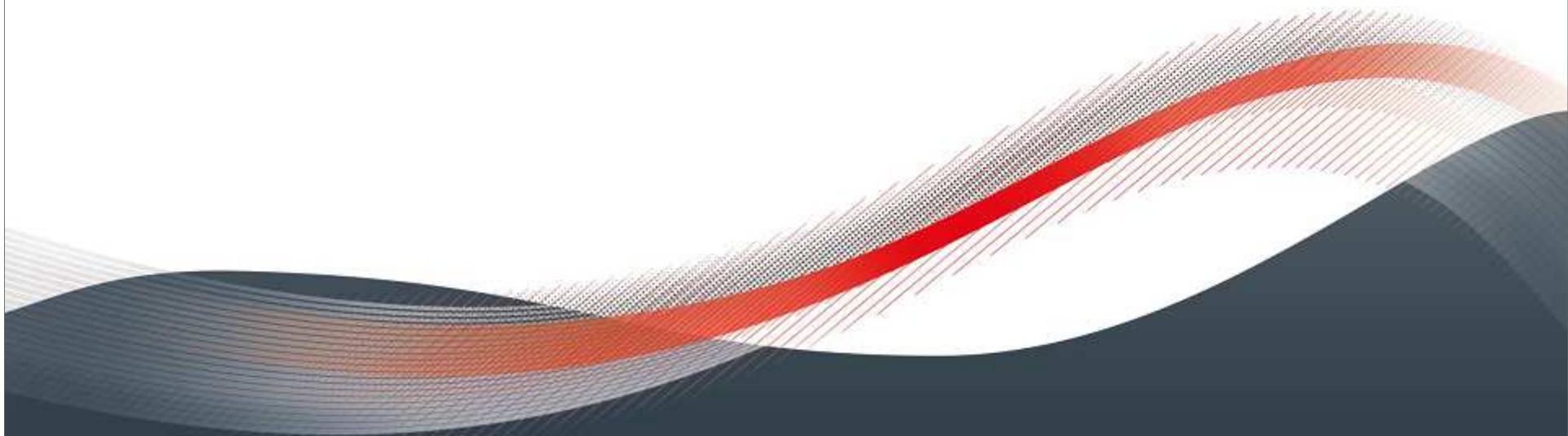


Netzwerktechnik 1

Teil1: Grundlagen

Kai Reidelbach



Nur zum internen Gebrauch, nicht zur Veröffentlichung im Internet

Inhalte

- Grundlagen der Netzwerktechnik, Begriffsdefinitionen
- Topologien, Adressierung, Übertragungsmedien
- Strukturierte Verkabelung
- ISO-OSI Modell
- Ethernet und Netzwerkstandards
- CSMA/CD, Kollisionsdomäne, Broadcastdomäne
- Repeater, Hub, Switch, Router
- IPv4 und IPv6
- Subnetting, CIDR, Routing



Informationsquellen

www.wikipedia.de

www.elektronik-kompendium.de

www.w3schools.com

kompendium.infotip.de

Vorsicht: Keine Primärquellen, in wissenschaftlichen Arbeiten nicht zitierfähig



Literaturhinweis

Andrew S. Tanenbaum
David J. Wetherall
„Computernetzwerke“

Pearson Studium
5. Erweiterte Auflage

ISBN-13: 978-3868941371



Primärquellen 1

- ANSI

American National Standards Institute

- » US-Industrienormen, vergleichbar der DIN, Mitglied der ISO, Bsp. ANSI-C (Programmiersprache)
- » www.ansi.org

- IEEE

Institute of Electrical and Electronics Engineers

- » Internationaler Verband der Elektroingenieure, div. Standards der Elektro- und IT-Technik, beispielsweise für die Netzwerktechnik IEEE802 Ethernet (LAN-Standard),
- » www.ieee.org

- ISO

International Organization for Standardization

- » Weltverband nationaler Standardisierungsgremien, allgemeine Industrienormen, Bsp. ISO3103 Zubereiten von Tee, ISO7498 OSI-Modell, ISO9660 Dateisystem opt. Datenträger usw.
- » www.iso.org



Primärquellen 2

- **ITU-T**

Telecommunication Standardization Sector der ITU International Telecommunication Union

- » Standardisierungsgremium des Weltverbandes der Telekommunikationsunternehmen, Normen der Telekommunikation und Netzwerke, Bsp. X.25 WAN über Telefonleitungen, G.992 ADSL, X.200 OSI-Modell
- » www.itu.int/ITU-T

- **ETSI**

European Telecommunications Standards Institute

- » Normierungsgremium der Europäischen Telekommunikationsunternehmen, Urheber der Normen für Mobilfunk wie z.B. GSM Global System for Mobile Communications und UMTS Universal Mobile Telecommunications System
- » www.etsi.org



Primärquellen 3

- IETF **Internet Engineering Task Force der ISOC Internet Society**
 - » Urheberin der als RFC Request For Comments bekannten Internetstandards, Bsp. RFC791 IPv4 Adressierung, RFC2460 IPv6 Adressierung
 - » www.ietf.org



Dienste

- Abstrakte Funktion
- Realisiert durch Dienstanbieter
- Datenbasiert
- Anwendungsorientierung
- Nutzung in Systemumgebungen
- Übertragung in Netzwerken
- Bereitstellung auf Plattformen (Hard- und Software)
- Zugriff und Kommunikation über Protokolle

Dienst != Protokoll



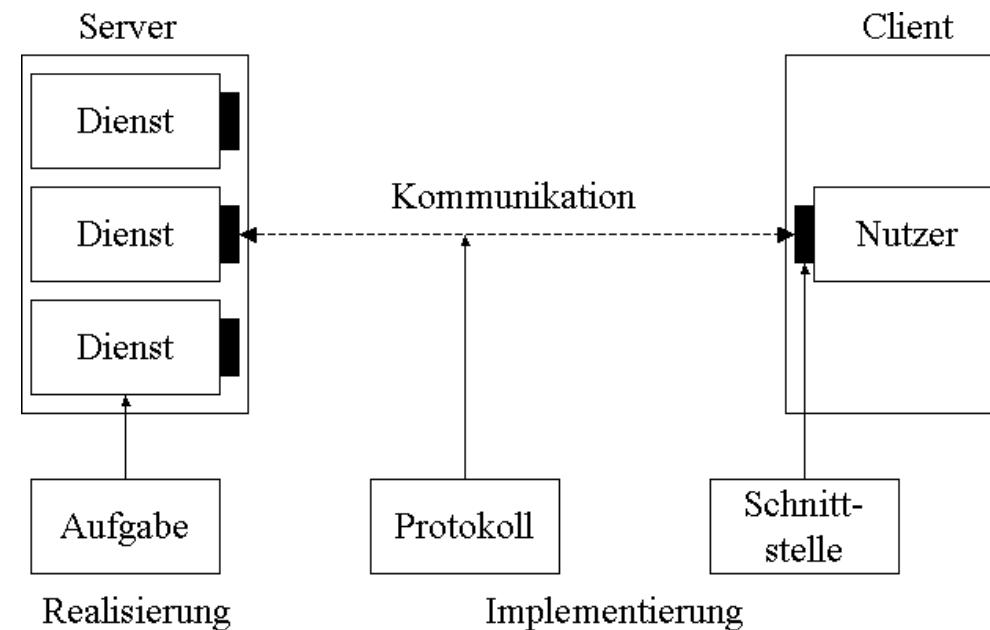
Protokolle

- Ablauf der Kommunikation zeitlich, syntaktisch, semantisch
- Dienstanbieter <-> Dienstnutzer
- Maschine zu Maschine
- Prozess zu Prozess
- Präzise und eindeutig
- Strukturiert und hierachisch
- Keine Interpretation der Semantik
- Standardisierung und Normierung
- Proprietäre Protokolle

Ein Dienst -> mehrere Protokolle



Client und Server



Client: Dienstnutzer
Server: Dienstanbieter



Diskussion

Welche Dienste kennen Sie?

Mit welchen Protokollen werden diese realisiert?

Warum gibt es so viele Protokolle?

Was ist ein „Server“ ?



Beispiele Dienste und Protokolle

Dienst

World Wide Web

Fileserver

eMail

Netzwerkmanagement

Remote Login

VOIP

Protokoll

HTTP, HTTPS

FTP, SMB, CIFS, NFS

POP3, IMAP, SMTP

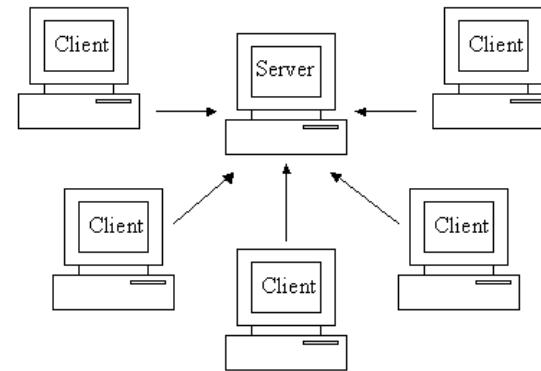
SNMP, DHCP, DNS, IGMP

Telnet, SSH

SIP, SSIP, RTP, RTPS



Client Server Kommunikation



Kommunikation ist von Clienten auf Server gerichtet.

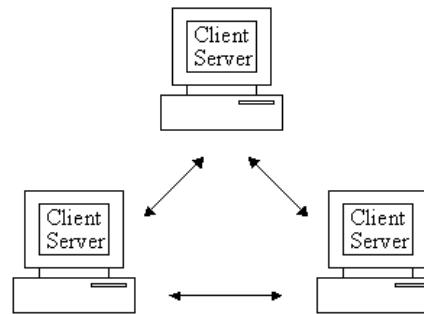
Client zu Client Kommunikation findet nicht statt

Server, Dienstanbieter: immer passiv, wartet auf Verbindungsauftakt

Client, Dienstnutzer: aktiv, baut Verbindung auf



Peer to Peer Kommunikation



Peer: Gleicher unter Gleichen

Keine vorgegebene Kommunikationsrichtung

Aber: Peer = Client + Server (Wer baut Verbindung auf?)



Arten von Netzwerken

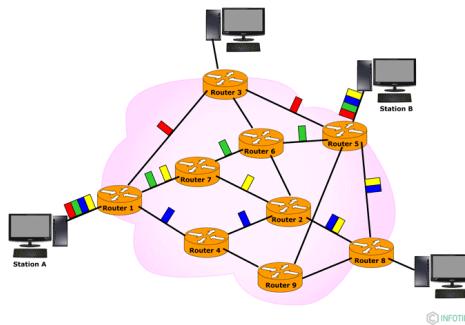


Abb.1 Paketvermittlung

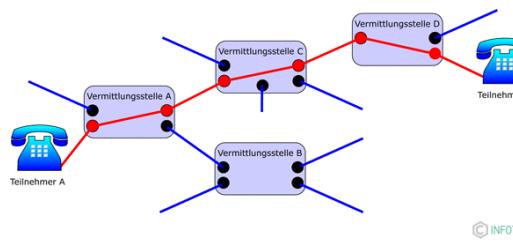


Abb.2 Leitungsvermittlung

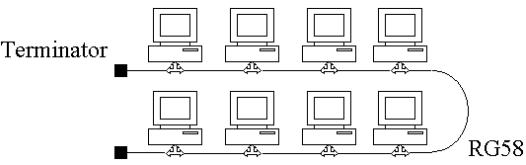


Abb.3 Broadcastnetz

- Point to Point bzw. Direktverbindung

Zwei Netzwerkknoten haben eine exklusiv genutzte Leitungsverbindung

Beispiel: Telefonnetz mit Leitungsvermittlung

Datennetze Weitbereichsverbindung mit Paketvermittlung

- Broadcastnetz

Viele Netzwerkknoten nutzen ein gemeinsames Übertragungsmedium

Beispiel: Datennetz lokal mit Paketvermittlung

Quelle: Abb. 1 und 2 aus: <https://kompendium.infotip.de/netzwerktechnologie1-historisches-und-grundlagen.html>

Zugriffsverfahren

Problemstellung Broadcastnetze Mehrfachzugriff mehrerer Stationen: **Kollision**

<u>Zugriffsverfahren</u>	<u>Organisation</u>	<u>Anwendung</u>
Master-Slave	zentral	USB, industrielle Bussysteme Master steuert zentral den Zugang zum Medium für alle Knoten
ALOHA	dezentral	deprecated, experimental stochastischer Zugriff
CSMA/CD	dezentral	Ethernet IEEE802.3 Carrier Sense, Multiple Access, Collision Detection
CSMA/CA	dezentral	Ethernet IEEE802.11 Carrier Sense, Multiple Access, Collision Avoidance
Tokenpassing	zentral/dezentral	Tokenring IEEE802.5 Senderecht (Token) wird von Station zu Station weitergegeben



Diskussion

Was ist von „Push“-Diensten zu halten?

Warum ist ein Datennetz mit vielen Teilnehmern prinzipiell eine Herausforderung?

Ist das Telefonnetz das bessere Netzwerk?

Warum ist Leitungsvermittlung keine Lösung?

Welcher entscheidende Aspekt fehlt noch für eine Paketvermittlung?



Netzwerkadressen

Netzwerkadressen kennzeichnen einen Netzwerkknoten eindeutig.

Paketvermittlung setzt eine Absender- und Empfängeradresse voraus.

Übliche Netzwerkadressen

MAC	48 bit	fix	lokal
-----	--------	-----	-------

Physische Adresse
Netzwerkartenhersteller erkennbar

IPv4	32 bit	veränderlich	global
------	--------	--------------	--------

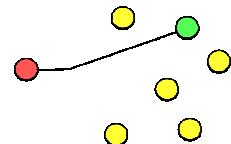
Logische Adresse
IP-Adresse besteht aus Netzwerk- und Hostadresse

IPv6	128 bit	veränderlich	lokal/global
------	---------	--------------	--------------

Logische Adresse
MAC-Adressen können Teil der IPv6-Adressen sein

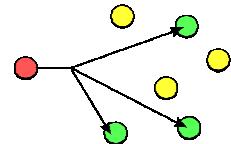


Adressierungsarten



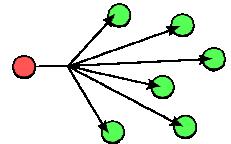
Unicast:

Die Netzwerkadresse adressiert genau einen Zielknoten



Multicast:

Die Netzwerkadresse adressiert eine Gruppe von Netzwerknoten



Broadcast:

Die Netzwerkadresse adressiert alle erreichbaren Knoten im Netz

- Die Adressierungsart ist eine Eigenschaft der Netzwerkadresse z.B. aufgrund bestimmter Adressbereiche. Die Wirkung entfaltet eine Netzwerkadresse beim Empfänger, der entscheidet über die Annahme und Verarbeitung eines Datenpakets.

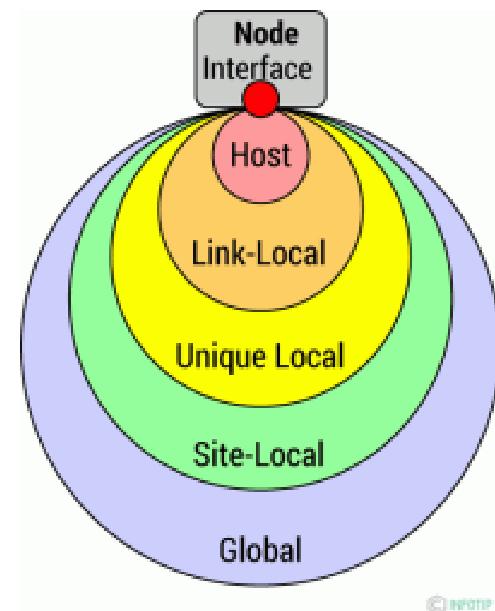


Scope (IPv6)

Eine Besonderheit weisen IPv6 Adressen auf:

Der Scope kennzeichnet die Reichweite einer IPv6 Adresse.

- Der Scope Global ist mit öffentlichen IPv4 Adressen vergleichbar.
- Private IPv4 Adressen verhalten sich in etwas wie Link-Local oder Site-Local.
- Unique-Local Adressen haben keine Entsprechung im IPv4 Adressraum, sie gelten zwar nur lokal, sind aber trotzdem global eindeutig.
- Der Scope-Host gilt nur im abgeschlossenen System (Loopback).



Quelle: kompendium.infotip.de/netzwerktechnologie1-historisches-und-grundlagen.html

Reichweite von Netzen

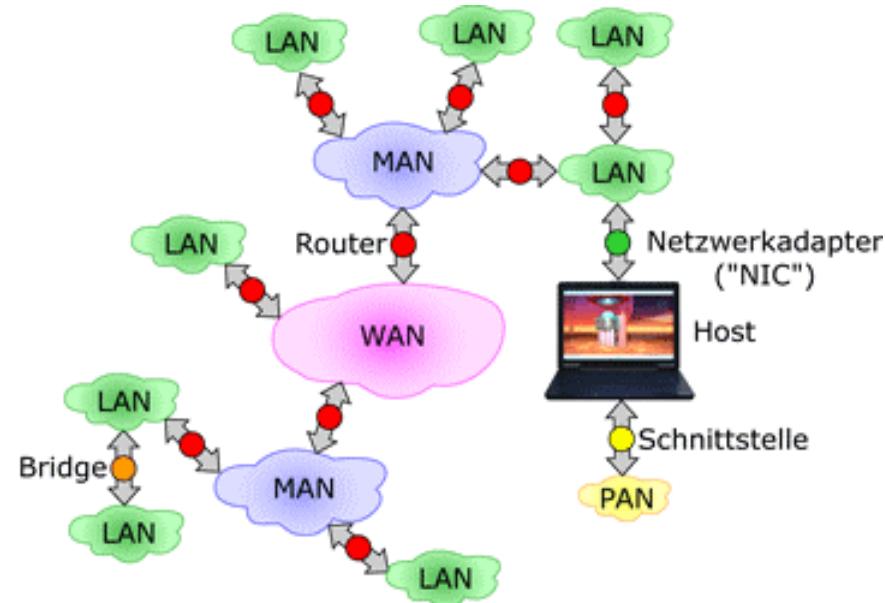
physische Ausdehnung

<u>Bezeichnung</u>	<u>Reichweite</u>	<u>Beispiel</u>
BAN Body Area Network	körpernah bzw. körperintern	medizinische Anwendung
PAN Personal Area Network	1m	Bluetooth-Piconet, USB, IrDA
LAN Local Area Network	10m ... 100m	Ethernet, WLAN
CAN Campus Area Network	1km	Tokenring, WiMAX
MAN Metropolitan Area Network	10km ... 100km	FDDI, Kabel-TV
WAN Wide Area Network	100km ... 1.000km und mehr	ATM, X.25
GAN Global Area Network	10.000km	dto.

Anmerkung: Die Entferungen sind als Angabe einer Größenordnung zu verstehen



Verwendung Netzwerke



Netzwerke und Verbindungselemente

Quelle: kompendium.infotip.de/netzwerktechnologie1-historisches-und-grundlagen.html

Reichweite diverse Netze

BEREICH		SYSTEM	MEDIUM KABELTYP	DATENRATE THEORETISCH	DATENRATE NETTO (ca.)	FREQUENZ- BEREICH	REICHWEITE	BEMERKUNGEN
ACCESS-Networks	GAN Global Area Network	(A)DSL	Draht	300-16000Mb/s	25Mb/s		max. 5km	Asymmetrische Kommunikation: Upload-Geschwindigkeit meist wesentlich geringer (z.B.64Kb/s)
		ADSL 2	Draht	16Mb/s			max. 8km	
		VDSL	Glasfaser u. Draht	50Mb/s			max. 3km	
	WAN Wide Area Network	SDSL	Draht	8Mb/s Duplex			max. 2,5	Zugang zu festversch. Netzen (ISDN)
		WiMAX	Mikrowelle	108 Mb/s (28 MHz BB)		2-11GHz	max. 50km	IEEE 802.16
	MAN Metropolitan Area Network	ISDN	Draht	64Kb/s	60 Kb/s			
		Analog Telefon	Draht 28,8/56k Modem	28,8/53 Kb/s	19/38Kb/s			
		SkyDSL	Satelliten-Downlink	4000-8000Kb/s				Upload-/Rückkanal meist ISDN/DSL
		UMTS	Drahtlos	2Mb/s	z.Zt.: 384Kb/s		Sichtweite	
		GPRS	Drahtlos	171,2Kb/s	z.Zt.: 53,6Kb/s		Sichtweite	8 gebündelte GMS-Kanäle
BETRIEBS-NETZWERKE	LAN Local Area Network	Ethernet 10Base	Koaxialkabel	10Mb/s	3Mb/s	100-500m		
		Ethernet 100Base	Twisted Pair (CAT5)/GF	100Mb/s	30Mb/s	100m/2000m		
		Ethernet 1000Base	Twisted Pair (>CAT5e)/GF	1000MB/s	300Mb/s	100m/2000m		
	WLAN Wireless Local Areal Network	Powerline (PLC)	Stromnetz	Homeplug: 14 Mb/s HomeplugAV: 100Mb/s			200m	
		WLAN 802.11a	Drahtlos	6-54Mb/s	35Mb/s	5GHz	10-25m	nur Indoor, reduzierte Sendeleistung, hohe Dämpfung (wg. hoher Frequenz)
		WLAN 802.11b ("Wi-Fi")	Drahtlos	11Mb/s	2,5-5Mb/s	2,4GHz	10-300m	auch Outdoor, Richtantennen möglich
		WLAN 802.11g	Drahtlos	54Mb/s	35Mb/s	2,4GHz	10-300m	kompatibel zu 802.11b
		WLAN 802.11h	Drahtlos	54Mb/s	35Mb/s	5GHz	10-70m	Ergänzung zu 802.11a für EU. Erhöhte Sendeleistung, TPC, DFS
		WLAN 802.11n	Drahtlos	540Mb/s	35Mb/s	5GHz	10-70m	Multiple Input Multiple Output (MIMO)
	PAN Personal Area Network	USB 1 / 1.	Kabel	1,5Mb/s / 12Mb/s	640Kb/s / 8Mb/s		5m	
		USB 2	Kabel	480Mb/s	z.Zt.: 30Mb/s		5m	
		IEEE1394a	Kabel	100, 200, 400Mb/s	100, 200, 400Mb/s		4,5m	
		IEEE1394b	div. Kabel / GF	800Mb/s	800Mb/s		bis 100m	
		Bluetooth	Drahtlos	Vers. 1: 732,2Kb/s Vers. 2: bis 2,2Mb/s	Asym: 732,2 / 57,6Kb/s Sym: 2x433,9Kb/s	2,4GHz	10-100m	Störanfällig gegen WLAN, DECT-Telefone, Mikrowellen, Radar
		IrDA	Infrarot	9,6-115Kb/s (SIR) bis 16Mb/s (VFIR)			1m	

Beispiele für diverse Netze und deren Reichweite und Medien

Quelle: kompendium.infotip.de/netzwerktechnologie1-historisches-und-grundlagen.html

Diskussion

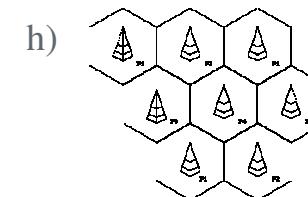
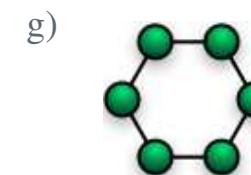
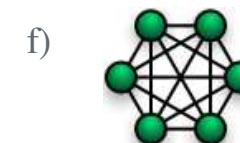
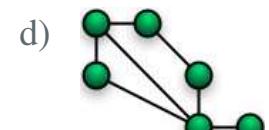
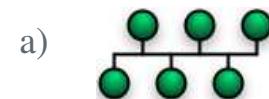
- Nennen Sie praktische Beispiele für BAN, LAN, WAN, GAN
- Kennen Sie irgendein reales CAN? Warum ist das kaum gebräuchlich?
- Welcher Zusammenhang besteht zwischen der Netzwerkadressierung und der Netzwerkgröße?
- Wo findet man point to point? Wo ist Broadcast üblich?



