



Datenkommunikation über Ethernet

Alfred Läßle

Leibniz-Rechenzentrum

Barer Str. 21, 80333 München

Tel: (089) 289-28706, E-Mail: laepple@lrz.de

<http://www.lrz-muenchen.de/services/schulung/dvseminar/vortraege>

Gliederung



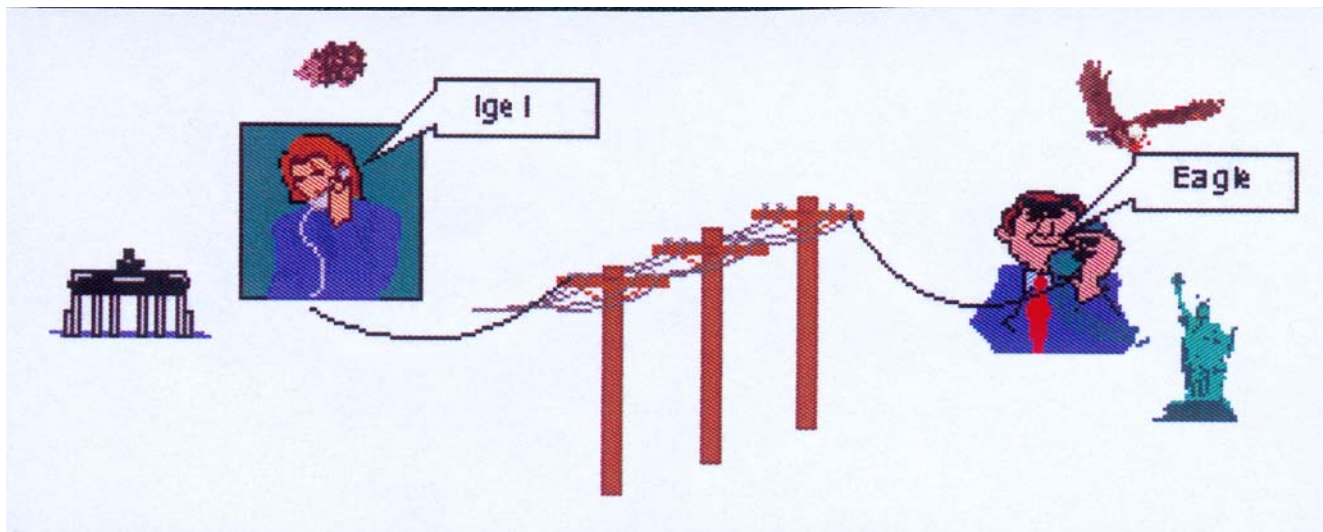
- Grundlagen**
- Strukturierte Verkabelung**
 - Normen, Bereiche
 - Medien
- Ethernet**
- Verbindungskomponenten**
 - Switches
 - Router
- TCP/IP**
 - Einordnung in Schichtenmodell
 - Protokolle der Schicht 3, IP-Adressen
 - Protokolle der Schicht 4, Ports
- VLANs**
- Literatur**

Grundlagen

Kommunikation

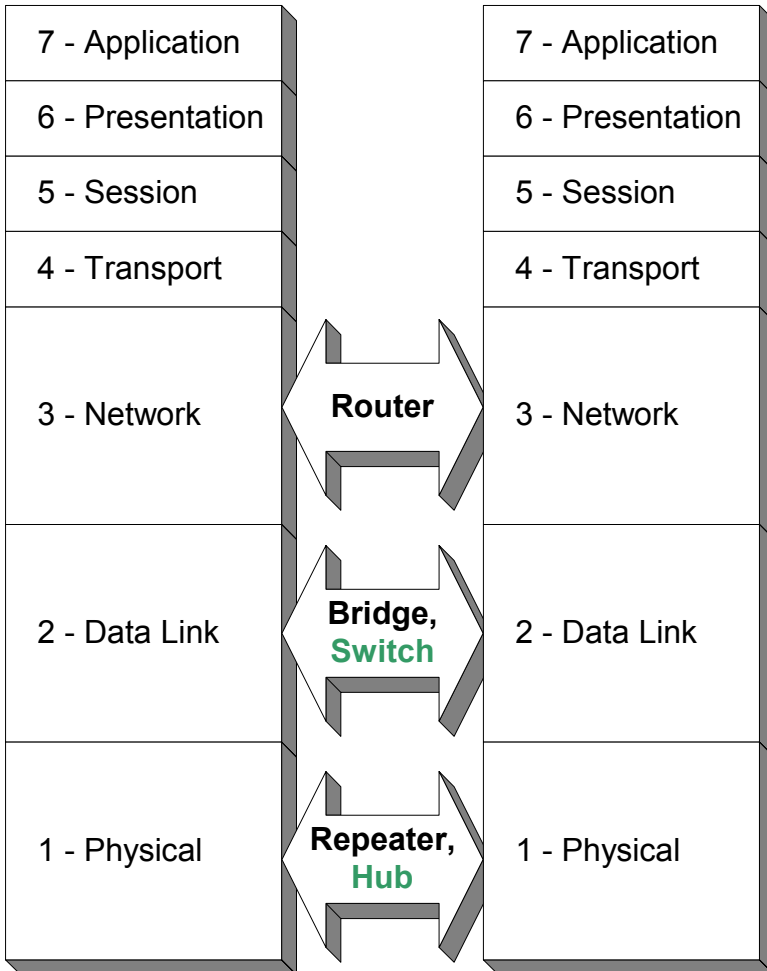


- ❑ Netze sind Verbindungssysteme, an die Teilnehmer zum Zweck der Kommunikation angeschlossen sind
- ❑ Kommunikation zwischen zwei Partnern bedarf Regeln
 - ❑ Kompatible Schnittstellen (Hardware)
 - ❑ Art und Weise des Informationsaustausches (= Protokolle)
- ❑ Festlegung von Schnittstellen und Protokollen durch Normen oder Standards
- ❑ Die reine Verbindung ist nicht gleich Kommunikation

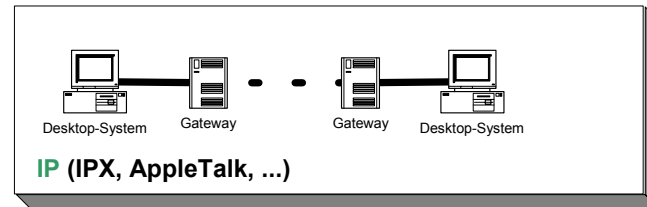


Grundlagen

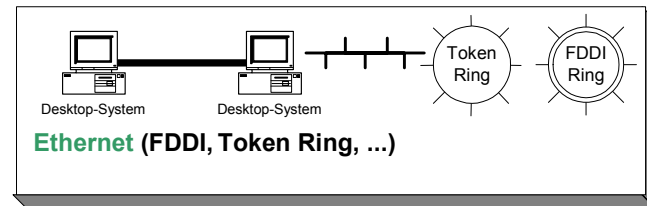
OSI-Modell



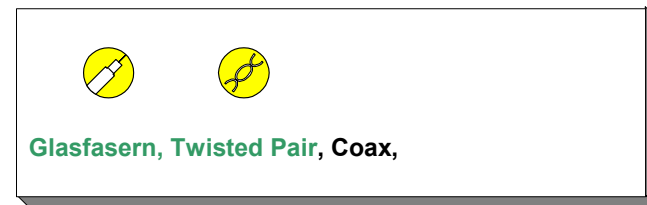
Dialog der Anwenderprogramme
 Darstellung/Codierung
 Kommunikationssteuerung
 Transportfunktion



