



Kommunikationstechnik KOTE / Netzwerkgrundlagen
Repetition

Prüfungsformat KOTE

- **Themen Prüfung KOTE (Open Book):**
 - Grundlagen Netzwerktechnik
 - IP-Netze unterteilen
 - Redundante Netzwerke planen
 - Grundlagen der Konfiguration
- **Hilfsmittel:**
 - Open book
 - Schriftlich und digital
 - Literatur, Eigene Zusammenfassung
 - Die Verwendung des Internets ausserhalb der eigenen Literatur Beschaffung ist untersagt
 - Notebook mit installiertem CISCO Pakettracer
- **Formate:**
 - Wissensfragen mit teils auch Multiple-Choice
 - Anwendungsfragen mit Planung und Konfiguration
- **Dauer: 90 Minuten**

Agenda



Repetition **«Protokolle für** **Troubleshooting»**

Wichtige Protokolle für das Troubleshooting

Protokoll	Werkzeuge und Erweiterungen
ICMP (Internet Control Message Protocol) <ul style="list-style-type: none">- RFC 792, IETF September 1981 <p>Dient dem Austausch von Informationen und Fehlermeldungen im Netzwerk.</p>	<ul style="list-style-type: none">- Ping- Traceroute / Tracert
SNMP (Simple Network Management Protocol) <ul style="list-style-type: none">- SNMP RFC 1067, 1098, 1157, 1990- SNMPv3 RFC 3410 – 3417 + 3430, 2002 <p>Dient der Überwachung und Steuerung in Netzwerken.</p>	Remote Monitoring Standard: <ul style="list-style-type: none">- RMON (IETF, RFC 2819)- RMON2 (IETF, RFC 2021)

ICMP

Internet Control Message Protocol (RFC 792)

ICMP wird zur Überprüfung und Überwachung der Netzwerkverbindungen genutzt. Dazu können mit dem ICMP Protokoll Informationen und Fehlermeldungen zwischen Stationen ausgetauscht werden.

ICMP-Type	Meldung
0	Echo Reply (von Ping)
3	Destination Unreachable
4	Source Quench (Warteschlange ist voll)
5	Redirect (Pfad wird umgeleitet)
8	Echo Request (bei PING)
11	Time exceeded (TTL abgelaufen oder Zeitlimit überschritten)
12	Parameter Problem

Wichtige Troubleshooting Anwendungsbeispiele

Befehl	Anwendungszweck
tracert 192.168.1.3 tracert www.meinedomain.ch	So wird die gewählte Route sichtbar. Nützliches Onlinetool www.visualroute.ch
ping 192.168.1.3 Ping www.meinedomain.ch	ICMP Abfrage um den TTL-Wert zu erhalten und zu schauen ob eine Ziel-Adresse erreichbar ist.
ping 192.168.1.3 -t	Der Pingbefehl wird permanent ausgeführt. Abbruch mit Ctrl+C
netstat -an	Aktuelle Verbindungen (Connections) anzeigen
ipconfig /all	Zeigt aktuelle IP-Konfiguration aller Adapter an.
ipconfig /release	IP-Adressen werden von den Adaptern gelöst.
ipconfig /renew	IP-Adressen und Einstellungen werden vom DHCP-Server neu bezogen
route print	Zeigt die aktuelle Routingtabelle an
arp -a	Zeigt ARP-Tabelle an (IP zu MAC-Adresse)
nslookup www.meinedomain.ch	Fragt Namensserver ab. Nützlicher Link www.dnstools.ch

Agenda

**«Repetition
Quality of Service»**

Was soll durch Quality of Service (QoS) oder deutsch «Dienstgüte» erreicht werden?

- Dienstgüte ist der Zustand, welcher vom Nutzer als akzeptabel erwartet wird. Zum Beispiel:
 - Telefonieren ohne Unterbrüche (VoIP).
 - Live Fussballübertragung ohne verzerrtes Bild.
 - Annehmbare Geschwindigkeit beim Besuchen von externen (Extranet) und internen Webseiten (Intranet).
- Dienstgüte kann durch saubere Priorisierung erreicht werden.
 - Z.B. hat VoIP Telefonie Priorität vor dem E-Mailverkehr.

Mögliche Unterteilung in Prioritätskategorien

Kategorie	Beschreibung der Priorität
Zeitkritische Kommunikation	Hohe Priorität z.B. IP-Telefonie, Videotelefonie
Zeitunkritische Kommunikation	Niedrige Priorität Mailverkehr, Websurfen, FTP-Download
Hohe organisatorische Wichtigkeit	Hohe Priorität Steuerung der Produktionsabläufe Online-Bestellsystem (Webshop)
Unerwünschte Kommunikation	Keine Priorität, kann gesperrt werden z.B. Live-Video-Streaming, Peer-to-Peer Anwendungen

Quelle: Mark A. Dye, Rick McDonald, Antoon W. Ruffi, Netzwerkgrundlagen, CCNA Exploration Companion Guide, Cisco Networking Academy, Addison Wesley Verlag, S. 52ff

Die Dienstqualität als Funktionsgarant

Quality of Service (QoS)

Dienstqualitätsgrößen	Beschreibung
Übertragungsrate	<ul style="list-style-type: none">- Übertragungsgeschwindigkeit in Mbit/s- Vielfach fälschlicherweise als Bandbreite* bezeichnet
Latenz (Verzögerung)	<ul style="list-style-type: none">- Wie lange dauert das Senden vom Sender zum Empfänger- Einfaches bidirektionales Messverfahren in Millisekunden (z.B. mit PING)- Bei hoher Latenz gibt es z.B. Echos in Gesprächen
Varianz (Jitter, Verzerrung)	<ul style="list-style-type: none">- Die Varianz bei der Latenz wird als Jitter bezeichnet- Verursacht Übertragungsunterbrüche
Paketverlustrate	<ul style="list-style-type: none">- Wie viele Pakete kommen nicht an

*Bandbreite = Frequenzbereich zwischen tiefster und höchster Frequenz

Gerade bei VoIP-Telefonie oder Videokonferenzen ist eine kontinuierliche Datenverbindung wichtig! Ansonsten treten Verzögerungen (Unterbrüche) auf.

Agenda



Repetition «Netzklassen und Subnetting»

CCNA1 Kapitel 11 – 14

Repetition

Historische Netzklassen

Netzkategorie	Präfix	Adressbereich	Verwendung	CIDR Suffix
Kategorie A	0000 0000	0.0.0.0 – 127.255.255.255	Verteilung	/8
Kategorie B	1000 0000	128.0.0.0 – 191.255.255.255	Verteilung	/16
Kategorie C	1100 0000	192.0.0.0 – 223.255.255.255	Verteilung	/24
Kategorie D	1110 0000	224.0.0.0 – 239.255.255.255	Multicast	
Kategorie E	1111 0000	240.0.0.0 – 255.255.255.255	Reserviert	

CIDR = Classless Inter-Domain Routing – Die Präfixlänge beim Subnet ist damit frei wählbar

Repetition

Klassenbezogene A-, B- und C-Netze

$$2^H - 2$$

Klasse	Netzbits (N)	Hostbits (H)	Anzahl Netze	Anzahl Hosts - 2	Subnetzmaske (DDN-Maske*)	Präfix-maske
A	8	24	126	16'777'214	255.0.0.0	/8
B	16	16	16'384	65'534	255.255.0.0	/16
C	24	8	2'097'152	254	255.255.255.0	/24

*DDN = Dotted decimal notation

Private IP-Adressen (RFC 1918)

CDIR = Classless Inter-Domain Routing = **Subnetting**

CIDR-Adressblock	Adressbereich	Klasse (historisch)
10.0.0.0/8	10.0.0.0 bis 10.255.255.255	255.0.0.0
172.16.0.0/12	172.16.0.0 bis 172.31.255.255	255.255.0.0
192.168.0.0/16	192.168.0.0 bis 192.168.255.255	255.255.255.0

Quelle: <http://de.wikipedia.org/wiki/IP-Adresse>

Private IP-Adressen werden nicht ins Internet geroutet!

Es werden NAT (Network Address Translation)- resp. PAT (Port Address Translation) -Funktionen dafür benötigt.

Vergabe von IPv4-Netzwerkadressen an Hosts

Vergabe	Beschreibung	Verwendung
Statische IP	IP wird manuell konfiguriert	Server Netzwerkgeräte Drucker
Dynamische IP	IPs werden dynamisch durch DHCP zugewiesen. Dazu wird ein Adress-Pool definiert. Es gibt im Netz nur einen DHCP. Mit DHCP können auch weitere Werte verteilt werden, wie: <ul style="list-style-type: none">• z.B. Standardgateway, DNS-Server,..	Clients

Das Wichtigste ist es zwingend Adresskonflikte zu vermeiden! Daher ist ein sauberes IP-Konzept für die Vergabe der Adressen zu definieren. Vergebene fixe Adressen sind zu dokumentieren!

Speziell reservierte Netzwerkadressen

Adressblock	Reserviert für	RFC
0.0.0.0/8	Aktuelles Netzwerk (eigenes Netzwerk)	RFC 1122
100.64.0.0/10	Shared Transition Space	RFC 6598
127.0.0.0/8	Loopback Adresse (Lokaler Computer)	RFC 1122
169.254.0.0/16	Autokonfiguration (link local), APIPA	RFC 3927
192.0.0.0/24	IETF Protocol Assignments	RFC 5735
192.0.2.0/24	Test-Net-1	RFC 5735
192.88.99.0/24	IPv6 zu IPv4 Relay	RFC 3068
198.18.0.0/15	Benchmark-Tests im Netzwerk	RFC 2544
198.51.100.0/24	Test-Net-2	RFC 5735
203.0.113.0/24	Test-Net-3	RFC 5735
255.255.255.255/32	Limited Broadcast (werden nicht geroutet)	RFC 919 RFC 922

Repetition

Grundlagen Subnettierung

- Die Subnettierung ist notwendig um Netze zu teilen, meist aus..
 - ..Ressourcen Gründen (Broadcast eindämmen)
 - ..aus Sicherheitsgründen
- Die Subnettierung erfolgt durch die **Subnetz Maske**:
 - z.B. **255.255.255.0 (DDN)**
 - oder **11111111. 11111111. 11111111.00000000**
 - oder **/24 (Präfix)**

Übung macht den Meister

Berechne selbständig

Umrechnung Binär zu Dezimal:

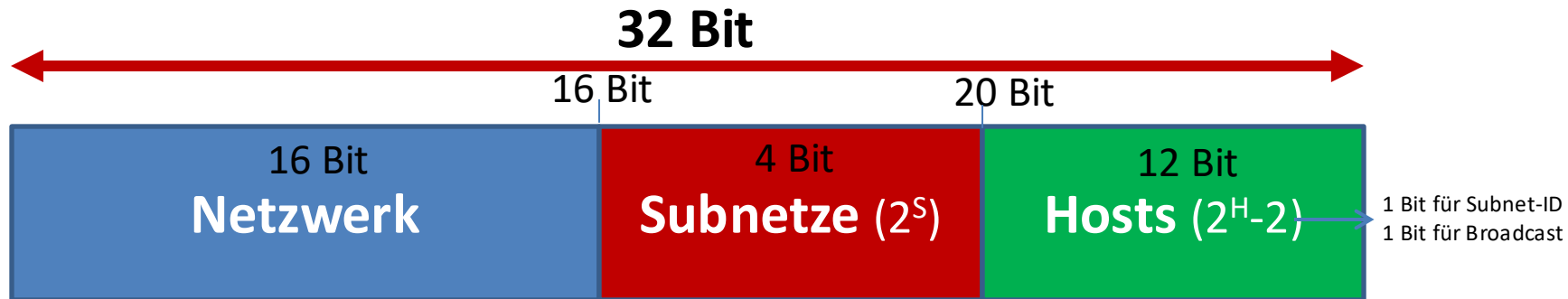
Wert								
Dezimal	128	64	32	16	8	4	2	1
Binär	0	1	1	0	1	1	0	0
Wert	0	64	32	0	8	4	0	0

Berechnung = 108

Wert								
Dezimal	128	64	32	16	8	4	2	1
Binär	0	0	0	1	0	0	0	1
Wert								

Berechnung = 17

Grundlegende Subnettierung



z.B. 128er Netz 16 Bit reserviert für Netz → für Subnetze und Hosts stehen 16 Bit zur Verfügung

z.B. B-Klasse-Netzwerk mit Maske = **255.255.240.0** Präfix = /20

Binär: **1111 1111 1111 1111** **1111** 0000 0000 0000

B-Netzwerk Subnetze Hosts

Netzwerk (N) = 16 (B-Netzwerk)

Subnetze (S) = 4

Hosts (H) = 12

Beispiel

Beispiel: (klassenlose) IPv4-Adresse `203.0.113.195/27`

	Dezimal	Binär	
			Subnet 27
IP-Adresse	203.000.113.195	11001011 00000000 01110001 11000011	<i>ip-adresse</i>
Netzmaske	255.255.255.224	11111111 11111111 11111111 11100000	AND <i>netzmaske</i>
Netzwerkadr.	203.000.113.192	11001011 00000000 01110001 11000000	= <i>netzwerkteil</i>
			Netzadresse
IP-Adresse	203.000.113.195	11001011 00000000 01110001 11000011	<i>ip-adresse</i>
Netzmaske	255.255.255.224	11111111 11111111 11111111 11100000	
		00000000 00000000 00000000 00011111	AND (NOT <i>netzmaske</i>)
Geräteteil	3	00000000 00000000 00000000 00000011	= <i>geräteteil</i>
			Geräteadresse

Bei einer Netzmaske mit 27 gesetzten Bits ergibt sich eine Netzadresse von `203.0.113.192`. Es verbleiben 5 Bits und selbst und für den Broadcast benötigt, so dass 30 Adressen für Geräte zur Verfügung stehen.

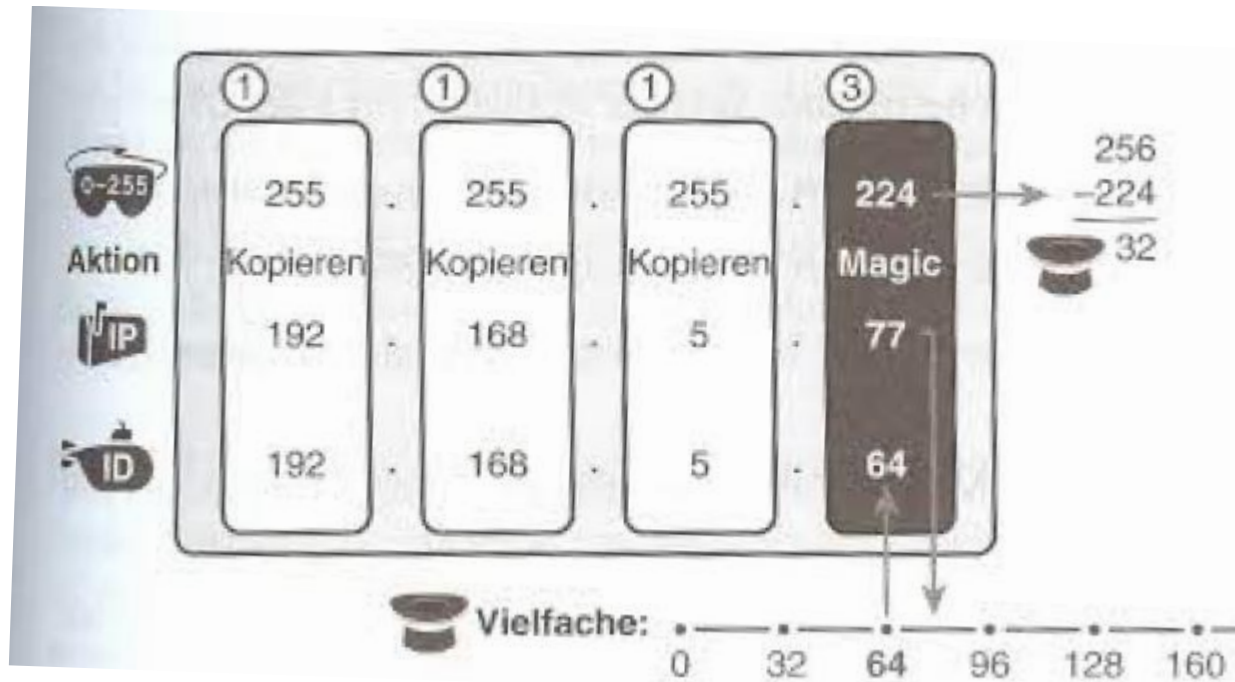
Oktett

$2^5 - 2$

Bestimmung des Subnetzes

- Es wird dazu das **Boolesche UND** verwendet
 - $1 \text{ UND } 1 = 1$
 - $0 \text{ UND } 1 = 0$
 - $1 \text{ UND } 0 = 0$
 - $0 \text{ UND } 0 = 0$
- Der Hostanteil bei einem Subnet besteht aus Nullen.

Zugehöriges Subnetz ermitteln (Magic number)



2. Aufgabe

Konkrete Subnettierung bestimmen

Sie bekommen als Netzwerktechniker/in folgenden konkreten Auftrag:

Erstellen Sie für den privaten IP-Range (RFC 1918) **172.16.0.0/12** eine Subnettierung in mind. 4 Netze mit je mind. 300 möglichen Host Adressen. Wie sehen die vier Netze genau aus (IP-Range und Subnetadresse)?

