



Kommunikationstechnik KOTE / Netzwerkgrundlagen
5. Unit

Übersicht der einzelnen Modulblöcke (roter Faden)

**Grundlagen aus
relevanten Kapiteln**
Cisco CCNA 200-301
Volume 1+2

Modulaufgaben
Vorbereitung und
Vertiefung

*Simulationsübungen
mit dem CISCO
Pakettracer und mit
Wireshark*

Stoffumfang KOTE:

CCNA1/ Kap. 1 – 6 / 8 / 9 / 11 – 14 / 18

CCNA2/ Kap. 1 + 13

CCNA1/Kap. 2
CCNA2/Kap. 13

**Grundlagen Netzwerkmanagement und
Netzwerk**

NetAcad/Kap. 1

CCNA1/Kap. 1
CCNA1/Kap. 3

**Netzwerkcommunication LAN/WAN
ISO/OSI Referenzmodell**

NetAcad/Kap. 3

CCNA2/Kap. 1

**Standards und Gremien
L7,L4 und L3 analysieren**

NetAcad/Kap. 10
NetAcad/Kap. 9

CCNA1/Kap. 11
CCNA1/Kap. 12
CCNA1/Kap. 13
CCNA1/Kap. 14

IPv4 Funktionen und Subnettierung

NetAcad/Kap. 6
NetAcad/Kap. 7
NetAcad/Kap. 8

CCNA1/Kap. 4
CCNA1/Kap. 5/6

ICMP, Routing, Switching und CLI-Grundlagen

NetAcad/Kap. 4
NetAcad/Kap. 5

CCNA1/Kap. 8

VLAN und IEEE 802.1Q konfigurieren

CCNA1/Kap. 9

Redundante Netzwerkdesigns

CCNA1/Kap. 18
(Commands)

**Netzwerk für ein KMU konfigurieren
Troubleshooting im Netzwerk**

**NPDO - Netzwerk, Planung, Design und
Optimierung**

NIUS - Netzwerkinstallation und Störungsbehebung

Lernziele des 5. Modulblocks

- **Du kannst...**

1. ...die wichtigsten Funktionen von ICMP erklären.
2. ...den Routingprozess anhand des statischen IPv4-Routings erklären.
3. ...die Funktionen der Sicherungsschicht anhand des Ethernet-Protokolls beschreiben.
4. ...die grundlegenden Funktionen und IEEE-Standards des Ethernet LAN-Switching erläutern.
5. ...die grundlegenden Cisco CLI Commands beschreiben.

Agenda

**«Repetition und
Hausaufgabenbesprechung»**

Gruppenarbeit

Repetition Block 4

Auftrag: Jede Gruppe löst eine der folgenden 4 Aufgaben soweit, dass sie das Resultat im Anschluss im Plenum erklären kann.

Form: keine Vorgabe

Zeit: Vorbereitung 30 Minuten

Aufgaben:

1. Übung Anhang F: 3. und 18. Aufgabe der Maskenanalyse
2. Übung Anhang F: 4. und 19. Aufgabe der Maskenanalyse
3. Übung Anhang F: 9. und 20. Aufgabe der Maskenanalyse
4. Übung Anhang F: 10. und 21. Aufgabe der Maskenanalyse

Alle Gruppen setzen sich mit der **binären Berechnung der Subnetz- und Broadcast-Adresse** auseinander und

alle Gruppen setzen sich mit der Berechnung der Subnetz- und Broadcast-Adresse mittels **Subnetz-Diagramm (Magic Number)** auseinander

Repetition Block 4

Net Academy Kapitel 6, 7 und 8: Fragen?

Fragen zur Vertiefung:

- CCNA1 Kapitel 11 «Perspectives on IPv4 Subnetting»
- CCNA1 Kapitel 12 «Analyzing Classful IPv4 Networks»
- CCNA1 Kapitel 13 «Analyzing Subnet Masks»
- CCNA1 Kapitel 14 «Analyzing existing Subnets»
- Network Academy: <https://www.netacad.com/portal> Cisco NetAcademy Kapitel 6.0 – 6.3 / 8.0 – 8.2

Lernvideos «Youtube»:

Suche ein gutes Lernvideo über die IPv4 Subnettierung und nimm deinen Vorschlag in den Unterricht für den gemeinsamen Austausch mit.