Topologien

Grundlegend:

- Linie
- Bus
- Ring
- Stern
- Masche
- Zelle



Speziell:

- Vollvermatscht
- Baum

Hybride:

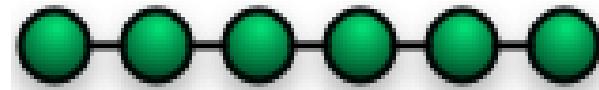
Kombinationen von verschiedenen Topologien



Topologien: Linie

Linie:

- Eine Kette von Netzwerkknoten



Vorteile:

Einfache Struktur
Point to point
Keine Zugangssteuerung
Keine Kollisionen
Keine Wegefindung

Nachteile:

Lange Verzögerungen
Extrem störanfällig für Nodestörung
Extrem störanfällig Kabelbruch
Hohe Netzlast bei den Nodes

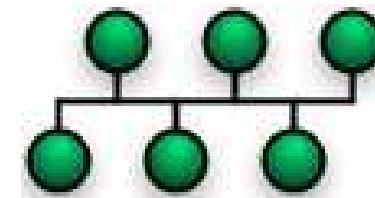
Beispiel: Telegraphie 19. Jhdt.



Topologien: Bus

Bus:

- Netzwerknoten gemeinsam an einem Kabel
- Name stammt vermutlich von *Omnibus Bar* (Stromschiene)



Vorteile:

- Einfache Struktur
- Geringer Materialaufwand
- Keine Vermittlung nötig

Nachteile:

- Broadcastnetz mit Kollisionen
- Zugriffsverfahren nötig
- Anfällig für Kabelbruch
- Niedrige Auslastungsgrenzen
- Begrenzte Reichweite (Keine Verstärker)

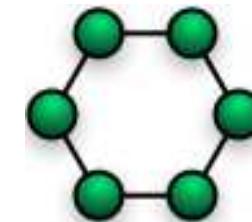
Beispiel: Ethernet 10Base2, 10Base5



Topologien: Ring

Ring:

- Netzwerknoten werden über point to point verbunden
- Auch als Doppelring üblich



Vorteile:

- Keine Kollisionen
- Kurze definierte Verzögerungen
- Hohe Auslastungsgrenze

Nachteile:

- Hoher Materialaufwand
- Komplexes Protokoll (Tokenring)

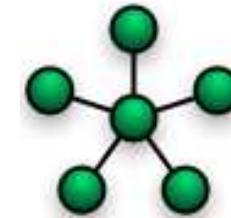
Beispiel: Tokenring IEEE802.5, FDDI



Topologien: Stern

Stern:

- Netzwerknoten werden über Zentralknoten verbunden
- Point to point möglich oder Broadcastnetz



Vorteile:

- Störfest Kabelbruch
- Störfest Nodestörung
- Point to Point: Hoher Datendurchsatz
- Point to Point: Keine Kollisionen
- Broadcast nur Verstärker nötig

Nachteile:

- Hoher Materialaufwand
- Single Point of Failure Zentralknoten
- Broadcast: Hohe Netzlast
- Broadcast: Kollisionen, Zugriffsverfahren
- Point to Point: Verteiler nötig

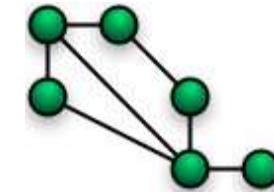
Beispiel: CSMA/CD-Ethernet IEEE802.3



Topologien: Masche

Masche:

- Leitungswege bei Bedarf, unstrukturiert
- Point to point Verbindungen



Vorteile:

Sehr störfest gegen alle Störungen
Höchste Ausfallsicherheit
Verkehrsumleitung möglich
Skalierbar

Nachteile:

Komplexe Vermittlungstechnik
Hoher Verkabelungsaufwand
Strukturinformationen nötig (Routing)
Oft viele Netzbetreiber im Verbund

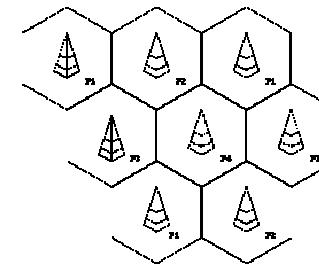
Beispiel: Internet



Topologien: Zelle (Funk)

Zelle:

- Keine physikalische Verkabelungsstruktur
- Definiert über Frequenzbänder und Reichweite



Vorteile:

Keine Verkabelung
Störfest Nodestörung

Nachteile:

Störanfälliges Medium
Broadcastnetz, Kollisionen
Zugriffsverfahren nötig
Unkontrollierbare Ausbreitung
Stark eingeschränkte Datenrate
Freie Frequenzen Mangelware

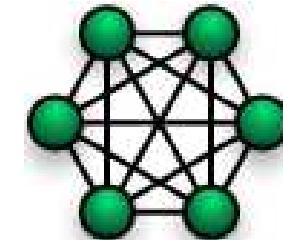
Beispiel: WLAN, Bluetooth, Mobilnetze



Topologie: Vollvermascht

Vollvermascht:

- Alle möglichen Leitungswege existieren
- Point to point Verbindungen
- Theoretische, akademische Topologie



Vorteile:

Maximale theoretische Datenrate

Maximale Ausfallsicherheit

Nachteile:

Maximaler Materialaufwand

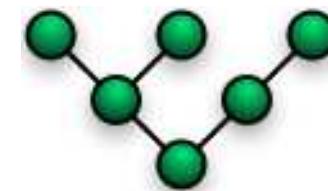
Beispiel: keins



Topologie: Baum

Baum:

- Zusammengesetzt aus Sternen in Hierarchieebenen
- Wichtige Topologie für LAN (DIN EN 50173)



Vorteile:

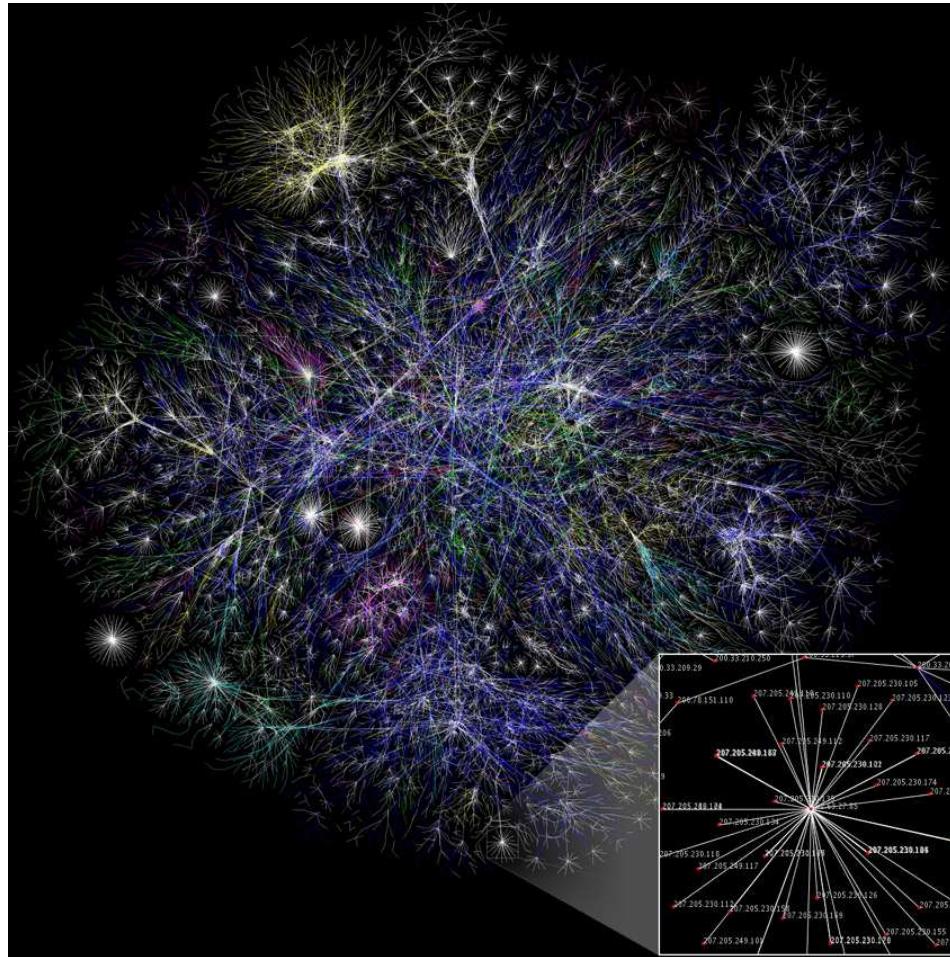
- Alle Vorteile wie Stern
- Weniger Materialaufwand als Stern
- Größere Reichweite als Stern
- Bedarfsgerechte Segmente

Nachteile:

- Alle Nachteile wie Stern
- Mehr Zentralknoten als bei Stern
- Single Point of failure bis Ausfall Baum
- Netzlast an der Wurzel

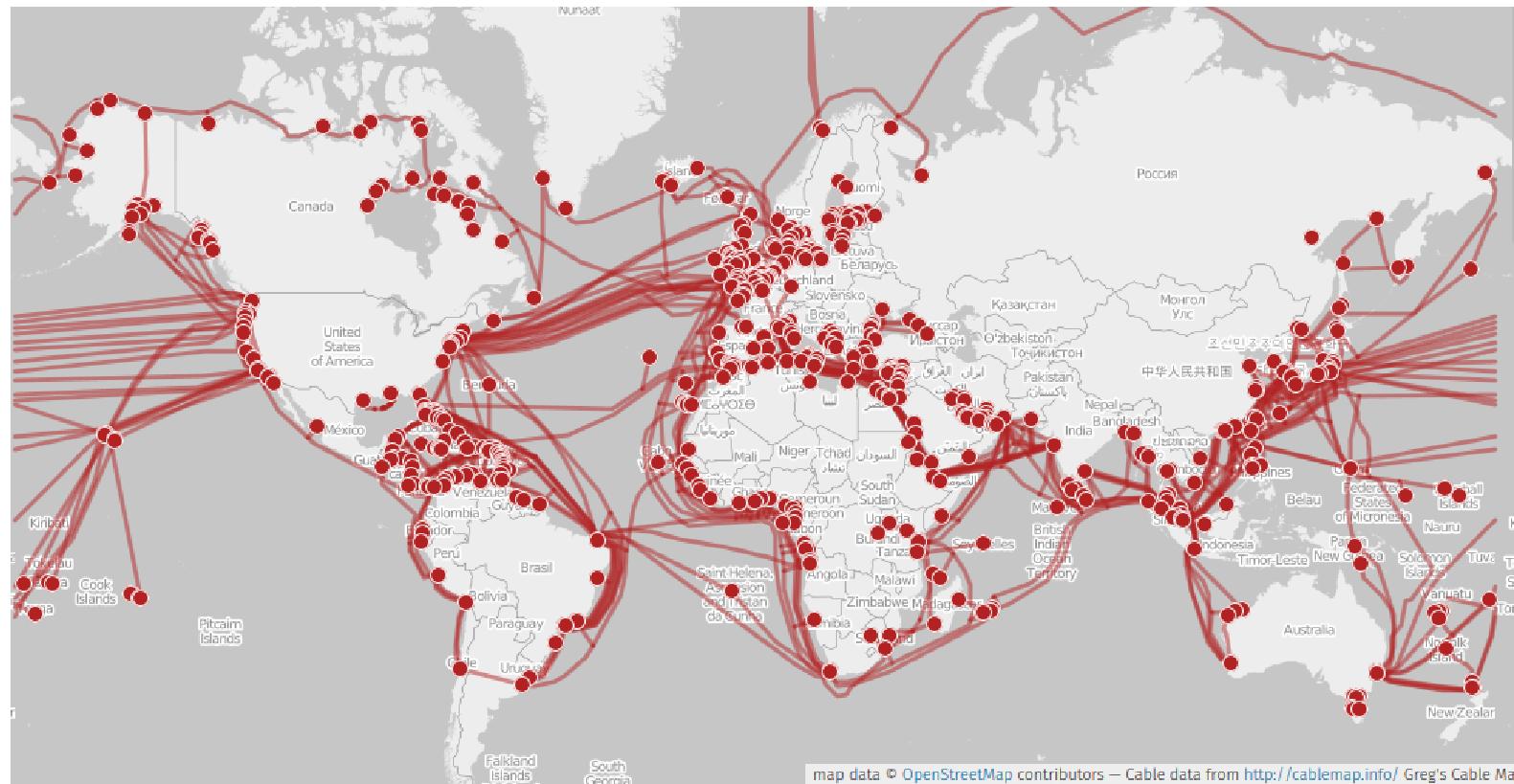


Beispiel: Routen des Internets



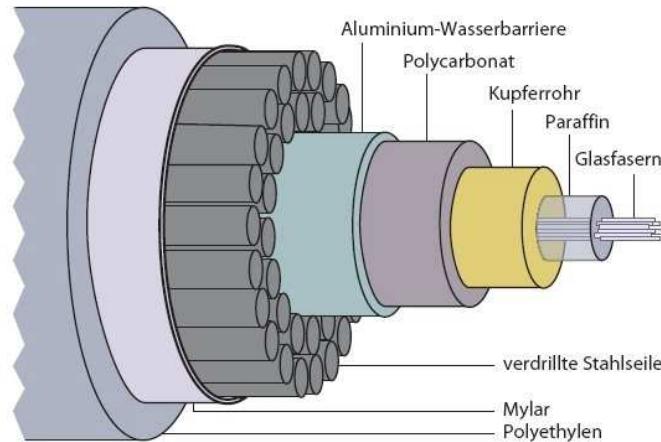
Quelle: upload.wikimedia.org/wikipedia

Beispiel: Globale Topologie Unterseekabel (2015)



Quelle: de.wikipedia.org/wiki/Seekabel

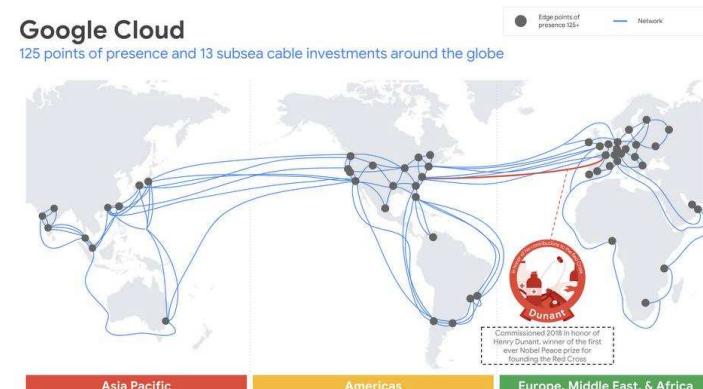
Technik Unterseekabel



Unternehmenseigene Infrastruktur
(Google 2020)

13 Seekabel
125 „points of presence“

Aufbau eines Seeglasfaserkabels
Stromversorgung (DC) der opt. Repeater
über das Kabel (Kupferrohr)
Bis zu 1,24 Tbit/s Datenrate

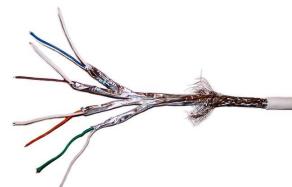


Quelle: www.heise.de/newsticker/meldung/Seekabel-bringt-schnelles-Internet-nach-Ostafrika-7623.html

bestcompanyseo.info/worldwide-infrastructure-google-publicizes-the-development-of-a-fourth-clear-underwater-cable-between-america-and-europe/

Übertragungsmedien

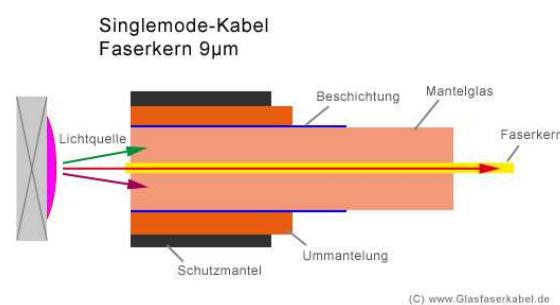
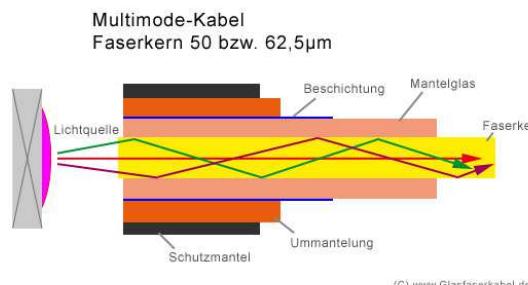
Kupfer:
Koaxialkabel



Twisted Pair Kabel

Lichtwellenleiter:
Multimode-Faser

Single Mode Faser



Funk:
Frequenzbänder mit unterschiedlichen Ausbreitungseigenschaften

Quelle: de.wikipedia.org

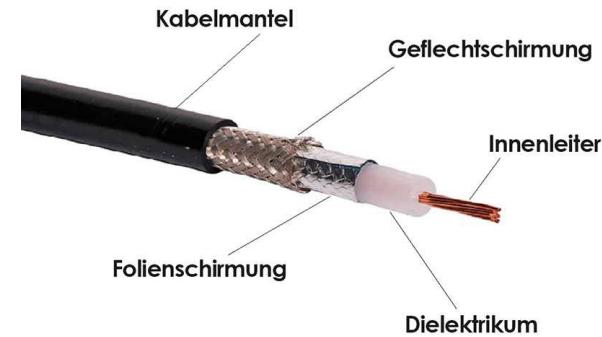
www.glasfaserkabel.de/Der-Unterschied-zwischen-Singlemode-und-Multimode-LWL-Kabeln:_13.html

Netztechnik 1, Kai Reidelbach, Sommersemester 2020

Koaxialkabel

Eigenschaften:

- Betriebsfrequenz bis mehrere 10 GHz
- Typisch für Bustopologie
- Im LAN derzeit keine Anwendung
- Für Antennen netze und HF-Signale
- Typen: RG58 (Thinwire), RG8 (Thickwire)



Vorteile:

- Kostengünstig
- Hohe Bandbreite und gute Schirmung
- Abzweige möglich
- Einfache Steckverbinder

Nachteil:

- Ausfall nach Kabelbruch

Stecker.