Zeit: 5 Minuten

2. Aufgabe Musterlösung

IP-Range	Netzwerk Adresse	Broadcast Adresse	Maske	Anzahl zuweisbarer Hosts
172.16.0.0 – 172.16.1.255	172.16.0.0	172.16.1.255	255.255.254.0 Suffix /23	510
172.16.2.0 – 172.16.3.255	172.16.2.0	172.16.3.255	255.255.254.0 Suffix /23	510
172.16.4.0 – 172.16.5.255	172.16.4.0	172.16.5.255	255.255.254.0 Suffix /23	510
172.16.6.0 – 172.16.7.255	172.16.6.0	172.16.7.255	255.255.254.0 Suffix /23	510

<http://www.subnet-calculator.com/>

Subnetz-Aufteilung

Das gegebene Subnetz ist 192.168.128.128/25. Wir wollen es in vier gleich grosse Subnetze unterteilen:

Schritt 1: Analyse des vorhandenen Subnetzes

- Netzwerkadresse: 192.168.128.128
- Subnetzmaske: /25 entspricht 255.255.255.128
- Adressbereich: 192.168.128.128 (Netz-ID) bis 192.168.128.255 (Broadcast)
- Anzahl der IP-Adressen: $2^7 = 128$ **Adressen** (inkl. Netz- und Broadcast-Adresse)

Schritt 2: Aufteilung in 4 gleich grosse Subnetze

Um das Netzwerk in 4 Subnetze zu unterteilen, benötigen wir eine feinere Subnetzmaske. Dazu erhöhen wir die Präfixlänge von /25 auf /27 (2 Bit höher, da 4 Subnetze benötigt werden $2^2 = 4$ Subnetze)

- Neue Subnetzmaske: /27 entspricht 255.255.255.224
- Anzahl der IP-Adressen pro Subnetz: $2^5 = 32$ **Adressen** (inkl. Netz- und Broadcast-Adresse)

Schritt 3: Neue Subnetze berechnen

- Die **Subnetzsprünge** werden durch die neue Blockgrösse bestimmt:
- Blockgrösse = $256 - 224 = 32$ (Magic Number!)

Subnetz	Netzwerkadresse	Erster Host	Letzter Host	Broadcast-Adresse
1	192.168.128.128/27	192.168.128.129	192.168.128.158	192.168.128.159
2	192.168.128.160/27	192.168.128.161	192.168.128.190	192.168.128.191
3	192.168.128.192/27	192.168.128.193	192.168.128.222	192.168.128.223
4	192.168.128.224/27	192.168.128.225	192.168.128.254	192.168.128.255

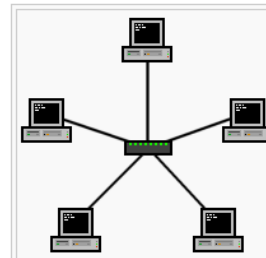
Agenda



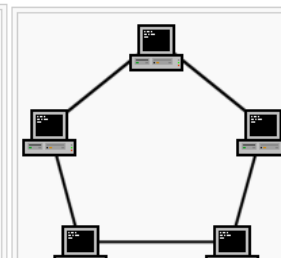
Repetition «Topologien»

Netzwerk-Topologien

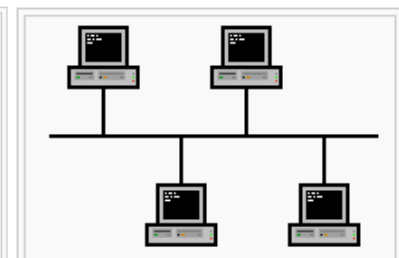
- Wir kennen folgende **physischen** Topologien ...
 - Sterntopologie
 - Ringtopologie
 - Bustopologie
 - Baumtopologie
 - Maschentopologie (Full oder Partial)
 - Zellen-Topologie (Funktechnologie)



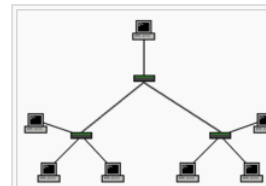
Jedes Endgerät ist mit dem Verteiler verbunden, die Endgeräte untereinander sind nicht verbunden



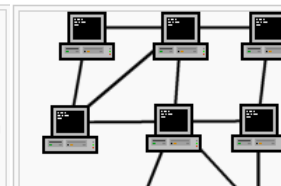
Jedes Endgerät ist mit genau zwei anderen verbunden



Alle Endgeräte sind an den Bus angeschlossen



Jedes Endgerät ist mit dem Verteiler verbunden, die Verteiler untereinander sind verbunden



Die Endgeräte sind miteinander verbunden

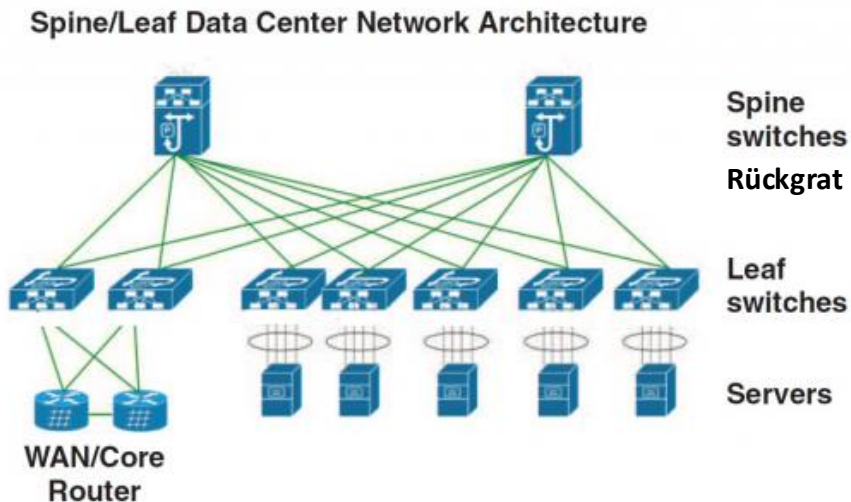
Das hierarchische Netzwerkmodell

Hierarchie	Beschreibung
Access-Layer (Zugangsschicht)	Verbindung zwischen Endgeräten (PCs, Druckern, IP-Telefonen. Umfasst Router, Switches, Access-Points.
Distribution-Layer (Verteilerschicht, Aggregation Layer)	Steuert den Fluss der Netzdaten. Realisiert Routingfunktionen zwischen den VLANs. Distribution Layer Switches sind Hochleistungsgeräte (Verfügbarkeit / Redundanz)
Core-Layer (Kernschicht)	Highspeed-Backbone des Netzwerks. Müssen Leistungsstark und hochverfügbar sein.

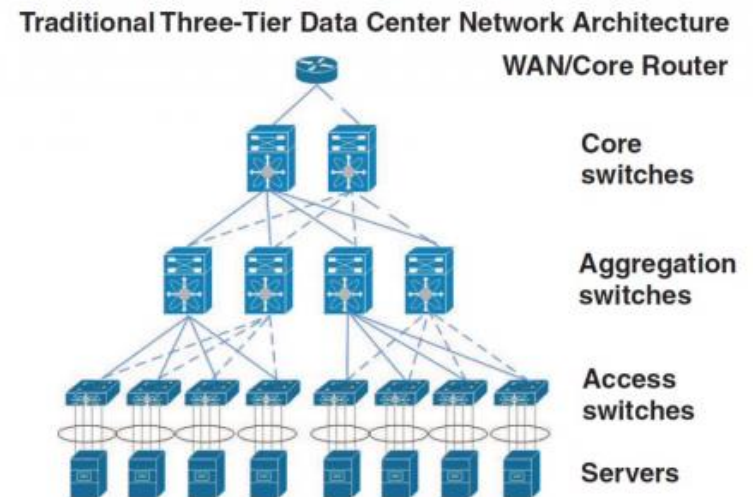
In kleineren Netzen ist meist die Distribution- und Core-Schicht zusammengefasst.

3-Tier Topologie / Spine-Leaf-Topologie

Spine-Leaf



Traditional 3-Tier



Agenda

Repetition **«Übertragungsmedien»**

Überblick der Übertragungsmedien

Medium	Medien-Typen	Wichtige Details
Kupferkabel (Twisted Pair, verdreht)	UTP = Unshielded Twisted Pair STP = Shielded Twisted Pair Elektronische Signale	RJ45-Stecker 4 verdrehte Aderpaare
Lichtwellenleiter (Glasfaserkabel)	Multimode (bis ca. 500m) Monomode/Singlemode (bis zu 50 KM mit 1Gbit/s) Optische Datenübertragung	SC-Stecker ST-Stecker LC-Stecker LWL-BNC-Stecker
Funk (Wireless LAN)	Access Point IEEE 802.11g – 54Mbit/s (2.4GHz) IEEE 802.11a – 54Mbit/s (5GHz) IEEE 802.11n – 600Mbit/s (2.4GHz und 5GHz) IEEE 802.11ac – 6.77Gbit/s	WEP (unsicher), WPA und WPA2 Verschlüsselung (sicher) WiFi (Wireless Fidelity) www.wi-fi.org

Agenda

Repetition
**«Vermittlung und
Schichtenmodelle»**

Repetition Kommunikationsgrundlagen

Verbindungsarten

Simplex



Halbduplex



Duplex



Grundlegende **Kommunikationsarten**

- **Unicast** (Punkt zu Punkt)
 - Telefonverbindung
- **Multicast** (Punkt zu Gruppe)
 - Client-Server-Applikationen, Pay TV
- **Broadcast** (Punkt zu allen)
 - Radio, Fernsehen, ARP
- **Anycast** (*Punkt zu einem in der Gruppe*)
 - Mehrere Teilnehmende treten als Einziger auf
 - Ausfallsicherheit und Lastverteilung
 - z.B. bei einigen Root DNS-Server

Grafische Darstellung der **Kommunikationsarten**

Unicast



Multicast



Grafische Darstellung der **Kommunikationsarten**

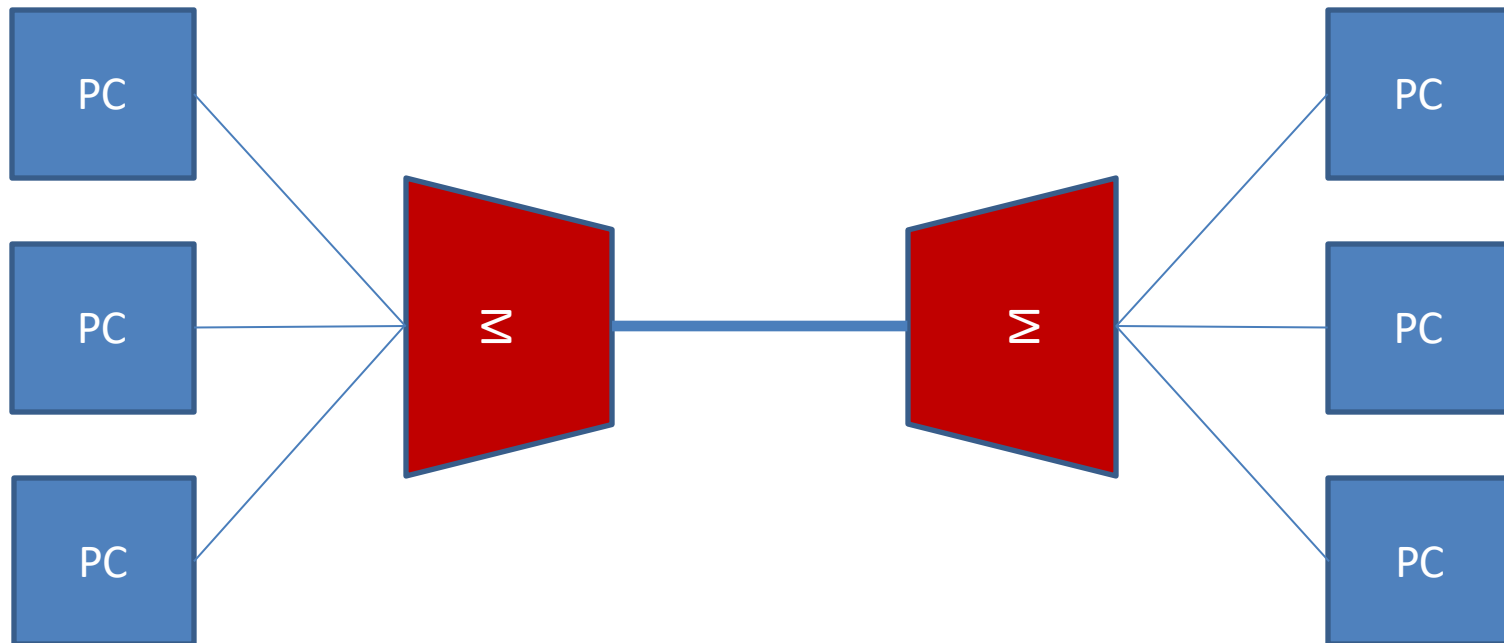
Anycast



Broadcast



Multiplexing

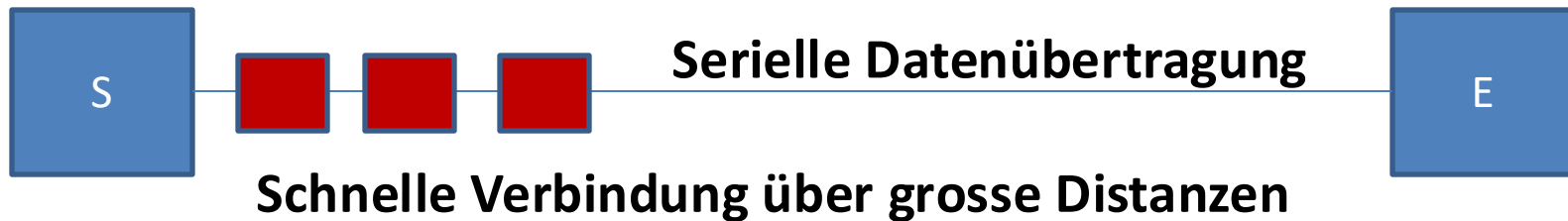


Zusammenfassen verschiedener Datenverbindungen:

Multiplexing bedeutet, mehrere Signale oder Informationsströme auf einer Leitung gleichzeitig in Form eines einzigen, komplexen Signals zu übertragen und dann auf der Empfangsseite wieder in separate Signale zu zerlegen.

Ein Kanal überträgt die verschiedenen Signale in unterschiedlichen Zeitschlitzten oder unterschiedlichen Lichtwellenlängen

Seriell vs. Parallel



Vergleich OSI und TCP/IP Modelle

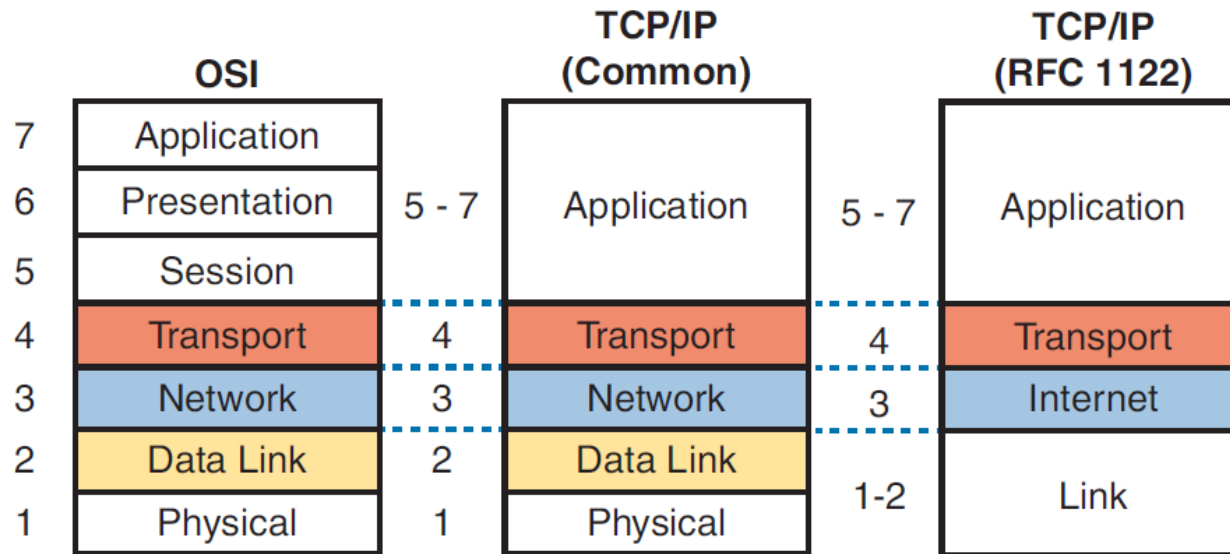


Figure 1-14 *OSI Model Compared to the Two TCP/IP Models*

NOTE The CCNA exam topics no longer mention the OSI or TCP/IP models; however, you should know both and the related terminology for everyday network engineering discussions. While today you will see the five-layer model used throughout the industry, and in this book, the figure includes the original RFC 1122 four-layer model for perspective.