Praxistransfer: Besprechung in den Gruppen

Agenda

«Kurztest»

Ablauf Kurztest

- Versuche die Aufgaben bestmöglich zu lösen. Du hast jeweils **5 Minuten Zeit pro Folie**. Danach kommt die nächste Aufgabe.
- Schreibe die Lösungen sinnvoll auf ein Blatt, so dass eine Korrektur möglich ist.
- **Es handelt sich hier um eine Einzelarbeit!**
- **Es gibt keine Note!**

1. Aufgabe

Rechnen Sie bitte folgende Subnet-Beispiele Dezimal in Binär

Maske/Dezimal	Maske/ Binär nur letztes Oktett	Anzahl Subnetze	Anzahl gültige Adressen
255.255.255.0			
255.255.255.128			
255.255.255.192			
255.255.255.224			
255.255.255.240			
255.255.255.248			
255.255.255.252			

Sucht zu zweit die Lösung.
Was ist der Sinn dahinter?

Zeit: 5 Minuten

Wichtig: Die **oberste Adresse** im Subnet ist immer die **Broadcast** Adresse und die **unterste Adresse** definiert das **Netz** selber.

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

1. Aufgabe Musterlösung

Dezimal	Binär		Anzahl Subnetze	Anzahl gültige Adressen
255.255.255.0	11111111. 11111111.11111111.00000000		1 ($=2^0$)	254 ($=2^8-2$)
255.255.255.128	11111111. 11111111.11111111.10000000		2 ($=2^1$)	126 ($=2^7-2$)
255.255.255.192	11111111. 11111111.11111111.11000000		4	62
255.255.255.224	11111111. 11111111.11111111.11100000		8	30
255.255.255.240	11111111. 11111111.11111111.11110000		16	14
255.255.255.248	11111111. 11111111.11111111.11111000		32	6
255.255.255.252	11111111. 11111111.11111111.11111100		64	2

N=Netzwerkbits

S=Subnetbits

Wichtig: Die **oberste Adresse** im Subnet ist immer die **Broadcast Adresse** und die **unterste Adresse** definiert das **Netz** selber.

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/>

Agenda



«Grundlagen ICMP»

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
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

Nützliche Windows CMD-Befehle um die Vermittlungsschicht zu testen

CMD-Befehl	Zweck
<code>route print</code>	Lokale Routingtabelle anzeigen
<code>ping 127.0.0.1</code>	Loopback-Ping um lokalen Stack zu testen
<code>ping 192.168.1.1</code>	Testen der Konnektivität zu einem Host (z.B. zum Gateway oder einem Remote-Host)
<code>tracert/traceroute www.domain.ch</code> <code>tracert/traceroute 192.168.2.1</code>	RTT (Round-Trip Time) für jeden Hop auf dem Pfad wird ausgegeben. Tracert verwendet dazu die TTL.

Selber aufzeichnen / ICMP PING Echo Request PING-Aufzeichnung mit Wireshark

The image shows a Wireshark capture of ICMP PING Echo requests and replies. The filter is set to 'icmp'. The packet list shows 14 packets, with the first 13 being Echo (ping) requests and the last one being an Echo (ping) reply. The packet details pane shows the structure of the ICMP Echo (ping) request, including the type, code, checksum, identifier, sequence number, and data. The packet bytes pane shows the raw data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
2625	76.8579930	192.168.77.45	192.168.77.1	ICMP	74	Echo (ping) request id=0x0001, seq=2/512, ttl=128
2626	76.8604840	192.168.77.1	192.168.77.45	ICMP	74	Echo (ping) reply id=0x0001, seq=2/512, ttl=254
2627	77.8538770	192.168.77.45	192.168.77.1	ICMP	74	Echo (ping) request id=0x0001, seq=3/768, ttl=128
2628	77.8581100	192.168.77.1	192.168.77.45	ICMP	74	Echo (ping) reply id=0x0001, seq=3/768, ttl=254
2629	78.8520970	192.168.77.45	192.168.77.1	ICMP	74	Echo (ping) request id=0x0001, seq=4/1024, ttl=128
2630	78.8546990	192.168.77.1	192.168.77.45	ICMP	74	Echo (ping) reply id=0x0001, seq=4/1024, ttl=254
2631	79.8505450	192.168.77.45	192.168.77.1	ICMP	74	Echo (ping) request id=0x0001, seq=5/1280, ttl=128
2632	79.8529910	192.168.77.1	192.168.77.45	ICMP	74	Echo (ping) reply id=0x0001, seq=5/1280, ttl=254
2646	94.0484580	192.168.77.45	192.168.77.1	ICMP	106	Echo (ping) request id=0x0001, seq=6/1536, ttl=1
2647	94.0507970	192.168.77.1	192.168.77.45	ICMP	106	Echo (ping) reply id=0x0001, seq=6/1536, ttl=254
2648	94.0515510	192.168.77.45	192.168.77.1	ICMP	106	Echo (ping) request id=0x0001, seq=7/1792, ttl=1
2649	94.0565100	192.168.77.1	192.168.77.45	ICMP	106	Echo (ping) reply id=0x0001, seq=7/1792, ttl=254
2650	94.0574540	192.168.77.45	192.168.77.1	ICMP	106	Echo (ping) request id=0x0001, seq=8/2048, ttl=1
2651	94.0597480	192.168.77.1	192.168.77.45	ICMP	106	Echo (ping) reply id=0x0001, seq=8/2048, ttl=254