Paket-Vermittlung



Sicherungsschicht



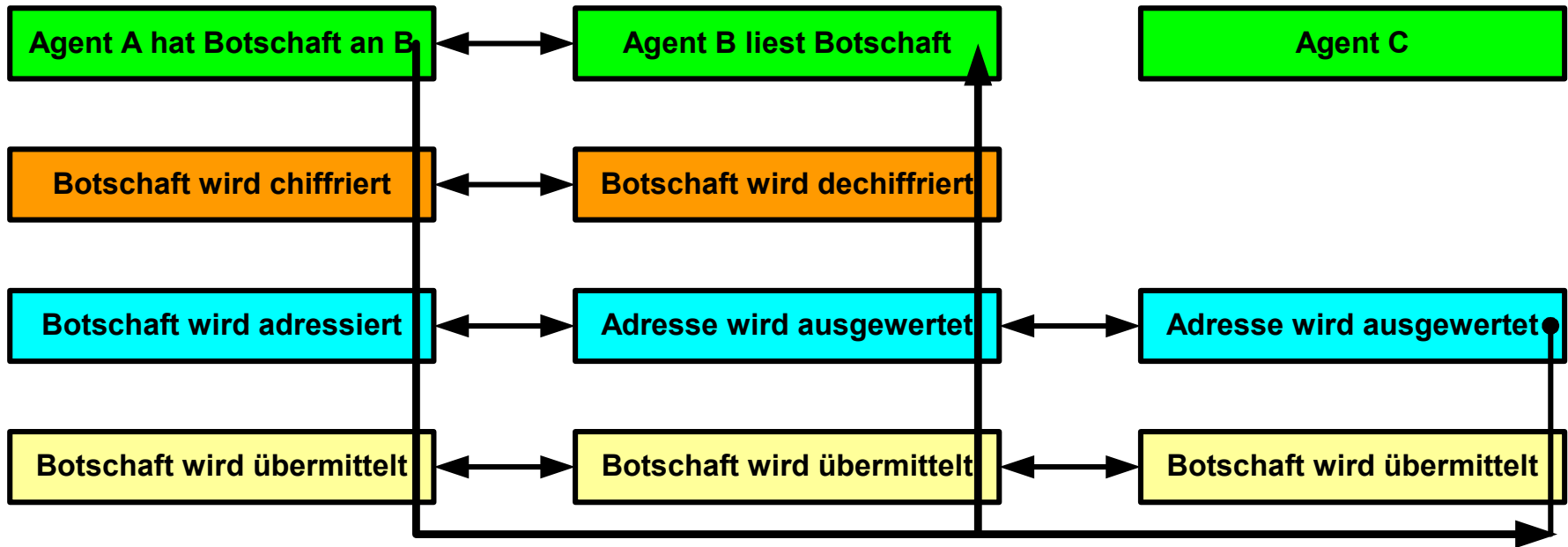
Bitübertragung

Grundlagen

Veranschaulichung Schichtenmodell



Agent A will verschlüsselte Botschaft zum Agenten B senden



Kommunikation in Schichten

Komme sofort → **Bleibe immer** → **Bleibe immer in Bonn** →

Geheimdienstchef sagt: Bleibe immer in Bonn

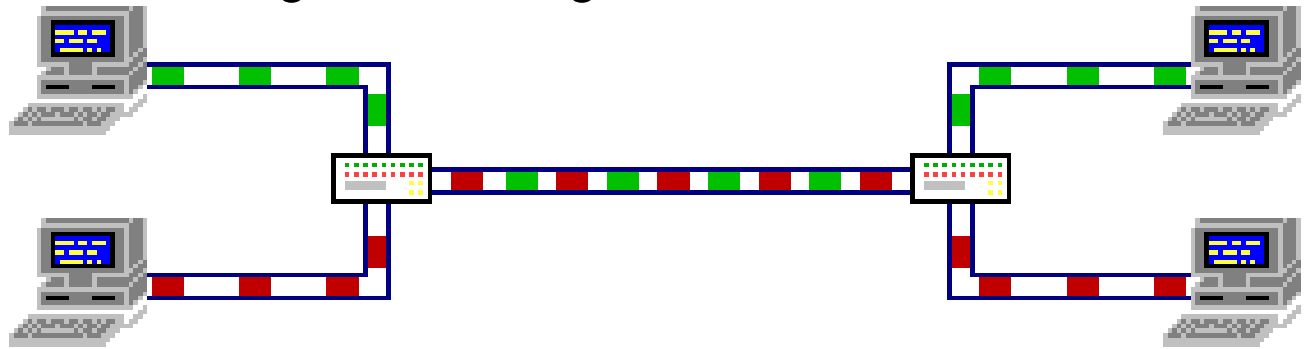
Grundlagen

Paket- versus Leitungsvermittlung



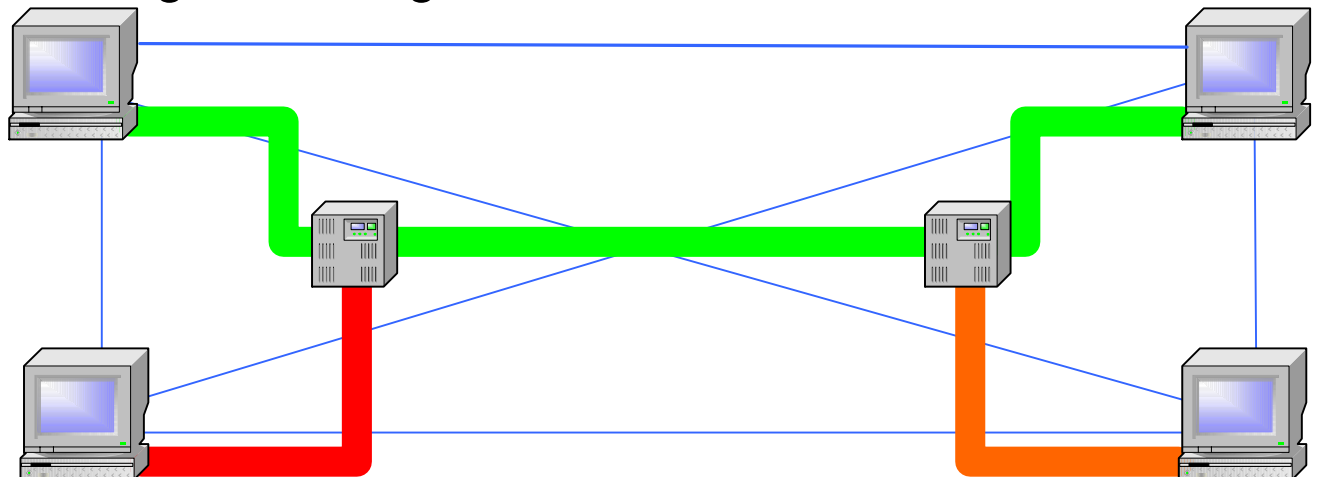
Paketorientiert

Gemeinsame Ausnutzung von Leitungen



Leitungsorientiert

Blockierung bei belegter Leitung



Strukturierte Verkabelung

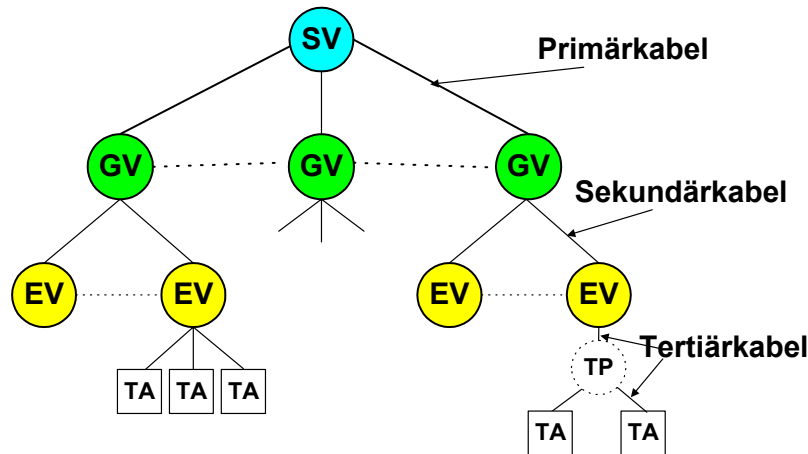
Normen



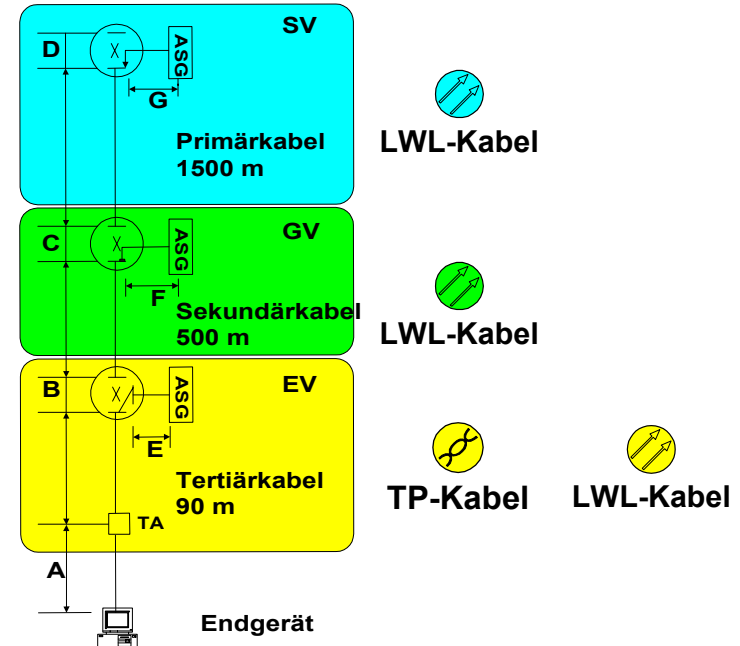
- Netztechnik hat sich an genormte Verkabelung anzupassen**
- Flächendeckend**
 - Jeder Arbeitsplatz hat eigenen Datenanschluss
- Normen**
 - EN 50173 (Europa)
 - ISO/IEC 11801 (Weltweit)
 - EIA/TIA 568 A/B (Nordamerika)
- Bereiche**
 - Primärbereich:** stellt die gebäudeübergreifende Verkabelung zwischen Gebäuden auf einem Gelände (Campusbereich) dar.
 - Sekundärbereich:** umfasst die Verbindungen zwischen dem zentralen Hauptverteiler bzw. Gebäudehauptverteiler und den Bereichsverteilern.
 - Tertiärbereich:** deckt die Verbindungen zwischen den Bereichsverteilern und den Netzendpunkten (Anschlussdosen am Arbeitsplatz) ab
- Hierarchische physische Sternstruktur**

Strukturierte Verkabelung

Prinzip



SV Standortverteiler
GV Gebäudeverteiler
EV Etagenverteiler
TP Kabelverzweiger (optional)
TA Informationstechnische
Anschlußdose



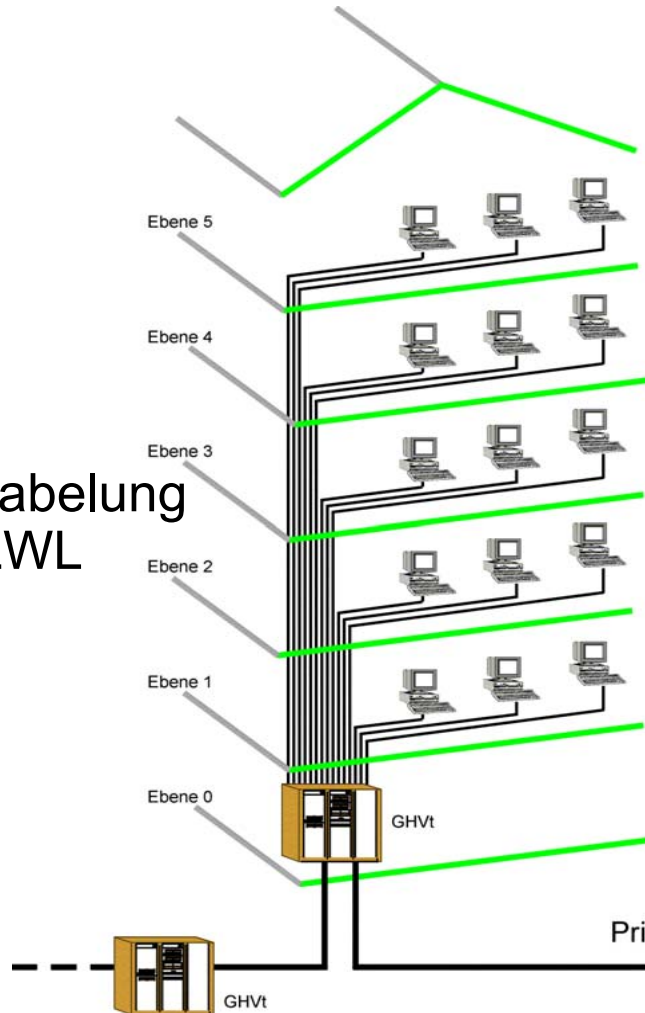
- Das richtige Kabel ist nicht alles, aber ohne das richtige Kabel ist alles ...
- Die richtige Struktur ergibt eine zukunftssichere Basis

Strukturierte Verkabelung

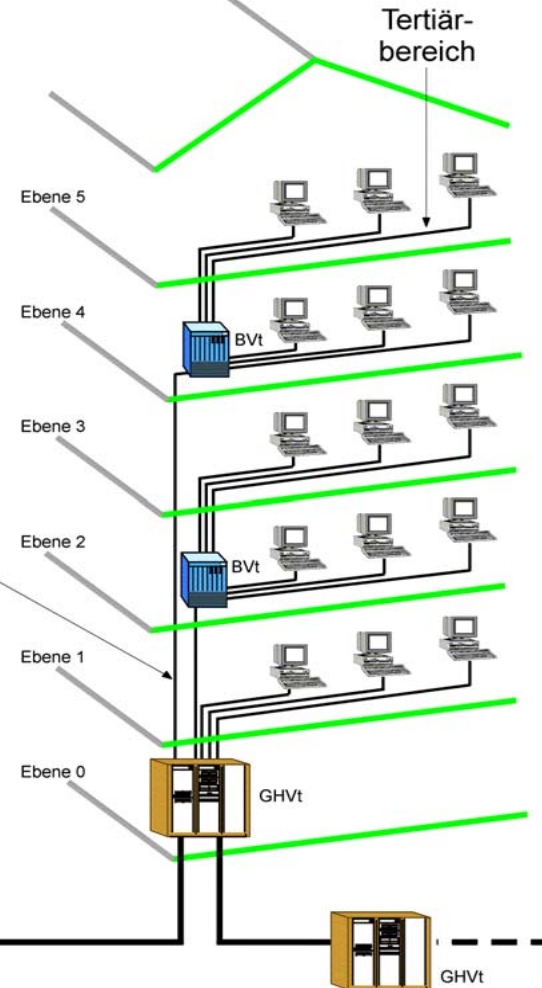
Schema



Verkabelung
mit LWL



Sekundär-
bereich



Verkabelung
mit Kupfer

Strukturierte Verkabelung

Kabelmedium Kupfer



- Kupferadern (0,5 – 0,6 mm)
 - paarweise verdrillt
 - Kabelaufbau
 - S/STP-Kabel
 - S/UTP-Kabel
- EMV-Problematik
 - elektromagnetische Störungen
 - gut geschirmte Kabel
- 2 Aderpaare pro Anschluss
- 4 Aderpaare bei 1000 Mbit/s-Ethernet



Dose



RJ45-Stecker

S/UTP-Kabel



Gesamtschirm aus Folie und Kupfergeflecht

Cat 5 100 MHz

S/STP-Kabel



Paarschirm aus Folie und Gesamtschirm aus Kupfergeflecht

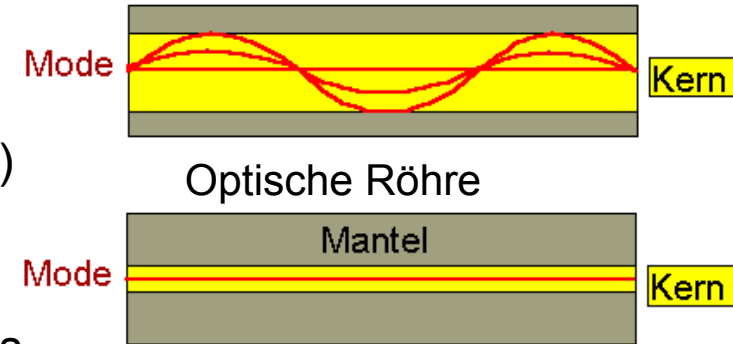
bis Cat 7 und 1200 MHz

Strukturierte Verkabelung

Kabelmedium Glas



- Multimode
 - 50/125 μ (Europa)
 - 62.5/125 μ (Nordamerika)
 - Länge ohne Verstärkung : ca. 2 km (10 Mb/s)
- Monomode
 - 9/125 μ
 - Länge ohne Verstärkung : ca. 40 km (10 Mb/s)
- Optische Fenster (Dämpfung gering)
 - 850 nm
 - 1310 nm
 - 1550 nm
- Kabelaufbau
 - Vollader (Patchkabel)
 - Bündelader (Spleißboxen)
- keine EMV-Problematik
- kleinere Kabeldurchmesser
- 2 Fasern pro Verbindung



