere Strecken)
- HDSL (High Data Rate Digital Subscriber Line, über Telefonleitungen in beiden Richtungen bis zu 2 MBit/s. Ermöglicht die schnelle Kopplung von lokalen Netzwerken.)
- SDSL (Single Line Digital Subscriber Line), wie HDSL, auf einfacher Leitung.
- VDSL (Very High Data Rate Digital Subscriber Line, ermöglicht Übertragungsraten von mehr als 50 MBit/s über sehr kurze Verbindungen zwischen Netzknoten und Endgeräten oder über Glasfaser)

DSL-Techniken bilden auf der Basis von Kupferadern digitale Datenleitungen zwischen Vermittlung und Kundenanschluss. Dabei wird ein weitaus größeres Frequenzspektrum als bei analogen bzw. ISDN-Übertragungen genutzt. Die Übertragung erfolgt über herkömmliche Kupferleitungen.

Die Unterschiede zwischen den DSL-Techniken bestehen zum einen aus der Anzahl der verwendeten Kupferpaare, zum anderen aus den verwendeten Übertragungsfrequenzen bzw. den Modulationsverfahren. ADSL verwendet nur ein Kupferpaar und kann über herkömmliche Telefonleitungen betrieben werden. Da ADSL eine höhere Frequenz verwendet, kann Telefonie, wie bei ISDN, nebenher betrieben werden. Eine Frequenzweiche beim Kunden und in der Vermittlungsstelle trennen die jeweiligen Datenströme.

ADSL kann sehr hohe Übertragungsraten erzielen, wenn eine genaue Einmessung des Kabels erfolgt. Dies wird von Anbietern aus Kostengründen aber meistens vermieden, wodurch normalerweise eine sichere Übertragungsrate von 896 kBit/s beim Endkunden verwendet wird. ADSL arbeitet nicht mit für Modems herkömmlichen Bitströmen, sondern mit Paketen. Diese Pakete können Daten einer übergeordneten Netzwerkschicht enthalten (ATM, Ethernet, IP, usw.), wobei die Frames gleich im ADSL-Modem verpackt

werden. TDSL bietet gar eine Ethernet- bzw. ATM-Schnittstelle.

Asymmetric-DSL bedeutet, dass Hin- und Rückkanal jeweils unterschiedlich große Datenmengen transportieren. Beim Surfen im Internet wird beim Upstream (Hochladen von Adressen zum Provider) über den Rückkanal eine Geschwindigkeit bis zu 768 Kilobit erreicht. Beim Downstream (Runterladen von Daten aus dem Internet) bis zu 9 Megabit über den größeren Hinkanal.

Name	Max. Datenrate (Download)	Max. Entfernung zur Vermittlungsstelle
ADSL	1,5–9 Mbit/s	bis 5,5 km
DSL lite	1,5 Mbit/s	bis 5,5 km
HDSL	1,5–2 Mbit/s	bis 4 km
SDSL	768 Kbit/s	bis 3,5 km
VDSL	13–52 Mbit/s	bis 14 km
zum Vergleich: ISDN	128 Kbit/s	bis 5,5 km

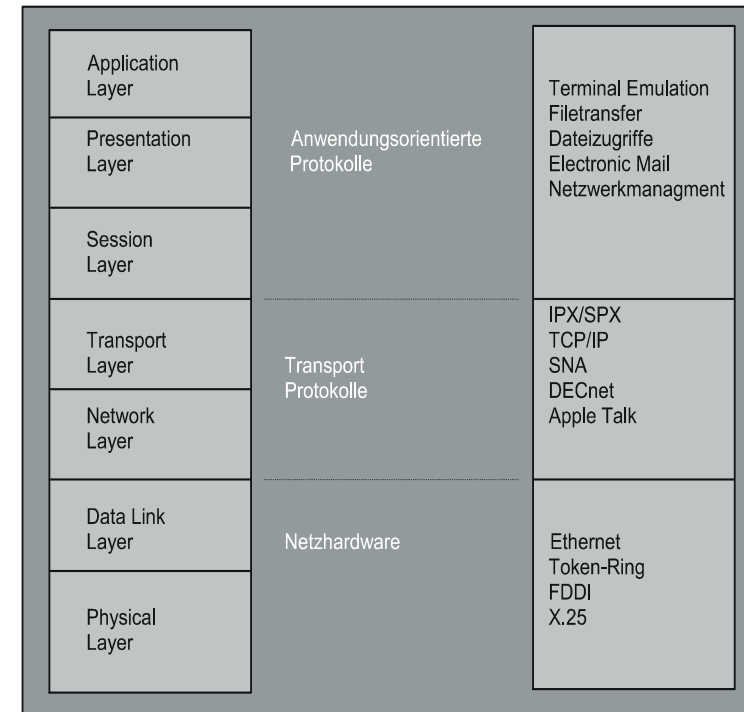
Das OSI-Schichten-Modell (OpenSystem Inter-connection)

Um vielen herstellerspezifischen Eigenheiten im Bereich der Netzwerktechnik aus dem Weg zu gehen und ein einheitliches Modell für die Netzwerktechnik zu schaffen, wurde das OSI-Schichten-Modell entwickelt, welches bestimmte Vorgaben für die Kommunikation offener Systeme darlegt.

Das Modell ermöglicht Herstellern, ihre Produkte für den Netzwerkeinsatz aufeinander abzustimmen.

OSI-Schichten-Modell

Schichten 1-3 = systembezogen
Schichten 5-7 = anwendungsbezogen



Schicht 1 Physical-Layer (Physikalische oder Bitübertragungsschicht)

Sie gibt die Informationen ins physikalische Netzwerk und empfängt Pakete oder Frames vom Netzwerk (senden und empfangen von Datenbits).