Grundlagen ICT

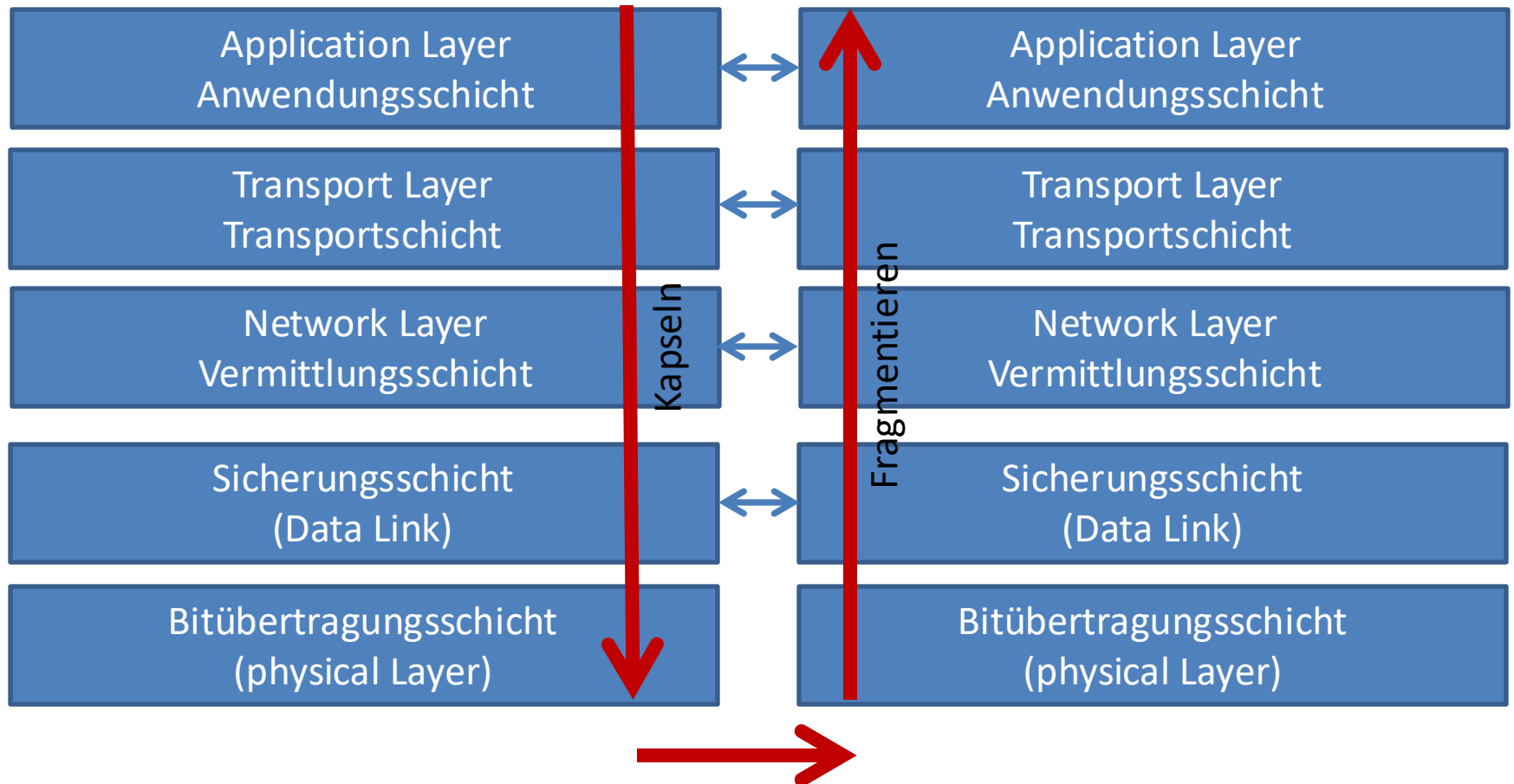
Übersicht ISO/OSI-Modell

TCP/IP

OSI-Schicht	Einordnung	DoD-Schicht	Protokollbeispiel	Einheiten
7 Anwendungen (Application)	Anwendungs-orientiert	Anwendung	HTTP FTP HTTPS SMTP LDAP NCP	Daten
6 Darstellung (Presentation)				
5 Sitzung (Session)				
4 Transport (Transport)	Transport-orientiert	Transport	TCP UDP SCTP SPX	TCP = Segmente UDP = Datagramme
3 Vermittlung (Network)		Vermittlung	ICMP IGMP IP IPsec IPX	Pakete
2 Sicherungsschicht (Data Link)		Netzzugriff	Ethernet Token Ring FDDI ARCNET	Rahmen (Frames)
1 Bitübertragung (Physical)				Bits

Quelle: wikipedia.org
DoD = Department of Defense

Einordnung der Übertragung in das aktualisierte fünf Schichten TCP/IP-Modell



Die Vermittlungsarten

- **Leitungsvermittlung**

- Ressourcen entlang der Übertragungsstrecke werden reserviert (z.B. Klassische Telefonie)



- **Paketvermittlung**

- Ressourcen entlang der Übertragungsstrecke werden **nicht** reserviert (Internet)



Verbindungslos und verbindungsorientiert

Beispiel TCP und UDP

- **Verbindungsorientiert**

z.B. TCP: Transmission Control Protocol

– Paketempfang wird bestätigt (ACK)



- **Verbindungslos**

z.B. UDP: User Datagram Protocol

– Paketempfang wird nicht bestätigt



Agenda

Repetition
**«Protokolle und
Übertragungsprozess»**

Grundlagen ICT

Übersicht ISO/OSI-Modell

TCP/IP

OSI-Schicht	Einordnung	DoD-Schicht	Protokollbeispiel	Einheiten
7 Anwendungen (Application)	Anwendungs-orientiert	Anwendung	HTTP FTP HTTPS SMTP LDAP NCP	Daten
6 Darstellung (Presentation)				
5 Sitzung (Session)				
4 Transport (Transport)	Transport-orientiert	Transport	TCP UDP SCTP SPX	TCP = Segmente UDP = Datagramme
3 Vermittlung (Network)		Vermittlung	ICMP IGMP IP IPsec IPX	Pakete
2 Sicherungsschicht (Data Link)		Netzzugriff	Ethernet Token Ring FDDI ARCNET	Rahmen (Frames)
1 Bitübertragung (Physical)				Bits

Quelle: wikipedia.org
DoD = Department of Defense

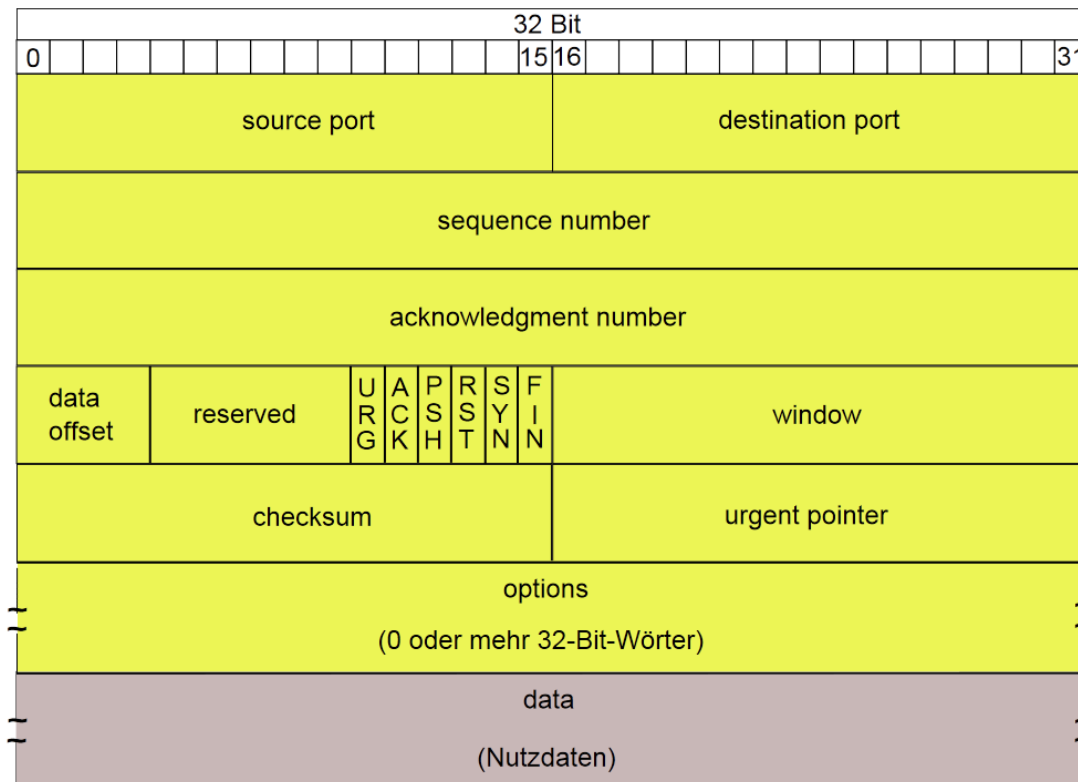
User Datagram Protocol


UDP-Header

0-15 Bit	16-31 Bit
Source Port	Destination Port
Packet Länge	Checksumme

- Unzuverlässig (keine Kontrolle)
- Weniger Overhead als TCP
- UDP überwacht keine Sequenznummern
 - Setzt deshalb Datagramme nicht in der richtigen Reihenfolge zusammen. Anwendung muss dies tun.

TCP-Header



 TCP-Header

Quelle: Wikipedia.org, Appaloosa, 23:04, 6. Jul. 2007 (CEST)

http://de.wikipedia.org/w/index.php?title=Datei:TCP_Header.svg&filetimestamp=20070706210301

https://en.wikipedia.org/wiki/Transmission_Control_Protocol

Grundlagen IPv4

- IPv4 Paket Header

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	Bit	
Version			IHL			TOS (Type of Service)									Paket-Gesamtlänge inkl. Header (Mind. 576 Bytes, Max 65535 Bytes)																	
Kennung (Identifikation)															Flags			Fragment Offset														
TTL (Time to live)						Protokoll									Header Checksumme																	
Quell-IP-Adresse (Source Address)																																
Ziel-IP-Adresse (Destination Address)																																
Optionen und Füllbits (Padding)																																

Version = V4/V6

IHL= IP Header Length

Paketlänge = gesamtes Paket inkl. Kopfdaten

Flags = 0,1,2 Fragmentierung Kontroll-Schalter

TTL = Lebensdauer des Pakets Anzahl Hops (Max. 255)

Header Checksumme = sichert Header

<https://de.wikipedia.org/wiki/IPv4>

TOS = Type of Service (Priorität)

Kennung = Fragmente erkennen

Fragmentoffset = Aufteilung

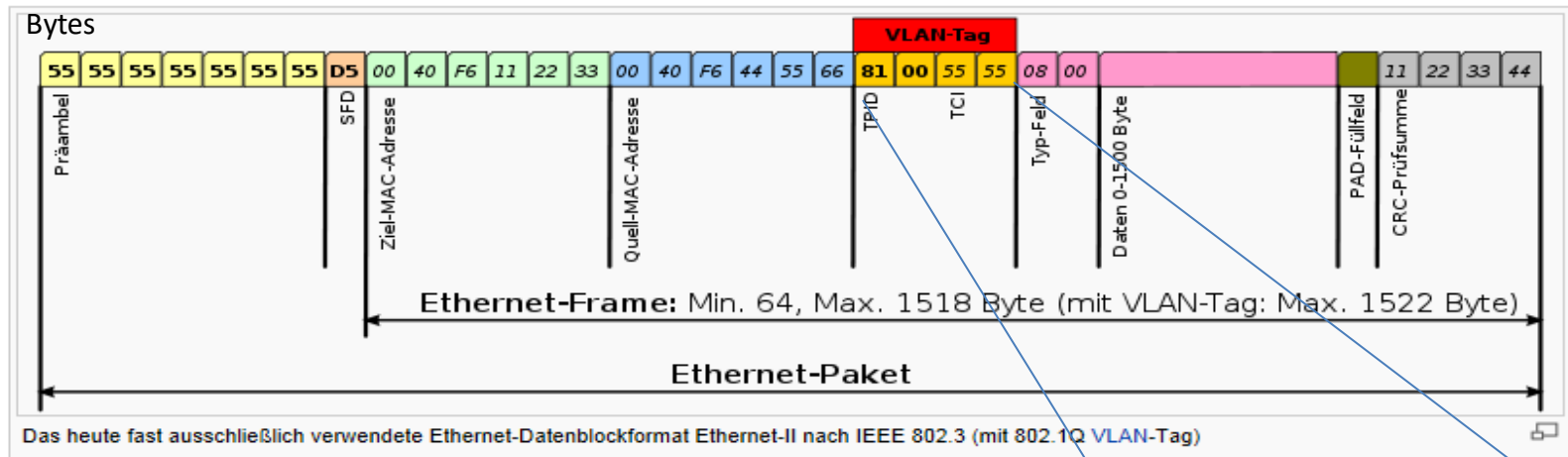
Protokoll = Folgeprotokoll (TCP/UDP)

Optionen/Füllbits = Zusatzinfos

Repetition IEEE 802.3

Beispiel Ethernet Frame

- Frames (Ethernet IEEE 802.3)



- Präambel / Start Frame Delimiter (aus kompatibilitätsgründen, diente der Synchronisation) (8 Byte – L1 Header)
- VLAN-Tag für die Definition von VLANs (4 Byte)
- Type Feld für die Definition des folgenden Protokolls auf höherer Schicht
- PAD Feld dient der Definition der Mindestgrösse von 64 Byte
- Trailer: CRC Prüfsumme / FCS-Feld - Frame Check Sequence (4 Byte)

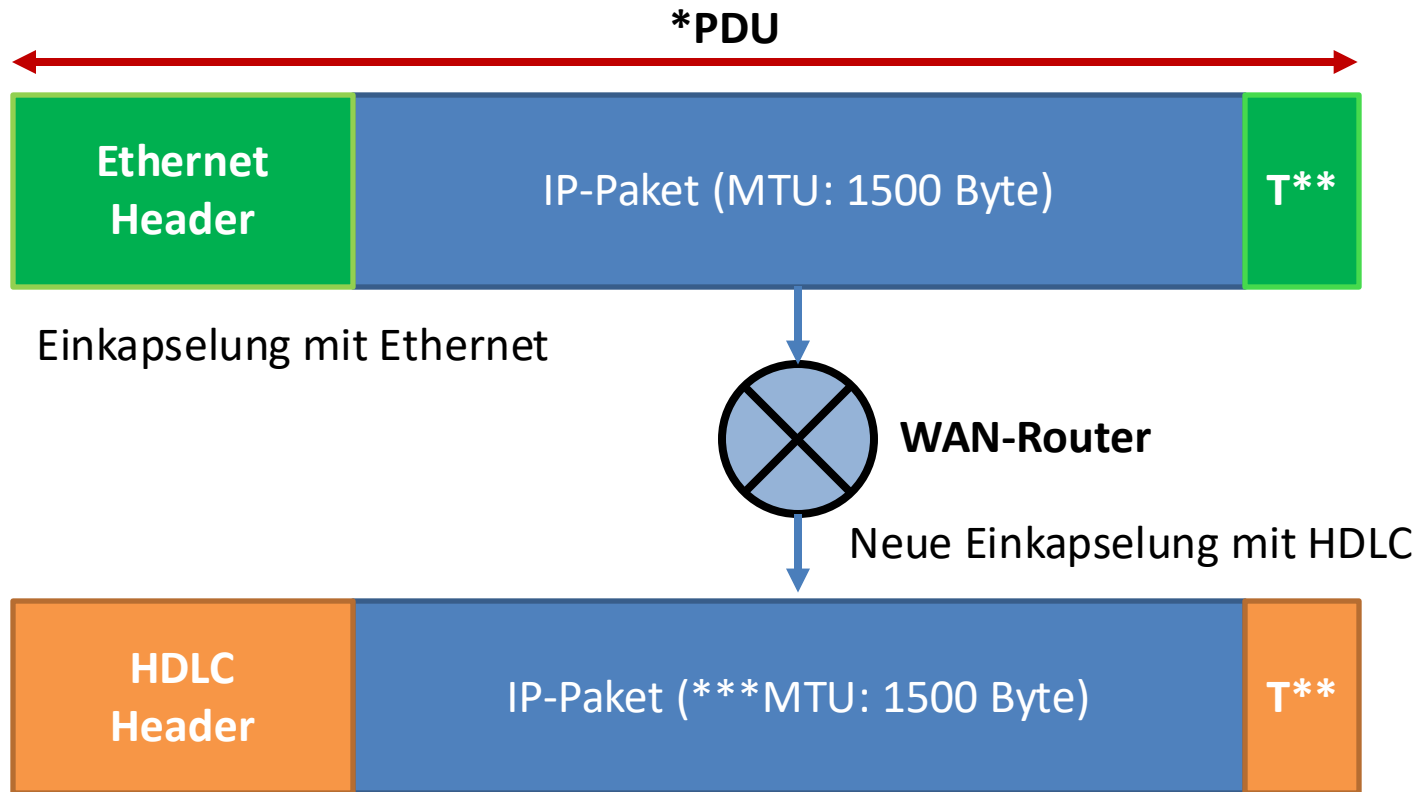
Quelle Grafik: Wikipedia.org

16 bits	3 bits	1 bit	12 bits
TPID	TCI		
	PCP	DEI	VID

VID = VLAN-ID (4096 mögliche VLANs, 2^{12})