Strukturierte Verkabelung

Vergleich Draht und Glas



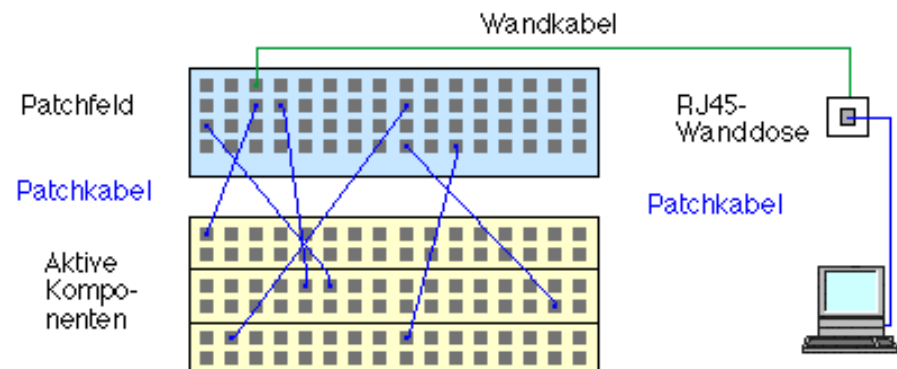
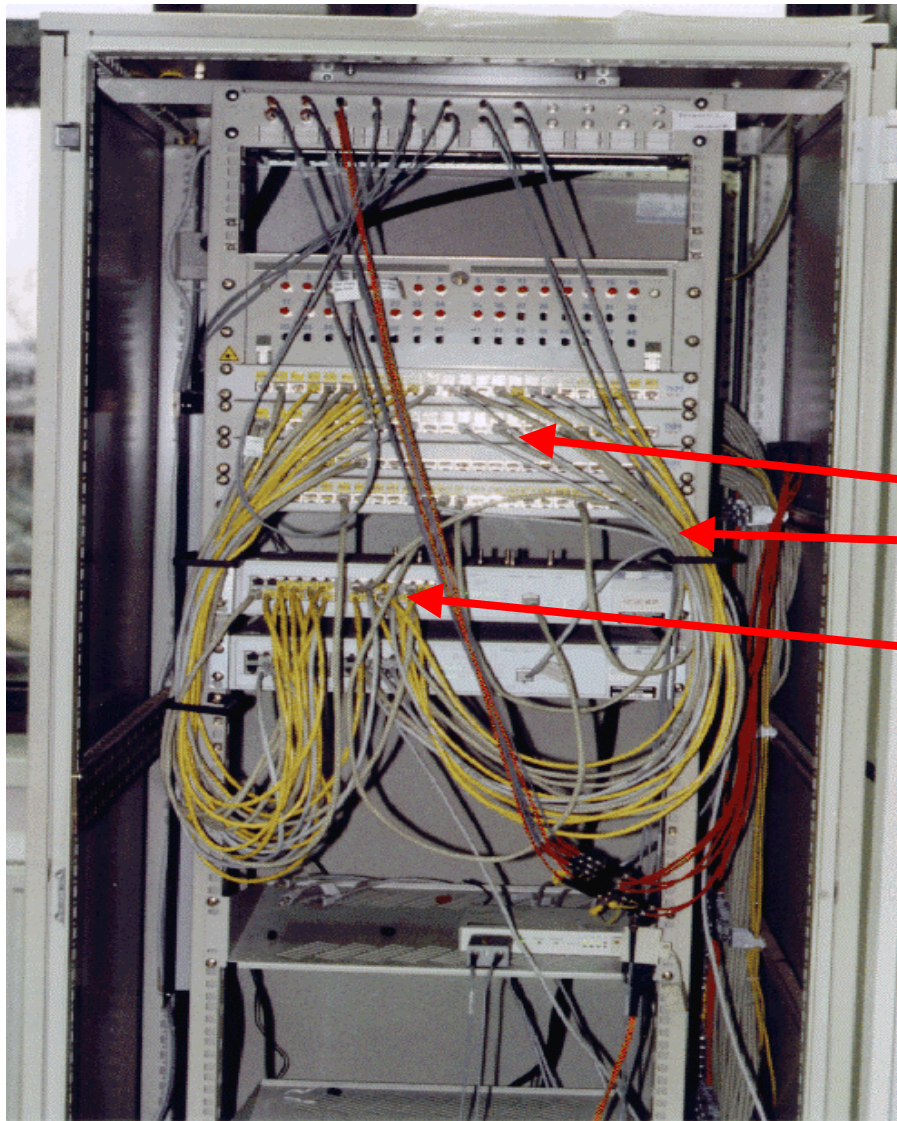
	<i>Draht</i>	<i>Glas (MM)</i>	<i>Glas (SM)</i>
Längenbeschränkung	0	+	++
Bandbreiten	0	+	++
Größe der notwendigen Kabelkanäle	-	+	+
Anzahl der Verteilerstandorte	-	+	+
Brandlast	-	+	+
Kosten der aktiven Komponenten	+	-	--
Verfügbarkeit aktiver Komponenten	+	-	--

Allgemeine Meinung :

- Glas ist zukunftssicherer
- in der Regel aber wesentlich teurer (pro Anschluss bis € 300)
- Kupfer kann Strom leiten

Strukturierte Verkabelung

Beispiel Etagenverteiler

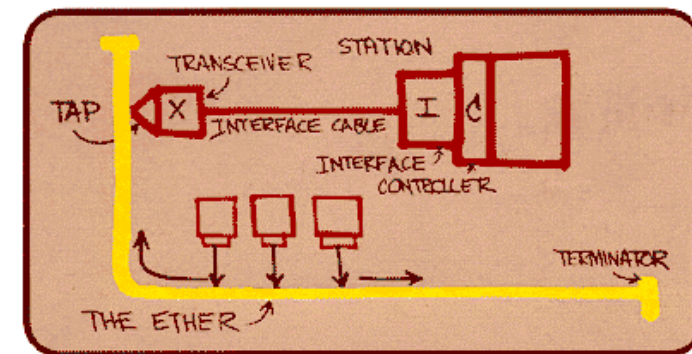


Ethernet

Grundlagen



- ❑ Intel, DEC, Xerox 1980 Ethernet V1.0
- ❑ Ethernet ist **die** Netztechnologie
 - ❑ im LAN (Lokal Area Network) fast absolut
 - ❑ im MAN (Metropolitan Area Network) zum Teil
 - ❑ und bald im WAN (Wide Area Network)
- ❑ Ethernet hat Erweiterungen erfahren bezüglich
 - ❑ Übertragungsgeschwindigkeit
 - ❑ 10 Mbit/s
 - ❑ 100 Mbit/s
 - ❑ 1000 Mbit/s (1 Gbit/s)
 - ❑ 10 Gbit/s (bald)
 - ❑ Übertragungsmedium (Koax, **Glas, Twisted Pair**)
 - ❑ Übertragungsverfahren (vollduplex)
- ❑ **stabile Schnittstelle**
 - ❑ gleiches Frameformat
 - ❑ gleiches Zugriffsverfahren (CSMA/CD)



Zeichnung von Metcalfe

(1976)

Ethernet

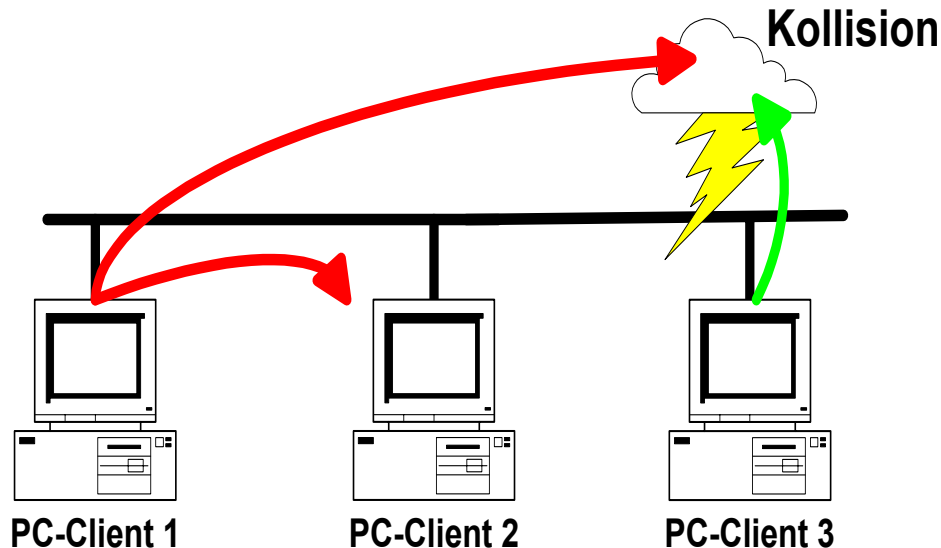
Einsatzbereiche



Ü-Rate	Bezeichnung	Medium	Einsatzbereich	„Spitzname“
1 Mbit/s	1 Base-5	Kupfer-Kabel	veraltet	StarLAN
10 Mbit/s	10 Base-5	Koax-Kabel	veraltet	Yellow Cable
10 Mbit/s	10 Base-2	Koax-Kabel	veraltet	Cheapernet
10 Mbit/s	10 Base-T	Kupfer-Kabel CAT 3	Arbeitsplatz	Twisted Pair
10 Mbit/s	10 Base-F	LWL-Kabel	Arbeitsplatz	Fibre Optics
100 Mbit/s	100 Base-T	Kupfer-Kabel CAT 5 (4)	Arbeitsplatz, Server	Fast Ethernet
100 Mbit/s	100 Base-X	LWL-Kabel	Arbeitsplatz, Server	Fast Ethernet
1000 Mbit/s	1000 Base-X	LWL-Kabel	Server, Backbone	Gigabit-Ethernet
1000 Mbit/s	1000 Base-T	Kupfer-Kabel CAT 5 (8)	Server	Gigabit-Ethernet
10 Gbit/s	10000 Base-X	LWL-Kabel	Backbone	10 Gigabit-Ethernet

CSMA/CD Medien-Zugangsprotokoll

- ❑ Medium (Kabel) kann nur von einer Station verwendet werden
- ❑ einzelne Stationen wechseln sich ab mit Senden
- ❑ wollen zwei Stationen gleichzeitig senden, kommt es zur **Kollision**