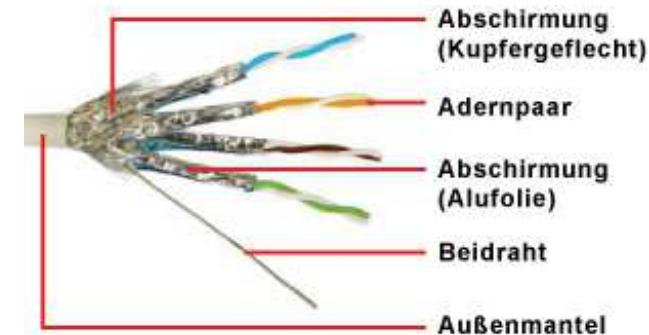
Quelle: de.rs-online.com/web/generalDisplay.html?id=ideen-und-tipps/koaxialkabel-leitfaden



Twisted Pair Kabel

Eigenschaften:

- Betriebsfrequenz bis mehrere GHz
- Standard Netzwerkabel
- Typisch für symmetrische digitale Signale
- 4 verseilte Päärchen zu 2 Adern
- Verschiedene Abschirmungen üblich



Vorteile:

- Massenware, sehr preiswert
- In vielen Kategorien erhältlich
- Geringe Störkopplung

Nachteil:

- Nur begrenzte Reichweite
- Niedrigere Bandbreite als Koaxialkabel

Stecker:



Quelle: www.elektronik-kompendium.de/sites/net/0603191.htm



TP Kabel Bezeichnung ISO/IEC-11801

Standardisierte Kabelbezeichnung:

XX/ Y ZZ

XX: Gesamtschirmung

U	kein Schirm
F	Folienschirm
G	Drahtgeflechtsschirm
SF	Folien- und Geflechtsschirm

Y: Paarschirmung

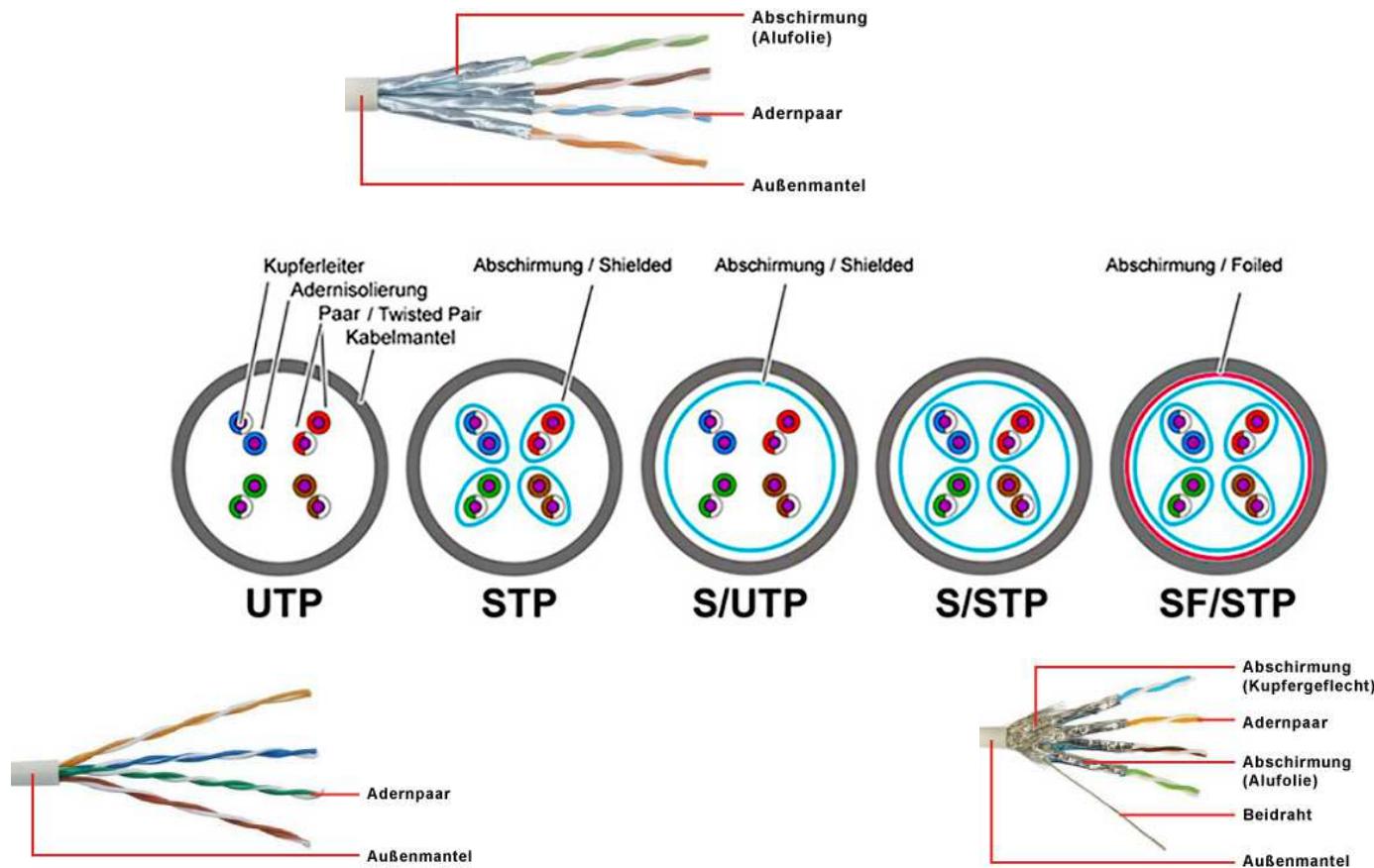
U	kein Schirm
F	Folienschirm
G	Drahtgeflechtsschirm

ZZ: Verseilungsart

TP	Twisted Pair
QP	Quad Pair



TP Kabel Schirmung



Quelle: edu.juergarnold.ch/fach_it/netzwerktheorie/article1.html

www.elektronik-kompendium.de/sites/net/0603191.htm

Netztechnik 1, Kai Reidelbach, Sommersemester 2020

Kategorien

EIA/TIA 568 und ISO/IEC 11801

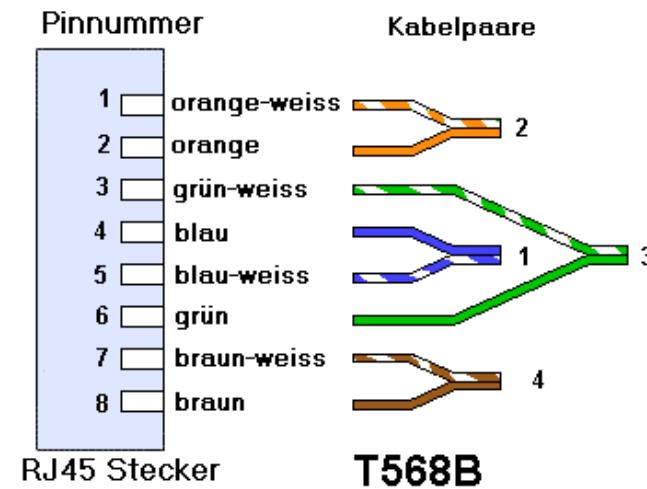
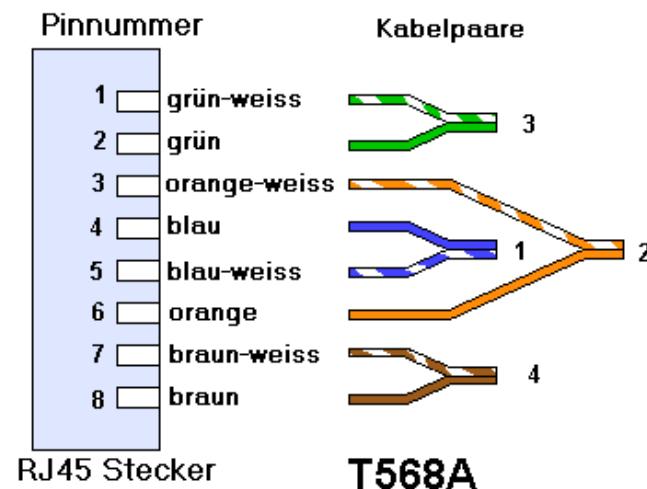
<u>Kategorie:</u>	<u>Grenzfrequenz:</u>	<u>Bemerkung:</u>
CAT1	100 kHz	Nur für Sprache/Telefon
CAT2	4 MHz	Digitale Sprachdienste, ISDN
CAT3	16 MHz	Netzwerk 10Mbit/s
CAT4	20 MHz	speziell für 16 Mbit/s Tokenring (veraltet)
CAT5	100 MHz	Netzwerk 100 Mbit/s
CAT5e	100 MHz	Verbessert für 1 Gbit/s Ethernet Netzwerk
CAT6	250 MHz	Ideal für 1 Gbit/s Netzwerk
CAT6a	500 MHz	Netzwerk 10 Gbit/s (max. 50 m)
CAT7	600 MHz	Netzwerk 10 Gbit/s (100m)
CAT8	~1500 MHz	Netzwerk 40 Gbit/s bis 100 Gbit/s

Kabel und andere Komponenten werden in Kategorien eingeteilt



TP Kabel Farbfolge

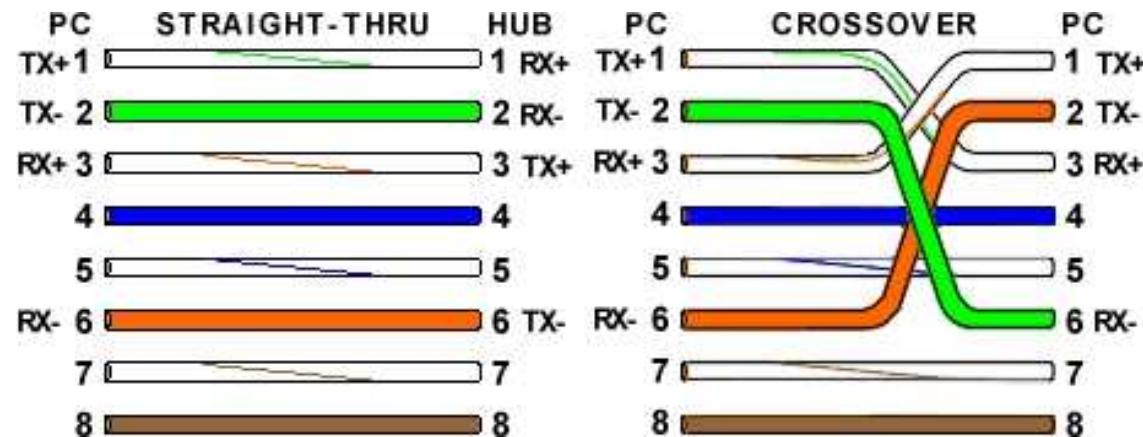
- Die Aderfarben von TP-Kabel und die Zuordnung zum RJ45 Stecker sind genormt
- Es gibt es zwei übliche Zuordnungen
- T568A oder T568B sind wahlfrei, müssen einheitlich sein



Quelle: www.netzmafia.de/skripten/netze/twisted.html

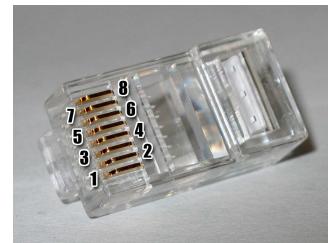
Patchkabel

- Netzwerkkabel und Installationen sind 1 zu 1 verbunden
- Ausnahme Cross Over Kabel für 10Base-T



TP Kabel Stecker

Western Stecker:



RJ45 (8P8C) ungeschirmt

Nachfolger:



GG45 (Nexxan)



RJ45 (8P8C) geschirmt



TERA (DIN EN 50173)

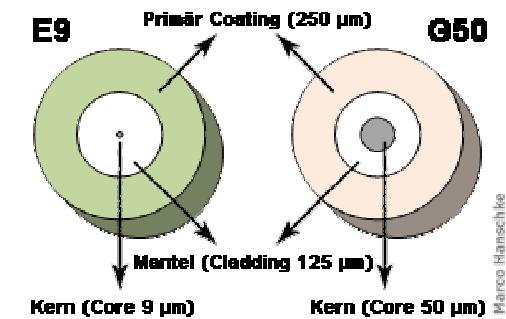


Lichtwellenleiter

Grundlegende Eigenschaften:

- Kunststoff- oder Glasfaser mit Kunststoff Coating
- Lichtleitung durch Totalreflektion
- Multimode Faser 50/63 µm core
- Monomode Faser 3,5 - 10,4 µm core
- Infrarot, Wellenlänge ca. 500 nm bis 1700 nm

Querschnitt einer Einmoden- und Multimodefaser



© Marco Hänschke

Vorteile:

- Sehr geringe Dämpfung
- Keine EMV-Probleme
- Hohes Bandbreitenlängenprodukt
 - Hohe Datenrate einige Tbit/s
 - Hohe Reichweite bis 100km

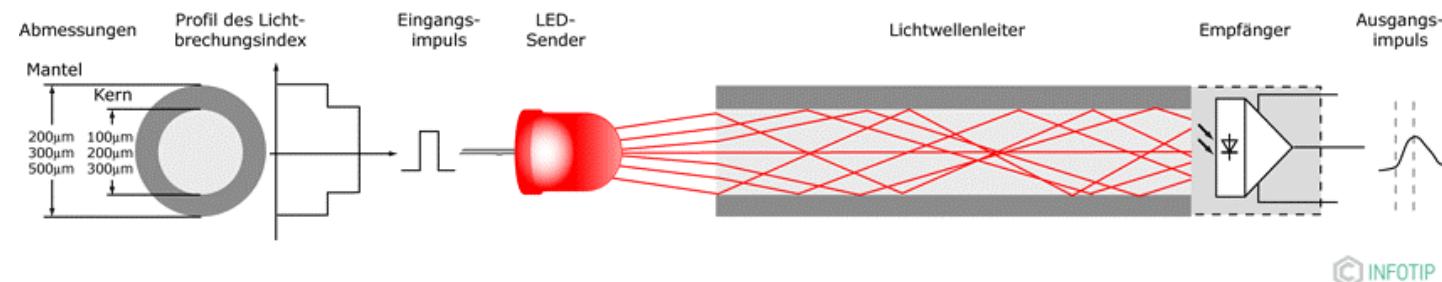
Nachteile:

- Mechanisch empfindlich
- Teure Tranceiver nötig
- Nur Point to Point, kein Bus
- Zwei Fasern (Senden/Empfangen)
- Viele Steckertyp
- Aufwändige Verarbeitung

Quelle: www.isimko.de/index.php?page=lichtwellenleiter

Multimodefaser

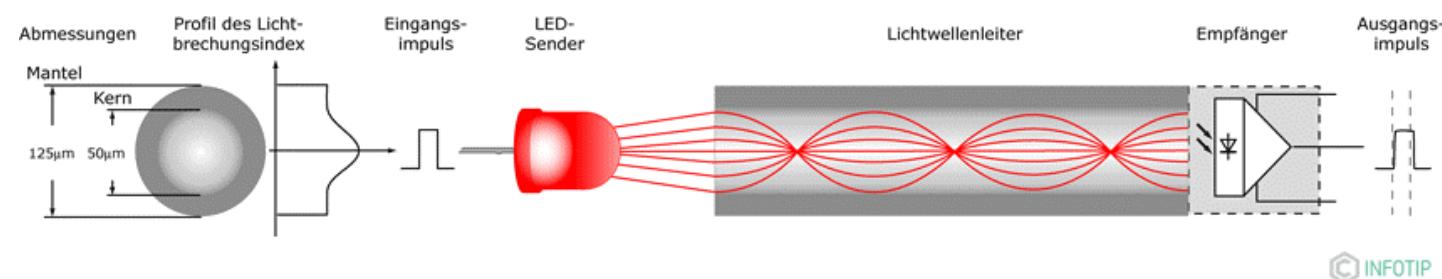
Stufenindex:



 **INFOtip**

Problem: Dispersion

Gradientenindex:



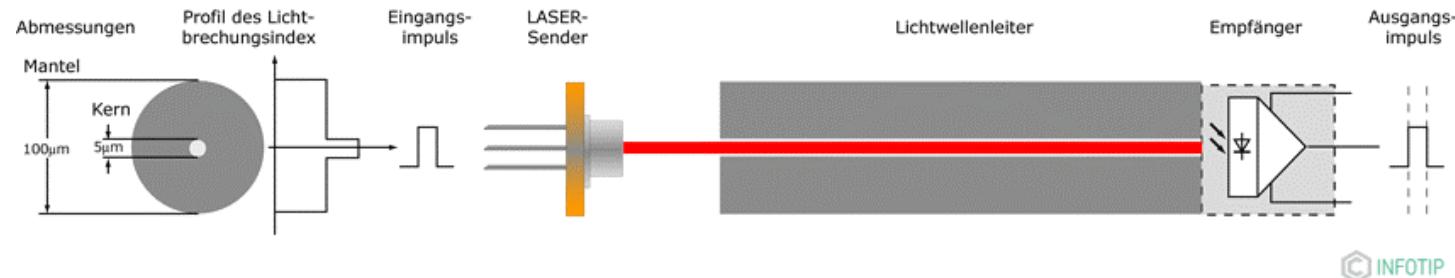
 **INFOtip**

Quelle: kompendium.infotip.de/uebertragungsmedien-kupfer-und-lichtwellenleiter.html



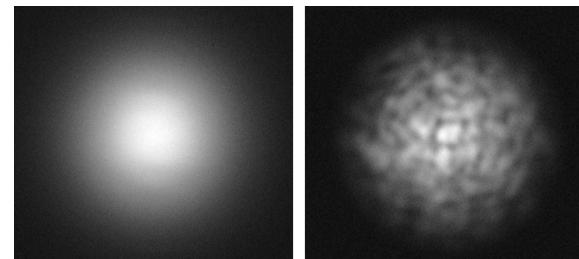
Monomodefaser

Stufenindex:



© INFOTIP

Praktisch Dispersionsfrei



Lichtverteilung:

Monomodefaser

Multimodefaser

Quelle: kompendium.infotip.de/uebertragungsmedien-kupfer-und-lichtwellenleiter.html

Handelsübliche Fasertypen

Reichweite Ethernet

<u>Multimodefasern:</u>	100 Mbit/s		10 Gbit/s			100Gbit/s
	<u>850nm</u>	<u>1310nm</u>	<u>850nm</u>	<u>1310nm</u>	<u>1550nm</u>	<u>850nm</u>
OM1 G62,5/125	300 m	2000 m	30 m	550 m		
OM2 G50/125	300 m	2000 m	80 m	550 m		
OM3 G50/125	300 m	2000 m	300 m	550 m		70 m
OM4 G50/125		2000 m	500 m	550 m		100 m
OM5 G50/125		2000 m		550 m		

Singlemodefasern:

OS1 E9/125	10 km	10 km	40 km
OS2 E9/125	10 km	10 km	40 km

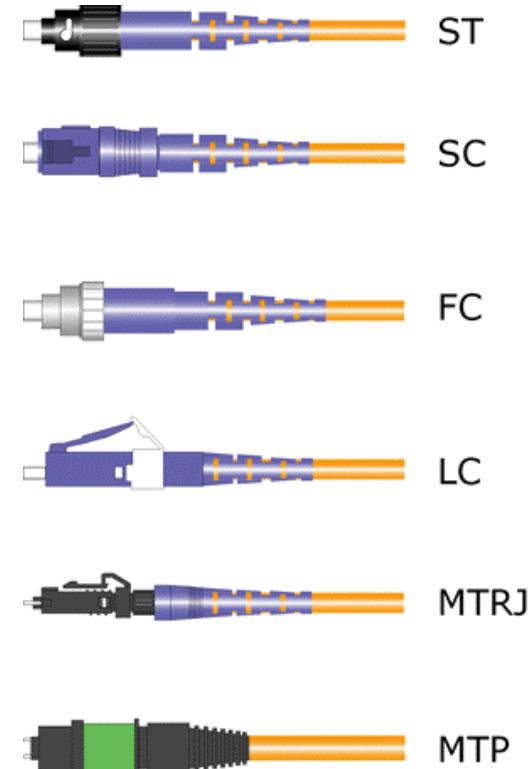
G50/125. Gradient, 50 µm core, 125 µm coating



Lichtwellenleiter Steckertypen

Probleme:

- Viele verschiedene Steckertypen
- Aufwändige langwierige Montage
- Sehr teuer (bei Singelmodefaser)
- Spezielles Werkzeug
- Jedes Patchkabel Sonderanfertigung
- Spleißen von Pigtails
- Spezielle Cassetten für LWL
- Durchgangsmessung Dämpfung



 INFOTIP

Quelle: kompendium.infotip.de/uebertragungsmedien-kupfer-und-lichtwellenleiter.html



Strukturierte Gebäudeverkabelung

DIN EN 50173

Standardisierung der Anforderungen an Gebäudeverkabelungen von Büros

Problemstellung:

- Bisher jeder Dienst, jede Technologie: eigener Verkabelungsstandard
- Viele unabhängige Netze mit unterschiedlicher Topologie, Kabel, Stecker usw.
- Teure unflexible Verkabelung, kaum skalierbar, nicht wiederverwendbar
- Ohne Kundenanforderung nicht planbar, nicht installierbar
- Praktisch unzählige Kabel „gewachsene“ Altinstallation

Zielstellung:

- Dienstunabhängige universelle Gebäudeverkabelung
- Einheitliche Planungsvorgaben
- Berücksichtigung bei der Bauplanung, Gebäudeerrichtung



Tertiärbereich

DIN EN 50173

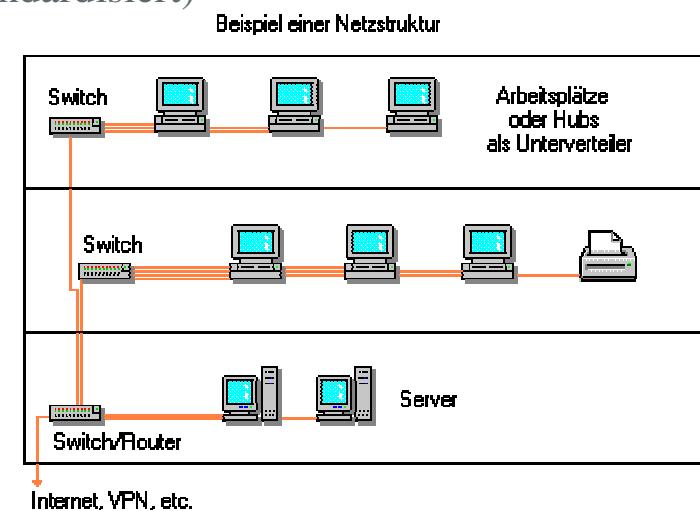
- Etagenverkabelung
- Anschluß der Endgeräte
- Zwei Universalanschlußeinheiten pro Arbeitsplatz
- Zentraler Etagenverteiler (EV) pro Etage
- Medium Kupfer-TP bis 100m Länge (davon max. 10m Patchkabel)
- Komponenten: Netzwerkdose, Patchpanel, aktiver Verteiler (switch)



Sekundärbereich

DIN EN 50173

- Optionale Gebäudeverkabelung
- Versorgung der Etagenverteiler über einen Gebäudeverteiler (GV)
- Baumtopologie, der Sekundärbereich selbst ist Stern
- Verkabelung Kupfer TP bis 100 m alternativ LWL bis 500 m
- Höhere Netzlast als im Tertiärbereich
- Kein Anschluß von Endgeräten an GV
- Anschluß Router/Serversysteme optional (nicht standardisiert)



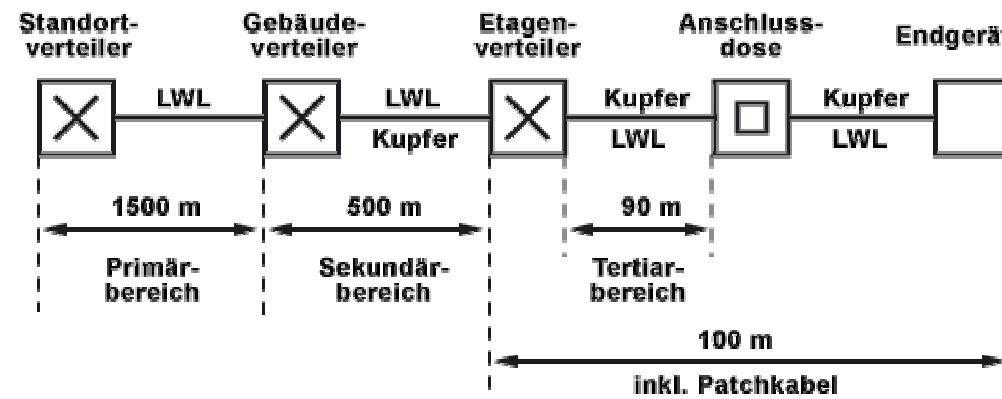
Quelle: www.netzmafia.de/skripten/netze/planung.html



Primärbereich

DIN EN 50173

- Optionale Standortverkabelung zwischen Gebäuden
- Versorgung der Gebäudeverteiler über einen Standortverteiler (GV)
- Baumtopologie, Primärbereich selbst ist Stern
- Verkabelung nur LWL bis 1500 m
- Höchste Netzlast
- Standortverteiler kritisch, Single Point of Failure



Aktive/Passive Komponenten

Kriterium: Komponenten ohne Verstärker/Verarbeitung sind passiv
Praktisch Alles ohne Stromversorgung

Passiv: Stecker, Buchsen, Kabel, Patchpannel, ...