Repetition

Der Kapselungsprozess (Encapsulation)



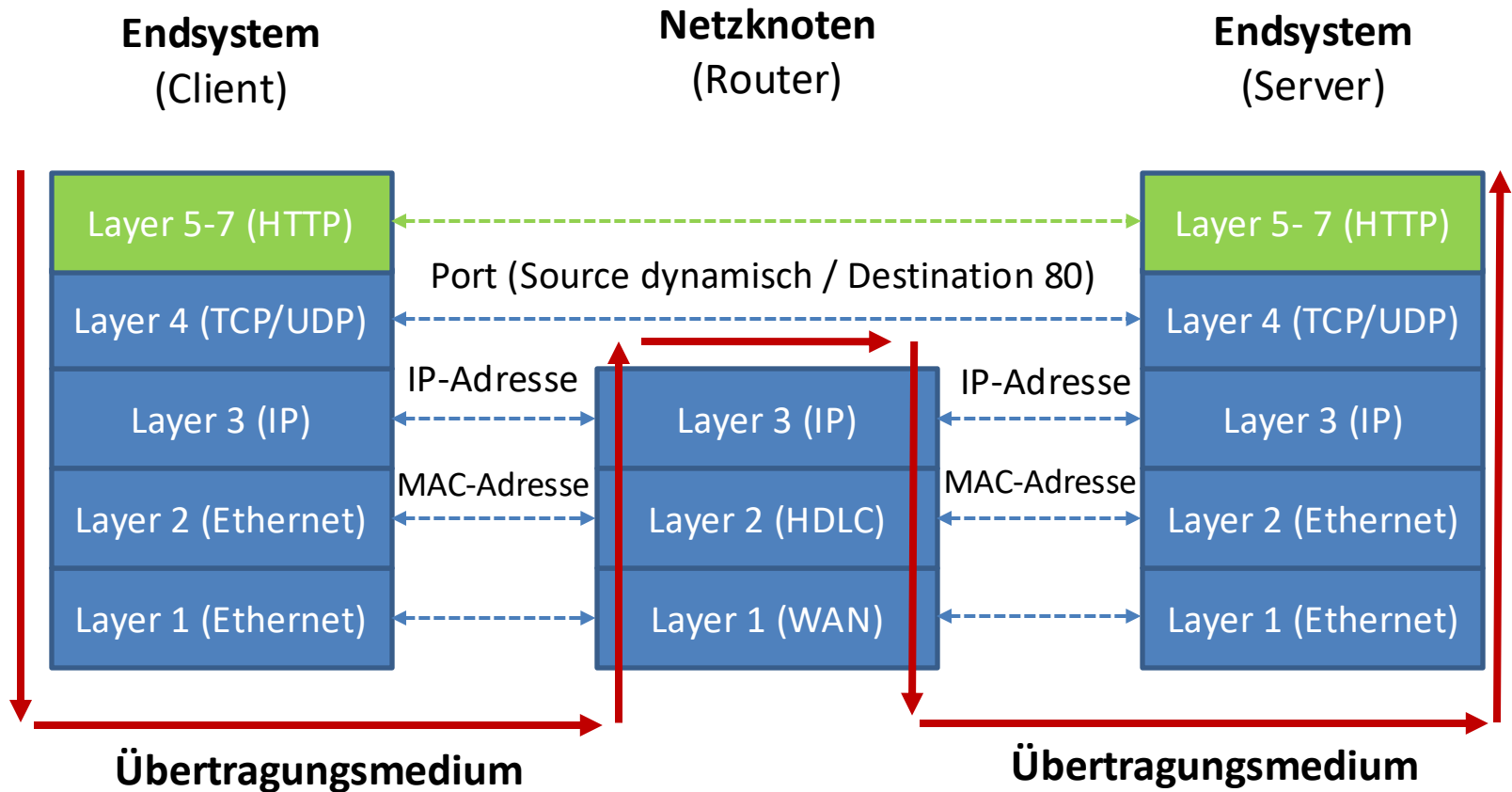
*Protocol Data Unit

**Trailer / CRC-Prüfsumme

***Maximum Transmission Unit (Bezieht sich hier auf max. Nutzdatenteil bei Ethernet.)

Repetition

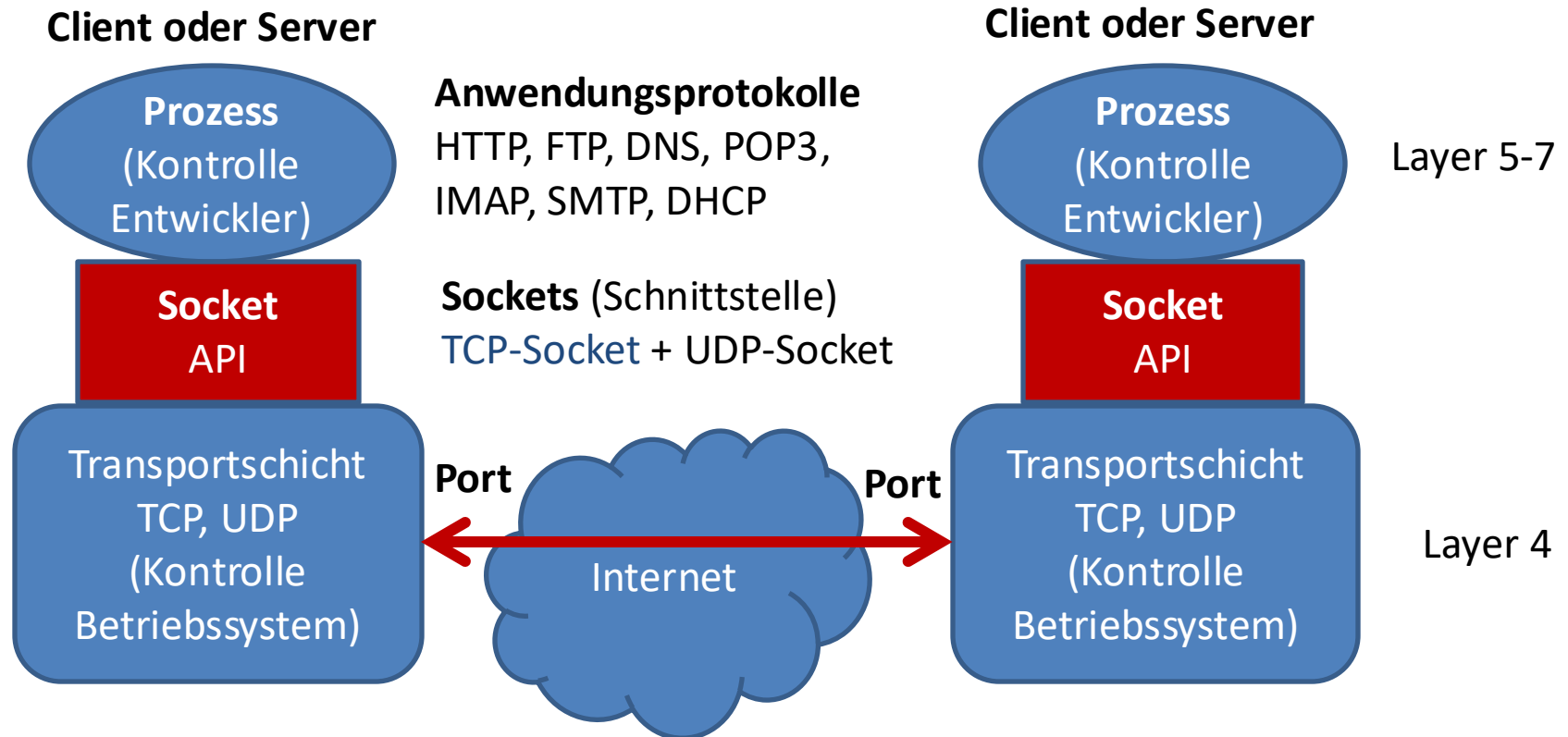
Der Übertragungsprozess



Agenda

Repetition
**«Ports, Sockets, TCP-
Verbindungen»**

Verbindung Anwendung mit Transportschicht (OSI-Layer 4)



Socket = Port-Nummer + IP-Adresse für eindeutige Zuordnung zu einem Prozess

In Anlehnung an Quelle:

Kurose J. F., Keith W. R., S.193, Computernetzwerke. 5. akt. Auflage, Pearson Deutschland GmbH

Port-Nummern

Ein Port wird benötigt um den Datenstrom einem Prozess/Programm zuzuordnen

Port-Arten	Port-Nummern
Well-Known-Ports (Sind für Dienste und Anwendungen reserviert)	0 - 1023
Registrierte Ports (Werden Benutzerprozessen oder Benutzeranwendungen zugeordnet)	1024 - 49151
Dynamische oder private Ports (Werden dynamisch Clientanwendungen zugewiesen)	49152 - 65535

Socket = Port-Nummer + IP-Adresse für eindeutige Zuordnung zu einem Prozess

Die wichtigsten Anwendungen und deren Ports

1. Teil

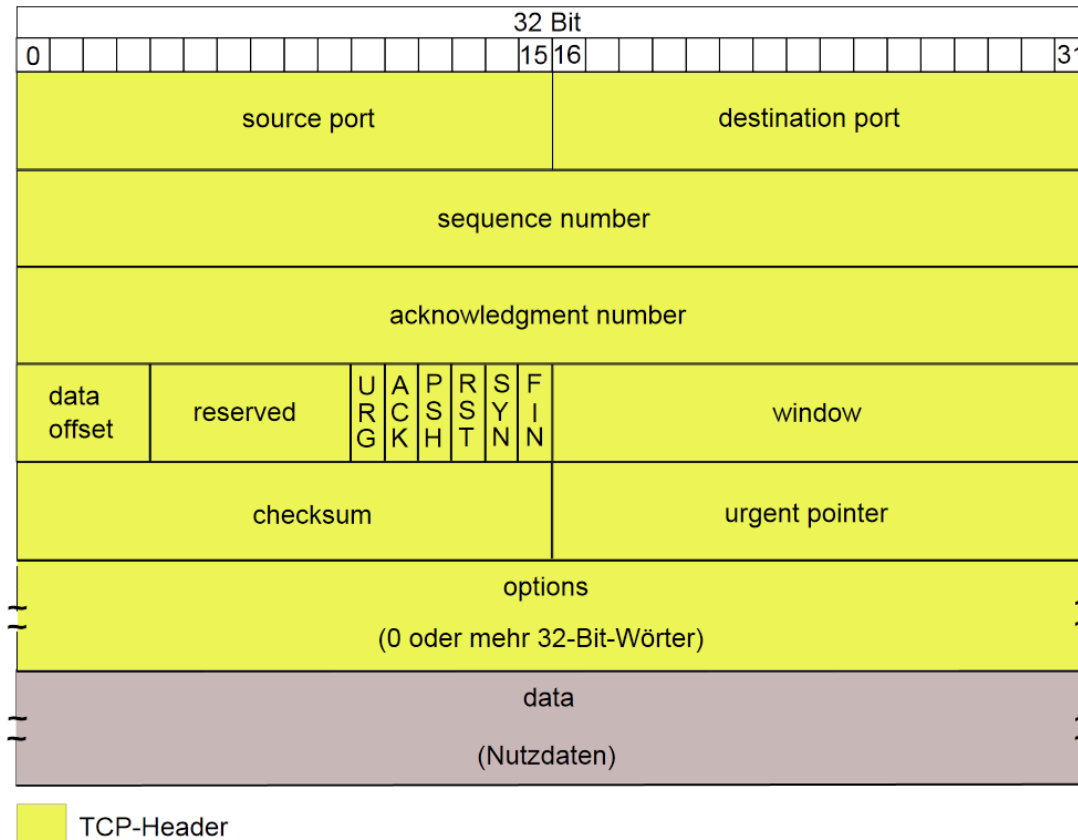
Dienstbezeichnung	Protokoll	Ports
Dateifreigabe (Serverdienste)	SMB 2.1 (Win 7 / Win Server 2008 R2) SMB 3.0 (Win 8 / Win Server 2012) SMB 3.1.1 (Win 10 / Win Server 2016)	TCP 445
WWW-Webdienste	HTTP HTTPS (SSL/TLS)	TCP 80 TCP 443
E-Mail-Dienste	SMTP (Mailversand) SMTPS (SSL/TLS) POP3 (Mailempfang) POP3S (SSL/TLS) IMAP (Mailempfang) IMAPS (SSL/TLS)	TCP 25 TCP 465 TCP 110 TCP 995 TCP 143 TCP 993
Namensauflösung	DNS (Domain-Namen in IP-Adressen)	UDP 53
Automatische IP-Vergabe	DHCP (Server oder Relay-Agent) DHCP (Client Anfragen)	UDP 67 UDP 68

Die wichtigsten Anwendungen und deren Ports

2. Teil

Dienstbezeichnung	Protokoll	Ports
Datenübermittlung	FTP (Datenübertragung) FTP (Kontrollport)	TCP 21 TCP 20
Zeitsynchronisierung	NTP (Network Time Protocol)	UDP 123
Verzeichnisdienste	LDAP LDAPS (SSL/TLS)	TCP/UDP 389 TCP/UDP 636
IP-Telefonie VoIP	SIP SIP (SSL/TLS)	UDP 5060 (TCP) TCP 5061
Netzwerkverwaltung	SNMPv3 SNMPv3 (Trap)	UDP 161 UDP 162
VPN Site-to-Site	IPSEC, IKE	UDP 500
Konsolenverbindung (Fernwartung)	SSH (Secure Shell)	TCP 22

TCP-Header



Quelle: Wikipedia.org, Appaloosa, 23:04, 6. Jul. 2007 (CEST)

http://de.wikipedia.org/w/index.php?title=Datei:TCP_Header.svg&filetimestamp=20070706210301

Three-Way-Handshake SYN-Aufzeichnung mit Wireshark

Wireshark 1.8.4 (SVN Rev 46250 from /trunk-1.8) - Capturing from Microsoft:\Device\NPF\{37FAF8A3-D329-4408-8FE7-FBB87A4D8901}

Filter: tcp

No.	Time	Source	Destination	Protocol	Length	Info
4	0.75281500	192.168.77.45	173.194.44.216	TCP	66	53611 > http [SYN] Seq=0 win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
5	0.77380000	173.194.44.216	192.168.77.45	TCP	66	http > 53611 [SYN, ACK] Seq=0 Ack=1 win=5840 Len=0 MSS=1452 SACK_PERM=1 WS=64
6	0.77384700	192.168.77.45	173.194.44.216	TCP	54	53611 > http [ACK] Seq=1 Ack=1 win=17424 Len=0
8	0.86517700	192.168.77.45	173.194.44.216	HTTP	370	GET / HTTP/1.1
10	0.87339300	192.168.77.45	83.145.197.2	TCP	66	53613 > http [SYN] Seq=0 win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
11	0.88684700	173.194.44.216	192.168.77.45	TCP	60	http > 53611 [ACK] Seq=1 Ack=317 win=6912 Len=0
12	0.94406500	83.145.197.2	192.168.77.45	TCP	66	http > 53613 [SYN, ACK] Seq=0 Ack=1 win=5840 Len=0 MSS=1452 SACK_PERM=1 WS=128
13	0.94411900	192.168.77.45	83.145.197.2	TCP	54	53613 > http [ACK] Seq=1 Ack=1 win=17424 Len=0
14	0.94947900	192.168.77.45	83.145.197.2	HTTP	516	GET /0.4/update?id=e4ac84f4c9f4d90bd90e308d09a92882d17c96af&nonce=74ad37d9ee59d1130b4d2b1332b873d74e0bb5d9&format=4&lang=de-D
15	0.96598700	173.194.44.216	192.168.77.45	TCP	1506	[TCP segment of a reassembled PDU]
16	0.96827400	173.194.44.216	192.168.77.45	TCP	1506	[TCP segment of a reassembled PDU]
17	0.96829700	192.168.77.45	173.194.44.216	TCP	54	53611 > http [ACK] Seq=317 Ack=2905 win=17424 Len=0
18	0.97023300	173.194.44.216	192.168.77.45	TCP	1122	[TCP segment of a reassembled PDU]
19	0.97269200	173.194.44.216	192.168.77.45	TCP	1506	[TCP segment of a reassembled PDU]
20	0.97272400	192.168.77.45	173.194.44.216	TCP	54	53611 > http [ACK] Seq=317 Ack=5425 win=17424 Len=0

Internet Protocol Version 4, Src: 192.168.77.45 (192.168.77.45), Dst: 173.194.44.216 (173.194.44.216)

Transmission Control Protocol, Src Port: 53611 (53611), Dst Port: http (80), Seq: 0, Len: 0

Source port: 53611 (53611)
Destination port: http (80)
[Stream index: 0]
Sequence number: 0 (relative sequence number)
Header length: 32 bytes

Flags: 0x002 (SYN)

- 000. = Reserved: Not set
- ...0 = Nonce: Not set
- ...0 = Congestion window Reduced (CWR): Not set
-0. = ECN-Echo: Not set
-0. = Urgent: Not set
-0. = Acknowledgment: Not set
-0. = Push: Not set
-0. = Reset: Not set
-0. = Syn: Set
-0. = Fin: Not set

window size value: 8192
[calculated window size: 8192]
Checksum: 0x47cf [validation disabled]
Options: (12 bytes), Maximum segment size, No-Operation (NOP), window scale, No-Operation (NOP), No-Operation (NOP), SACK permitted

0000 00 13 49 fd 7a 80 10 0b a9 6a 7d d8 08 00 45 00 ..I.Z...}}...E.
0010 00 34 03 1d 40 00 00 06 0f 37 c0 a8 4d 2d ad c2 .4..@...7..M-..
0020 2c d8 d1 6b 00 50 d8 ac 74 6e 00 00 00 00 80 02 ..K.P..tn.....
0030 20 00 47 cf 00 00 02 04 05 b4 01 03 03 02 01 01 ..G.....
0040 04 02

Frame (frame), 66 bytes
Packets: 3379 Displayed: 2519 Marked: 0
Profile: Default

TCP Verbindung aufbauen und gewährleisten (three-way-handshake)

1.