Hier werden sämtliche Spezifikationen festgelegt für:

- das Übertragungsmedium (Koaxkabel, Zweidraht, Glasfaser)
- das Übertragungsverfahren (Basisband, Breitband)
- die Topologie
- Codierung der Datenbits
- realisiert die physikalische Verbindung zwischen Computer und Netzwerk

Schicht 2 Data-Link (Verbindungsschicht oder Sicherungsschicht)

- beinhaltet die Kommunikation von Geräten innerhalb eines Netzwerksegments

- beinhaltet die Kommunikation von Geräten innerhalb eines Netzwerksegments
- zur Identifizierung von Datenpaketen werden MAC-Adressen verwendet und jedes Gerät ist dafür verantwortlich, das Netzwerk zu überwachen und diejenigen Rahmen zu empfangen, die für das Gerät selbst bestimmt sind

Hier erfolgt die erste Bewertung der eingehenden Daten:

- Überprüfung auf korrekte Reihenfolge und Vollständigkeit der Pakete
- Übertragungsfehler werden sofort erkannt
- zudem werden hier die Knotenadressen (MAC) im Netz erkannt und ausgewertet
- packt und entpackt Daten

Schicht 3 Network-Layer (Netzwerkschicht oder Vermittlungsschicht)

- Bearbeitet die Kommunikation von Geräten auf logisch voneinander getrennten Netzwerken und verwendet dazu Routing-Algorithmen, die Pakete vom Sende- zum Zielnetzwerk weiterleiten
- Unterstützt darüber hinaus Dienstadressen (Sockets oder Ports). Diese spezifiziert einen Kanal zu einem bestimmten Prozess auf einem Zielrechner (Dienstadressen sind Bestandteil der MAC- und IP-Adresse)
- hat den Überblick über Wegfindung und Paketzustellung im gesamten Netzwerksystem
- übernimmt die Verwaltung der Kommunikationspartner
- insbesondere werden die ankommenden bzw. abgehenden Datenpakete verwaltet, und zwar in der Form, dass Nachrichten von darüberliegenden Schichten in kleinere Datagramme fragmentiert werden, die in ihrer Größe für die physikalische Schicht geeignet sind
- außerdem trägt die Netzwerkschicht auch die Verantwortung für die Wiederherstellung von Nachrichten aus empfangenen Datagrammen
- eindeutige Zuordnung über die Vergabe der Netzwerkadressen (logische IP-Adressen)
- fügt der Verbindung weitere Steuerinformationen hinzu
- realisiert das Routing der Daten durch das Netz (legt also die Route durchs Netzwerk fest, die Pakete über eine Serie von Routern vom Quell- zum Zielrechner nehmen)

Schicht 4 Transport-Layer (Transportschicht)

- überträgt Information in eine Sprache, die das andere System versteht
- sorgt für eine zuverlässige Zustellung von Nachrichten an die Zielgeräte
- Fehlerkontrolle (Transportschicht muss diese Fehlerkorrektur initiieren)
- Festlegung der Reihenfolge von Paketen
- Ende zu Ende Flusskontrolle (Neben einer negativen Bestätigung für unvollkommene Übertragung von Daten kann die Transportschicht auch ein erneutes Senden anfordern)
- stellt die Verbindung zwischen den Schichten 1–3 und 5–7 her
- fügt Infos zur Adressierung und Ansprechen der Datenendgeräte hinzu
- baut die nötige Verbindung auf
- leitet die Datenpakete gemäß der Adressierung weiter

- realisiert die Weitergabe und die Bestätigung der Übertragung

Schicht 5 Session-Layer (Sitzungs- oder Steuerungsschicht der Kommunikation)

- stellt Methode zur Erzeugung und Aufrechterhaltung einer log. Verbindung zwischen zwei Hosts zur Verfügung
- verwaltet die Dialoge zwischen 2 Computern (Simplex, Halbduplex, Vollduplex)
- festlegen des Verbindungsaufbaus (Sitzungsaufbau, Datentransfer, Sitzungsabbau)
- Eine Sitzung besteht aus:
 1. Festlegung der benötigten Dienste
 2. Benutzeranmeldung und andere Sicherheitsprozeduren
 3. Aushandlung von Protokollen und Protokollparametern
 4. Mitteilung von Sitzungsnummern

Schicht 6 Presentation-Layer (Darstellungsschicht)

- erzeugt im Falle von WIN-NT den SMB-Block, der dem anderen System mitteilt, was angefordert ist, oder erhält die Antwort auf eine Anfrage. Hier wird auch die Typenkonvertierung behandelt, wenn kommunizierende Hosts unterschiedlich sind.
- erledigt die Datenkonvertierung
- stellt sicher, dass die Daten in einem universellen Format übertragen werden
- Möglichkeiten der Datenein- bzw. -ausgabe werden bereitgestellt,
- dazu gehört Anzeige von Meldungen und Anweisungen
- Datenein- und -ausgabe wird überwacht

- Übertragungskonvertionen werden festgelegt
- Bildschirmdarstellungen werden angepasst
- Umsetzung der Bit-Reihenfolge
- Übersetzung der Byte-Reihenfolge
- Übersetzung des Zeichensatzes
- Übersetzung der Dateisyntax

Schicht 7 Application-Layer (Anwendungsschicht)

Erzeugt Anfragen und verarbeitet Anfragen, die sie erhält.

- erste Schnittstelle zwischen Rechner und Anwendungsprogramm
- hier werden die verwendeten Anwendungen eingesetzt
- liefert dem Netzwerk Dienste (Datei-, Drucker-, E-Mail-, Datenbankdienste)