Nicht mehr relevant
bei Switches und
strukturierter
Verkabelung
voll duplex

Senden PC1 und PC3 gleichzeitig
kommt es zur Kollision

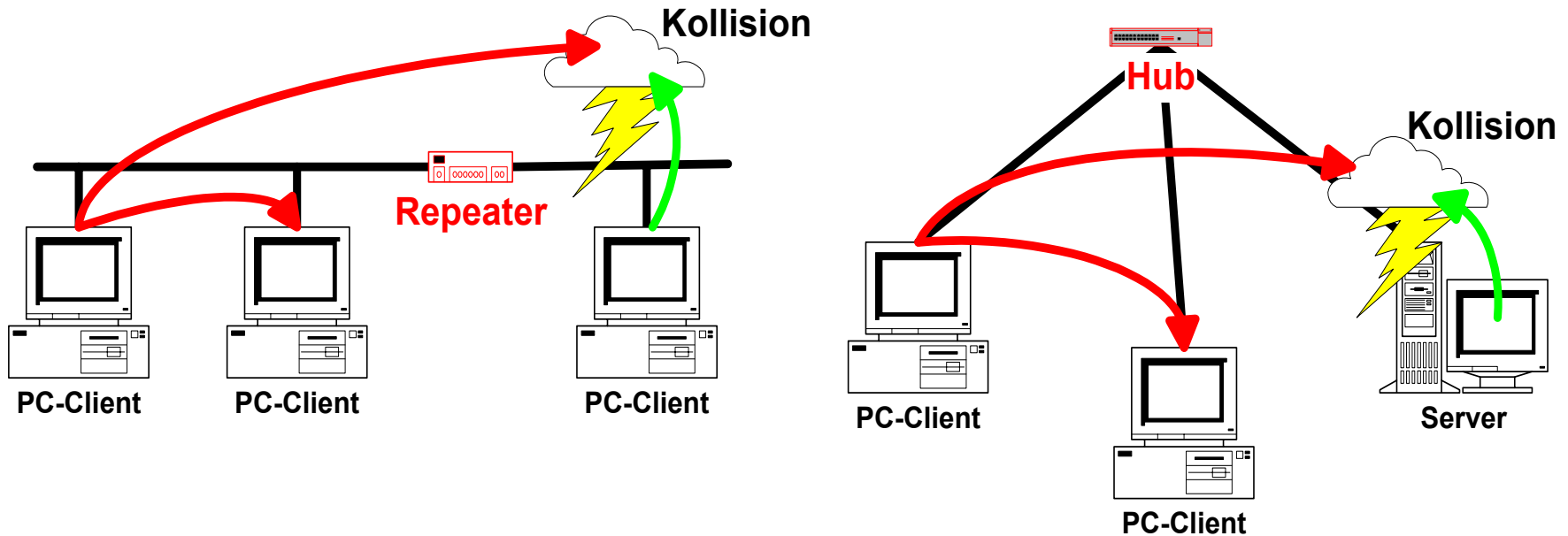
Verbindungskomponenten

Repeater und Hubs (OSI-Schicht 1)



Prinzip: Signalverstärkung (bitserielle Weitergabe)

- ❑ Aufhebung von Beschränkungen
- ❑ elektrische Fehler werden separiert
- ❑ verbindet unterschiedliche physikalische Medien



Kollisionen werden nicht verhindert



HUB und Repeater sind Auslaufmodelle

Verbindungskomponenten

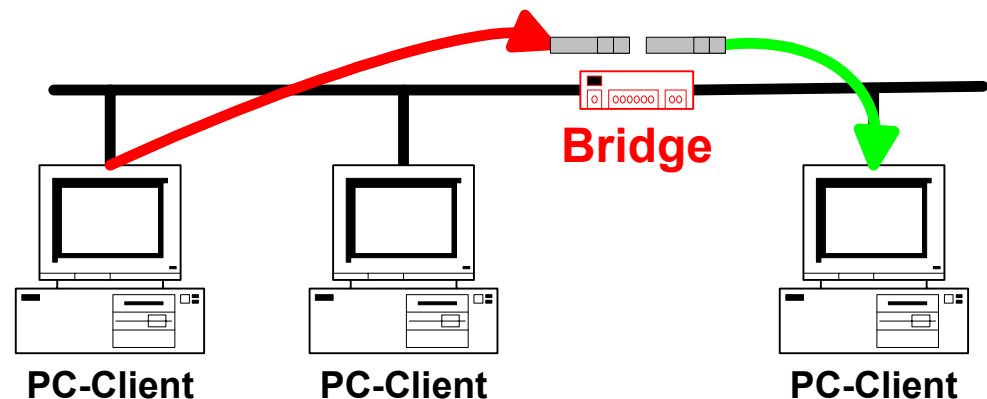
Bridges und Switches (OSI-Schicht 2)



Prinzip: Store-and-Forward auf Frame-Ebene

überträgt nur Frames auf die andere Seite, wenn diese dorthin gehören

- schließt Funktionen von Repeatern/Hubs ein bzgl. Beschränkungen, Fehler separieren, unterschiedliche physikalische Medien
- Verwendung von MAC-Adressen
- Lasttrennung bis auf Broadcasts
- Redundanz möglich (mit Spanning Tree-Algorithmus)



Verbindungskomponenten

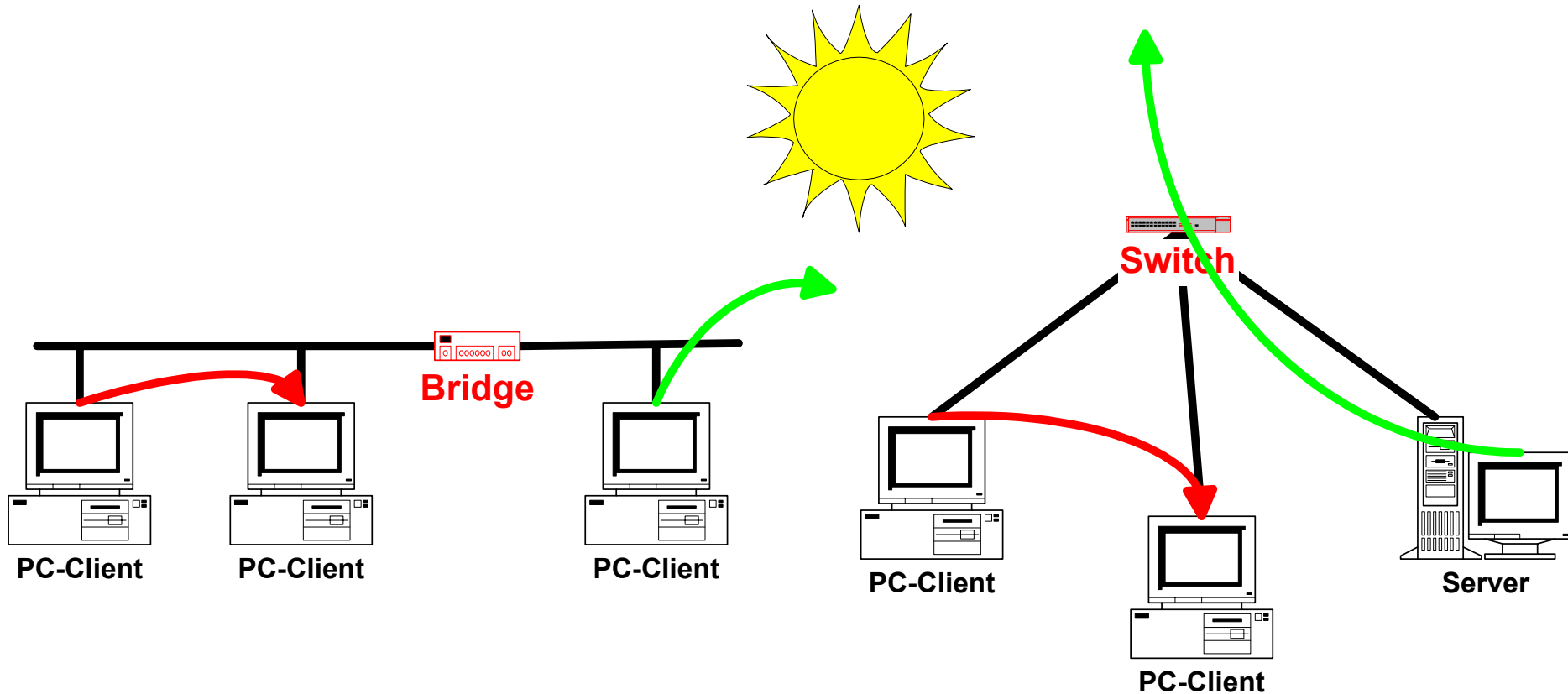
Bridges und Switches (OSI-Schicht 2)



- Bridge** (in der Regel 2 Ports)
- Switch**
 - gleiche Funktion wie Bridge, aber (viel) mehr Ports
 - Mikrosegmentierung (volle Geschwindigkeit pro Endgerät)
 - TP und LWL Anschluss
 - wird hauptsächlich bei strukturierter Verkabelung eingesetzt
 - verschiedene physikalische Medien
 - Geschwindigkeitsumsetzung
 - aber weiterhin gleiches Frameformat

Verbindungskomponenten

Bridges und Switches (OSI-Schicht 2)



lokale Datenkommunikation bleibt ungestört



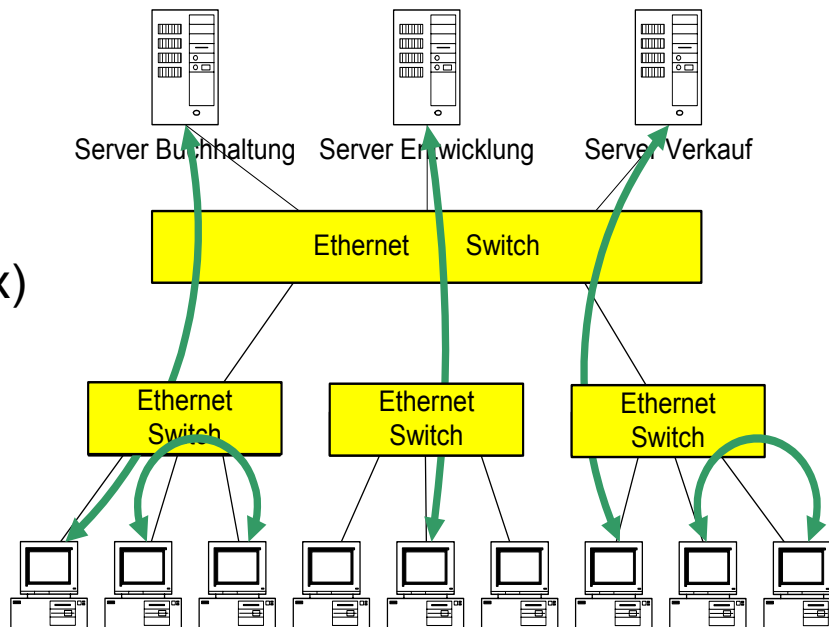
Switches state of the art

Verbindungskomponenten

Erhöhung der aggregierten Bandbreite durch Switching

Switch :

- mehrere Kommunikationsbeziehungen gleichzeitig
- Vermittlungseinheiten (ASICs oder spezielle RISC-Prozessoren)
- Weiterleiten der Frames
 - Cut-Through (sobald wie möglich)
 - Store and Forward
- Zusatzfunktionen
 - Filter
 - VLAN
 - Zugangsabprüfung (IEEE 802.1x)