Sende SYN

(SEQ=100, CTL=SYN)

2.

Empfange SYN

Sende SYN-ACK

(SEQ=300, ACK=101,
CTL=SYN, ACK)

3.

SYN wurde empfangen

Verbindung aufgebaut

Sende ACK

(SEQ=101, ACK=301,
CTL=ACK)

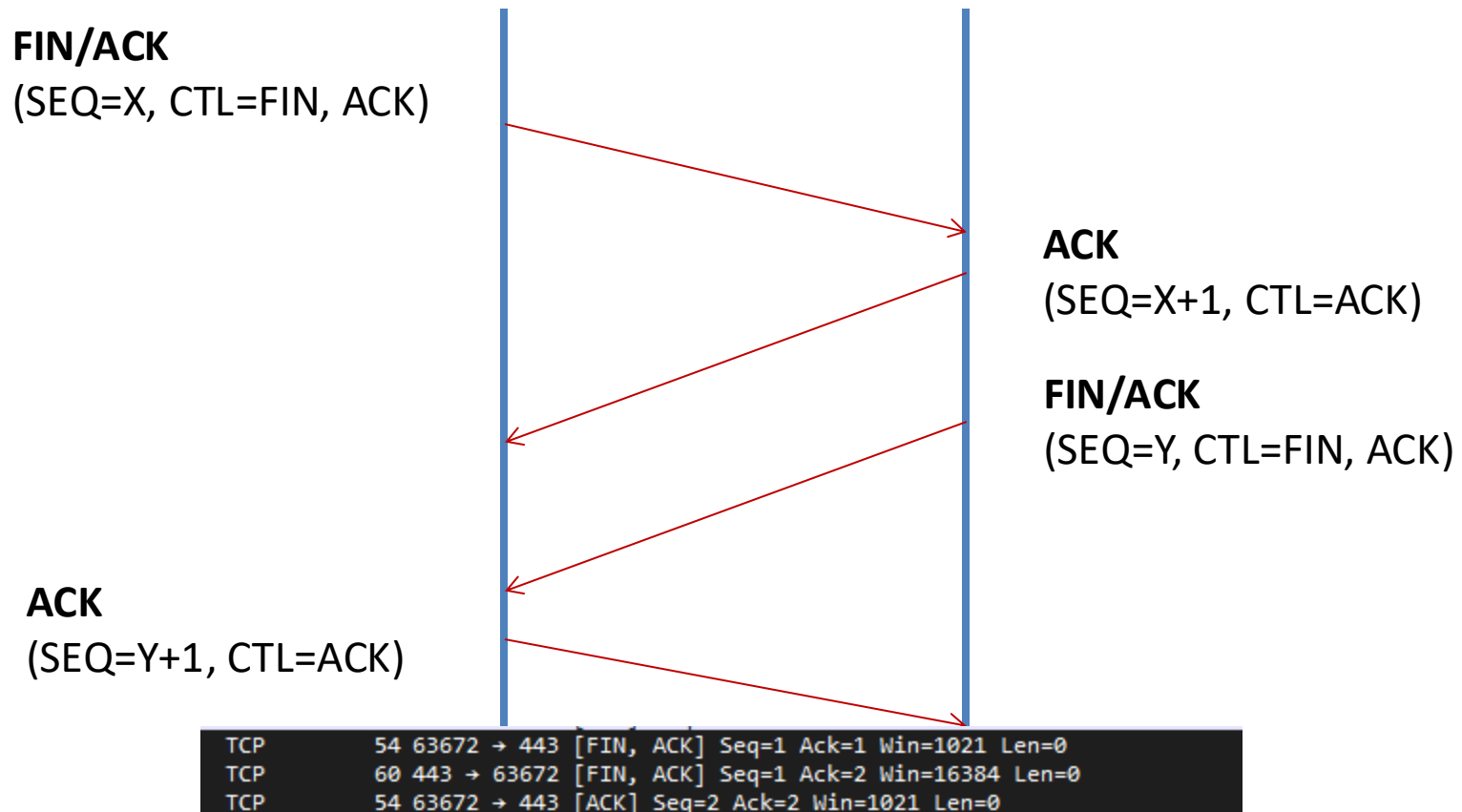
```
sequenceDiagram
    participant A
    participant B
    A->>B: 1. SYN (SEQ=100, CTL=SYN)
    B-->A: 2. SYN-ACK (SEQ=300, ACK=101, CTL=SYN, ACK)
    A->>B: 3. ACK (SEQ=101, ACK=301, CTL=ACK)
```

TLSv1.3	1777	Client Hello (SNI=campus.ifa.ch)
TLSv1.2	156	Application Data
TLSv1.2	92	Application Data
TCP	54	63607 → 443 [ACK] Seq=7741 Ack=53497 Win=1026 Len=0

[http://de.wikipedia.org/
wiki/Drei-Wege-
Handschlag](http://de.wikipedia.org/wiki/Drei-Wege-Handschlag)

TCP Verbindung abbauen

TCP teardown process (ordentlich)



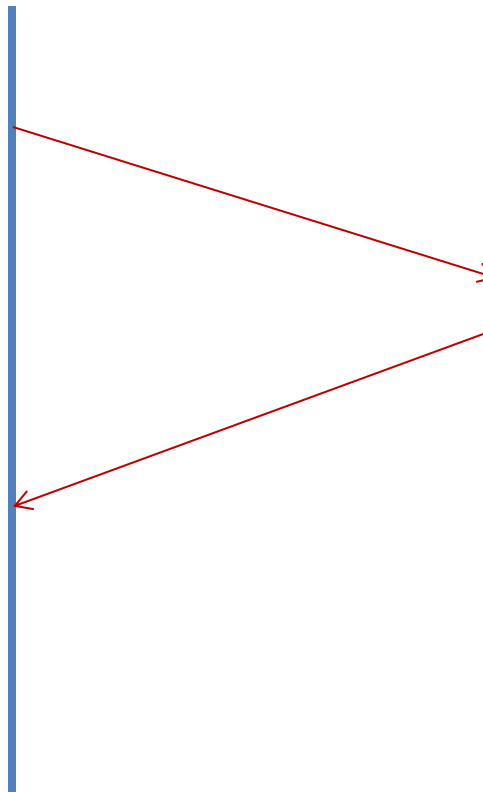
TCP Verbindung abbrechen

Reset / RST-Flag

SYN
(SEQ=X, CTL=SYN)

RST/ACK
(SEQ=X+1, CTL=RST, ACK)

Verbindung ist beendet



CTL Werte (Flags)

CTL-Wert	Beschreibung
URG	Urgent, dringend (selten gebraucht)
ACK	Acknowledgement (Bestätigung des TCP-Segment Empfangs)
PSH	Push (kleinere Segmente werden gesandt, vorher und nachher gepuffert)
RST	Reset (Abbruch der Verbindung, Probleme oder Abweisung)
SYN	Synchronize (Synchronisation von Sequenznummern)
FIN	Finish (Schlussflag, keine Daten kommen mehr)

Nützliches zu TCP ist auf Wikipedia.org zu finden.

http://de.wikipedia.org/wiki/Transmission_Control_Protocol

Datenflusssteuerung

TCP Receive Window-Size (Empfangsfenster)

- Mit der Window-Size ist TCP in der Lage mehrere Pakete zu senden ohne bei jedem versandten Paket die Bestätigung ACK abwarten zu müssen.
- Dazu wird eine Window-Size, also ein Empfangsfenster bestimmt.
- Dies ist dann auch das Maximum, welches ohne Empfangsbestätigung ACK gesandt werden kann.
- So ist sichergestellt, dass der Empfangsspeicher (Puffer) nicht überläuft.

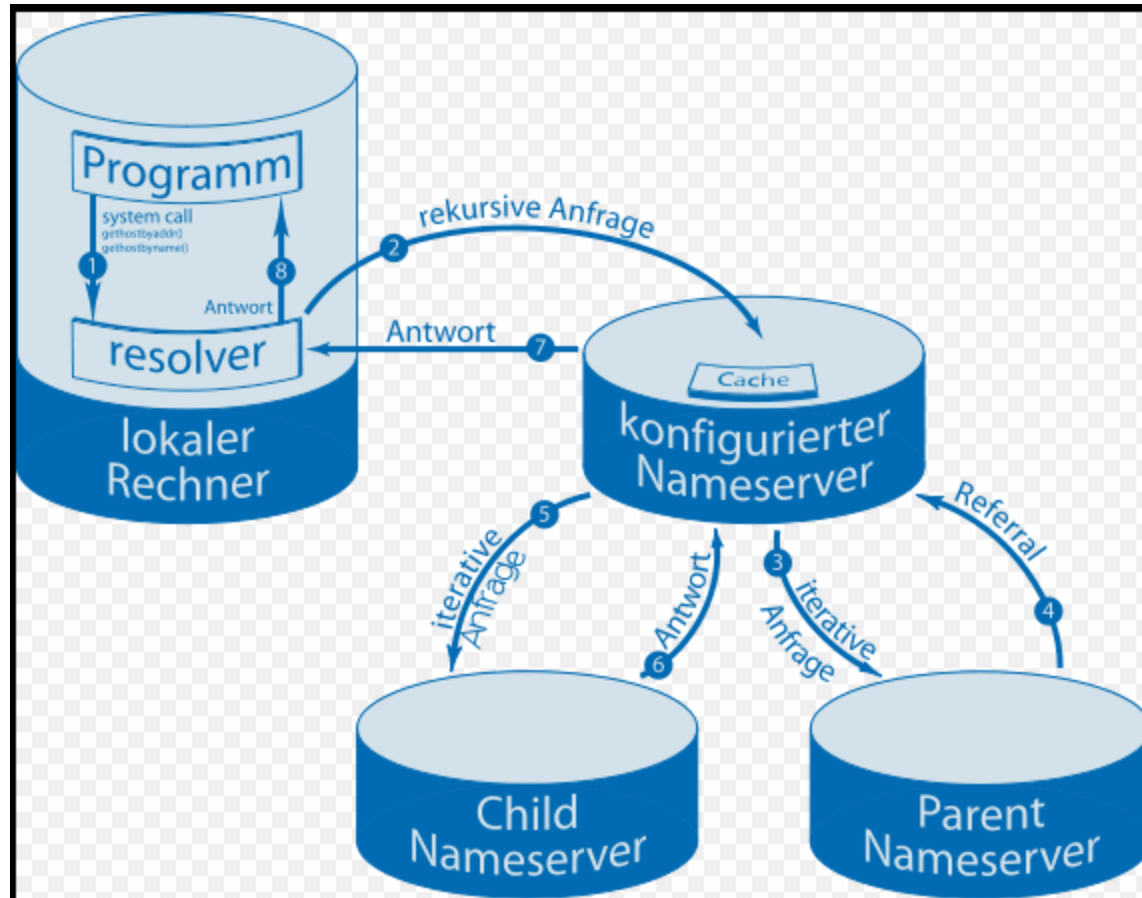
Agenda

Repetition
«DNS, Routing, ARP»

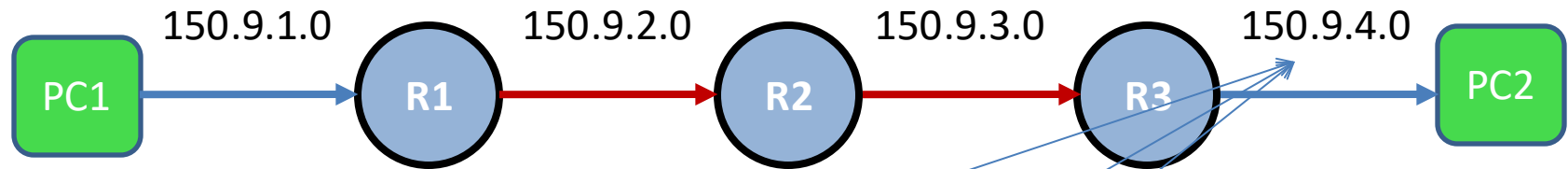
Wichtiges zu DNS

Bezeichnung	Kurzbeschreibung
FQDN – Fully Qualified Domain Name z.B. www.google.ch	<ul style="list-style-type: none">• Absolute eindeutige Adresse
Resolver (Programm auf lokalem Gerät, zur Anfrage an DNS Server)	<ul style="list-style-type: none">• Es braucht dazu mindestens einen DNS-Server-Eintrag• Iterativ (immer weitergeleitet von Server zu Server, z.B. DNS-Server)• Rekursiv direkte Antwort der IP-Adresse oder Name nächster DNS Server
Ressource Records (RR) DNS-Objekte (Beinhalten die Antwort vom DNS Server) (siehe auch nächstes Slide)	<ul style="list-style-type: none">• Z.B. mit einem Resource Record «A» wird einem DNS-Namen eine IPv4-Adresse zugeordnet• Diese werden in einer Zonendatei gespeichert (z.B. Hosts)

Funktion DNS-Abfrage



Beispiel einfacher Routingprozess



Routingtabelle Router **R1**

Subnetz	interface	Nächster Hop
150.9.4.0	Serial 0	150.9.2.0

Routingtabelle Router **R2**

Subnetz	Interface	Nächster Hop
150.9.4.0	Ethernet 0	150.9.3.0

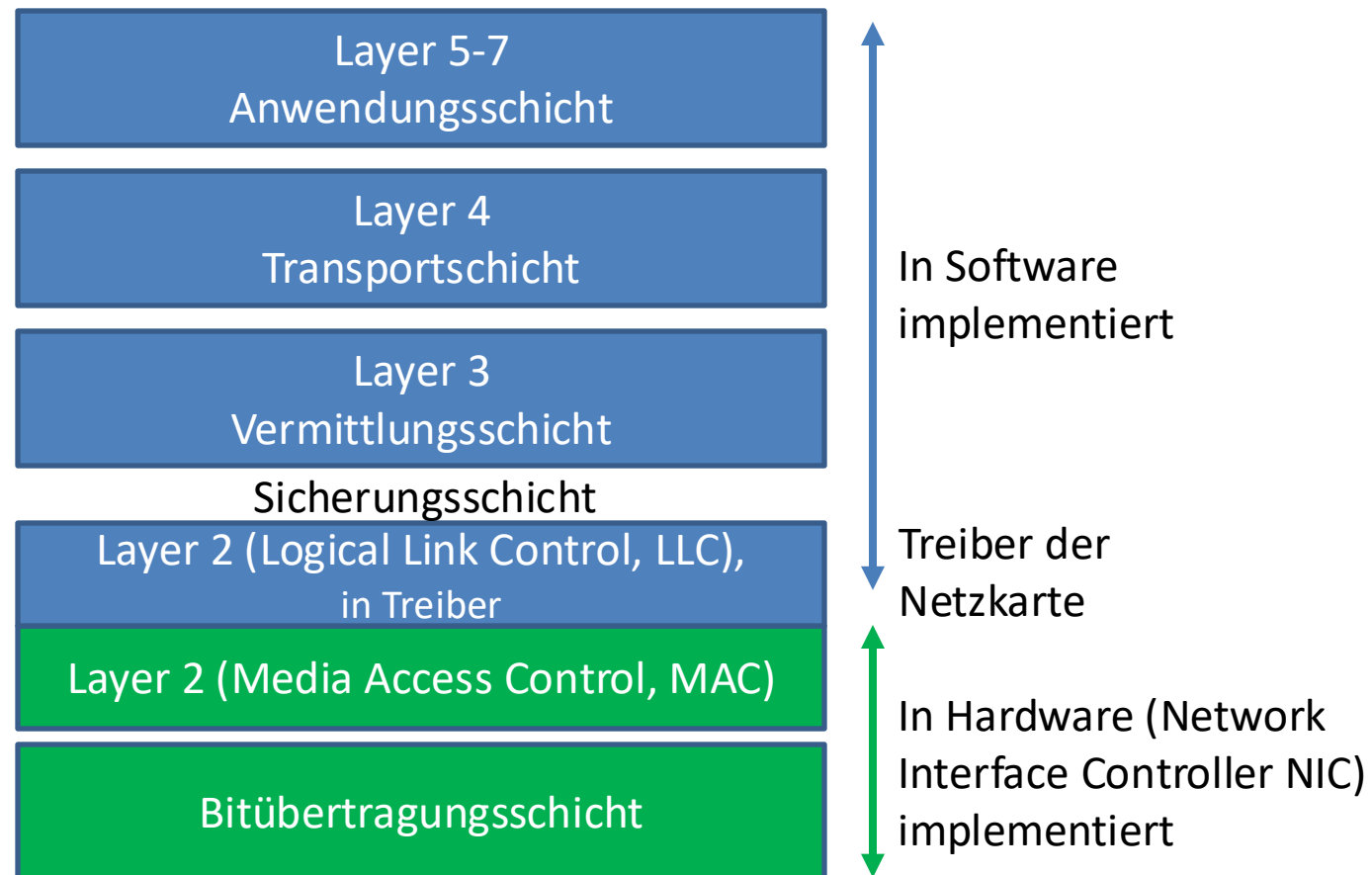
Routingtabelle Router **R3**

Subnetz	Interface	Nächster Hop
150.9.4.0	Ethernet 0	Nicht anwendbar

Wichtig:

Siehe Seite 108 für ein Beispiel mit der korrekten Cisco Notation.