Aktiv: Medienkonverter, Repeater, Hub, Switch, Appliance, Rechner, ...

Funktion: Router, Gateway, Firewall, Server, Client

Z.B. Routing ist eine Funktion, realisiert durch Software auf einer aktiven Komponente
Ein Router ist eine Kombination aus Hard- und Software
Die Hardware ist Voraussetzung aber nicht kennzeichnend für die Funktion Router
Router können in jeder erdenklichen Form realisiert sein



IEEE802

Netzwerkstandards (Auszug):

- IEEE802.1
 - IEEE802.1D
 - IEEE802.3
 - IEEE802.3a
 - IEEE802.3u
 - IEEE802.3ab
 - IEEE802.3ae
 - IEEE802.11
 - IEEE802.15
 - IEEE802.15.1
 - IEEE802.16

IEEE802.1	High Level Interface
IEEE802.1D	Spanning Tree Protocol
IEEE802.3	CSMA/CD
IEEE802.3a	10Base2
IEEE802.3u	Fast Ethernet (100 Mbit/s)
IEEE802.3ab	Gigabit Ethernet
IEEE802.3ae	10 Gigabit Ethernet
IEEE802.11	WLAN
IEEE802.15	WPAN
IEEE802.15.1	Bluetooth
IEEE802.16	WIMAX



IEEE802 Ethernet im ISO OSI Modell

Ethernet Standards werden den OSI Schichten zugeordnet:

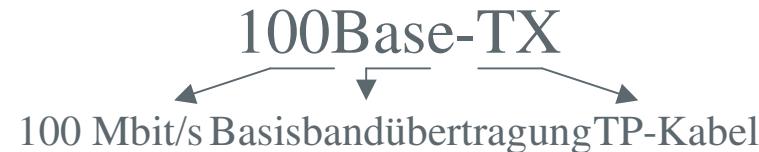
Layer 3 .. 7	...		
Layer 2 Data Link	802.2 LLC (Logical Link Control)		
	802.1 MAC (Media Access Control)		
Layer 1 Physical	802.3 CSMA/CD	802.5 Tokenring	802.11 WLAN

Die Ethernetstandards sind älter als das ISO OSI Modell
Logical Link Control spielt im LAN keine Rolle



IEEE802.3

Namensschema (Auszug):



10	10 Mbit/s	E	LWL, single 1500nm
100	100 Mbit/s	S	LWL, multi 850 nm
1000	1 Gbit/s	L	LWL, multi 1350 nm
10G	10 Gbit/s	T	TP-Kabel
40G	40 Gbit/s	2	Koaxialkabel 185m
100G	100 Gbit/s	5	Koaxialkabel 500m

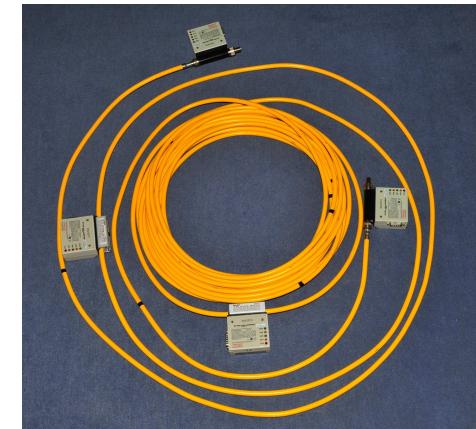
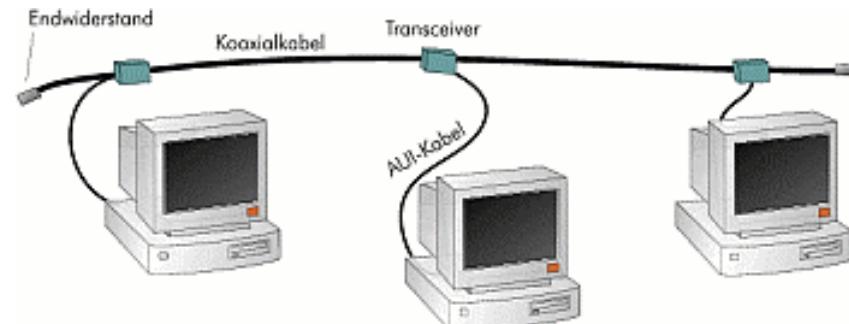
und Ergänzungsbuchstaben mit spezieller Bedeutung z.B. X in 100Base-TX



IEEE802.3

10Base5

- Antik!
- Koaxialkabel RG8 (ca. 10mm - Thickwire)
- Terminatoren am Leitungsende
- Bustopologie bis 500 m und 100 Knoten
- „Vampirklemme“ und Tranceiver
- 10 Mbit/s Datenrate
- CSMA/CD Zugriffsverfahren



Quelle:tech.mattmillman.com/projects/10base5/

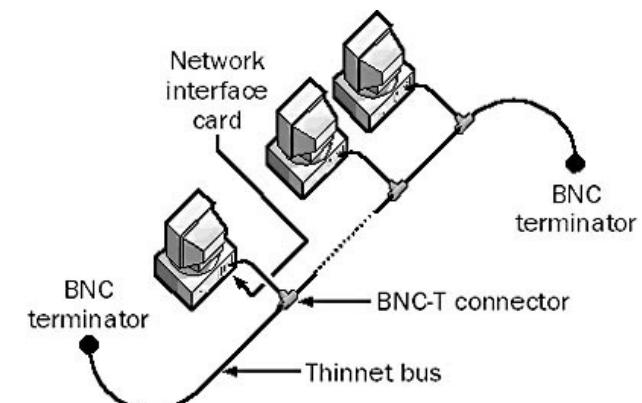
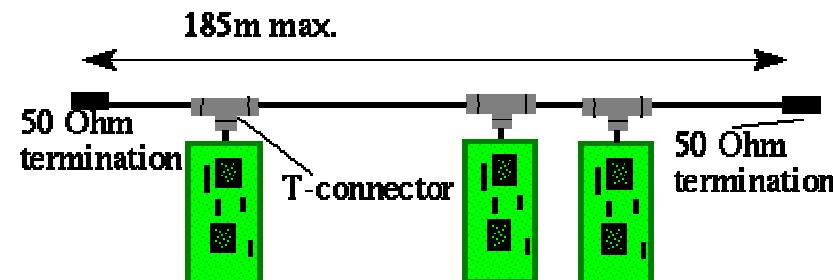
www.airnet.de/cr1-gfe/de/html/GrundPrinzEth_learningObject4.xml

Netztechnik 1, Kai Reidelbach, Sommersemester 2020

IEEE802.3

10Base2

- Historisch!
- Bustopologie 185 m Segmentlänge
- Günstiges Koaxialstandardkabel (RG58)
- BNC Steckverbinder mit T-Stücken
- Anschluß direkt an Netzwerkkarte
- 10 Mbit/s Datenrate
- Keine weiteren Komponenten nötig



Quelle: www.linuxfocus.org/Deutsch/January2000/article134.shtml

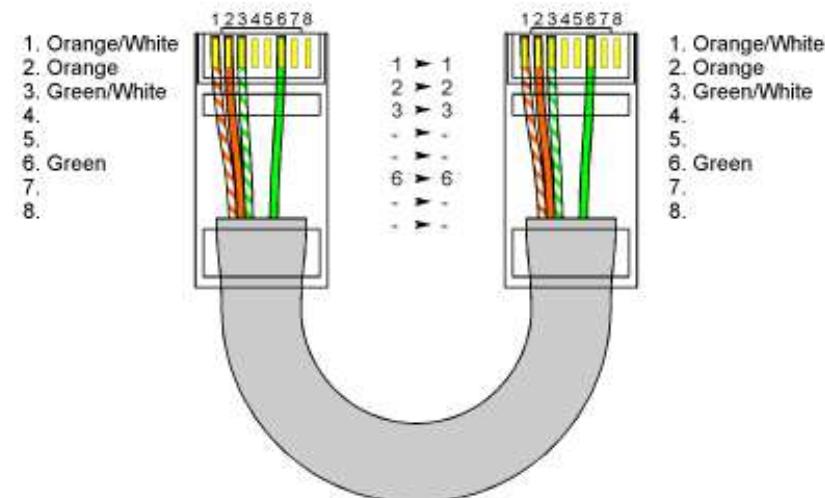
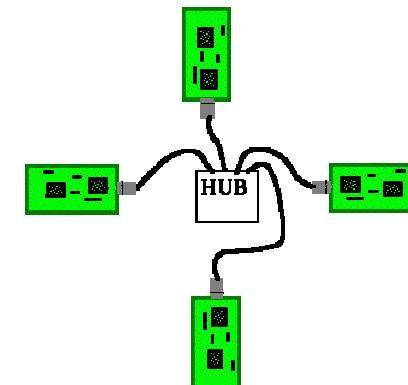
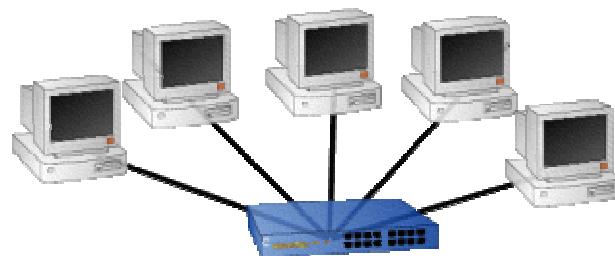
networkencyclopedia.com/10base2/

Netztechnik 1, Kai Reidelbach, Sommersemester 2020

IEEE802.3

10Base-T

- Sterntopologie
- Twisted Pair Kabel (Cat3, U/UTP)
- Zentraler Verteiler
- 100 m Segmentlänge
- Kabel „Halbbelegung“, 2 Paare
- 10 Mbit/s Datenrate
- RJ45 Stecker
- Ursprung aller modernen Standards
- „komische“ Kontaktbelegung



Quelle: www.linuxfocus.org/Deutsch/January2000/article134.shtml

www.lawerence.de/map/standard.php

Netztechnik 1, Kai Reidelbach, Sommersemester 2020

IEEE802.3

Neuere Standards (Auswahl)

Gemeinsamkeiten der Standards:

- Stern topologie mit TP Kabel
- Kabellänge max. 100m
- RJ45 Stecker
- Kompatibel, Schnittstelle umschaltbar
- Autonegotiation

<u>Standard</u>	<u>Belegung</u>	<u>Kabel</u>	<u>Vermittler</u>
10Base-T	2 Paare	Cat3	Hub/Switch
100Base-TX	2 Paare	Cat5	Hub/Switch
1000Base-T	4 Paare	Cat5e	Switch
10GBase-T	4 Paare	Cat6a	Switch
40GBase-T	4 Paare	Cat8	Switch

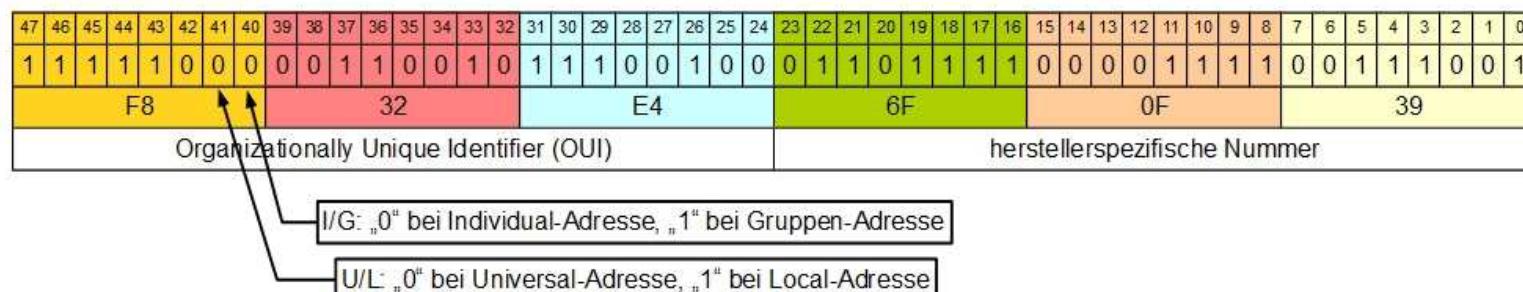


IEEE802.1

MAC Adressen

Netzwerkadressen des Ethernets:

- Vergabe durch IEEE, weltweit eindeutig (außer Local)
- 48 bit Umfang
- Schreibweise xx:xx:xx:xx:xx:xx xx = hexadezimal 00 bis FF
- Broadcastadresse FF:FF:FF:FF:FF:FF
- Schema:

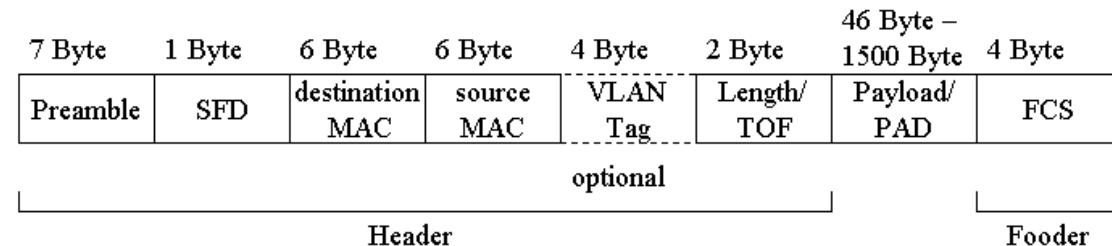


Quelle: de.wikipedia.org/wiki/MAC-Adresse

IEEE802.3

Ethernetframe-II

Struktur:



Felder:

Preamble

Erläuterung:

Vorspannung Bitmuster Synchronisation

SFD

Start Frame Delimiter, Bit zeigt Start der Daten an

Destination MAC

Netzwerkadresse Ziel

Source MAC

Netzwerkadresse Absender

VLAN Tag

Optional, QOS Flags und VLAN ID (IEEE802.1Q)

TOF

Type Of Field (z.B. 0x0800 für IPv4)

Payload

Nutzlast

FCS

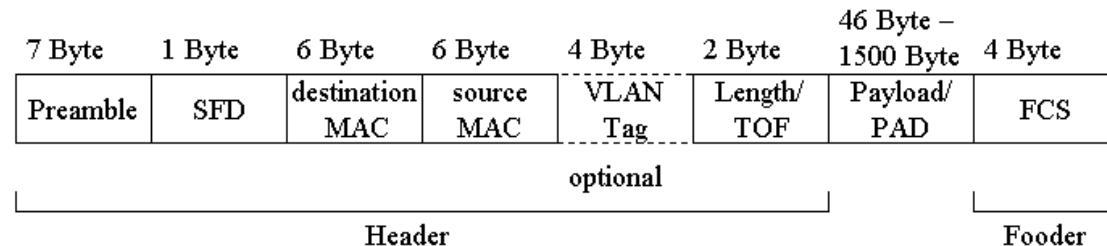
Frame Check Sequence (CRC Prüfsumme)



IEEE802.3

Ethernetframe-II

Struktur:



- Die Länge eines Frames wird nicht mehr angegeben
- Standard Ethernetframes haben kein VLAN Tag, sind also untagged
- Frames mit VLAN Tag, tagged, treten z.B. zwischen VLAN Switchen auf
- Frames haben eine variable Größe ja nach Nutzlast
- Mindestgröße 64 Byte (ohne Präamble)
- Maximalgröße untagged 1518 Byte, Jumboframes auch 8 kByte oder mehr
- Fehlende Nutzdaten werden aufgefüllt (Padding)
- Schicht 3 Protokoll muss MTU (Maximum Transfer Unit) beachten

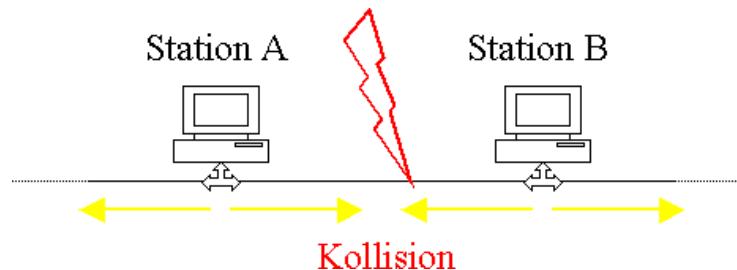


IEEE802.3

CSMA/CD

Problem:

Broadcastmedium mit Kollisionen
Zwei Netzwerknoten senden gleichzeitig



Lösung:

CSMA/CD

CS: Carrier Sense

MA: Multiple Access

CD: Collision Detection

Senden nur wenn Medium frei

Jeder Knoten hat Zugriff auf das Medium, auch mehrfach

Reagieren auf Kollision und Medium wieder freigeben



IEEE802.3

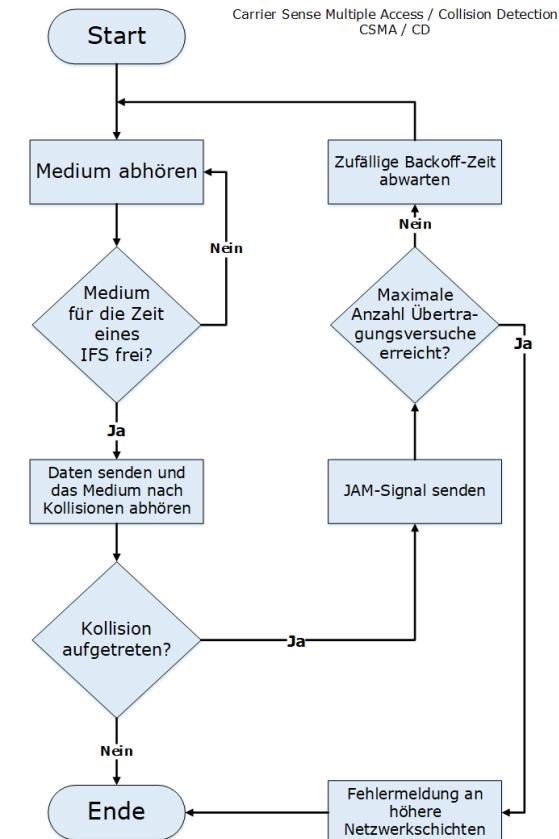
CSMA/CD

Details:

- Carrier Sense kann keine Kollisionen verhindern
- IFS Inter Frame Spacing (4,7 us bei 10Mbit/s)
- Kollisionen werden an unzulässiger Spannung erkannt
- Sofortiger Abbruch Sendung
- JAM Signal löscht Empfangspuffer
- Backoff Time basiert auf Zufallszahl
- Vermeidung wiederholter Kollision
- Zu hohe Anzahl von Kollisionen → Timeout

Ziel:

- Dezentrale Zugriffssteuerung
- Faire Verteilung der Bandbreite
- Zugang zum Medium für alle Knoten



Quelle: de.wikipedia.org/wiki/Carrier_Sense_Multiple_Access/Collision_Detection

IEEE802.3

Round Trip Delay Time

Lichtgeschwindigkeit im Medium:

$$c_M = 200000 \frac{km}{s}$$

Bitzeit bei 10 Mbit/s:

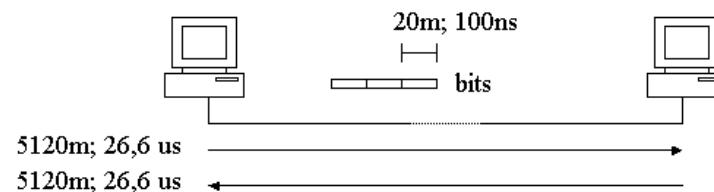
$$t_{bit} = \frac{1}{10 * 10^6} s = 100ns$$

Laufstrecke Signal pro Bitzeit:

$$l_{bit} = c_M * t_{bit} = 200000 \frac{km}{s} * 100ns = 20m$$

Max. Entfernung für Hin- und Rückweg:

$$l_{max} = \frac{512 * 20m}{2} = 5120m$$



Bei 10 Mbit/s und 512 bit Frames dürfen zwei Stationen max. 5.120 m Entfernung haben, um eine sichere Kollisionserkennung zu gewährleisten



IEEE802.3

Round Trip Delay Time 10 Mbit/s

Beurteilung von 10Mbit/s Netzen (aus IEEE802.3) :

<u>Technologie</u>	<u>Kabel</u>	<u>max. Länge</u>	<u>Bitzeiten (pro m)</u>
10Base2	Koaxial	185 m	0,1026
10Base5	Koaxial	500 m	0,0866
10BaseT	TP Kabel	100 m	0,113
10BaseF*	LWL	2000 m	0,1
Hub/Repeater	(am Besten mit Maxwert rechnen)		40 – 70
Erstes Segment			+ 10

Nur für 10 Mbit/s Netze, Summe darf für ein Netz 512 Bitzeiten nicht überschreiten

Kein Rechnen mit Lichtgeschwindigkeit

Faktor 2 für Hin- und Rückweg enthalten

*) beliebiger Lichtwellenleiter



IEEE802.3

Round Trip Delay Time 10 Mbit/s

Vereinfachung 5-4-3 Regel:

Ein 10 Mbit/s Netzwerk entspricht den Anforderungen wenn:

- Max. 5 Segment
- Max. 4 Repeater/Hub
- Max. 3 aktive Segmente

<u>Überprüfung:</u>	<u>Kabel:</u>	<u>Laufzeit Kabel:</u>	<u>Repeater:</u>
Segment 1	500m RG8	$500*0,0866=43,3$	10
Segment 2	500m RG8	$500*0,0866=43,3$	70
Segment 3	500m RG8	$500*0,0866=43,3$	70
Segment 4	500m RG8	$500*0,0866=43,3$	70
Segment 5	500m RG8	$500*0,0866=43,3$	70
<u>Summe</u>			506,5



IEEE802.3

Round Trip Delay Time 100 Mbit/s

Die 5-4-3 Regel funktioniert bei 100 Mbit/s nicht:

Die 10 fach höhere Datenrate führt zu einer entsprechend kürzeren Bitzeit

Nach IEEE802.3 ist mit folgenden Round Trip Delay Bitzeiten zu rechnen:

<u>Komponente:</u>	<u>Bitzeit:</u>	<u>Maximum:</u>
TP-Kabel	1,112 pro m	für 100m: 111,2
LWL	1,0 pro m	für 400m: 400
Repeater Kupfer/Kupfer	92	
Repeater Kupfer/LWL	140	

Auch hier darf die Summe für ein Netz 512 Bitzeiten nicht überschreiten.