Verbindungskomponenten

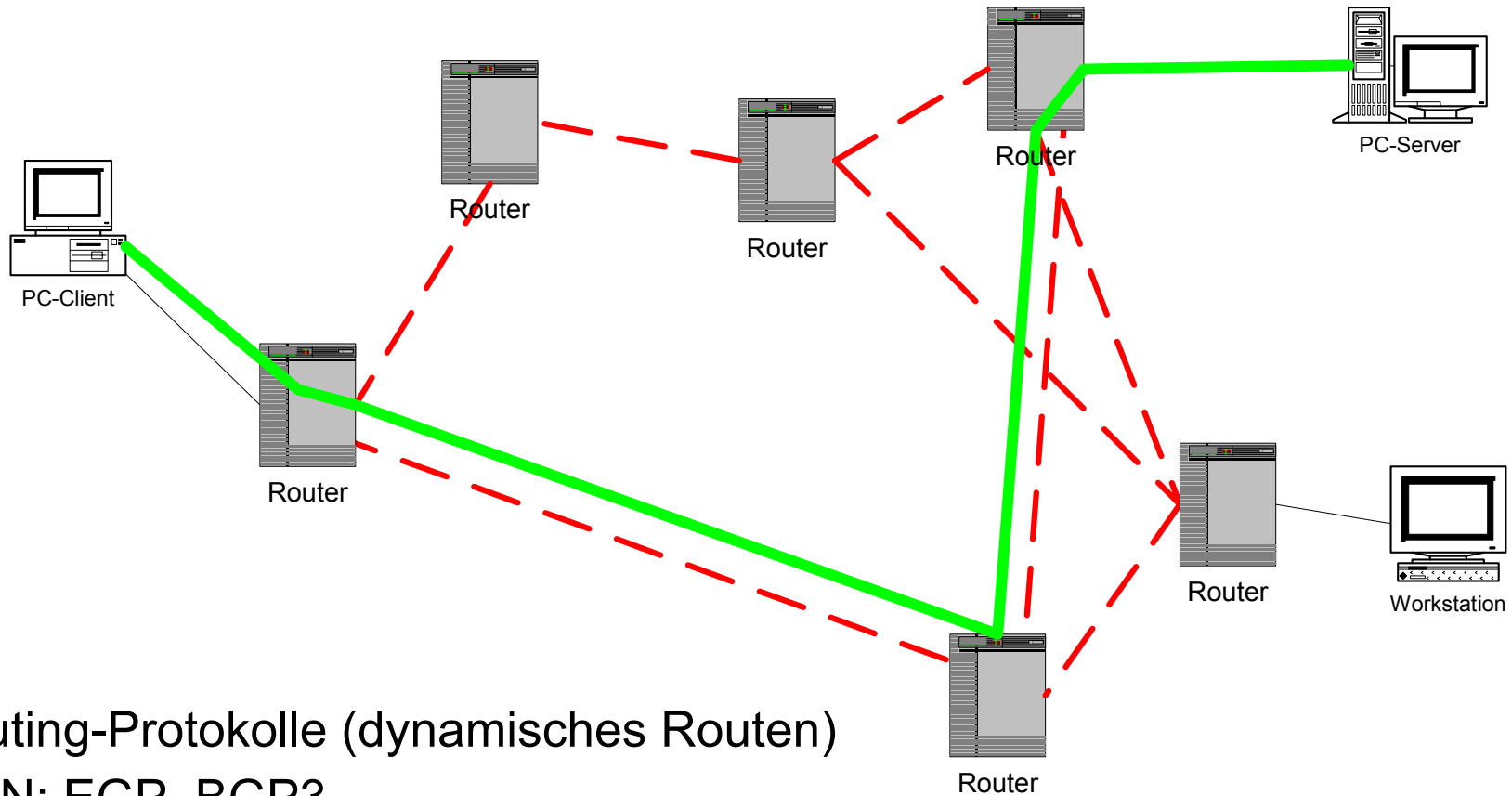
Router (OSI-Schicht 3)



- Verbindung zwischen Netzen unterschiedlicher Technologie**
 - LAN zu LAN
 - WAN zu LAN
- Strukturierung großer Netze**
- Verwendung von IP-Adressen**
- Rechnerverbindungen im gleichen Subnetz (gleicher Subnetzanteil) gehen direkt von Rechner zu Rechner (ARP)**
- Rechnerverbindungen zwischen Subnetzen gehen über **Router****
- Wie komme ich am kürzesten zu meinem gewünschten Ziel ?**
= beste **Route**
- Paket muss analysiert werden** **→** **Filter**

Verbindungskomponenten

Bester Weg durch Routernetz



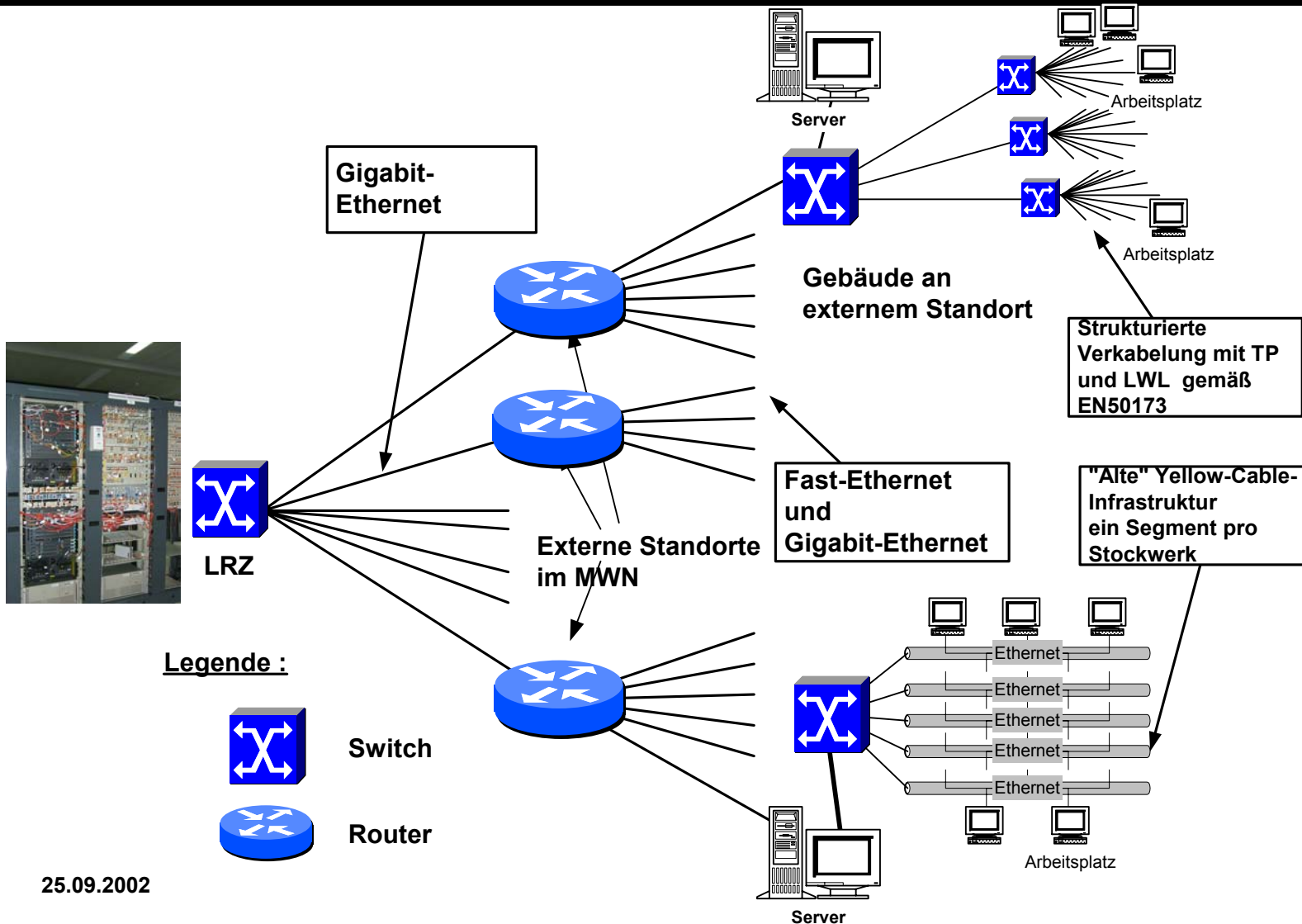
Routing-Protokolle (dynamisches Routen)

WAN: EGP, BGP3

LAN: IGP, RIP, OSPF

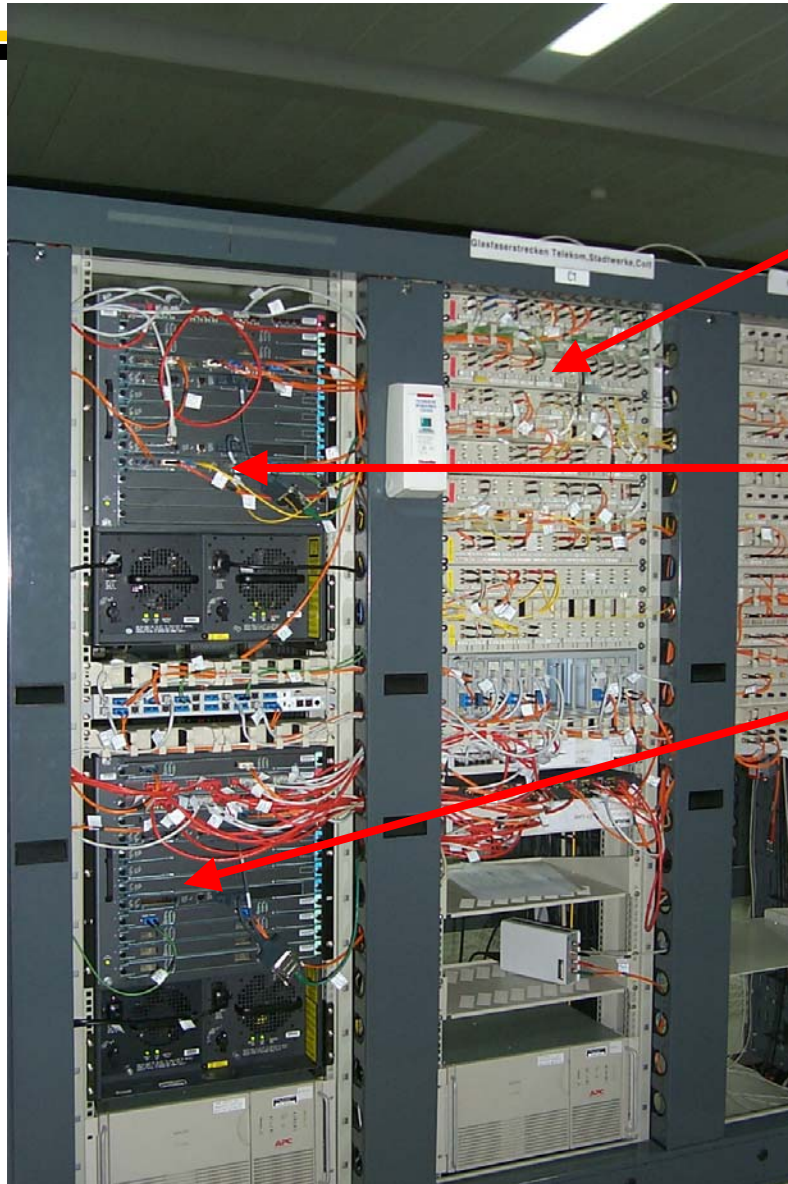
Verbindungskomponenten

Switch und Router im MWN



Verbindungskomponenten

Switch und Router im LRZ



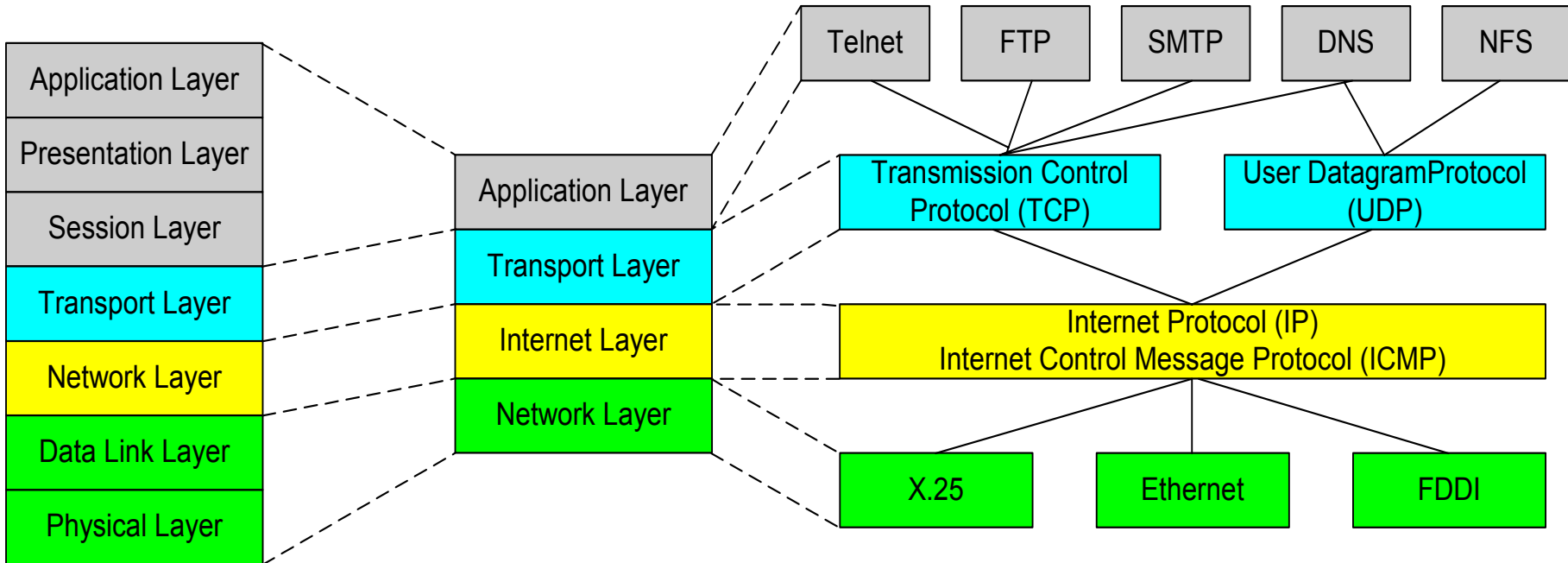
LWL-Strecken von externen Standorten

Switch von CISCO

Router von CISCO

TCP/IP-Protokolle

Abbildung OSI zu TCI/IP



FTP = File Transfer Protokoll
SMTP = Simple Mail Protokoll
DNS = Domain-Name-Server
NFS = Network file System