Unterteilung und Implementierung der Sicherungsschicht



Unterteilung der Sicherungsschicht in die Teilschichten MAC und LLC (Ethernet)

Bezeichnung	Details Teilschichten der Sicherungsschicht bei Ethernet	Layer 2 (Logical Link Control)
		Layer 2 (Media Access Control)
LLC	<p>Logical Link Control (IEEE 802.2, LLC)</p> <p>LLC stellt die Verbindung zwischen der unteren L2 MAC-Teilschicht und der jeweiligen L3-Schicht (meist IP) der Netzwerksoftware her.</p> <p>Die MAC-Schicht kann sich je nach Medienzugriffsverfahren ändern, die LLC bleibt dabei gleich. Wird mit einem Treiber auf dem Computer implementiert, ist also ein Softwareprozess.</p>	
MAC	<p>Media Access Control (IEEE 802.3, CSMA/CD)</p> <p>Kapselt die L3-PDU in einen Frame und sorgt für den Medienzugriff im Ethernet Netzwerk. Das Datenformat (PDU) nennt sich Ethernet-Frame und ist 1518 Byte ohne und mit VLAN-Tag 1522 Byte gross. Ein Frame beginnt dabei mit dem Start Frame Delimeter = 10101011 und endet mit dem FCS-Feld (Frame Check Sequence). Durch die MAC Schicht wird ebenfalls die Datenflusssteuerung und Fehlererkennung übernommen. Die übermittelten Daten werden dabei entsprechend der Signalanforderungen des physischen Mediums getrennt. Daher ist die MAC-Teilschicht direkt in der Netzwerkkarte (NIC) als Hardwareprozess integriert.</p>	

Agenda



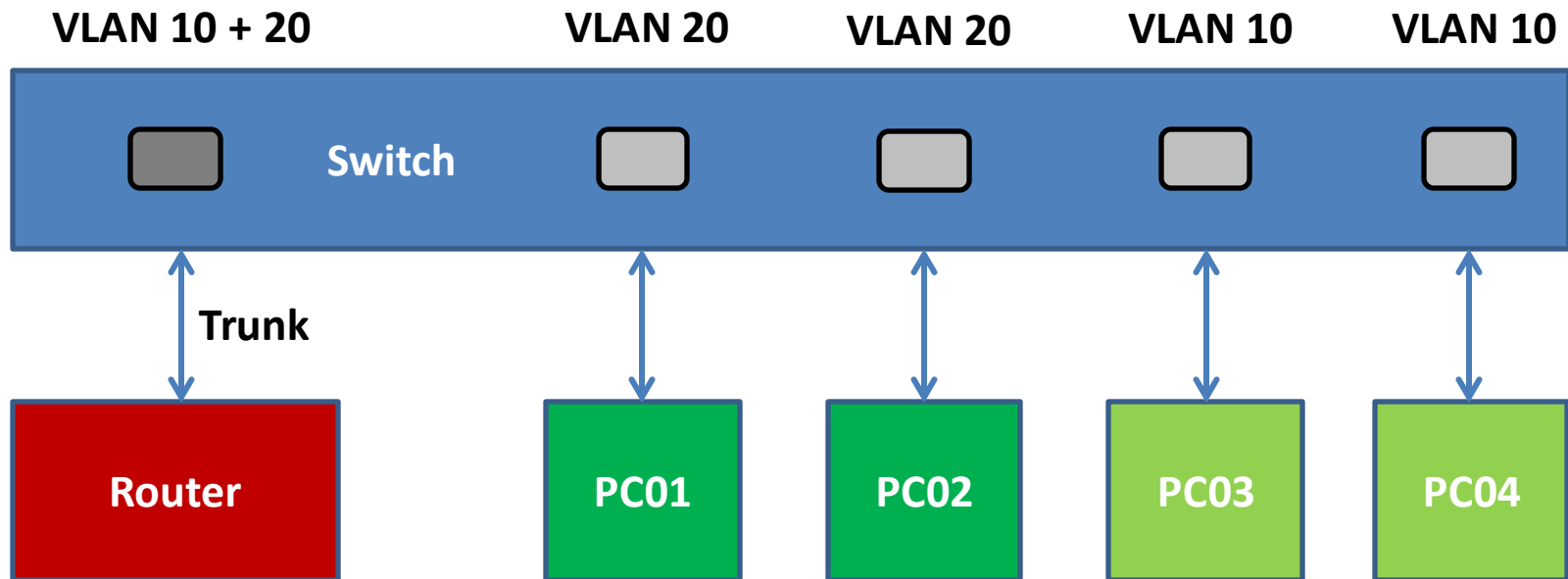
Repetition

«VLAN»



VLAN Grundlagen 802.1Q (tagged)

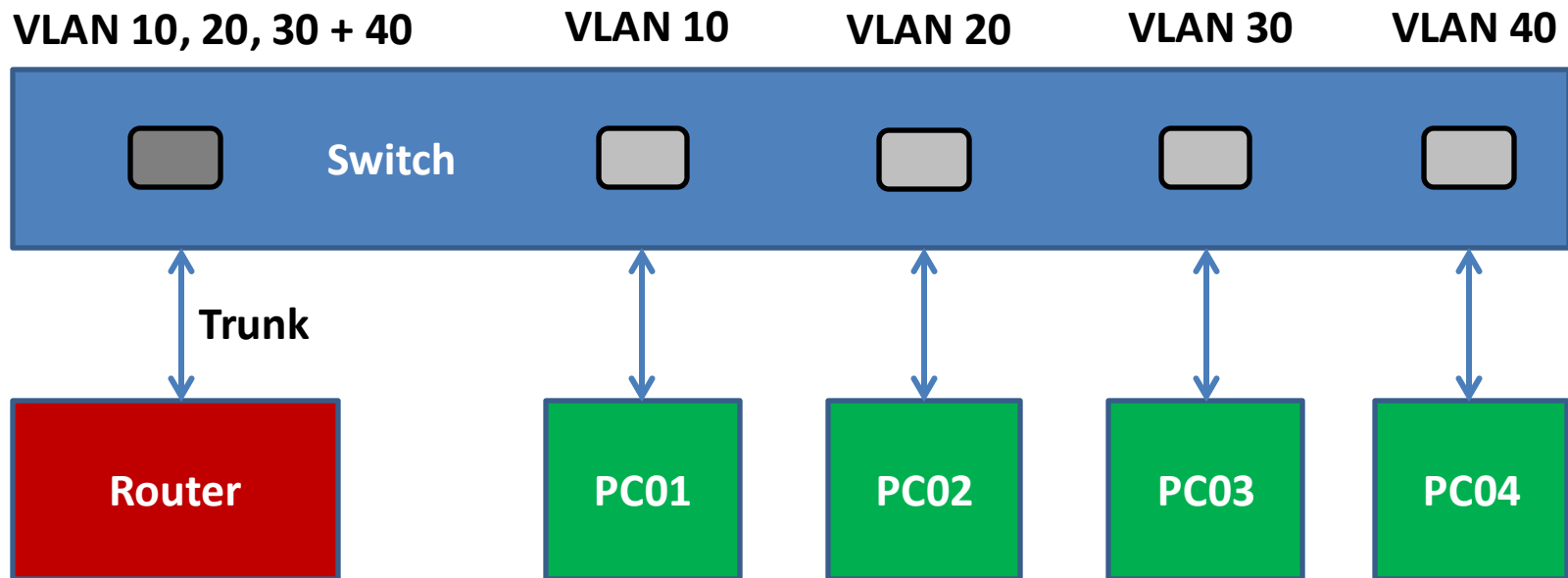
- Ein Computer in einem VLAN 1 kann nicht mit einem Computer in einem VLAN 2 kommunizieren. Über den Router können die VLANs verbunden werden.



- 802.1Q = IEEE-Standard** für «tagged» VLAN-Technik

VLAN Security 802.1Q (tagged)

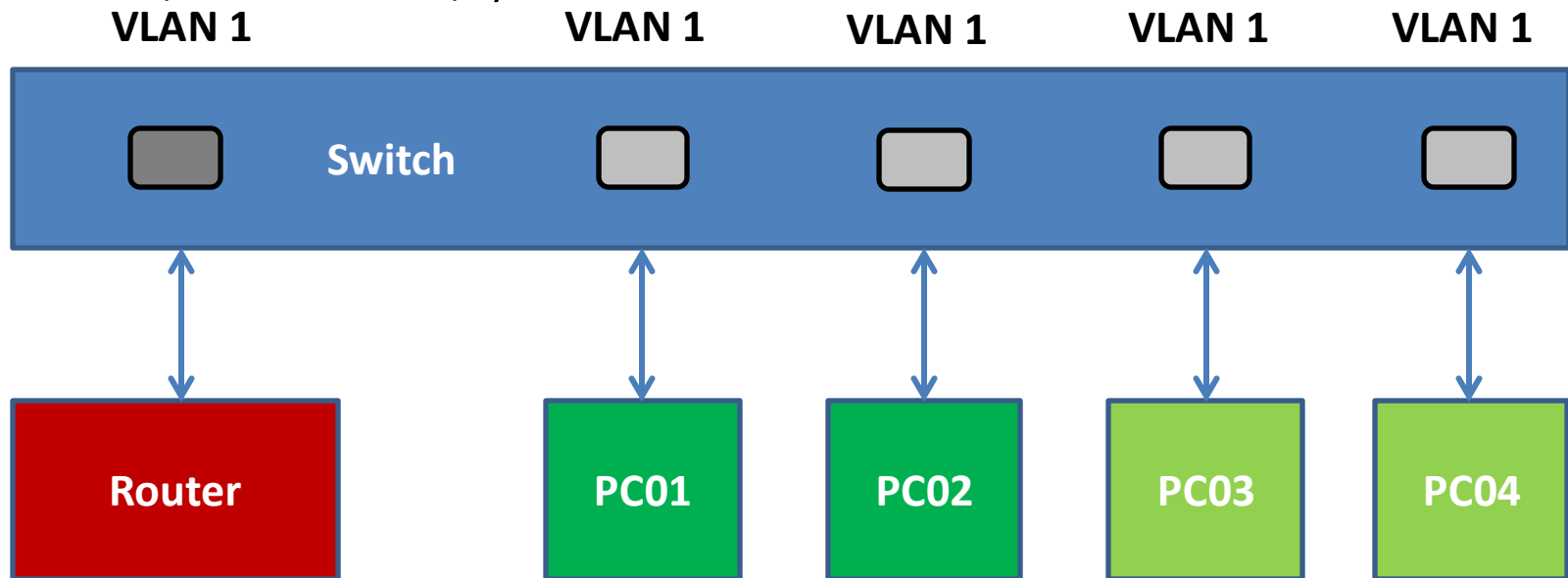
- Alle Computer sind in einem eigenen VLAN von allen anderen Computern getrennt.



VLAN Grundlagen

Natives/Default VLAN (Cisco **VLAN 1**)

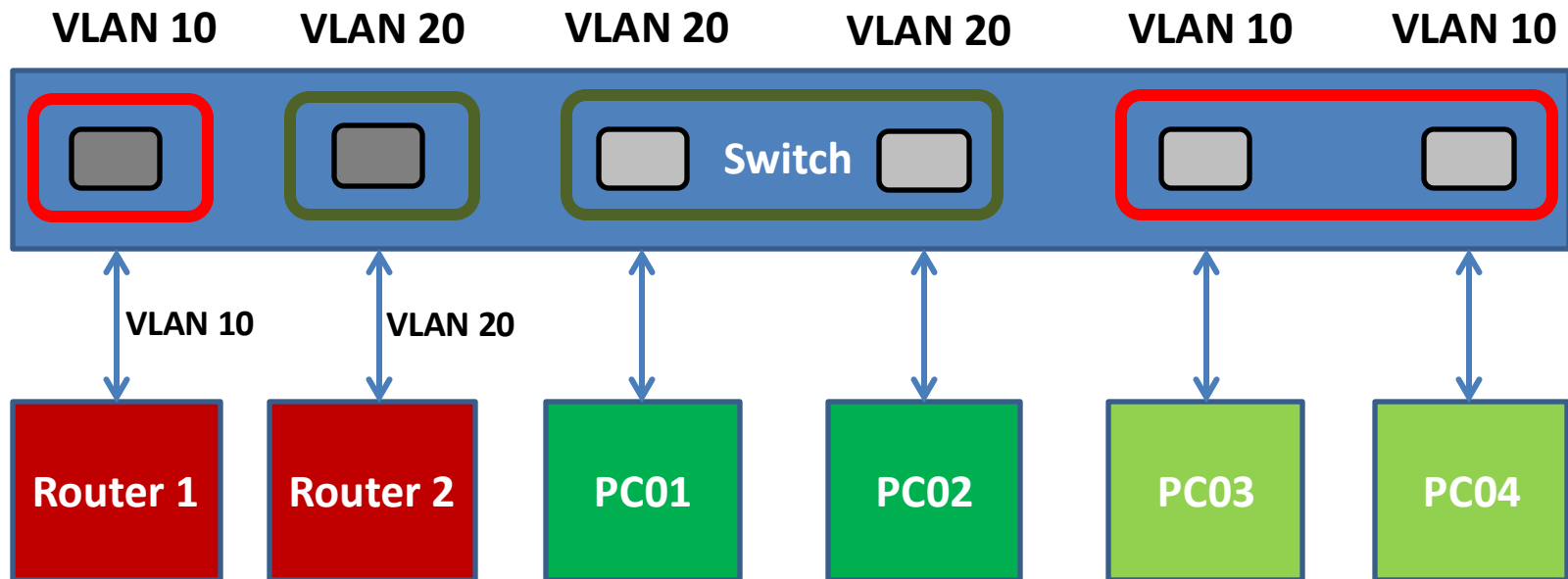
- **Nativ werden alle Port in das VLAN1 genommen** (Natives VLAN oder **Default VLAN**). VLAN1 erstellt kein VLAN-Tag und ermöglicht damit Kompatibilität zu nicht VLAN fähigen Netzgeräten. Das native (default) VLAN kann konfiguriert werden sollte aber auf allen Netzgeräten (Switch, Router, Access Point,..) das selbe sein!



VLAN Grundlagen

Portbasierte VLAN (Access Interfaces)

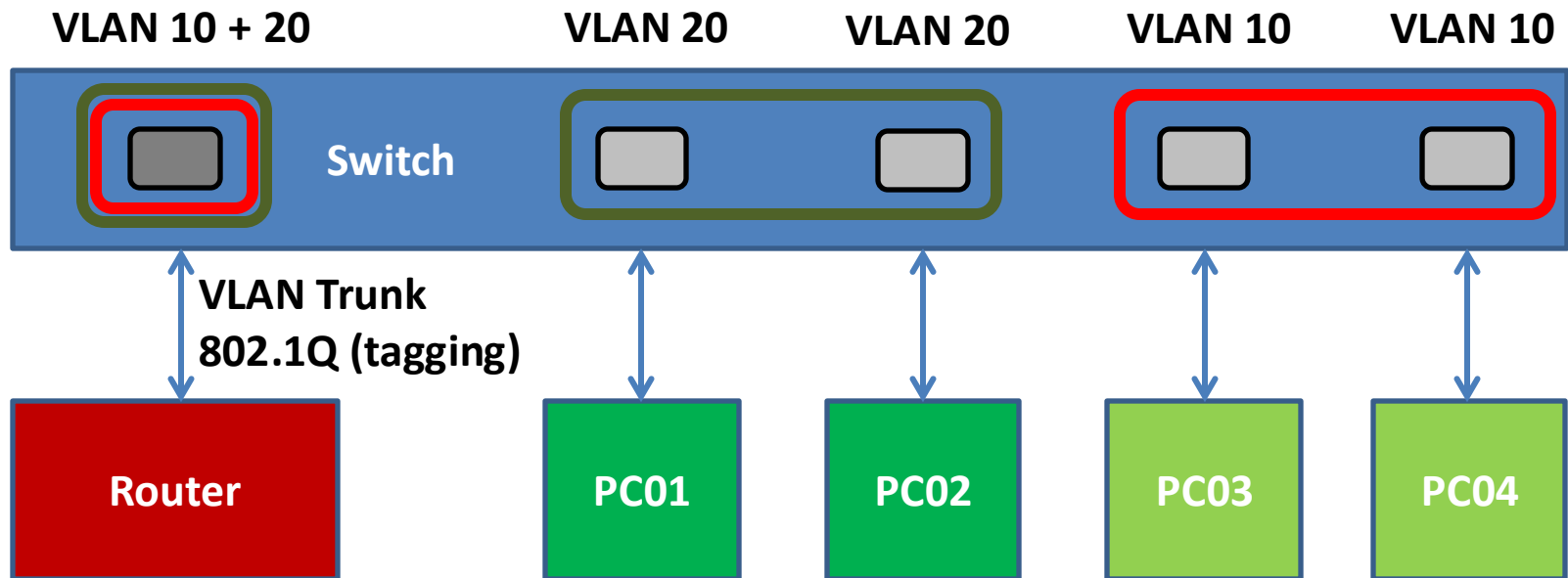
- Ein Computer in einem VLAN 10 kann nicht mit einem Computer in einem VLAN 20 kommunizieren. Bei **portbasierten VLANs** kann ein Interface nur einem VLAN angehören.