IEEE802.3

Round Trip Delay Time

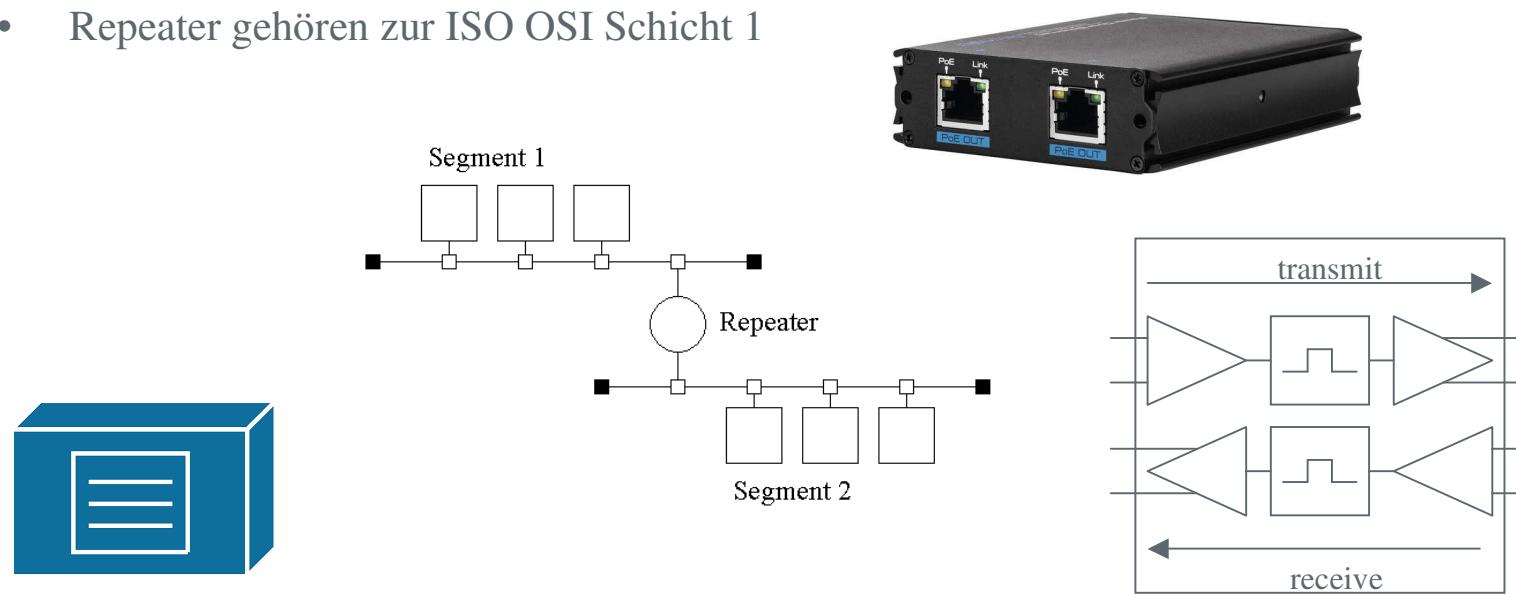
Fazit:

- Der CSMA/CD Entwurf und der Verzicht auf IEEE802.2 (Flußkontrolle und Quittierung) erfordert Kompromisse
- Sichere Kollisionserkennung ist nur unter bestimmten Bedingungen möglich
- Die Faktoren Lichtgeschwindigkeit im Medium, Datenrate, Mindestgröße Frame bestimmen die maximalen geometrischen Ausdehnungen einer Kollisionsdomäne
- Eine Sender muss die Kollision noch während der Sendung eines Frames erkennen
- Die Kabellänge und Netzwerkkomponenten haben Einfluß auf die Round Trip Delay Time
- Bei jedem Netz bis 100BaseTX muss die Round Trip Delay Time beachtet werden
- Bridge oder Switch unterbrechen die Kollisionsdomäne
- WLAN löst dass Problem auf andere Art (CSMA/CA)
- Ab 1000Base-T ist die Round Trip Delay Time irrelevant



IEEE802.3 Repeater

- Repeater verbinden Netzsegmente. Sie verstärken und regenerieren Signale
- Repeater haben 2 Ports
- Repeater können vollduplex betrieben werden
- Repeater leiten Kollisionen durch
- Repeater gehören zur ISO OSI Schicht 1



IEEE802.3

Medienkonverter

- Medienkonverter arbeiten wie Repeater
- Diverse Typen z.B. Kupfer-TP auf Koax oder Kupfer-TP auf LW
- Medienkonverter sollten vermieden werden (Latency)
- Auch als Module für Einschubschächte (GBIC, SFP, XFP)

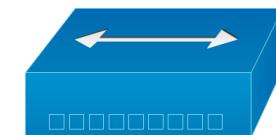


Quelle: de.wikipedia.org/wiki/Medienkonverter

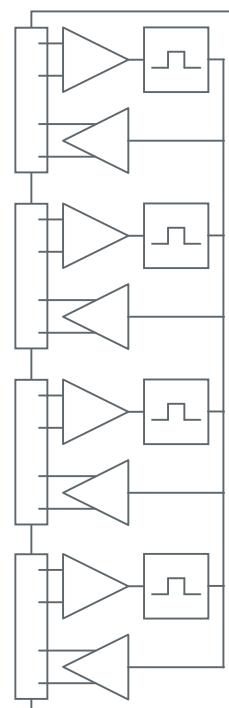
IEEE802.3

Hub

- Hubs verbinden mehrere Netzwerksegmente. Sie verstärken, regenerieren und verteilen Signale
- Hubs haben viele Ports
- Hubs leiten Kollisionen durch und arbeiten halbduplex
- Hubs haben intern eine Bustopologie trotz Sternverkabelung
- Hubs gibt es für 10 Mbit/s und 100 Mbit/s
- Hubs gehören auch zur ISO OSI Schicht 1



Small hub

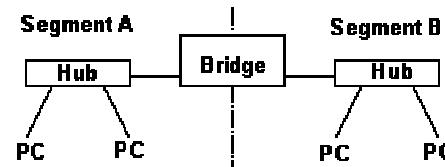


Quelle: [de.wikipedia.org/wiki/Hub_\(Netzwerktechnik\)](https://de.wikipedia.org/wiki/Hub_(Netzwerktechnik))

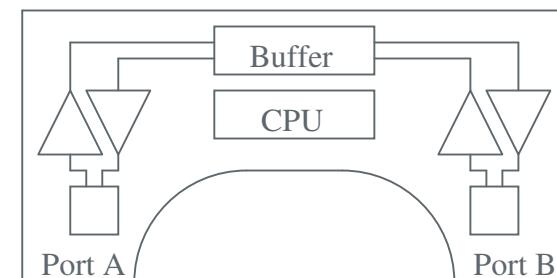
IEEE802.1D

Bridge

- Bridges verstärken und regenerieren Signale, vermitteln Frames
- Bridges verstehen Ethernetframes und MAC-Adressen
- Bridges können keine Kollisionen zwischen ihren Ports haben
- Bridges haben Empfangspuffer und trennen Kollisionsdomänen
- Bridges haben als Vorläufer der Switches nur wenige Ports
- Bridges filtern Ethernettraffic
- Bridges können die Datenrate anpassen
- Bridges koppeln Segmente
- Bridges gehören zur ISO OSI Schicht 2
- Bridges waren sehr teure Komponenten

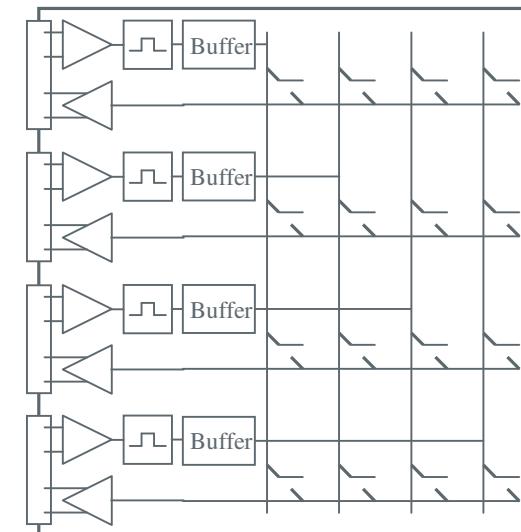
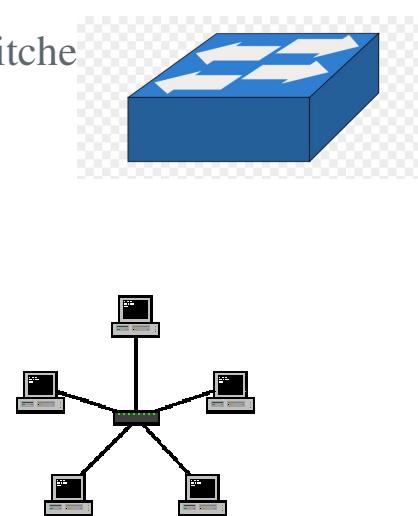


Bridge



IEEE802.1D Switch

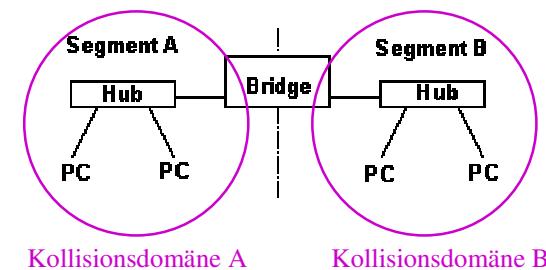
- Der Switch ist eine Multiportbridge und übernimmt alle Eigenschaften der Bridge
- Bridges sind zum Verbinden von Netzwerksegmenten vorgesehen, an Switches werden Endgeräte angeschlossen
- Switches sind in unterschiedlichen Ausführungen für unterschiedlichste Anforderungen erhältlich
- Switches ersetzen Hubs
- Ab 1000Base-T nur noch Switches
- Mikrokollisionsdomänen



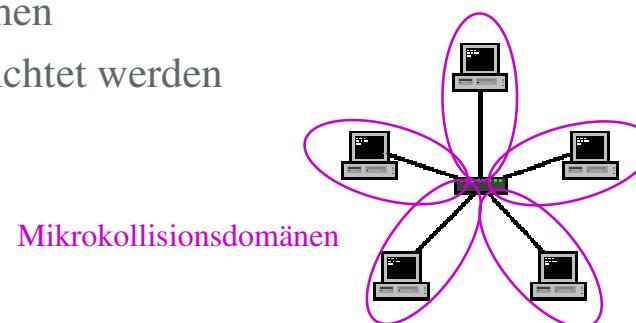
Quelle: en.wikipedia.org/wiki/Stackable_switch

Mikrokollisionsdomäne

- Bridges trennen Kollisionsdomänen, die Knoten beider Segmente können kommunizieren aber teilen die Kollisionen nicht
- CSMA/CD ist nötig
- Halbduplexbetrieb



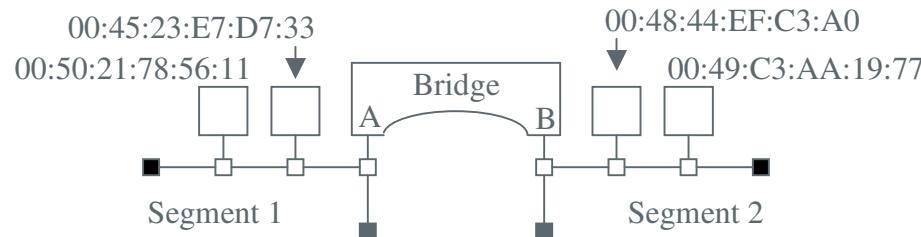
- Switches haben Mikrokollisionsdomänen
- Jeder Port bildet eine Kollisionsdomäne, allerdings können zwei Geräte alleine in einer Domäne keine Kollision verursachen
- Auf CSMA/CD könnte im Prinzip verzichtet werden
- Vollduplexbetrieb



Source Address Table

Transparent Switch

- In die Source Address Table trägt der Switch die MAC-Adressen aller Geräte ein
- Die Source Address Table dient dem gezielten Weiterleiten und Filtern der Frames
- Der Aging Wert gibt die Lebensdauer des Eintrags in Sekunden an
- Bei leerer Source Address Table leitet der Switch im Hub Mode Alles weiter
- Bei voller Source Address Table wird die Tabelle vollständig geleert

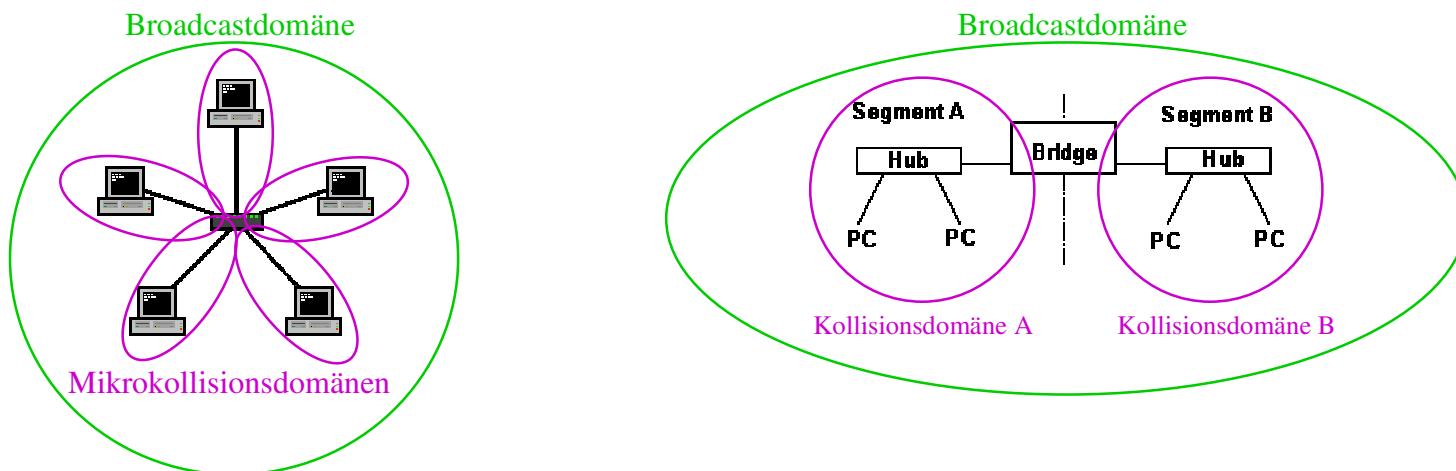


<u>MAC:</u>	<u>Port:</u>	<u>Aging</u>
00:50:21:78:56:11	A	300
00:45:23:E7:D7:33	A	300
00:48:44:EF:C3:A0	B	300
00:49:C3:AA:19:77	B	300



Broadcastdomäne

- Broadcastdomänen kennzeichnen die Reichweite von MAC-Adressen
- MAC-Adressen dienen Switchen zum Vermitteln von Ethernetframes
- Router verwenden keine MAC-Adressen, Broadcastdomänen enden hier
- Eine Broadcastdomäne kann mehrere Kollisionsdomänen enthalten
- Viele kleine LANs (SOHO) bestehen nur aus einer Broadcastdomäne



ISO OSI Referenzmodell

- Open Systems Interconnection Model
- 1984 von der ISO (International Telecommunication Union) veröffentlicht
- Jünger als aktuell verwendete Standards (NCP 1969, Ethernets 1973)
- Ein (nicht das) Schichtenmodell der Netzwerktechnik (7 Schichten)
- NICHT das Referenzmodell der aktuell im LAN und Internet verwendeten Netzwerktechnik
- Akademisches Modell mit Ausnahme einiger weniger Protokollimplementierungen in öffentlichen Telekommunikationsnetzen (ITU) und OSI Protokollen
- OSI Schichten heute Grundlage für die Zuordnung von Komponenten und Protokollen zu Schichten
- Beschreibung der OSI Schicht und der zugeordneten Protokolle und Komponenten können abweichen
- Nicht alle OSI Schichten mit realen Protokollen assoziierbar
- Schichten definieren Aufgaben im Sinne eines Konzeptes
- Schichten bzw. deren Realisierungen arbeiten zusammen



ISO OSI Referenzmodell

Schichten

Bezeichnung der Schichten:

<u>Englisch</u>	<u>Nummer</u>	<u>deutsche Bezeichnung</u>	<u>Beispiel</u>
Application Layer	7	Anwendungsschicht	HTTP, FTP, DNS, ...
Presentation Layer	6	Darstellungsschicht	-
Session Layer	5	Sitzungsschicht	-
Transport Layer	4	Transportschicht	TCP, UDP
Network Layer	3	Vermittlungsschicht	IP, ICMP
Data Link Layer	2	Sicherungsschicht	IEEE802.1D
Physical Layer	1	Bitübertragungsschicht	IEEE802.3

Fast alle Komponenten/Protokolle kann man den Schichten 1/2 und 7 zuordnen.