TCP/IP-Protokolle

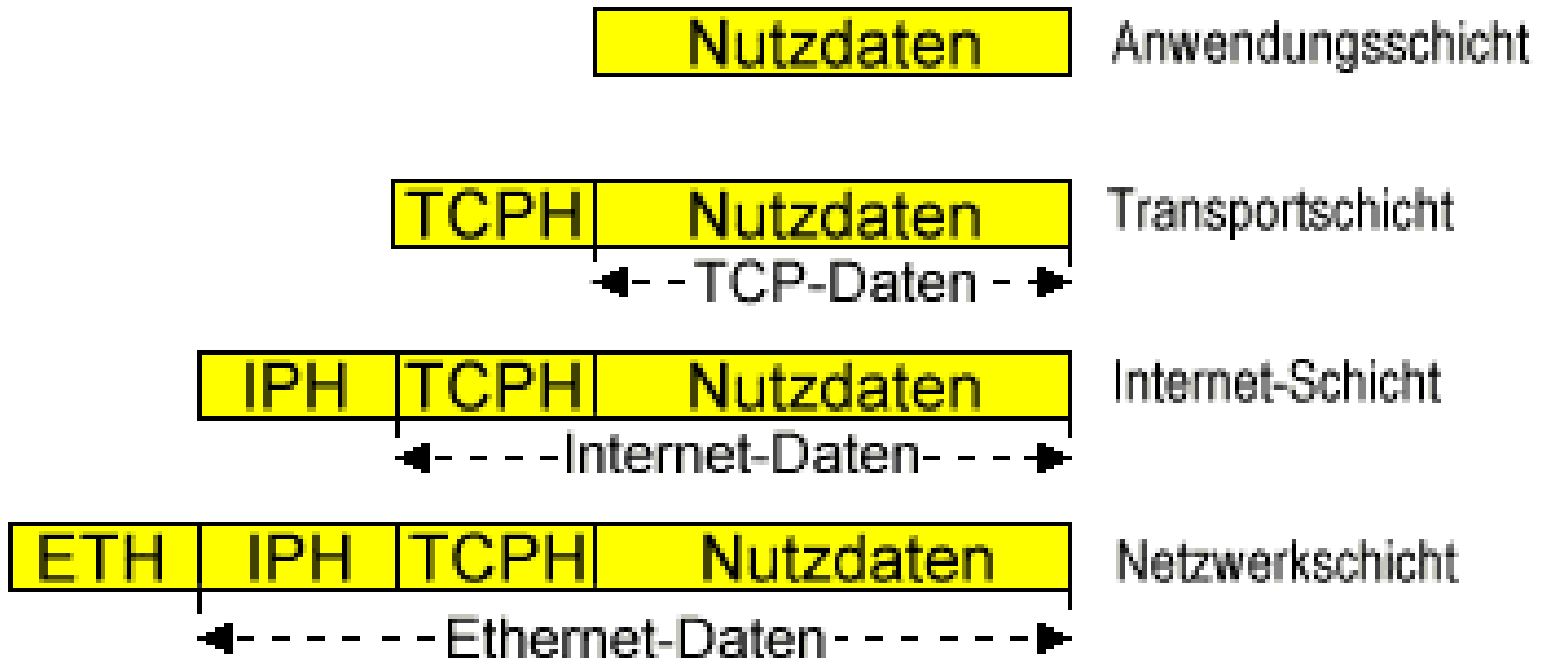
Internet Protokoll Suite



Internet-Protokolle									
OSI-Schicht	Internet Protokoll Suite							DOD Schicht	
7	Anwendung	File Transfer	Electronic Mail	Terminal Emulation	Usenet News	Domain Name Service	World Wide Web	Art der Kommunikation	
6	Darstellung	File Transfer Protocol (FTP) RFC 959	Simple Mail Transfer Protocol (SMTP) RFC 821	Telnet Protocol (Telnet) RFC 854	Usenet News Transfer Protocol (NNTP) RFC 977	Domain Name Service (DNS) RFC 1034	World Wide Web (WWW) RFC	Applikation	
5	Sitzung								
4	Transport	Transmission Control Protocol (TCP) RFC 793					User Datagram Protocol (UDP) RFC 768	Host to Host Kommunikation	
3	Netzwerk	Address Resolution Protocol (ARP) RFC 826	Internet Protocol (IP) RFC 791				Internet Control Message Protocol RFC 792	Internet	
2	Sicherung	Ethernet			Token Ring	DQDB	FDDI	ATM	lokales Netzwerk
1	Physikalische Übertragung	Twisted Pair	Lichtwellenleiter	Coaxkabel		Funk	Laser	Netzzugriff	

TCP/IP-Protokolle

Data-Encapsulation



ETH Ethernet-Header
IPH IP-Header
TCPH TCP-Header

TCP/IP-Protokolle

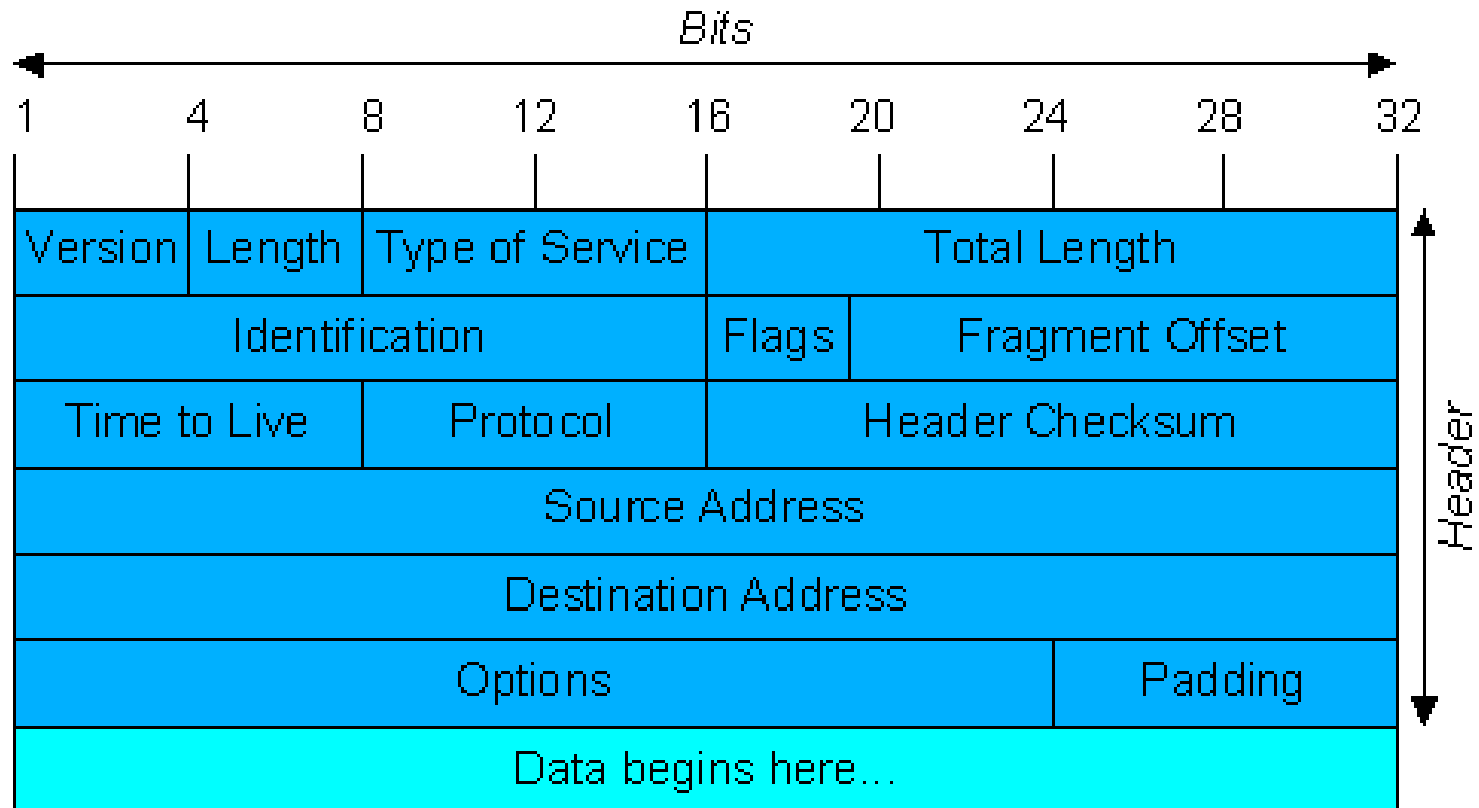
Protokolle auf Schicht 3



- ❑ **IP (Internet Protocol)**
 - ❑ verbindungslos (keine Flusskontrolle)
 - ❑ Fragmentierung in Pakete
 - ❑ IP-Adressen
 - ❑ nur Prüfsumme für Header
 - ❑ endliche Lebensdauer von Paketen
 - ❑ einheitliche Sicht auf verschiedene Netztechniken
- ❑ **ARP-Protokolle (Address Resolution Protocol),**
 - ❑ Auflösung logischer IP-Adresse in eine physikalische (z. B. Ethernet-MAC) Adresse
 - ❑ Broadcasts
- ❑ **Drei unabhängige Namens- bzw. Adressräume**
 - ❑ **Ethernet-Adresse (MAC)**
 - ↕ ARP
 - ❑ **IP-Adresse (Internet-Nummern)**
 - ↕ Domain-Name-Server (DNS)
 - ❑ **Domain-Namen**

TCP/IP-Protokolle

IP-Header



TCP/IP-Protokolle

IP-Adressen



- IP-Adressen bestehen aus einer 32 Bit langen Zahl.
Darstellung: 4 Bytes (zu je 8 Bit).
Bytes werden dezimal notiert und durch Punkte getrennt
(a.b.c.d).**
 Beispiel : 129.187. 12. 37
- Einteilung in**
 - Netzadresse
 - Rechneradresse,
 - Netzmaske bestimmt Bereich der Netzadresse
- Subnetze**
 - Lokale Verfeinerung durch Sub-Netzmaske
 - Nach außen Class B-Netz, im Innern lauter Class C-Netze

TCP/IP-Protokolle

IP-Adressen Netzklassen



	Klasse A - Netz	Klasse B - Netz	Klasse C - Netz
Netz-ID	8 Bit = 1 Byte	16 Bit = 2 Byte	24 Bit = 3 Byte
Host-ID	24 Bit = 3 Byte	16 Bit = 2 Byte	8 Bit = 1 Byte
Netzmaske	255.0.0.0	255.255.0.0	255.255.255.0
Wertebereich (theoretisch)	0.0.0.0 bis 127.255.255.255	128.0.0.0 bis 191.255.255.255	192.0.0.0 bis 223.255.255.255
Anzahl der Netze	128 ($= 2^7$)	16.384 ($= 2^6 * 256 = 64 * 256$)	2.097.152 ($= 2^5 * 256 * 256 = 32 * 256 * 256$)
Anzahl der Rechner im Netz	16.777.216 ($= 256^3$)	65.536 ($= 256^2$)	256 ($= 256^1$)