VLAN Grundlagen

802.1Q (tagged)

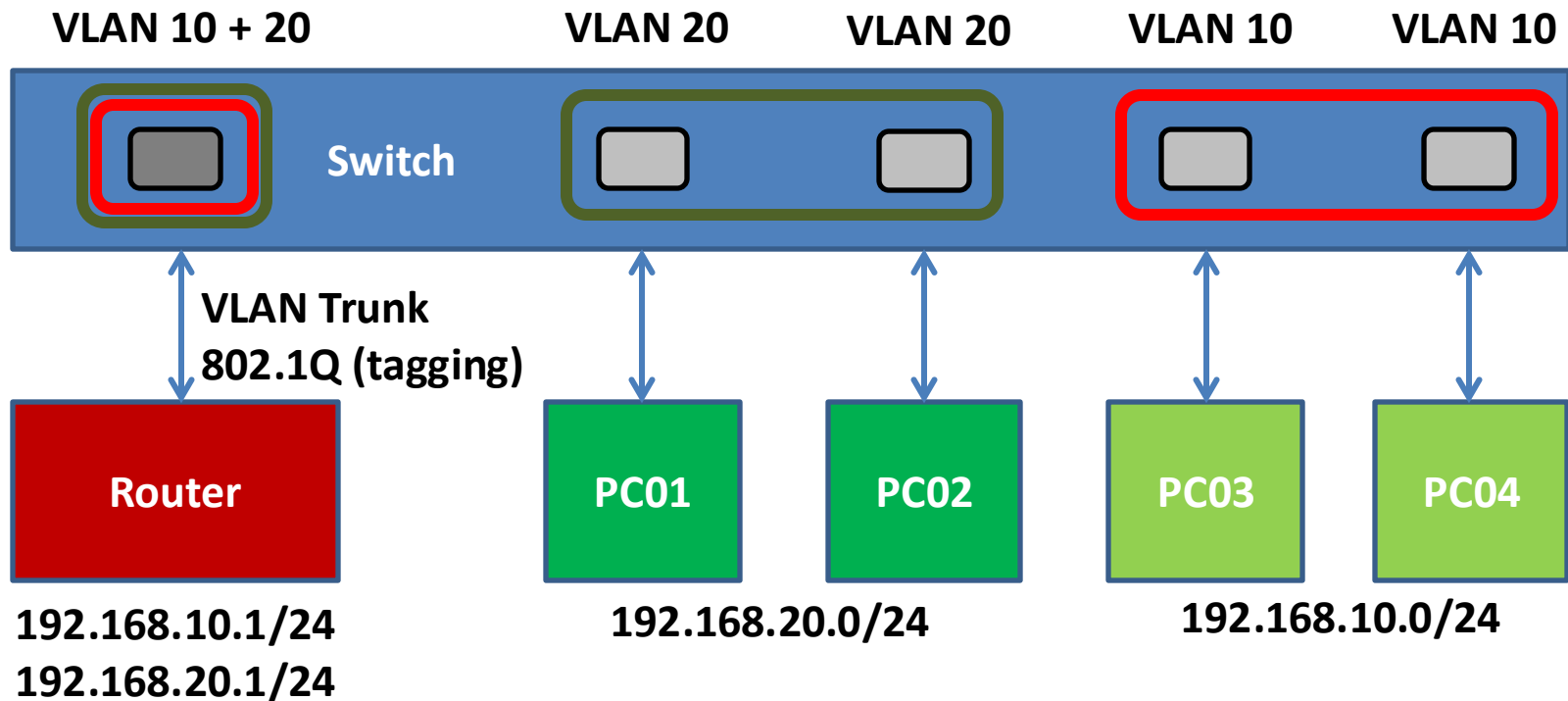
- Ein Computer in einem VLAN 10 kann nicht mit einem Computer in einem VLAN 20 kommunizieren.
Über den Router werden die betreffenden VLANs über ein Interface im **Trunk** Modus verbunden. Dazu werden **VLAN Tags** verwendet.



VLAN Grundlagen

VLANs werden über Layer3 mit Routing verbunden.

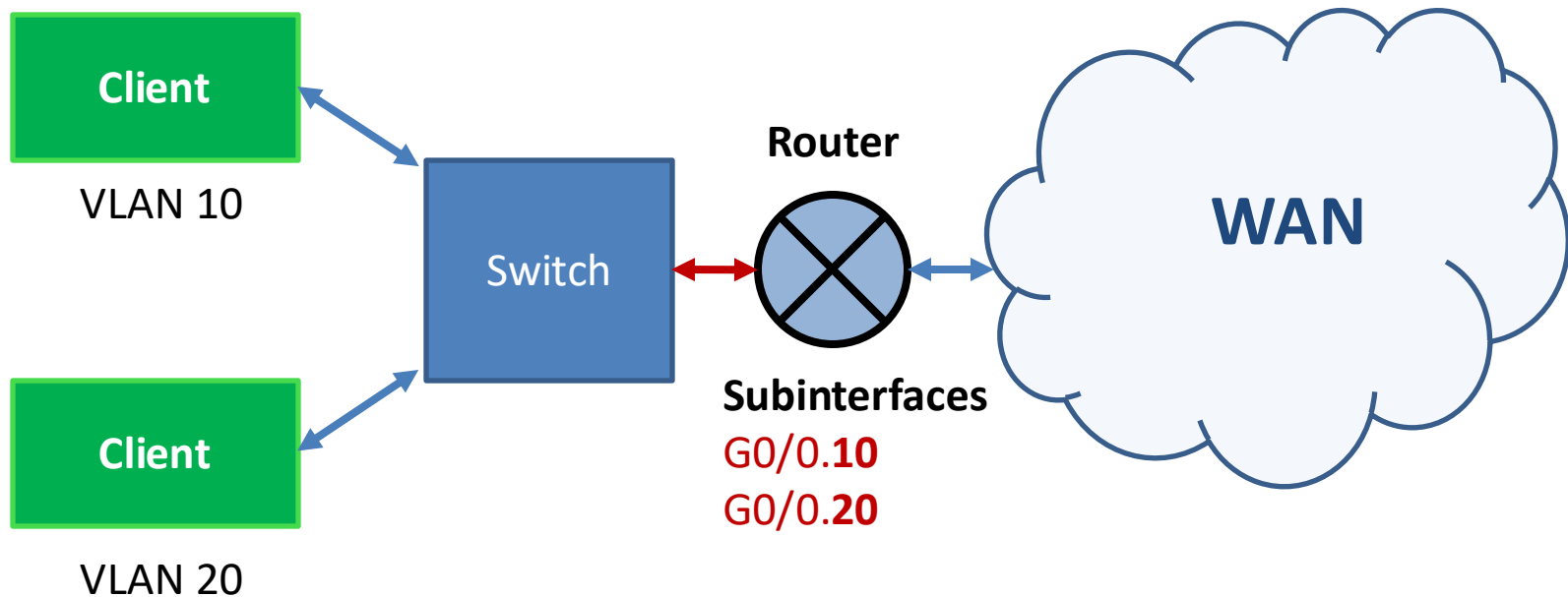
- VLANs können nur über **Routing** miteinander verbunden werden. Es benötigt daher einen Router oder einen **Layer 3** fähigen Switch (Multilayer Switch). Daher müssen sich alle VLANs in einem anderen IP-Netze befinden!



Inter-VLAN Routing (optional)

Router on a Stick «RoaS»

Router on a Stick ermöglicht die Anbindung mehrerer Subnetze an einen Anschluss mittels VLAN tagging und Subinterfaces



Zur besseren Übersicht werden bei den Subinterfaces die VLAN-IDs für die Nummerierung verwendet.

Cisco Konfigurationsbeispiel (optional)

„Roas Inter-VLAN Routing“

LAB>_

VLAN 10:

```
R1(config)# interface gigabitethernet 0/0.10
R1(config-subif)# encapsulation dot1Q 10
R1(config-subif)# ip address 10.1.1.254 255.255.255.0
```

VLAN 20:

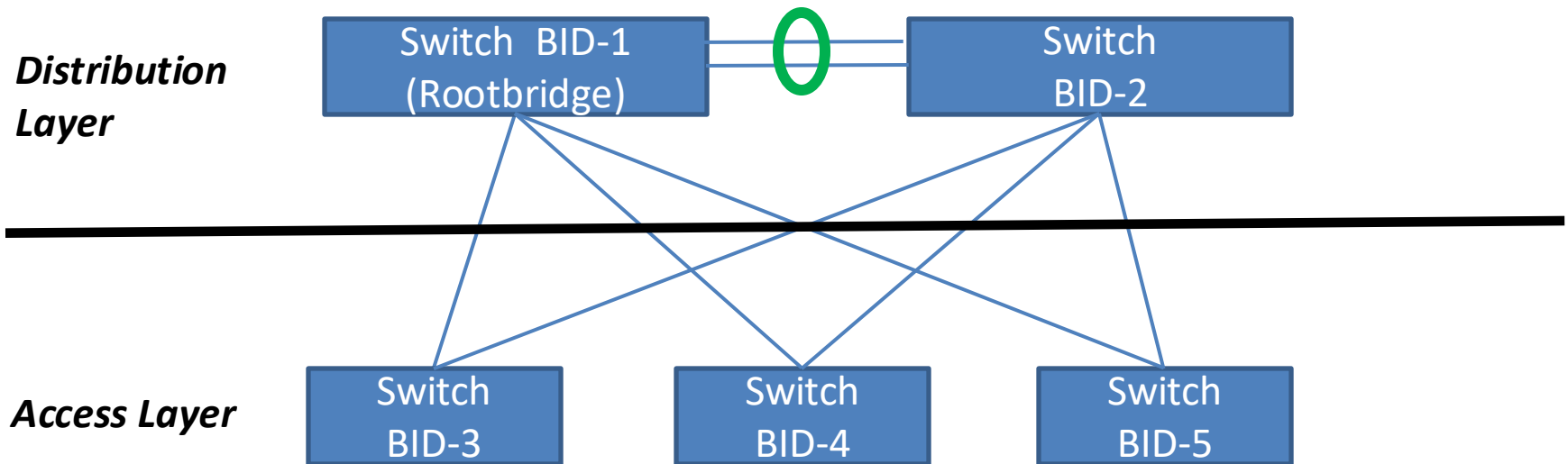
```
R1(config)# interface gigabitethernet 0/0.20
R1(config-subif)# encapsulation dot1Q 20
R1(config-subif)# ip address 10.2.1.254 255.255.255.0
.....
```

Vorsicht! Alle VLANs werden nun untereinander geroutet! Um dies zu verhindern müssen ACLs genutzt werden.

Agenda

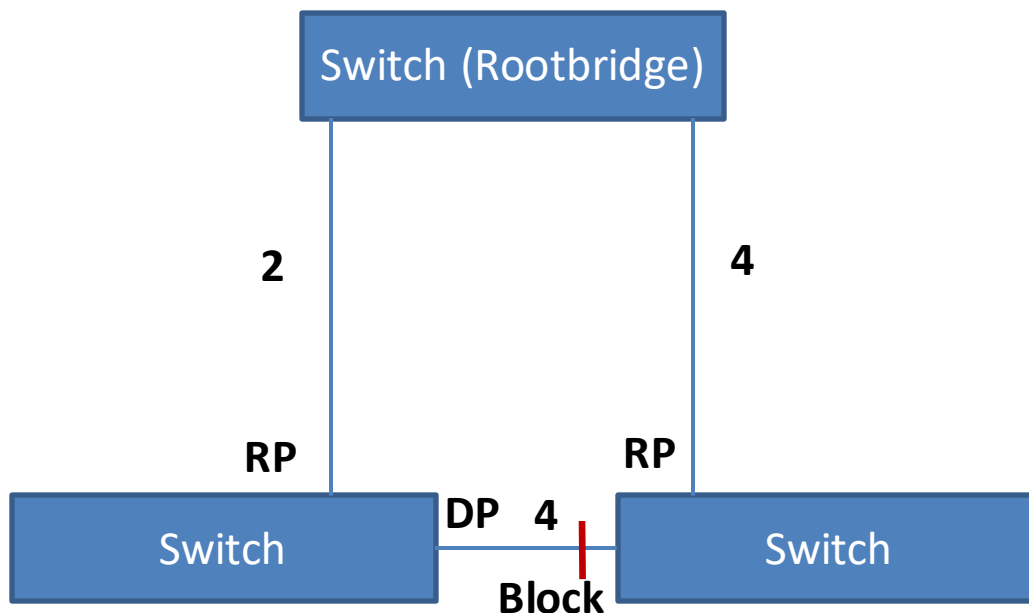
**«Repetition
Redundantes Design
Im Layer 2»**

Netzwerk-Design mit Redundanzen



***Wir brauchen ein Protokoll welches Redundanzen im Design erlaubt.
Dazu verwenden wir das Spanning-Tree Protocol.***

Spanning-Tree (STP) Grundlagen



DP = Designated Port (aller Verkehr geht über diesen Port)

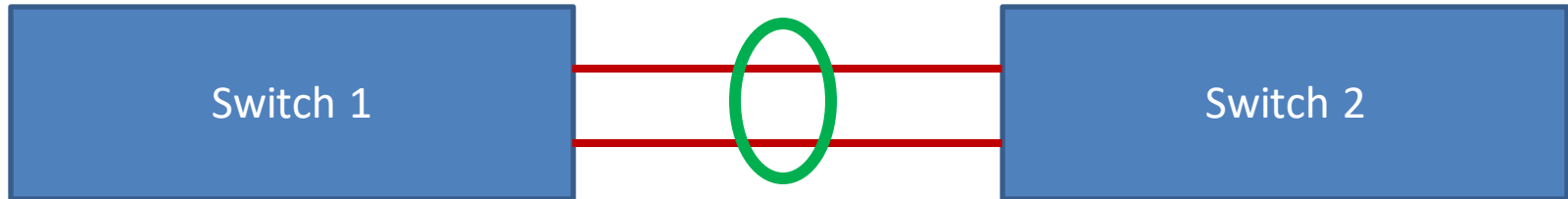
RP = Root Port

Block = Port empfängt keine Frames, er wartet auf Anweisungen

Spanning Tree (STP)

- Durch das Spanning Tree Protocol können Redundanzen zwischen den Switchen erstellt werden (Loops). IEEE 802.1d
- Es wird eine **Rootbridge** «Chef» unter den Switches gewählt um Rundsendungen durch Schleifen zu verhindern
- Weitere Informationen http://de.wikipedia.org/wiki/Spanning_Tree_Protocol

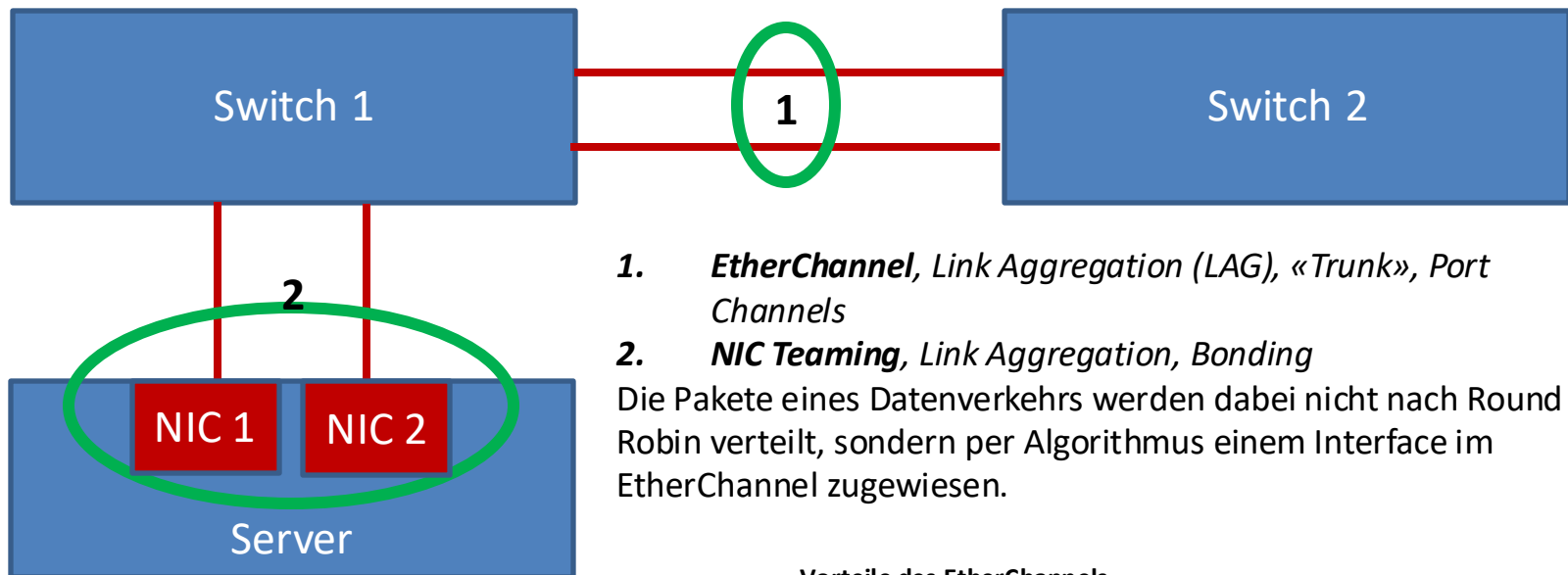
EtherChannel / Link Aggregation Grundlagen



Zusammengefasste Links zu einem EtherChannel

Der EtherChannel kann manuell oder mit Protokollen erfolgen. Cisco unterstützt das proprietäre Port Aggregation Protocol (**PAgP**) und das nach IEEE 802.3ad definierte Link Aggregation Control Protocol (**LACP**). *Mit EtherChannel können je nach Switchmodell bis zu 8 Ports im Loadbalancing zusammengefasst werden. Durch EtherChannel besteht kein Loop zwischen den Switches.*

EtherChannel / Link Aggregation Bezeichnungen



1. **EtherChannel**, Link Aggregation (LAG), «Trunk», Port Channels

2. **NIC Teaming**, Link Aggregation, Bonding

Die Pakete eines Datenverkehrs werden dabei nicht nach Round Robin verteilt, sondern per Algorithmus einem Interface im EtherChannel zugewiesen.