ISO OSI Referenzmodell Schichten

Physical Layer, 1:

- Technische Anbindung und Zugang zum Medium
- Elektrische Eigenschaften Kabel, Buchsen, Stecker, Signal
- Kodierung des Bitstroms zu einem Signal
- Erkennen und/oder Beheben von Bitfehlern und Kollisionen
- Art des Medienzugriffs (Multiplexing)

Data Link Layer, 2:

- Formt das Übertragungsmedium zu einem fehlerfreien Übertragungsweg
- Datenstrukturen für Datenpakete (Frames)
- Zugangssteuerung zum Medium
- Datenflußkontrolle
- Prüfsummen für Frames



ISO OSI Referenzmodell Schichten

Network Layer, 3:

- Verbindungen zwischen lokalen Netzen und Vermittlung von Paketen oder Kabelverbindungen in einem Netzwerkverbund
- Wegfindung (Routing)
- Bereitstellung eines Adressierungschemas für Netzwerkhosts
- Adaption unterschiedlicher Network Layer Protokolle (Tunneling)
- Host zu Host Kommunikation

Transport Layer, 4:

- Segmentierung der Datenströme
- Multiplexing der Datenströme
- Absicherung der Übertragung gegen Übertragungsfehler
- Adressierung der Dienste
- Ende zu Ende Kommunikation (App zu App)



ISO OSI Referenzmodell Schichten

Session Layer, 5:

- Verbindungsunabhängige Verwaltung von Sitzungen zwischen Prozessen
- Wiederherstellung von Sitzungen nach Abbruch mit Hilfe von Check Points
- In TCP/IP nicht realisiert

Presentation Layer, 6:

- Systemunabhängige Kodierung der Daten
- Verschlüsselung und Datenkompression
- In TCP/IP ebenfalls nicht implementiert

Application Layer, 7:

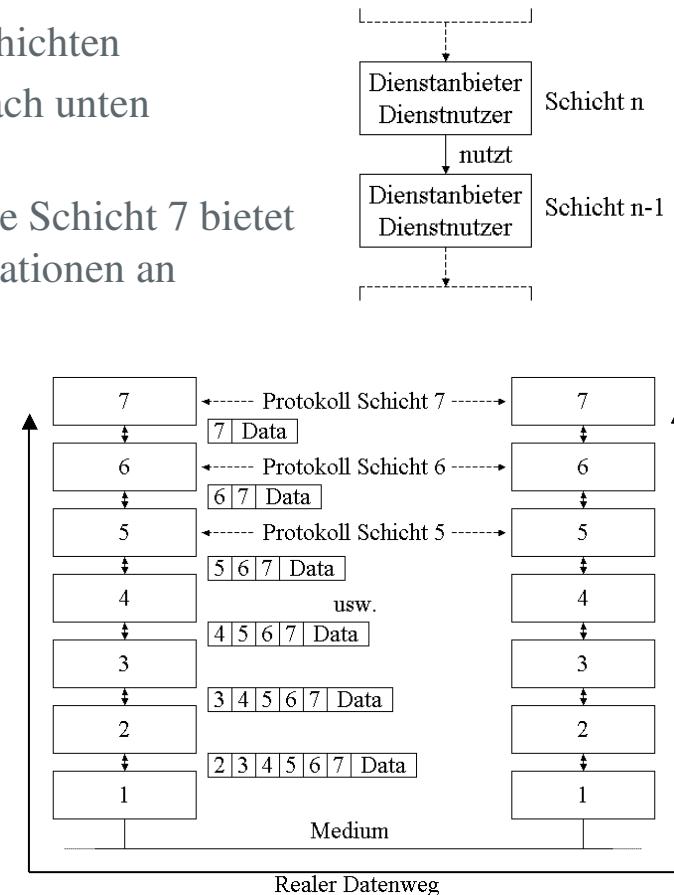
- Bereitstellung der Datenschnittstellen zum jeweiligen Prozess/Applikation die selbst aber nicht zum Application Layer gehören



ISO OSI Referenzmodell

Nutzung der Schichten

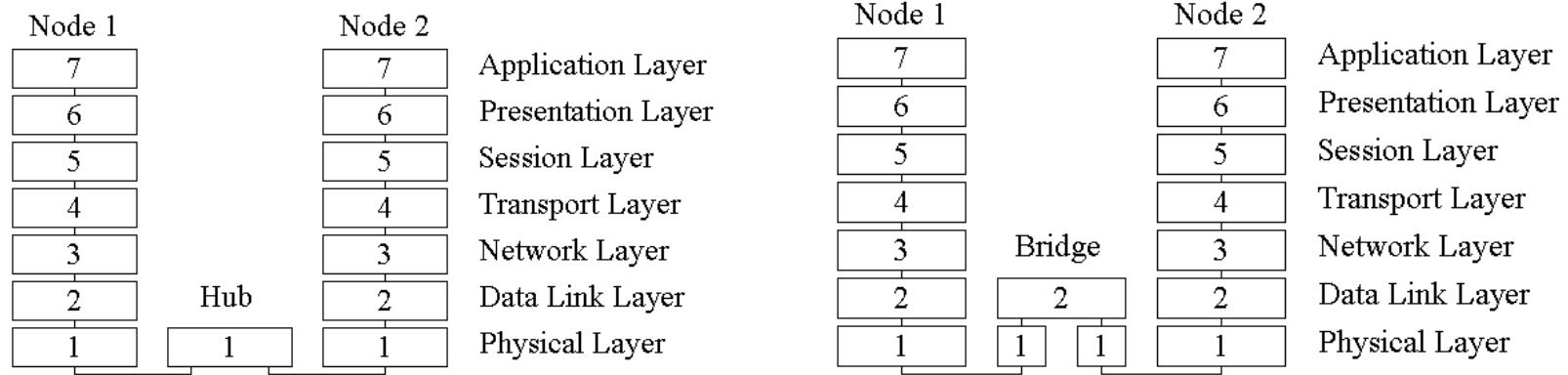
- Höhere Schichten nutzen Dienste der unteren Schichten
- Jede Schicht ist nach oben Dienstanbieter und nach unten Dienstnutzer
- Die Schicht 1 nutzte das Übertragungsmedium, die Schicht 7 bietet ihre Dienste unterschiedlichen Prozessen/Applikationen an
- Schichten setzen vor die Nutzdaten Protokollinformationen in Form von Headern
- Auf dem Weg durch den Stack "sammeln" sich die Header vor den Nutzdaten
- Die Header werden beim Empfänger auf dem Weg nach oben wieder entfernt
- Die Protokollinformationen sind für die korespondierende Schicht des Empfängers bestimmt



ISO OSI Referenzmodell

Hub und Bridge

Die Funktion von Hub und Bridge können wie folgt dargestellt werden:



- Hosts implementieren alle Layer des OSI Modells
- Das Übertragungsmedium ist von einem Hub oder Bridge unterbrochen
- Der Hub implementiert nur Aufgaben und Funktionen des OSI Layer 1
- Die Bridge kann auch die Funktionen des OSI Layer 2 übernehmen
- Der Datenfluß erfolgt bei der Bridge über Layer 2



RFC1122 TCP/IP Referenzmodell

RFC1122

Application Layer

Transport Layer

Internet Layer

Data Link Layer

ISO OSI

7, Application Layer

6, Presentation Layer

5, Session Layer

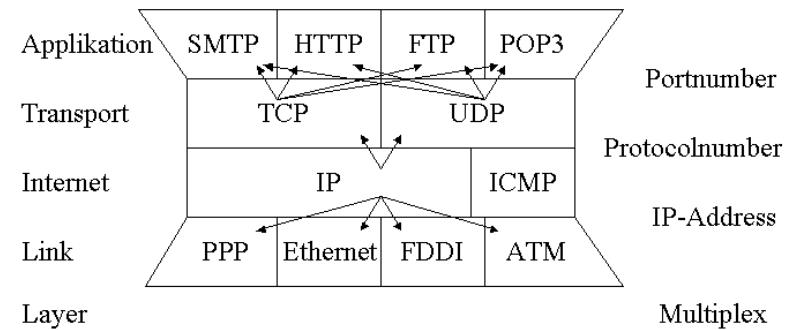
4, Transport Layer

3, Network Layer

2, Data Link Layer

1, Physical Layer

"Weinglasmodell":

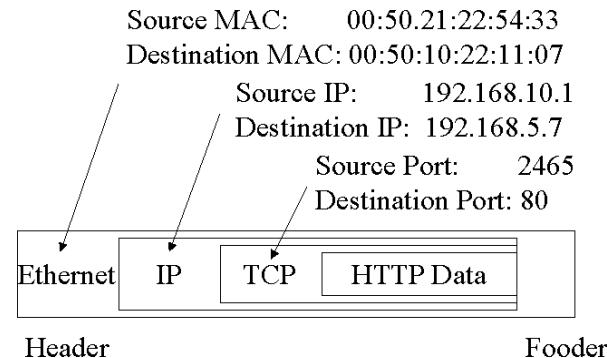


- Das TCP/IP Referenzmodell kennt nur 4 Schichten
- Die Zuordnung der ISO OSI Schichten ist (leider) akademisch veranlasst
- Die OSI Layer 5 bis 7 werden im Application Layer zusammengefasst
- Die OSI Layer 1 und 2 werden im Data Link Layer zusammengefasst



RFC1122 TCP/IP Referenzmodell

Auch im TCP/IP Referenzmodell werden Header vor die Nutzdaten gestellt:



- MAC Adressen gelten nur im lokalen Netz, der physische Netzwerkstandard des Data Link Layers ist auch nicht Gegenstand des TCP/IP Protokollstacks
- IP Adressen kennzeichnen die Schnittstelle des Hosts und das Netz
- Portnummern adressieren den Prozess/Dienst
- Das Dienstprotokoll, z.B. HTTP ist unabhängig von IP und TCP, nutzt diese aber



IP-Protokoll

Eigenschaften:

- Kommunikation über lokale Netze hinaus im Internet
- Hauptsächlich weltweit eindeutige Unicast Adressen
- Weitere Adressen für andere Adressierungsarten, z.B. Multicast, Broadcast usw.
- Zahlreiche Adressen für spezielle Aufgaben und Situationen (z.B. private Adressen)
- Es werden IP-Netze (Gruppe von zusammengehörigen Adressen) gebildet
- Unicast Adresse kennzeichnet Interface des Host **und** das Ziel IP Netz
- Zentrale Verwaltung der IP Adressen durch die IANA als Teil der ISOC
- Vergabe über eine Kette IANA -> Registry -> ISP -> Kunde
- IP Adressen kann man nicht "kaufen", sie sind zugeteilt (bis auf Widerruf)
- Typische Netzwerkkomponente für IP: Router
- IPv4 und IPv6 sind beide gebräuchlich, aber zwei inkompatible Protokolle
- IPv4 Adressraum und IPv6 Adressraum überschneiden sich nicht
- IPv4 Hosts können **nicht** mit IPv6 Hosts kommunizieren



IPv4 vs. IPv6

IPv4:

- 32 bit Adressen
- 4.294.967.296 Adressen
- Keine freien Unicast Adressen mehr verfügbar (außer Afrika)
- Über 80% des Internet Traffic

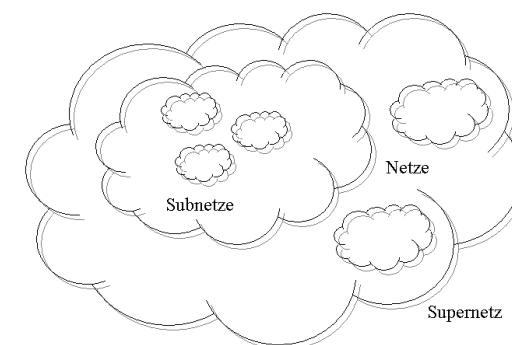
IPv6:

- 128 bit Adressen
- 340.282.366.920.938.463.463.374.607.431.768.211.456 Adressen
- IPsec im Standard integriert
- Kein NAT nötig
- Seit 1998 standardisiert aber immer noch Außenseiter



IP Netze

- Gruppen von zusammengehörigen IP Adressen bilden IP Netze
- IP Netze können zerlegt (Subnetting) und zusammengeführt (Supernetting) werden
- IP Netze werden zum Strukturieren von Netzen genutzt (Security und administrativ)
- IP Netze basieren rein auf der Vergabe der IP-Adressen (logische Netze)
- IP Netze setzen eine physische Vernetzung der Netzwerkhosts voraus
- IP Netze werden über Router verbunden und an das Internet angeschlossen
- IP Netze können unterschiedliche Größen haben
- Die Subnetzmaske bestimmt die Größe eines IP Netzes und teilt die IP Adresse
- IP Netze können als Wolke dargestellt werden
- Jeder Host kann mehrere IP Adressen haben
- Jeder Host kann zu mehreren IP Netzen gehören
- Jeder Host kann auch Router sein



Subnetzmaske

- Die Subnetzmaske teilt die IP Adresse in Netzadresse und Hostadresse (IPv4) bzw. Präfix und Interface Identifier (IPv6)
- Eine Subnetzmaske ist wie die IP Adresse eine Binärzahl und 32 bit bzw. 128 bit lang
- Eine 1 in der Subnetzmaske kennzeichnet das jeweilige Bit als Netzadresse bzw. Präfix, die 0 steht für die Hostadresse bzw. den Interface Identifier
- Einsen können nur von links (vom MSB) in die Subnetzmaske geschoben werden z.B. 1111 1111 1111 1111 0000 0000 0000
- Subnetzmasken werden bei IPv4 als Dotted Dezimal, wie IPv4 Adressen geschrieben ("255.255.240.0"), oder in der CIDR Schreibweise ("/20")
- In IPv6 ist nur noch die CIDR Schreibweise üblich ("/64")
- Die CIDR Schreibweise gibt die Anzahl der Einsen, also die Länge der Netzadresse bzw. des Präfix an
- Zu jeder IP Adresse gehört die Angabe der Subnetzmaske



Subnetzmaske IPv4

Unter der Angabe 192.168.17.33/24

Versteht man eine IPv4 Adresse, die sich aus der 24 bit langen Netzadresse 192.168.17.0 und der 8 bit langen Hostadresse .33 im vierten Oktett zusammensetzt.

Binär betrachtet lautet das wie folgt:

IP Adresse	1100 0000.1010 1000.0001 0001.0010 0001
Netzmaske	1111 1111.1111 1111.1111 1111.0000 0000
Netzadresse	<u>1100 0000.1010 1000.0001 0001.0000 0000</u> <u>24 bit Netz</u> <u>8 bit Host</u>

Wie man erkennt, ergibt sich die Netzadresse aus der bitweisen UND Verknüpfung von IP Adresse und Netzmaske.

Die Netzmaske kann alternativ auch als 255.255.255.0 geschrieben werden.



IPv4 Netz

Das Netz 192.168.17.33/24 hat folgenden Aufbau:

Netzadresse:	192.168.17.0	Anzahl IP Adressen:
Erste nutzbare HostAdresse:	192.168.17.1	$2^{(32-24)} = 2^8 = 256$
Letzte nutzbare HostAdresse:	192.168.17.254	Anzahl nutzbarer Hostadressen
BroadcastAdresse:	192.168.17.255	$2^{(32-24)} - 2 = 2^8 - 2 = 254$

- Die Netzadresse ist symbolisch. Sie steht für das gesamte IP Netz und kann nicht für die Adressierung von Hosts verwendet werden.
- Die Vergabe der verfügbaren Hostadressen ist völlig wahlfrei.
- Die BroadcastAdresse steht für alle Hosts des Netzes und kann folglich auch nicht für die Adressierung eines Hosts verwendet werden.
- Die erste Adresse im IP Netz ist immer die Netzadresse. -> alle Hostbits=0
- Die BroadcastAdresse ist immer die letzte IP Adresse des Netzes. -> alle Hostbits=1



RFC791

Struktur des IPv4 Adressraums:

Klasse:	Präfix:	Adressen:	Netzmaske:	Netze:
A	0...	0.0.0.0 – 127.255.255.255	255.0.0.0	128
B	10...	128.0.0.0 – 191.255.255.255	255.255.0.0	16.384
C	110...	192.0.0.0 – 223.255.255.255	255.255.255.0	2.097.152
D	1110...	224.0.0.0 – 239.255.255.255	Multicast	
E	1111...	240.0.0.0 – 255.255.255.255	reserviert	

Achtung: Die vorstehende Strukturierung ist veraltet. Heute gibt es nur noch die Klasse D und E. Alle anderen IP Adressen sind klassenlos, die Netzgröße individuell.

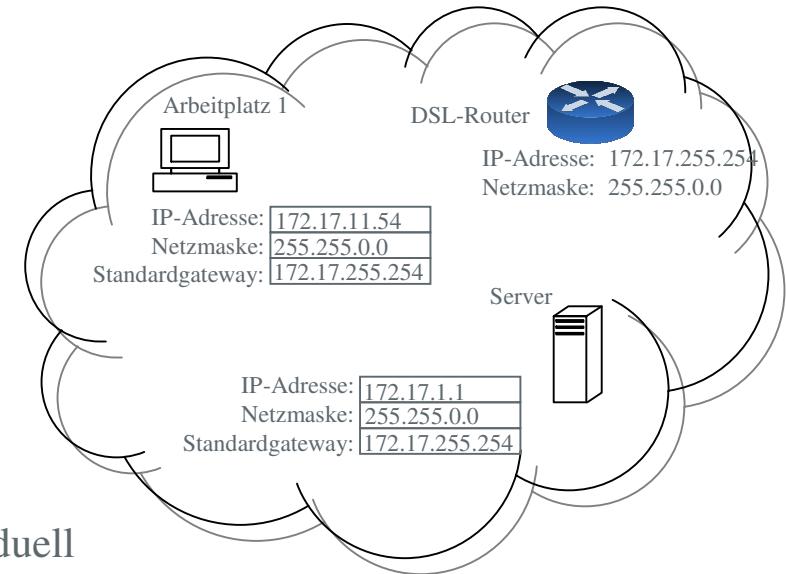
An dem binären Präfix konnte man ursprünglich die Netzgröße erkennen. Das gilt heute nicht mehr.



Konfiguration Host

Mindestangaben zur Netzwerkkonfiguration:

IP Adresse: 172.17.11.54
 Netzmaske: 255.255.0.0
 Standardgateway: 172.17.255.254



- Die IP Adresse kennzeichnet den Host individuell
- Die Netzadresse lautet: 172.17.0.0/16, ein früheres Klasse B Netz
- Die Broadcastadresse lautet 172.17.255.255/16
- Andere Hosts haben IP-Adressen zwischen 172.17.0.1/16 und 172.17.255.254/16
- Das Netz umfaßt 65.536 IP Adressen, davon sind 65.534 für Hosts nutzbar
- Das Standardgateway ist ein Router, über den alle anderen IP Netze erreichbar sind
- Ohne Router kann der Host nur mit Mitgliedern seines IP Netzes kommunizieren
- Ein Switch ist nicht gezeichnet, er wird vorausgesetzt (logische Sicht).

Sondernetze

Einige IPv4 Adressen sind für besondere Zwecke reserviert (Auwahl):

<u>Netz:</u>	<u>Adressumfang:</u>	<u>Verwendung:</u>	<u>Standard:</u>
0.0.0.0/0	0.0.0.0 bis 255.255.255.255	das Internet	
0.0.0.0/8	0.0.0.0 bis 0.255.255.255	das aktuelle Netz	RFC3232
10.0.0.0/8	10.0.0.0 bis 10.255.255.255	1 privates A-Netz	RFC1918
127.0.0.0/8	127.0.0.0 bis 127.255.255.255	Localnet (loopback)	RFC3330
127.0.0.1/32	127.0.0.1	Localhost (loopback)	RFC3330
169.254.0.0/16	169.254.0.0 bis 169.254.255.255	Zeroconf	RFC3927
172.16.0.0/12	172.16.0.0 bis 172.31.255.255	16 private B-Netze	RFC1918
192.168.0.0/16	192.168.0.0 bis 192.168.255.255	256 private C-Netze	RFC1918
224.0.0.0/4	224.0.0.0 bis 239.255.255.255	Multicast	RFC3171
240.0.0.0/4	240.0.0.0 bis 255.255.255.255	Reserviert	RFC3232
255.255.255.255/32	255.255.255.255	allgem. Broadcast	

Die Netzmaske "/0" kennzeichnet das gesamte Internet, "/32" kennzeichnet eine einzelne Adresse.



RFC1519

CIDR

- Der RFC1519 beschreibt das Classless Inter Domain Routing
- Aufhebung der starren Netzgrößen der Klasse A, B und C Netze
- Die Notation "/xx" gibt die Breite der Netzadresse in bit an und entspricht einer bestimmten Netzmaske in Dotted Dezimal Format.
- Alle CIDR Notationen von "/0" bis "/32" sind möglich, "/1" bis "/7" kommen in der Praxis nicht vor, die größten vergebenen IPv4 Netze sind "/8" (Klasse A) Netze
- Die Umwandlung eines "/xx" Wertes in das Dotted Dezimal Format erfolgt über eine 32 bit lange Binärzahl, die man in vier Oktette zerlegt und nach Dezimal wandelt.
- $\text{"/19" -> } \begin{array}{cccccc} 1111 & 1111 & 1111 & 1111 & 1110 & 0000 \\ \text{NM:} & \underbrace{255.} & \underbrace{255.} & \underbrace{224.} & 0 & \end{array}$
Netzgröße (IPs):
 $2^{(32-19)} = 2^{13} = 8192$
- $\text{"/25" -> } \begin{array}{cccccc} 1111 & 1111 & 1111 & 1111 & 1111 & 1000 \\ \text{NM:} & \underbrace{255.} & \underbrace{255.} & \underbrace{255.} & 128 & \end{array}$
Netzgröße (IPs):
 $2^{(32-25)} = 2^7 = 128$



Aufgaben:

Bestimmen Sie

- Anzahl IP Adressen
- Nutzbare Hostadressen
- Netzadresse
- Bereich Hostadressen
- Broadcastadresse
- Netzmaske in Dotted Dezimal

- a) 10.11.12.13/21
- b) 113.27.43.123/12
- c) 201.27.93.202/27



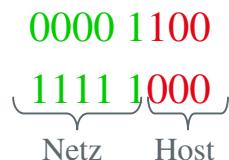
Lösung

Das Netz von 10.11.12.13/21 hat folgenden Aufbau:

Klassenloses Netz mit einer Netzadressbreite von 21 bit

IP 

Das 3. Oktett ist in Netz-, und Hostadresse geteilt und wird alleine binär betrachtet.

IP 

Die Wertigkeit 8 des Bit 3 gehört zur Netzadresse, das Bit 2 zur Hostadresse

Man setzt alle Hostbits auf 0, dann bleibt die Netzadresse stehen:

Netzadresse: 10.11.8.0/21

Netzmaske:

Erste nutzbare Hostadresse: 10.11.8.1/21

255.255.248.0

Letzte nutzbare Hostadresse: 10.11.15.254/21

Broadcastadresse: 10.11.15.255/21

Die Broadcastadresse erhält man, wenn alle Hostbits auf 1 gesetzt werden.

Anzahl IP Adressen:

$$2^{(32-21)} = 2^{11} = 2048$$

Anzahl Hostadressen

$$2^{(32-21)} - 2 = 2^{11} - 2 = 2046$$



Lösung

Das Netz von 113.27.43.123/12 hat folgenden Aufbau:

Klassenloses Netz mit einer Netzadressbreite von 12 bit

IP 

Anzahl IP Adressen:

$$2^{(32-12)} = 2^{20} = 1.048.576$$

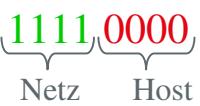
Anzahl Hostadressen

$$2^{(32-12)} - 2 = 2^{20} - 2 = 1.048.574$$

Das 2. Oktett ist in Netz-, und Hostadresse geteilt und wird alleine binär betrachtet.