- Alle Rechner mit der gleichen (Sub-)Netzadresse gehören zu einem Netz und sind untereinander direkt erreichbar.
- Zur Koppelung von Netzen unterschiedlicher Adresse wird ein Router, benötigt.
- Je nach Zahl der zu koppelnden Rechner wird die Netzklasse gewählt.
- Reservierte Adressen:

0 = Netzwerk, 255 = Broadcast, 250 – 254 = Netzmanagement für MWN

TCP/IP-Protokolle

Im MWN verwendete IP-Adressen



Im MWN werden u.a. verwendet

- | | |
|--|---------------------------------|
| <input type="checkbox"/> 129.187.0.0 | TUM, LMU, BADW, LRZ |
| <input type="checkbox"/> 141.40.0.0 | Campus Weihenstephan |
| <input type="checkbox"/> 141.84.0.0 | LMU, LRZ |
| <input type="checkbox"/> 141.39.240.0 - 141.39.255.255 | FH-München |
| <input type="checkbox"/> 131.159.0.0 | TU-Informatik |
| <input type="checkbox"/> 138.245.0.0 | Forschungsnetz der LMU-Kliniken |
| <input type="checkbox"/> 141.39.128.0 - 141.39.191.255 | Klinikum Rechts der Isar |
| <input type="checkbox"/> 192.48.107.0 | Rechnergestütztes Entwerfen |
| <input type="checkbox"/> 192.54.42.0 | Beschleuniger-Labor |
| <input type="checkbox"/> 192.55.197.0 | LS für Integrierte Schaltungen |
| <input type="checkbox"/> 192.67.170.0 | Rechnergestütztes Entwerfen |
| <input type="checkbox"/> 193.175.56 - 63.0 | Klinikum Rechts der Isar |

TCP/IP-Protokolle

IP-Adress-Mangel Abhilfen



- Private Networks nach RFC1597**
 - kein Routing, **keine Verbindung ins Internet**, **kein Angriff von außen**
 - Class-A-Netze (1) : 10.0.0.0 - 10.255.255.255
 - Class-B-Netze (16) : 172.16.0.0 - 172.31.255.255
 - Class-C-Netze (256) : 192.168.0.0 - 192.168.255.255
- Private IP-Adressen im MWN**
 - Zuteilung durch LRZ, Routing im MWN, **kein Angriff aus dem WiN**
 - 10.152.0.0/16 priv. Subnetze für die TUM
 - 10.153.0.0/16 priv. Subnetze für die LMU
 - 10.154.0.0/16 priv. Subnetze für die FH-Weihenstephan
 - 10.155.0.0/16 priv. Subnetze für sonstige Einrichtungen
- Dynamische IP-Adressen**
 - Wählzugang, VPN, Funk-Zugang
 - DHCP (dynamic host configuration protocol)
- NAT (Network Address Translation)** 1-privat zu 1-öffentlich
- PAT (Port and Address Translation)** n-privat zu 1- öffentlich, n TCP-Port
- IPv6**

TCP/IP-Protokolle

Ziele von IPv6



- Unterstützung von Milliarden von Hosts, auch bei ineffizienter Nutzung des Adressraums
- Reduzierung des Umfangs der Routing-Tabellen
- Vereinfachung des Protokolls, damit die Router Pakete schneller abwickeln können
- Höhere Sicherheit (Authentifikation und Datenschutz) als das heutige IP
- Mehr Gewicht auf Dienstarten, insbesondere für Echtzeitanwendungen
- Unterstützung von Multicasting durch die Möglichkeit, den Umfang zu definieren
- Möglichkeit für Hosts, ohne Adressänderung auf Reise zu gehen (Laptop)
- Möglichkeit für das Protokoll, sich zukünftig weiterzuentwickeln
- Unterstützung der alten und neuen Protokolle in Koexistenz für Jahre

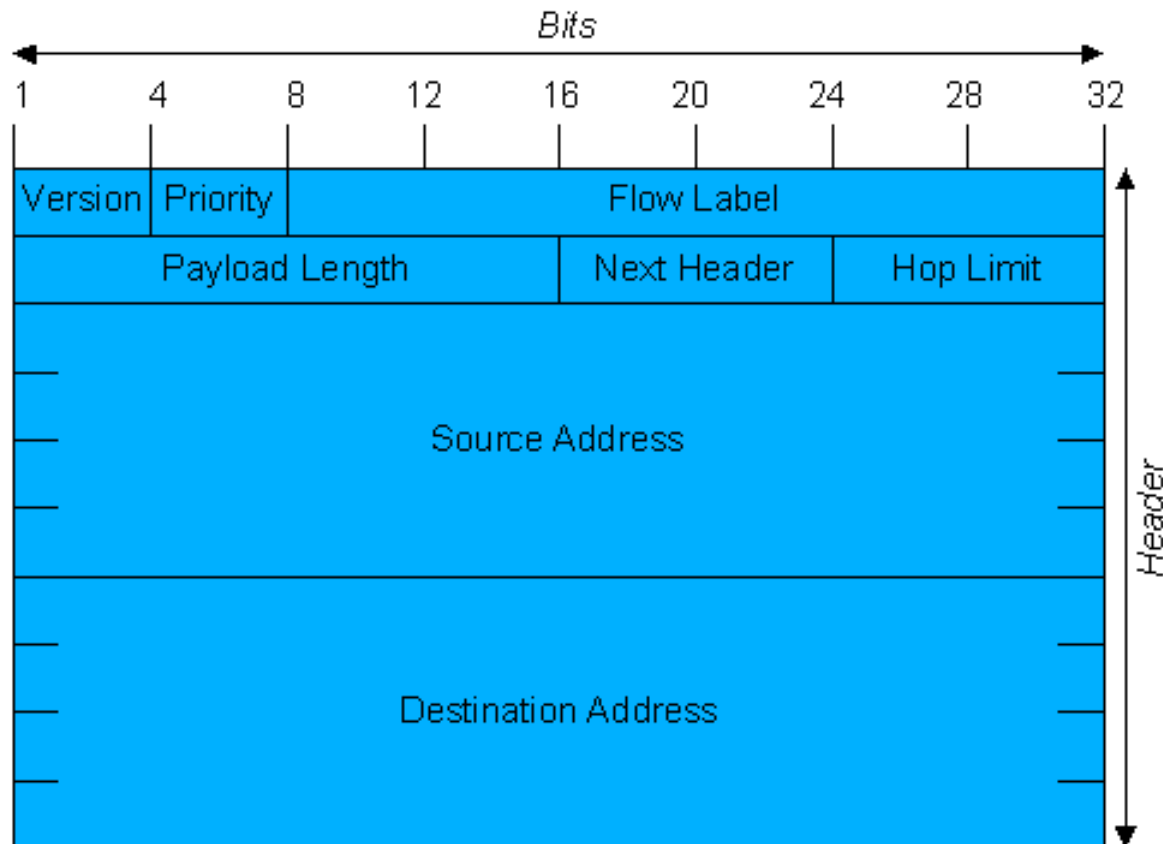
- IPv6 kommt dann, wenn es benötigt wird, hoher Aufwand
- inet6num: 2001:0638:0100::/48 netname: LRZ-MUNICH

TCP/IP-Protokolle

IPv6 Header



128-bit-Adresse



TCP/IP-Protokolle

Protokolle auf Schicht 4

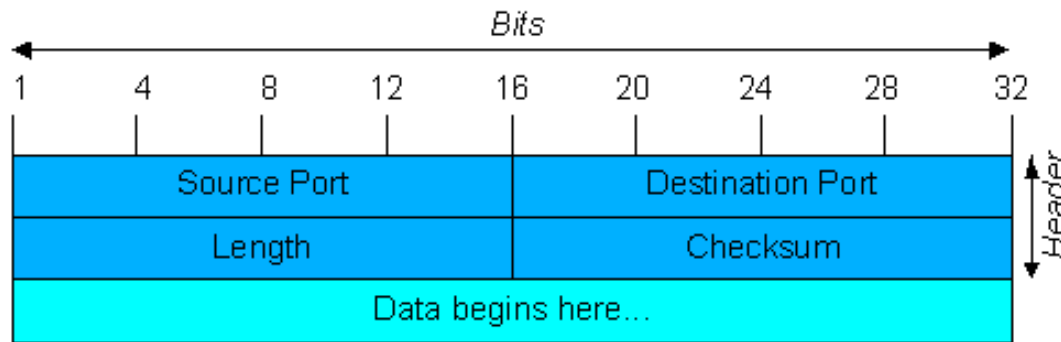


- ❑ **TCP (Transmission Control Protocol)**
 - ❑ verbindungsorientiert
 - ❑ geregelter Verbindungsaufbau und Abbau
 - ❑ Flusskontrolle (d. h. Empfangsbestätigung, etc.)
 - ❑ Windowing
 - ❑ Portnummer (mehrerer Anwendungsprogramme gleichzeitig auf einem Rechner)

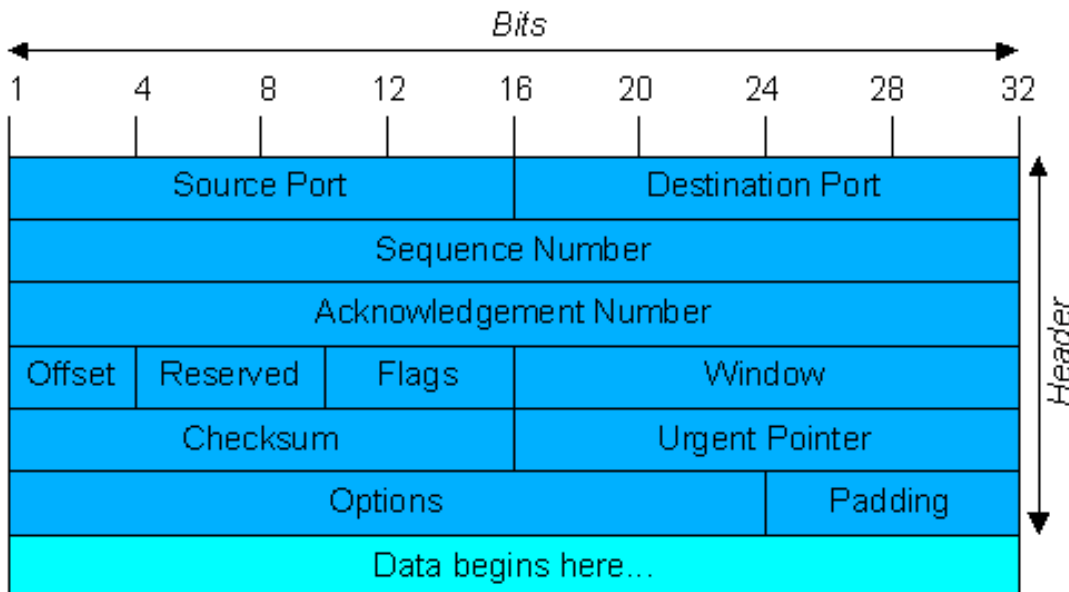
- ❑ **UDP (User Datagram Protocol)**
 - ❑ verbindungslos
 - ❑ ungesicherter Transport
 - ❑ z.B. für NFS

TCP/IP-Protokolle

UDP- TCP- Header



UDP-Header



TCP-Header

TCP/IP-Protokolle

TCP-Ports



Portnummer	Protokoll
20	FTP (Daten)
21	FTP (Befehle)
22	Secure Shell
23	Telnet
25	SMTP
53	DNS-Server
79	Finger
80	HTTP (Proxy-Server)
110	POP3
119	NNTP
143	IMAP
194	IRC
210	WAIS
256 - 1023	UNIX-spezifische Services
540	UUCP
1024 - 49151	Registered Ports
49152 - 65535	Dynamic / Private Ports

ausgewählte Ports:

Filesharing-Protokolle

- KaZaA 1214
- eDonkey 4661 bis 4665
- Gnutella 6346, 6347
- Napster 6699

SNMP-Abfragen 161,162

Netbios 139

Simple Mail Transfer 25

z.Z am WiN-Zugang des MWN gesperrt

Liste der Port-Nummern

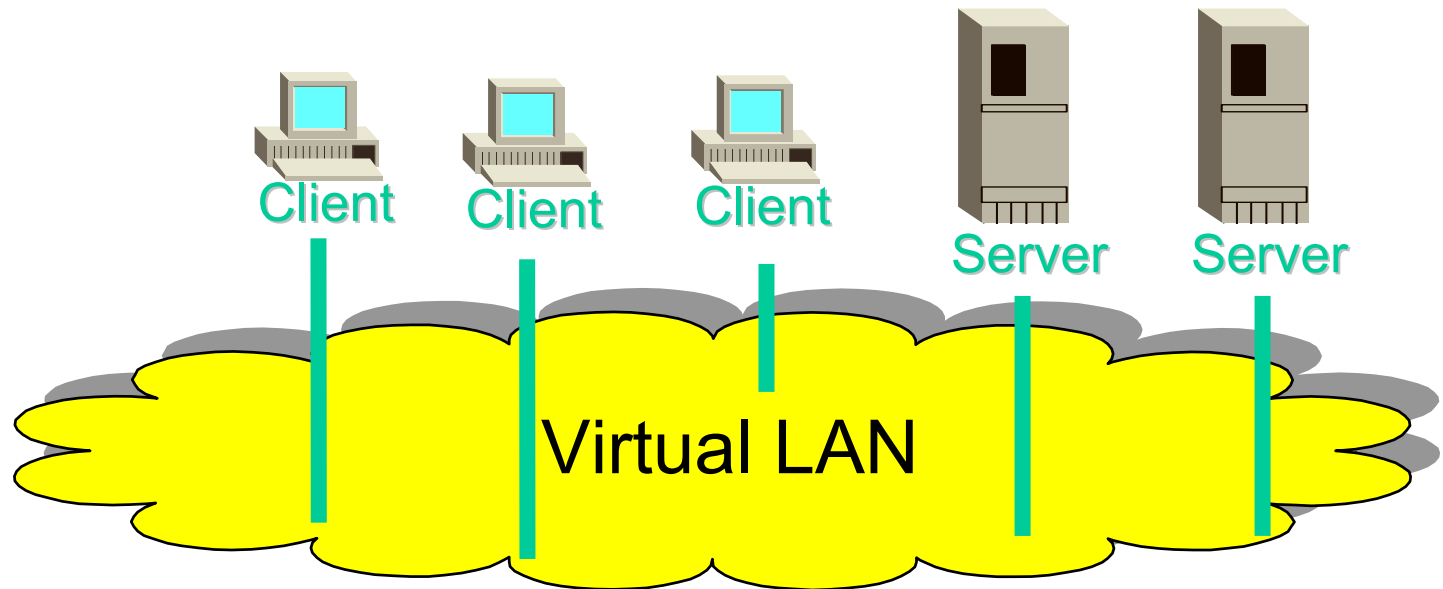
<http://www.iana.org/assignments/port-numbers>

VLAN

Definition



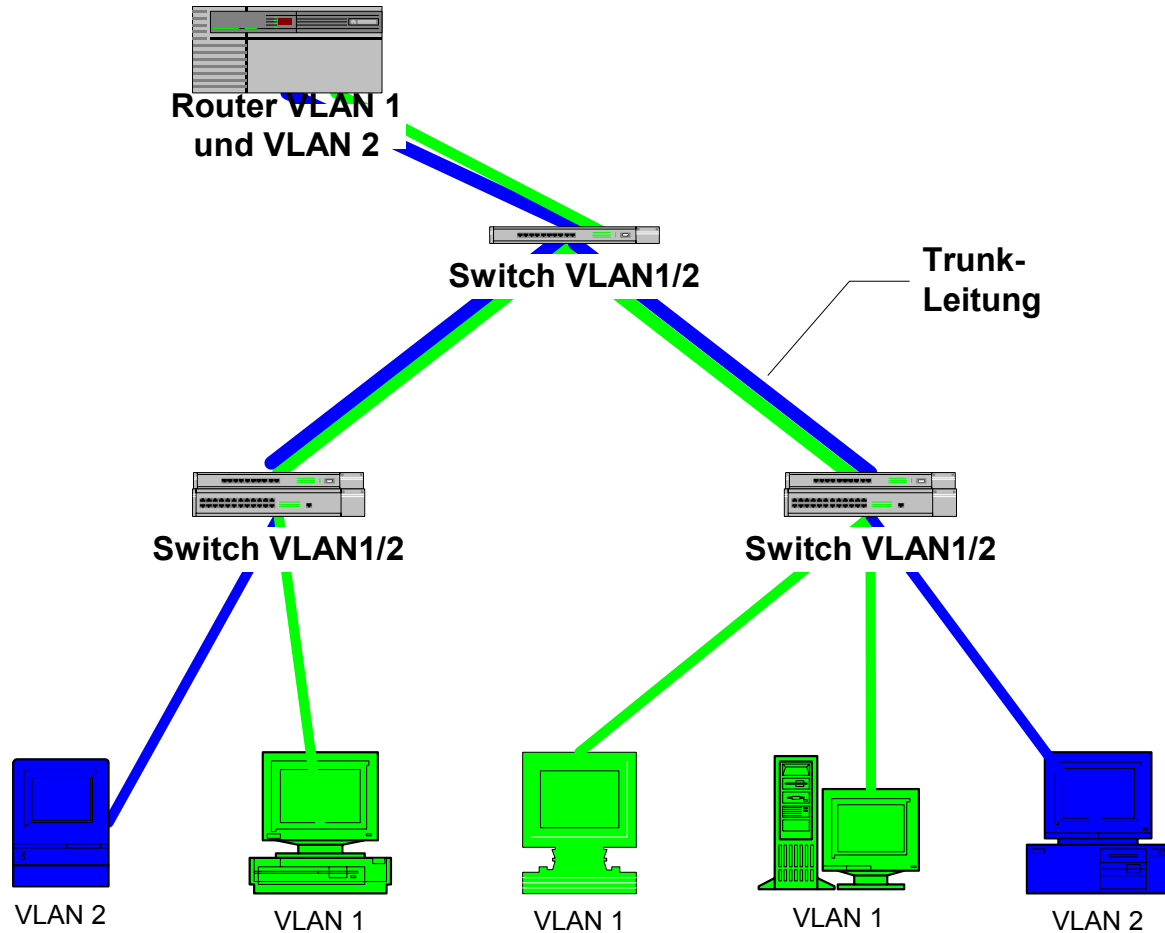
- Orts- / Topologie-unabhängige Zusammenfassung von Rechnern, die miteinander kommunizieren, wie wenn sie sich auf einem gemeinsamen, physischen LAN befänden



- ein VLAN = eine Broadcast-Domain, ein "klassisches LAN"
- zwischen Geräten in einem VLAN wird geschwitched
- zwischen verschiedenen VLANs wird geroutet

VLAN

Beispiel

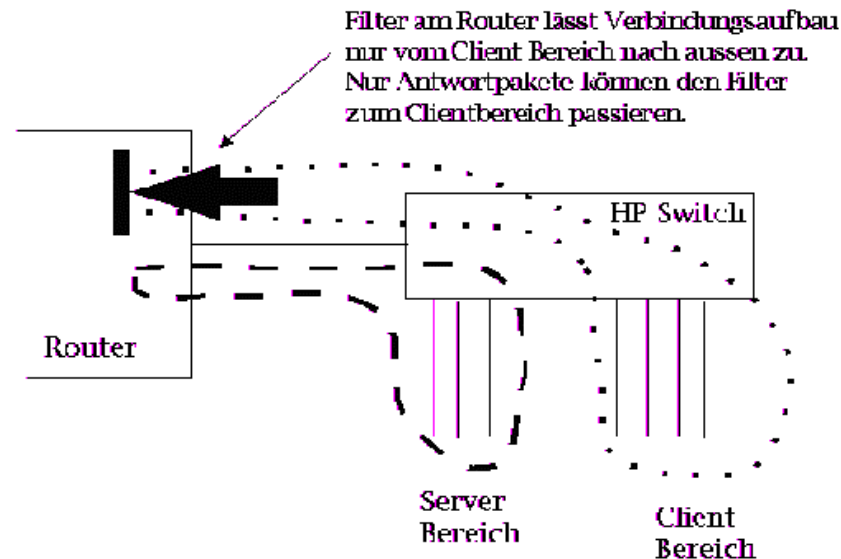


VLAN

Einsatzmöglichkeiten

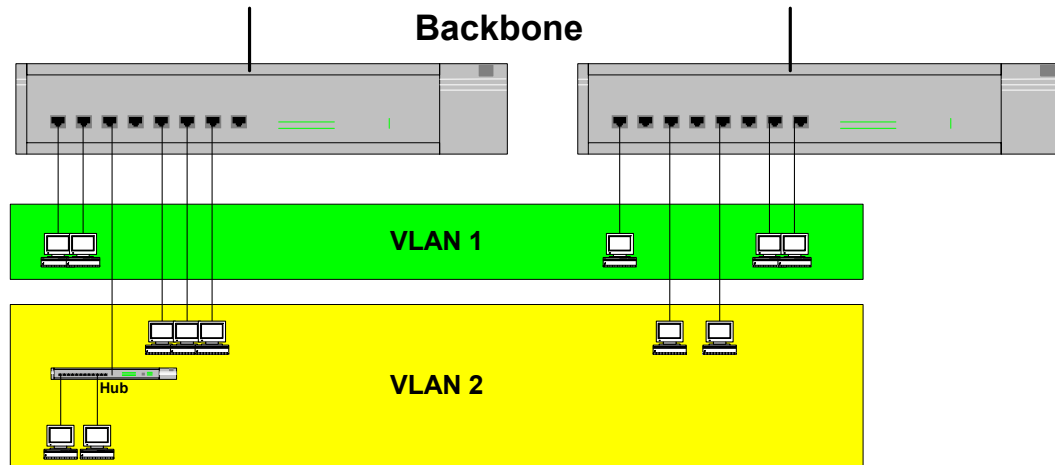


- weniger Komponenten notwendig
- keine parallelen physischen Infrastrukturen notwendig, wenn mehrere Institutionen / Arbeitsgruppen im gleichen Gebäude
- Segmentierung, kleinere Collisionsdomänen
- verteilte Arbeitsgruppen
- Sicherheit, Zugriffskontrolle (Firewalls)
- Merkmale zur Bildung von VLANs (herstellerspezifisch)
 - Port-basierend
 - MAC-basierend („user-based“)
 - Protokoll-basierend (IP, IPX, ..)
 - regelbasierend („policy-based“)
 - Anwendungs- / Dienst-spezifisch
- Verwendung im MWN
 - Verwaltungsnetze, Patientennetze
 - Netze hinter FW
 - Funk-LAN-Netz
- Hoher Aufwand



VLAN

Port-basierte VLANs



- Für jeden Switch-Port wird festgelegt, in welches VLAN die angeschlossenen Geräte gehören
- Switch wird aufgeteilt in mehrere Netze
- entspricht weitgehend herkömmlichen Installationen
- Hubs können problemlos eingesetzt werden
- Standard 802.1Q (Kennzeichnung der Pakete mit sog. Tag`s (12 Bit für VLAN))
- Hoher Konfigurations- und Dokumentationsaufwand
- schwierige Fehlersuche

- ❑ Einführung in Computernetze
- ❑ <http://www.rvs.uni-bielefeld.de/publications/books/NetworksBook.html>

- ❑ Skripten über Netze, u.a.
- ❑ <http://www.netzmafia.de/skripten/>

- ❑ Lernprogramme Datenkommunikation
- ❑ <http://www.fh-augsburg.de/informatik/projekte/emiel/datacom/literatur/internet.html>

- ❑ Netzwerke
- ❑ http://www.tu-chemnitz.de/informatik/HomePages/RA/kompendium/vortraege_98/netz/index.html

- ❑ Broschüre Netzwerke Grundlagen
[RRZN-Schriften-Reihe](#)

Vielen Dank für Ihre Aufmerksamkeit 

noch Fragen??