Hauptvorteile von NIC Teaming:

1. Erhöhte Zuverlässigkeit und Redundanz: Wenn eine der gebündelten Netzwerkkarten ausfällt, kann der Verkehr automatisch auf die anderen aktiven Karten umgeleitet werden, wodurch die Netzwerkverbindung des Servers aufrechterhalten bleibt.

2. Erhöhte Bandbreite: Durch das Kombinieren der Netzwerkbandbreite mehrerer physischer Netzwerkkarten kann die Gesamtbandbreite, die für Anwendungen zur Verfügung steht, erheblich erhöht werden.

3. Lastenausgleich: Die Netzwerklast kann über die verschiedenen NICs verteilt werden, was eine effizientere Nutzung der Netzwerkressourcen ermöglicht.

Vorteile des EtherChannels

1. Erhöhte Bandbreite: Durch das Zusammenführen mehrerer Netzwerkverbindungen in einen EtherChannel kann die Bandbreite erheblich erhöht werden. Zum Beispiel würde die Bündelung von vier 1-Gigabit-Ethernet-Links theoretisch eine Bandbreite von 4 Gbps bieten.

2. Lastverteilung: Der Verkehr über den EtherChannel wird über die verschiedenen physischen Links verteilt, was zu einer effizienteren Nutzung der Netzwerkkapazitäten führt.

3. Redundanz: Wenn einer der Links in einem EtherChannel ausfällt, wird der Verkehr automatisch auf die verbleibenden aktiven Links umgeleitet, was die Netzwerkverfügbarkeit erhöht.

4. Kostenersparnis: EtherChannel kann teurere Upgrades von Netzwerklinks vermeiden, indem vorhandene Verbindungen effizienter genutzt werden.

EtherChannel / Link Aggregation im Stack

Vorteile eines Multi-Chassis-Switches sind:

Hochverfügbarkeit und Redundanz

Durch die Verwendung von Multi-Chassis-Link-Aggregation (MLAG) oder ähnlichen Technologien können Verbindungen über mehrere physische Switches hinweg aggregiert werden. Dies bedeutet, dass bei Ausfall eines Switches die Netzwerkgeräte weiterhin Zugang zum Netzwerk haben, da die anderen Switches im Chassis weiterhin aktiv bleiben. Dies erhöht die Netzwerkverfügbarkeit und reduziert Ausfallzeiten.

2. Erhöhte Bandbreite und Leistung

Die Verteilung des Verkehrs auf mehrere physische Geräte ermöglicht es dem Multi-Chassis-Switch, eine höhere Gesamtbandbreite zu verarbeiten als ein einzelner Switch. Dies ist besonders nützlich in Umgebungen, in denen große Datenmengen übertragen werden müssen, wie zum Beispiel in Rechenzentren.

3. Skalierbarkeit

Multi-Chassis-Switching ermöglicht es, das Netzwerk leicht zu skalieren. Weitere Switches können hinzugefügt werden, um die Kapazität und Leistung des Netzwerks zu erhöhen, ohne die Architektur grundlegend ändern zu müssen.

4. Vereinfachtes Management

Obwohl die physische Infrastruktur aus mehreren Geräten besteht, wird sie als ein einzelner logischer Switch verwaltet. Dies vereinfacht das Netzwerkmanagement erheblich, da Änderungen, Updates und Fehlerbehebungen zentral durchgeführt werden können.

ein logischer Switch

Stack

Switch 1

Switch 2

EtherChannel

Switch 3

Mit Multi-Chassis Switches oder Stacking-Case
Mit VSS - Virtual Switching System
Mit vPC – Virtual Port Channel (Nexus)

Agenda



Repetition **«CLI Grundlagen»**

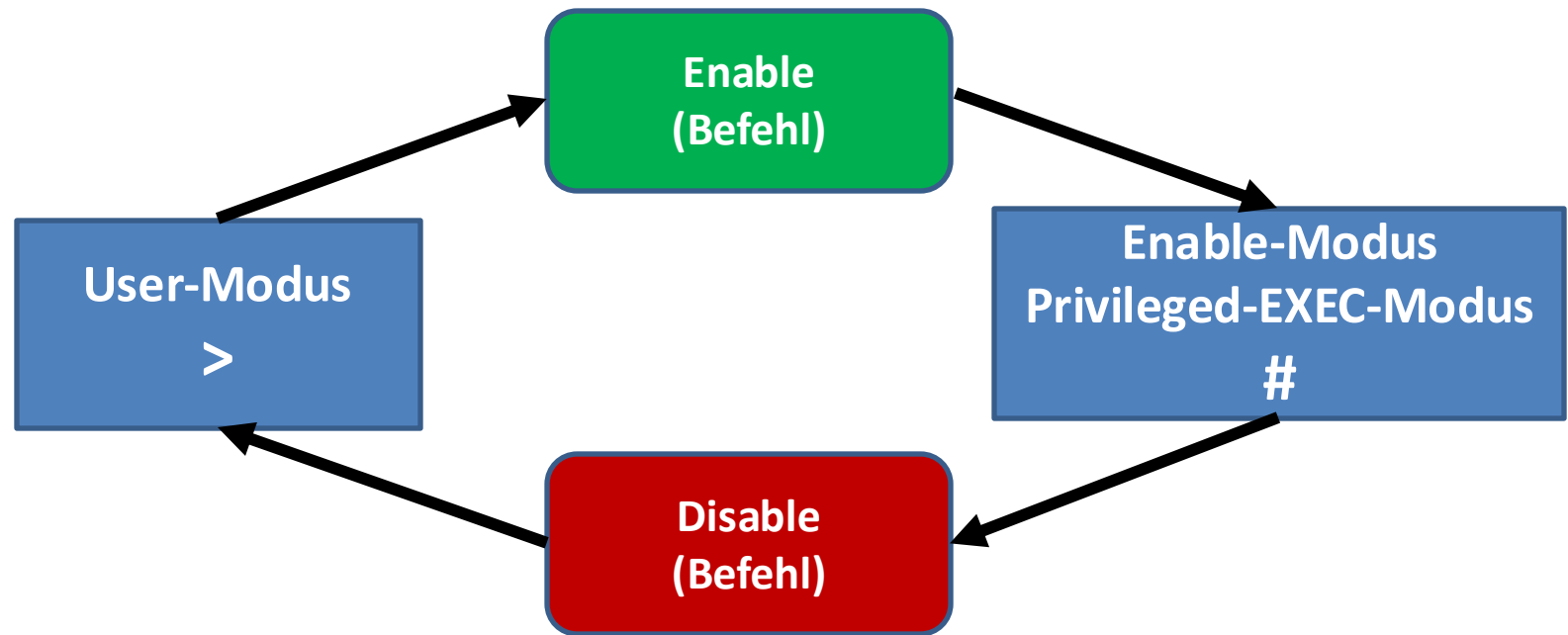
IOS Grundlagen

- Betriebssystem bei Cisco heisst **Internetwork Operating System (IOS)**
- Enthält Logik und Funktionen von Cisco Geräten
- Die Konfiguration erfolgt mit dem Command Line Interface (CLI)
 - Terminalemulation via Konsole, Telnet oder SSH

Command Line Interface Zugriff

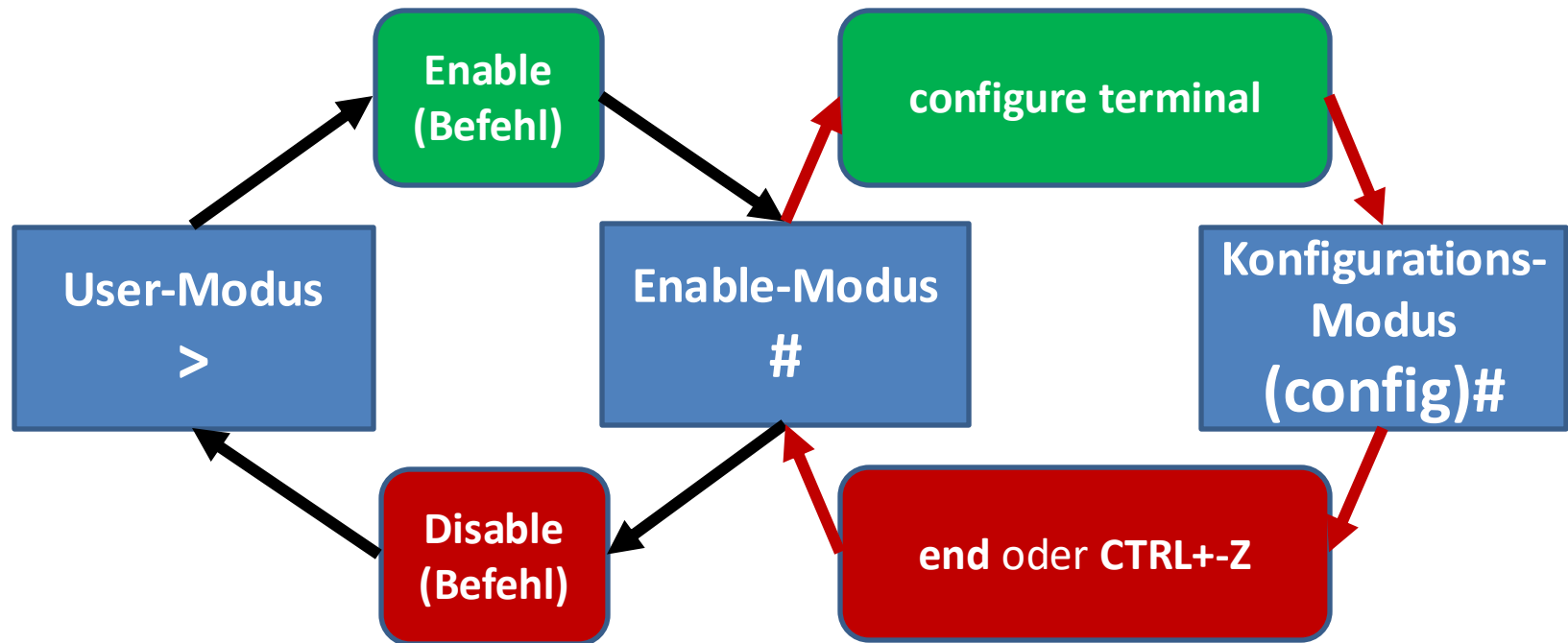
CLI-Zugriffsmöglichkeit	Beschreibung
Konsolen Port	<ul style="list-style-type: none">- Erfolgt über speziellen physischen Port (Konsolenkabel)- Benötigt Terminalemulations-Programm und seriellen Port auf PC Seite- Programme (Putty, Zterm Pro., ...)
Telnet	<ul style="list-style-type: none">- Erfolgt über das Netzwerk und benötigt IP-Adresse- Achtung unverschlüsselte Verbindung- VTY (Virtual Terminal Lines)- Port 23
SSH (Secure Shell)	<ul style="list-style-type: none">- Erfolgt über das Netzwerk und benötigt IP-Adresse- Verschlüsselte Verbindung (immer verwenden)- VTY (Virtual Terminal Lines)- Port 22

CLI-Berechtigungskonzept



Quelle: Wendell Odom, Cisco CCENT / CCNA, dpunkt.verlag, S.184

Der Konfigurationsmodus



Quelle: Wendell Odom, Cisco CCENT / CCNA, dpunkt.verlag, S.189

Speicherarten in Cisco Switches

RAM

Arbeitsspeicher
running config

Flash

Cisco IOS SW

ROM

Bootstrapper
sucht IOS SW

NVRAM

startup config

Quelle: Wendell Odom, Cisco CCENT / CCNA, dpunkt.verlag, S.192

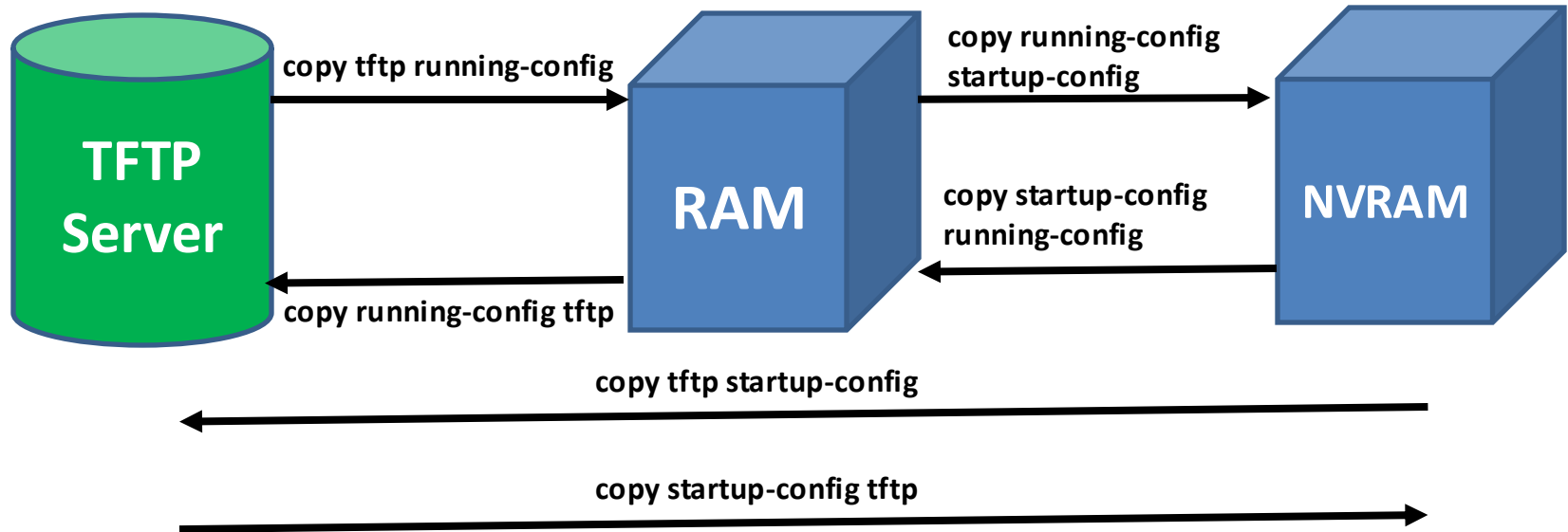
CISCO Switch Konfigurationsdaten speichern

Konfigurationsdatei	Funktion	Speicher
startup config	Konfiguration welche beim Neustart verwendet wird.	NVRAM
running config	Aktuelle Konfiguration mit allen gemachten Einstellungen. Achtung geht beim Neustart verloren, wenn diese nicht in die startup config geschrieben wird (copy running-config startup-config).	RAM

Mit **show running config** oder **show startup config** kann die entsprechende Konfiguration angezeigt werden.

Quelle: Wendell Odom, Cisco CCENT / CCNA, dpunkt.verlag, S.192

Konfigurationen kopieren und löschen



Quelle: Wendell Odom, Cisco CCENT / CCNA, dpunkt.verlag, S.194

Ende Block 7

«Ende»