IP 

Das 4. Bit mit der Wertigkeit 16 ist Netzadresse

NM 

Alle anderen gesetzten Bits sind Hostadresse

Man setzt alle Hostbits auf 0, dann bleibt die Netzadresse stehen:

Netzadresse: 113.16.0.0/12

Netzmaske:

Erste nutzbare Hostadresse: 113.16.0.1/12

255.240.0.0

Letzte nutzbare Hostadresse: 113.31.255.254/12

Broadcastadresse: 113.31.255.255/12

Die Broadcastadresse erhält man, wenn alle Hostbits auf 1 gesetzt werden.



Lösung

Das Netz von 201.27.93.202/27 hat folgenden Aufbau:

Klassenloses Netz mit einer Netzadressbreite von 27 bit

IP 

Das 4. Oktett ist in Netz-, und Hostadresse geteilt und wird alleine binär betrachtet.

IP 

Die Wertigkeit 128 und 64 gehört zur Netzadresse, der Rest zur Hostadresse

Man setzt alle Hostbits auf 0, dann bleibt die Netzadresse stehen:

Netzadresse: 201.27.93.192/27

Netzmaske:

Erste nutzbare Hostadresse: 201.27.93.193/27

255.255.255.224

Letzte nutzbare Hostadresse: 201.27.93.222/27

Broadcastadresse: 201.27.93.223/27

Die Broadcastadresse erhält man, wenn alle Hostbits auf 1 gesetzt werden.

Anzahl IP Adressen:

$$2^{(32-27)} = 2^5 = 32$$

Anzahl Hostadressen

$$2^{(32-27)} - 2 = 2^5 - 2 = 30$$



Subnetting

Elementar

IP Netze können zerlegt werden:

Das Netz 192.168.16.32/27 soll in zwei gleichgroße IP-Netze zerlegt werden:

- Die Netzmaske der neuen Netze ist /28 ausgehend von /27 des Ursprungsnetzes. Das ergibt sich zwingend aus der Netzgröße: $2^{(32-27)} = 2^5 = 32$ $2^{(32-28)} = 2^4 = 16$
- Das ist die einfachste Form der Zerlegung, die anders auch nicht möglich ist.
- Aus dem höchstwertigen Bit der Hostadresse des Ausgangsnetzes wird ein Netzadressbit der Zerlegungsnetze.

	1. Subnetz	2. Subnetz
Netzadresse	192.168.16.32/28	192.168.16.48/28
Erster Host	192.168.16.33/28	192.168.16.49/28
Letzer Host	192.168.16.46/28	192.168.16.62/28
Broadcast	192.168.16.47/28	192.168.16.63/28



Subnetting

Allgemein

Bei der Zerlegung eines IP-Netzes in mehr als zwei Netze entstehen immer 2^n gleichgroße Subnetze. Für die neue Netzmaske gilt alte Netzmaske + n.

Zerlegung von 113.16.0.0/12 in 6 Subnetze:

Eine Zerlegung in 6 gleichgroße Netze ist nicht möglich. Es müssen 8 Subnetze gebildet werden, n ergibt sich dann zu 3. Die neue Netzmaske ist /15 bzw. 255.248.0.0

Die binäre Darstellung des Ausgangsnetzes:

IP	<u>113.16.0.0/12</u>	Aufteilung 2. Oktett alt IP:	0001 0000
	12 bit Netz 20 bit Host	NM:	<u>1111 0000</u>
			Netz Host

Erstes Subnetz binär:

IP	<u>113.16.0.0/15</u>	Aufteilung 2. Oktett neu IP:	0001 0000
	15 bit Netz 17 bit Host	NM:	<u>1111 1110</u>
			Netz Host



Subnetting

Allgemein

Zerlegung von 113.16.0.0/12 in 6 Subnetze:

Die Berechnung der Subnetze kann mit Hilfe der Netzgröße erfolgen. $2^{(32-15)} = 2^{17} = 131.072$
 131.072 IPs kann auch geschrieben werden als 0.2.0.0 (256*256*2) Daraus ergibt sich die Schrittweite bei der Erstellung der Subnetze.

	Netzadresse	Broadcast	2. Oktett binär
1. Subnetz	113.16.0.0/15	113.17.255.255/15	0001 0000
2. Subnetz	113.18.0.0/15	113.19.255.255/15	0001 0010
3. Subnetz	113.20.0.0/15	113.21.255.255/15	0001 0100
4. Subnetz	113.22.0.0/15	113.23.255.255/15	0001 0110
5. Subnetz	113.24.0.0/15	113.25.255.255/15	0001 1000
6. Subnetz	113.26.0.0/15	113.27.255.255/15	0001 1010
7. Subnetz	113.28.0.0/15	113.29.255.255/15	0001 1100
8. Subnetz	113.30.0.0/15	113.31.255.255/15	0001 1110



Subnetting Beispiel

Zerlegung von 172.16.234.0/23 in 3 gleichgroße Subnetze:

- Nächste mögliche Zweierpotenz ist 4, also n=2
- Netzmaske alt /23, Netzmaske neu /25

$$2^{(32-23)} = 2^9 = 512$$

$$2^{(32-25)} = 2^7 = 128$$

			3. Oktett	4. Oktett
Ausgangsnetz	172.16.234.0/23	IP: NM:	1110 1010 0000 0000 1111 1110 0000 0000	
1. Subnetz	172.16.234.0/25	IP: NM:	1110 1010 0000 0000 1111 1111 1000 0000	
2. Subnetz	172.16.234.128/25	IP: NM:	1110 1010 1000 0000 1111 1111 1000 0000	
3. Subnetz	172.16.235.0/25	IP: NM:	1110 1011 0000 0000 1111 1111 1000 0000	
4. Subnetz IP	172.16.235.128/25	IP: NM:	1110 1011 1000 0000 1111 1111 1000 0000	



Subnetting

IPv6

- Das Subnetting von IPv6 funktioniert im Prinzip wie bei IPv4
- Kein Adressmangel bei IPv6, große Netze möglich
- Standardnetzmaske kleinstes Netz: /64, 64 bit Präfix, 64 bit Interface Identifier
- Vergabe wie IPv4 über eine Kette IANA -> Registry -> ISP -> Kunde
- Subnetting im Rahmen der Vergabekette und gegebenenfalls kundenseitig

Beispiel:

- 2001:0db8:85a3:08d3:**1319:8a2e:0370:7347** /64 Host im Kundennetz
- 2001:0db8:85a3:08d3:: /64 Netzadresse Segment Kunde
- 2001:0db8:85a3:0800::/56 IP Adresskreis Kunde
- 2001:0db8::/32 IP Adresskreis ISP
- 2001:0000::/22 IP Adresskreis Registry
- 2000::/3 IP Adresskreis Global Unicast



Zuweisung IP-Adresse

Möglichkeiten der IP Adresszuweisung:

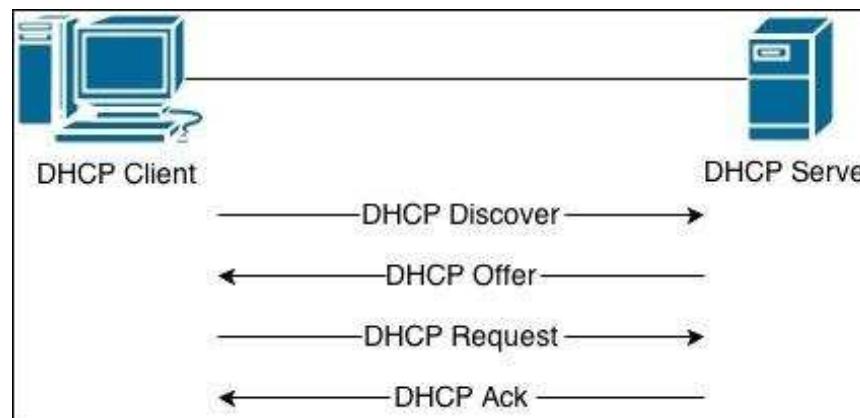
	IPv4:	IPv6:	Bemerkung:
Manuelle Zuweisung	ja	ja	
Autokonfiguration	ja	ja	bei IPv4 unüblich, bei IPv6 oft
DHCPv4 stateful	ja	nein	
DHCPv6 stateless	nein	ja	nur ergänzend, wenn nötig
DHCPv6 stateful	nein	ja	kommt nur selten zum Einsatz
Router	nein	ja	Präfix für Global Unicast
Ableitung von MAC	nein	ja	mit Privacy Extension
PPP	ja	ja	Point to Point Protocol



DHCP

Dynamic Host Configuration Protocol:

- Automatische Netzwerkkonfiguration eines Host (nicht nur IP-Adresse)
- Servergestützter Dienst, ergänzt durch Relay Agent auf Router
- Service stateful und stateless verfügbar, unterschiedliche Dienste IPv4, IPv6
- Verteilung von Optionen = Netzwerkeinstellungen wie z.B. Leasetime, IP Adresse, Netzmaske, Gateway, DNS Server IP, Domainname, Hostname, WINS Server usw.
- Kommunikation Broadcast per UDP und BOOTP



Quelle: geek-university.com/linux-deutsch/dynamische-tcp-ip-nummern-dhcp/

Private IP Adressen

Es sind drei IPv4 Bereiche als private Adressen definiert:

10.0.0.0/8	10.0.0.0 bis 10.255.255.255	1 privates Klasse A-Netz
172.16.0.0/12	172.16.0.0 bis 172.31.255.255	16 private Klasse B-Netze
192.168.0.0/16	192.168.0.0 bis 192.168.255.255	256 private Klasse C-Netze

- Private IP Adressen sind nicht eindeutig und können beliebig verwendet werden
- Private IP Adressen werden nicht im Internet geroutet
- Private IP Adressen sind ursprünglich für "nichtverbundene private Netze" gedacht
- Kein Internetzugang ohne NAT Router (Network Address Translation)
- IPv4 wäre ohne private IP Adressen heute nicht mehr verwendbar
- IPv6 hat vergleichbare Adressen: Link Local, Global Local Unique, Site Local usw.
- Hosts mit privaten IP Adressen sind nur eingeschränkt erreichbar (als Server)



NAT

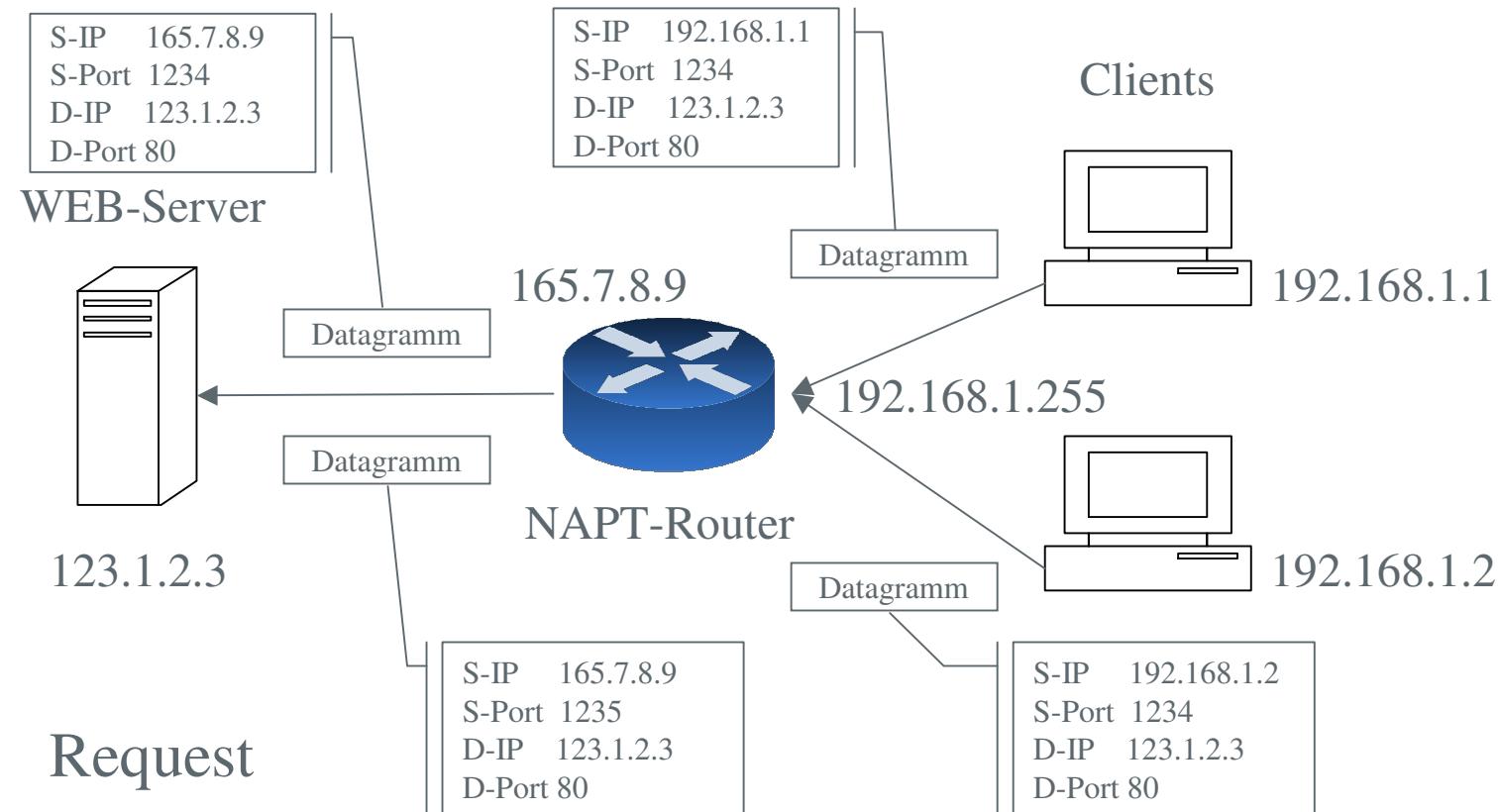
Network Address Translation ersetzt IP Adressen:

- NAT im LAN mit privaten Adressen wird auch als Source NAT bezeichnet
- Ursprünglich wurde jeder privaten IP Adresse auch eine öffentliche zugeordnet
- Heute wird allen privaten Adressen eines Netzes eine öffentliche IP zugeordnet
- NAT ist genaugenommen NAPT da auch die Portnummern ersetzt werden
- NAT ist stateful, es wird eine NAT Table benötigt
- Für das NAT ist das Standardgateway, üblicherweise DSL Router zuständig
- Es gibt Internetzugänge mit ISP seitigem Source NAT
- Probleme: Verbindungsaufbau in das LAN, Erreichbarkeit Server, IPsec, DNS
- Scheinsicherheit, NAT ist keine Firewall auch wenn Systeme hinter NAT Router nicht erreichbar sind
- Bei Protokollproblemen kann NAT-Traversal verwendet werden
- Serverseitiges NAT nennt man Destination NAT



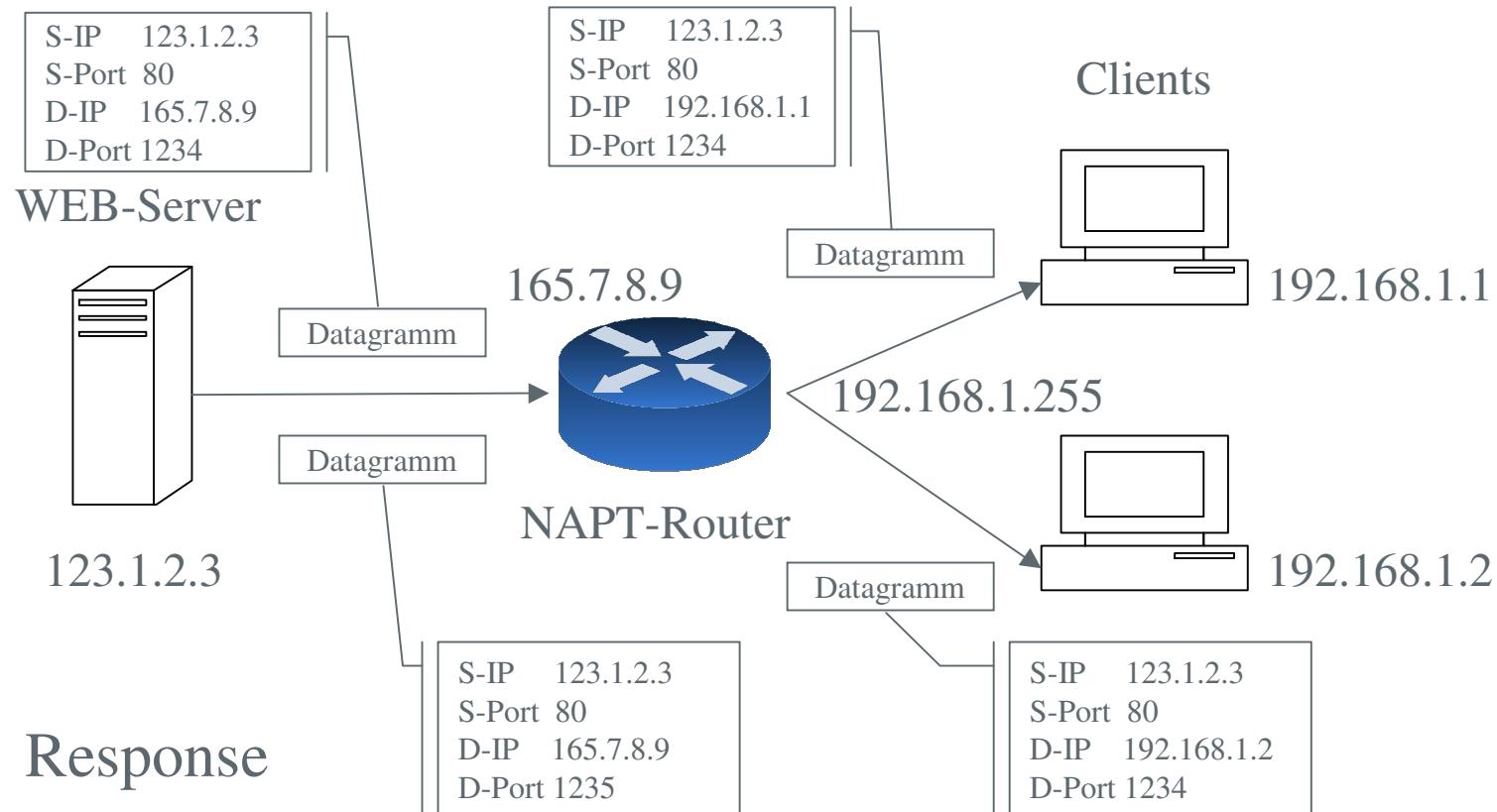
NAT

Beispiel Request



NAT

Beispiel Response



Response



Aufgaben:

Zerlegen Sie die folgenden Netzwerke:

- a) 22.22.20.0/22 in die größtmöglichen 5 Subnetze
- b) 192.168.80.0/20 in die max. mögliche Zahl von Subnetzen mit mind.
 1000 Host Adressen



Lösung:

Zerlegung von 22.22.20.0/22 in 5 größtmögliche Subnetze:

- Nächste mögliche Zweierpotenz ist 8, also n=3, die Netze sind dann zwangsläufig größtmöglich, 3 Netze bleiben ungenutzt
 - Netzmaske alt /22, Netzmaske neu /25
- $$2^{(32-22)} = 2^{10} = 1024$$
- $$2^{(32-25)} = 2^7 = 128$$

			3. Oktett	4. Oktett
Ausgangsnetz	22.22.20.0/22	IP:	0001 0100	0000 0000
		NM:	1111 1100	0000 0000
1. Subnetz	22.22.20.0/25	IP:	1110 1000	0000 0000
		NM:	1111 1111	1000 0000
2. Subnetz	22.22.20.128/25	IP:	1110 1000	1000 0000
3. Subnetz	22.22.21.0/25	IP:	1110 1001	0000 0000
4. Subnetz	22.22.21.128/25	IP:	1110 1001	1000 0000
5. Subnetz	22.22.22.0/25	IP:	1110 1010	0000 0000



Lösung:

Zerlegung von 192.168.80.0/20 in Netze mit Platz für 1000 Hostadr.:

- Nächste mögliche Netzgröße ist 1024, das ergibt 1022 nutzbare Hostadressen, also werden 10 Hostbits benötigt. Die Netzwerkmaske wird zu /22, es entstehen 4 neue Subnetze
- Netzmaske alt /20, Netzmaske neu /22 $2^{(32-20)} = 2^{12} = 4096$
- Die Netzgröße ist 1024 IP-Adressen, das kann man auch $2^{(32-22)} = 2^{10} = 1024$ als 0.0.4.0 (4x256) darstellen und damit rechnen

	Netzadresse	Broadcast	3. Oktett binär
Ausgangsnetz	192.168.80.0/20	192.168.95.255/20	0101 0000
1. Subnetz	192.168.80.0/22	192.168.83.255/22	0101 0000
2. Subnetz	192.168.84.0/22	192.168.87.255/22	0101 0100
3. Subnetz	192.168.88.0/22	192.168.91.255/22	0101 1000
4. Subnetz	192.168.92.0/22	192.168.95.255/22	0101 1100



Routing

Routing ist eine Funktion des ISO OSI Layer 3:

- Routing ist Teil der Layer 3 Protokolle
- Routing dient der Wegfindung zum Zielnetz
- Routing ist für die Kommunikation zwischen verbundenen Netzen nötig
- Routing wird nicht nur bei IP benötigt, auch wenn es z.Z. keine dem Internet vergleichbaren Netze gibt
- Routing benötigt Topologieinformationen der Netzwerkinfrastruktur
- Routing kann mit verschiedenen Algorithmen in verschiedenen Organisationsformen realisiert werden
- Routing ist statisch, dynamisch oder auch in Mischformen möglich
- Hostadressen sind für das Routing irrelevant, Routing basiert auf Netzadressen
- Forwarding, d.h. Weiterleiten von Daten ist Teil eines Layer 3 Protokolls aber kein Routing



Routing

statisch, dynamisch

Statisches Routing:

- Router haben feste, manuell vorgegebene Angaben zur Wegfindung und Routing (Routingtabelle)
- Änderungen sind nur durch manuellen Eingriff möglich
- Keine Reaktion auf Netzstörungen oder Veränderungen der Topologie
- Aufwändig und kostenintensiv, je größer das Netz und Anzahl der Router

Dynamisches Routing:

- Router benutzen Routingprotokolle um Routinginformationen auszutauschen
- Router passen sich geänderten Bedingungen an und können Störungen kompensieren
- Die Routingtabellen werden automatisch aktualisiert
- Routingverhalten kann durch Betreibervorgaben z.B. Kostenfaktoren gesteuert werden
- Zusätzliche Protokolle nötig, zusätzlicher Netzwerktraffic, steigende Komplexität



Routingverfahren

Distance Vector Routing

Distance Vector Routing ist ein dynamisches Routingverfahren:

- Router sammeln lokal Informationen, welche Nachbarnetze über welche Wege bzw. Router erreicht werden können. Lokale Sicht.
- Alle Wege werden mit einem Kostenfaktor "Metric" bewertet. Z.B. Zahl der Hops, Bandbreite der Leitung, Latency, Betreibervorgaben usw.
- Die Router tauschen die lokalen Routinginformationen untereinander aus
- Jeder Router berechnet für sich aufgrund der vorliegenden und erhaltenen Informationen die "kostengünstigsten" (kleinste Metric) Routen und benutzt diese
- Die eigenen Routinginformationen und deren Metric werden ständig mit den Nachrichten der Nachbarrouter aktualisiert und anschließend weitergegeben. Wege können sich ändern. Selbstorganisation des Routing.
- Die Aktualisierung der Routinginformationen aller Router kann sich verzögern, lokale Informationen abweichen und Störungen des Netzwerkverkehrs verursachen. Performance sinkt mit steigender Zahl der Router.
- Beispiele "Routing Information Protocol", "Interior Gateway Routing Protocol"



Routingverfahren

Link State Routing

Link State Routing ist ein dynamisches Routingverfahren:

- Das vollständige Netzwerk mit seiner Topologie und allen Eigenschaften wird in Datenbanken abgebildet
- Router tauschen Informationen aus, um diese Datenbanken aktuell zu halten
- Router haben nicht nur Kenntnis über die lokale Netzwerkumgebung. Globale Sicht
- Routingentscheidungen werden auf der Basis der Netzwerkdatenbanken getroffen
- Vielfältige Bedingungen können für die Routingentscheidung hinterlegt und berücksichtigt werden.
- Änderungen des Link State werden per "flooding" an alle Router weitergeleitet, sofortige Aktualisierung aller Datenbanken.
- Router überwachen die Verbindungen und Auslastung durch "hello" Pakete (Ping).
- Keine Konvergenzprobleme, unabhängig von der Netzwerkgröße und der Zahl der Router, aber hoher Traffic und Resourcenbedarf.
- Bewertung der Routen mittels Spannbaum (Graphentheorie)
- Beispiel: "Open Shortest Path First",



Routingverfahren

Hot/Cold Potatoe

Die Routingentscheidung in Providernetzen erfolgt auf unterschiedliche Weise:

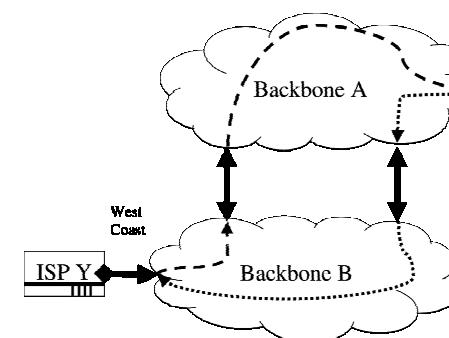
- Hot Potatoe

Datenpakete werden so schnell wie möglich in den Netzwerkverbund eines anderen Providers weitergeleitet. Die meisten Peers verhalten sich so u.a. um Kosten für die Datenübertragung zu sparen.

- Cold Potatoe

Datenpakete werden so lange wie möglich im eigenen Netzwerkverbund gehalten und erst spätestmöglich ausgeleitet. Das kann zusätzliche Kosten für Infrastruktur verursachen, gibt aber die Möglichkeit, z.B. auf die Dienstgüte (QoS) und Latency Einfluß zu nehmen.

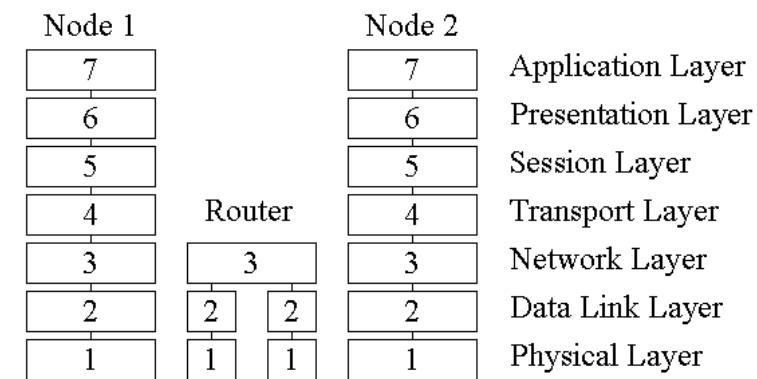
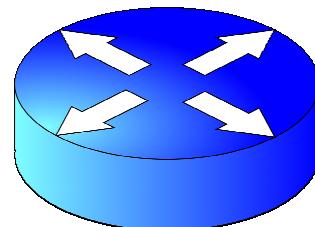
Entscheidend für das gewählte Verfahren sind die Ziele und Anforderungen des Netzbetreibers



IP-Router

IP-Router:

- IP-Router arbeiten wahlweise mit IPv4 oder IPv6 oder auch mit beiden Protokollen
- IP-Router haben deutlich weniger Netzwerkschnittstellen als Switches
- IP-Router müssen immer konfiguriert werden
- IP-Router sind Software auf einer Hardwareplattform
- Manche Kombigeräte, wie Fritzboxen, werden fälschlicherweise als Router bezeichnet
- Es gibt keine spezielle Routerhardware



IP-Routing

IP-Router haben zwei Aufgaben:

- | | |
|---------------|---|
| Wegfindung | Statisches Routing mit manuell erstellter Routingtabelle

Dynamisches Routing mit automatisierter Aktualisierung der Routingtabelle, aufgrund von Routingprotokollen |
| IP-Forwarding | IP-Pakete werden aufgrund der Einträge in der Routingtabelle weitergeleitet. Entscheidend dafür ist die Destination IP-Adresse.

Dabei können zwei unterschiedliche Situationen auftreten: <ol style="list-style-type: none">1. Der Zielrechner ist nicht über eine Routerschnittstelle erreichbar. D.h. der Router ist nicht mit dem Zielnetz verbunden und muß das IP-Paket an einen anderen Router weiterreichen.
Dazu verwendet er bei Ethernet die MAC-Adresse dieses Routers.2. Der Zielrechner ist in einem der mit dem Router verbundnen IP-Netze. Dann ermittelt der Router die MAC-Adresse des Zielhost und leitet das IP-Paket direkt an den Empfänger weiter. Nur in diesem Fall ist die IP-Hostadresse von Bedeutung. |



Routingtabelle

Die Routingtabelle ist fester Bestandteil des IP-Protokolls:

- Jeder Netzwerknoten, der eine IP-Adresse hat, hat auch eine Routingtabelle
- In der Routingtabelle stehen Ziele (IP-Netze oder einzelne Adressen) und der Weg zu den Zielen, d.h. ein weiter Router oder das direkt verbundene IP-Netz
- Routingtabellen können mehrdeutig sein, es sind mehrere Wege zum Ziel möglich
- Routingtabellen müssen den IP-Adressraum nicht vollständig abdecken
- Mehrdeutigkeiten werden über die Metric, kleinste Metric zuerst, entschieden
- Die Reihenfolge der Einträge spielt keine Rolle
- Die Routingtabelle spiegelt die logische Netzwerktopologie
- Routingtabellen haben, je nach Hersteller, unterschiedliche Formate
- Die Routingtabelle können in der Shell angezeigt werden.
- IPv4 und IPv6 haben eigene unabhängige Routingtabellen
- WIN-CMD: route print
- Linux Shell: ip route show oder netstat -r



Routingtabelle

IPv4

Eine Windows7 IPv4 Routingtabelle:

IPv4-Routentabelle						
Aktive Routen:						
Netzwerkziel	Netzwerkmaske	Gateway	Schnittstelle	Metrik		
0.0.0.0	0.0.0.0	192.168.34.1	192.168.34.12	10		
127.0.0.0	255.0.0.0	Auf Verbindung	127.0.0.1	306		
127.0.0.1	255.255.255.255	Auf Verbindung	127.0.0.1	306		
127.255.255.255	255.255.255.255	Auf Verbindung	127.0.0.1	306		
192.168.34.0	255.255.255.0	Auf Verbindung	192.168.34.12	266		
192.168.34.12	255.255.255.255	Auf Verbindung	192.168.34.12	266		
192.168.34.255	255.255.255.255	Auf Verbindung	192.168.34.12	266		
224.0.0.0	240.0.0.0	Auf Verbindung	127.0.0.1	306		
224.0.0.0	240.0.0.0	Auf Verbindung	192.168.34.12	266		
255.255.255.255	255.255.255.255	Auf Verbindung	127.0.0.1	306		
255.255.255.255	255.255.255.255	Auf Verbindung	192.168.34.12	266		

- Netzwerkziel und Netzwerkmaske kennzeichnen zusammen das mögliche Ziel eines IP-Pakets. CIDR ist bei WIN unüblich
- Unter Gateway wird die IP-Adresse des nächsten Hop eingetragen, wenn das Ziel nicht direkt über eine Schnittstelle erreichbar ist, ansonsten "Auf Verbindung"
- Unter Schnittstelle wird die IP-Adresse der lokalen Schnittstelle eingetragen, über die das IP-Paket weitergeleitet wird. 127.0.0.1 bedeutet, dass der Rechner selbst Ziel des Routing (=Empfänger) ist.

Routingtabelle

IPv4

Eine Windows7 IPv4 Routingtabelle:

IPv4-Routentabelle						
Aktive Routen:						
Netzwerkziel	Netzwerkmaske	Gateway	Schnittstelle	Metrik		
0.0.0.0	0.0.0.0	192.168.34.1	192.168.34.12	10		
127.0.0.0	255.0.0.0	Auf Verbindung	127.0.0.1	306		
127.0.0.1	255.255.255.255	Auf Verbindung	127.0.0.1	306		
127.255.255.255	255.255.255.255	Auf Verbindung	127.0.0.1	306		
192.168.34.0	255.255.255.0	Auf Verbindung	192.168.34.12	266		
192.168.34.12	255.255.255.255	Auf Verbindung	192.168.34.12	266		
192.168.34.255	255.255.255.255	Auf Verbindung	192.168.34.12	266		
224.0.0.0	240.0.0.0	Auf Verbindung	127.0.0.1	306		
224.0.0.0	240.0.0.0	Auf Verbindung	192.168.34.12	266		
255.255.255.255	255.255.255.255	Auf Verbindung	127.0.0.1	306		
255.255.255.255	255.255.255.255	Auf Verbindung	192.168.34.12	266		

- Ziel 0.0.0.0, Maske 0.0.0.0 kennzeichnet die Defaultroute - Standardgateway
- 127.0.0.0 ist das lokalnet (in der Größe eines Klasse A Netzes)
- 127.0.0.1 ist der localhost (loopback Adresse)
- Ziel 192.168.34.12, Maske 255.255.255.255 kennzeichnet die eigene IP-Adresse
- Ziel 224.0.0.0, Mask 240.0.0.0 ist der Multicastbereich, Klasse D
- Ziel 255.255.255.255, Mask 255.255.255.255 ist die allgemeine Broadcastadresse

Routingtabelle IPv6

Eine Windows7 IPv6 Routingtabelle:

```
IPv6-Routentabelle
=====
Aktive Routen:
If Metrik Netzwerkziel           Gateway
  1   306 ::1/128                Auf Verbindung
  11  266 fe80::/64              Auf Verbindung
  11  266 fe80::ad64:c954:bcde:4d9b/128
                                Auf Verbindung
  1   306 ff00::/8               Auf Verbindung
  11  266 ff00::/8               Auf Verbindung
=====
```

- Dieser Rechner ist nicht im IPv6 Internet (Keine Global Unicast Adresse)
- ::1/128 ist der localhost (loopback Adresse)
- fe80::/64 ist der Bereich der Link Local Adressen
- fe80::ad64:c954:bcde:4d9b/128 ist die Link Lokal Adresse des Host
- ff00::/8 ist der Bereich der Multicast Adressen (Der Host hat keine Multicast Adresse)
- Wenn man das IPv6 Protokoll abschaltet, verschwindet die Routingtabelle

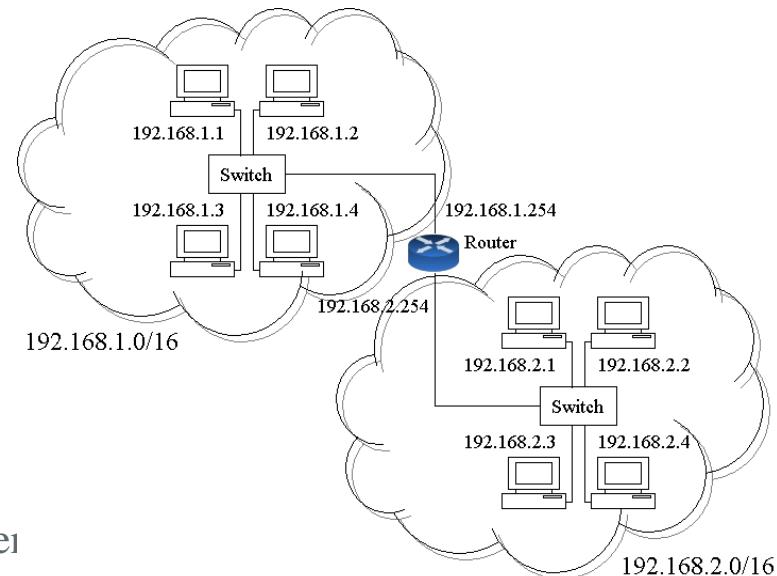


Routingtabelle Beispiel

Beispielnetz:

Eine Default Route ist nicht notwendig.
 Es ist keine Anbindung an das Internet
 Vorhanden.

Die Routingtabelle wird nicht manuell erstellt.
 Der Router kennt die verbundenen Netze schon
 aus der Konfiguration der Netzwerkschnittstelle



Ziel	Netzmaske	Gateway	Schnittstelle	Metrik
192.168.1.0	255.255.255.0	-----	192.168.1.254	1
192.168.2.0	255.255.255.0	-----	192.168.2.254	1

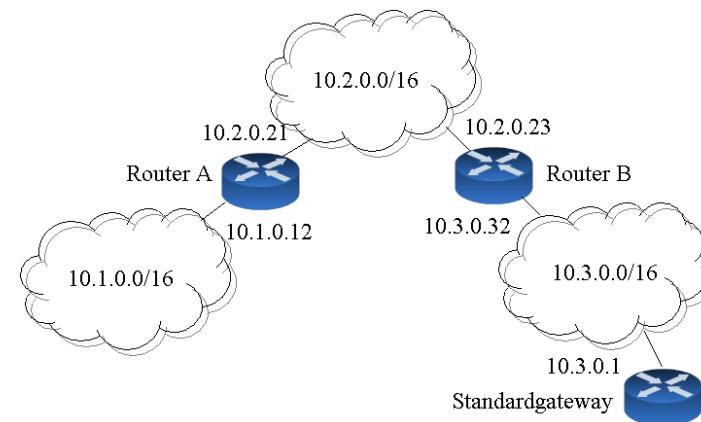


Routingtabelle

Beispiel

Beispielnetz:

Es gibt Netze, die nicht direkt mit allen Routern verbunden sind. Um diese Netze bekannt zu machen muss man manuell statische Routen nachtragen oder ein Routingprotokoll aktivieren.



Router A:

Ziel	Netzmaske	Gateway	Schnittstelle	Metrik
10.1.0.0	255.255.0.0	-----	10.1.0.12	1
10.2.0.0	255.255.0.0	-----	10.2.0.21	1
10.3.0.0	255.255.0.0	10.2.0.23	10.2.0.21	2
0.0.0.0	0.0.0.0	10.2.0.23	10.2.0.21	3



Routingtabelle Beispiel

Beispielnetz:

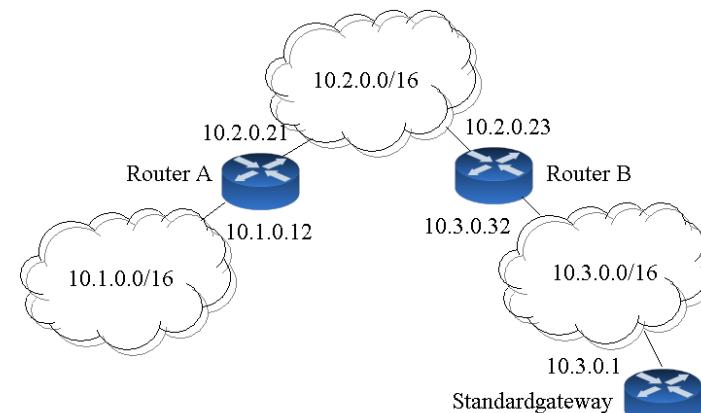
Jeder Router muss individuell konfiguriert werden.

Die Metrik gibt die Zahl der Hops bis zum Ziel an.

Netzwerkplan und Routingtabelle beschreiben die Topologie gleichwertig.

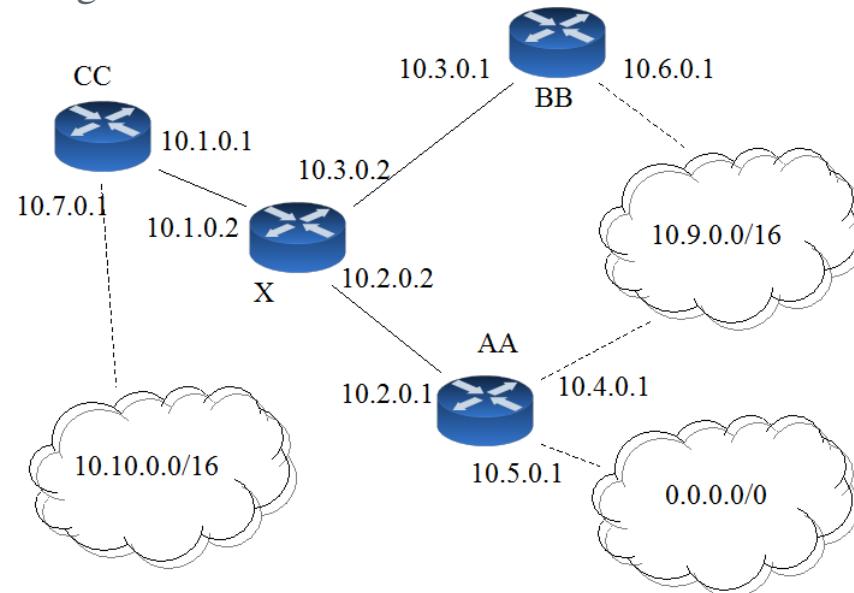
Router B:

Ziel	Netzmaske	Gateway	Schnittstelle	Metrik
10.1.0.0	255.255.0.0	10.2.0.21	10.2.0.23	2
10.2.0.0	255.255.0.0	-----	10.2.0.23	1
10.3.0.0	255.255.0.0	-----	10.3.0.32	1
0.0.0.0	0.0.0.0	10.3.0.1	10.3.0.32	2



Aufgabe:

Erstellen Sie die Routingtabellen für Router X:



Hinweis: Der Netzwerkplan ist unvollständig hinsichtlich der Verbindungen auf den gestrichelten Linien. Dies ist für Router X unerheblich. Allerdings müssen die Netze 0.0.0.0, 10.9.0.0, 10.10.0.0 erreichbar sein.



Lösung:

Die Routingtabelle für Router X:

Die Netzmasken muss man anhand der IP-Adressen sinnvollerweise zu /16 annehmen

Ziel	Netzmaske	Gateway	Schnittstelle	Metrik
10.1.0.0.	255.255.0.0	-----	10.1.0.2	1
10.2.0.0	255.255.0.0	-----	10.2.0.2	1
10.3.0.0	255.255.0.0	-----	10.3.0.2	1
10.4.0.0	255.255.0.0	10.2.0.1	10.2.0.2	2
10.5.0.0	255.255.0.0	10.2.0.1	10.2.0.2	2
10.6.0.0	255.255.0.0	10.3.0.1	10.3.0.2	2
10.7.0.0	255.255.0.0	10.1.0.1	10.1.0.2	2
10.9.0.0	255.255.0.0	10.2.0.1	10.2.0.2	3
10.9.0.0	255.255.0.0	10.3.0.1	10.3.0.2	3
10.10.0.0	255.255.0.0	10.1.0.1	10.1.0.2	3
0.0.0.0	0.0.0.0	10.2.0.1	10.2.0.2	4