Frame 2625: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
Ethernet II, Src: IntelCor_6a:7d:d8 (10:0b:a9:6a:7d:d8), Dst: zyxelCom_fd:7a:80 (00:13:49:fd:7a:80)
Internet Protocol Version 4, Src: 192.168.77.45 (192.168.77.45), Dst: 192.168.77.1 (192.168.77.1)
Internet Control Message Protocol
Type: 8 (Echo (ping) request)
Code: 0
Checksum: 0x4d59 [correct]
Identifier (BE): 1 (0x0001)
Identifier (LE): 256 (0x0100)
Sequence number (BE): 2 (0x0002)
Sequence number (LE): 512 (0x0200)
[\[Response in: 2626\]](#)
Data (32 bytes)
Data: 6162636465666768696a6b6c6d6e6f707172737475767761...
[Length: 32]

0000 00 13 49 fd 7a 80 10 0b a9 6a 7d d8 08 00 45 00 ..I.Z... .j}...E.
0010 00 3c 10 4b 00 00 80 01 0e f7 c0 a8 4d 2d c0 a8 .<.K....M...
0020 4d 01 08 00 4d 59 00 01 00 02 61 62 63 64 65 66 M...MY... .abcdf
0030 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 ghijklmn opqrstuv
0040 77 61 62 63 64 65 66 67 68 69 wabcdfgh i

Ready to load or capture Packets: 2716 Displayed: 14 Marked: 0 Dropped: 0 Load time: 0:00.093 Profile: Default

Selber aufzeichnen / ICMP PING Echo Reply

PING-Aufzeichnung mit Wireshark

The image shows a Wireshark capture of ICMP PING Echo Reply packets. The top pane displays a list of 14 packets, all of which are Echo (ping) replies. The bottom pane shows the details of the selected packet (No. 2626), which is an Echo (ping) reply from 192.168.77.1 to 192.168.77.45. The packet details include the Ethernet II header, the Internet Protocol Version 4 header, and the Internet Control Message Protocol header. The packet data is shown in hexadecimal and ASCII format at the bottom.

No.	Time	Source	Destination	Protocol	Length	Info
2625	76.8579930	192.168.77.45	192.168.77.1	ICMP	74	Echo (ping) request id=0x0001, seq=2/512, ttl=128
2626	76.8604840	192.168.77.1	192.168.77.45	ICMP	74	Echo (ping) reply id=0x0001, seq=2/512, ttl=254
2627	77.8538770	192.168.77.45	192.168.77.1	ICMP	74	Echo (ping) request id=0x0001, seq=3/768, ttl=128
2628	77.8581100	192.168.77.1	192.168.77.45	ICMP	74	Echo (ping) reply id=0x0001, seq=3/768, ttl=254
2629	78.8520970	192.168.77.45	192.168.77.1	ICMP	74	Echo (ping) request id=0x0001, seq=4/1024, ttl=128
2630	78.8546990	192.168.77.1	192.168.77.45	ICMP	74	Echo (ping) reply id=0x0001, seq=4/1024, ttl=254
2631	79.8505450	192.168.77.45	192.168.77.1	ICMP	74	Echo (ping) request id=0x0001, seq=5/1280, ttl=128
2632	79.8529910	192.168.77.1	192.168.77.45	ICMP	74	Echo (ping) reply id=0x0001, seq=5/1280, ttl=254
2646	94.0484580	192.168.77.45	192.168.77.1	ICMP	106	Echo (ping) request id=0x0001, seq=6/1536, ttl=1
2647	94.0507970	192.168.77.1	192.168.77.45	ICMP	106	Echo (ping) reply id=0x0001, seq=6/1536, ttl=254
2648	94.0515510	192.168.77.45	192.168.77.1	ICMP	106	Echo (ping) request id=0x0001, seq=7/1792, ttl=1
2649	94.0565100	192.168.77.1	192.168.77.45	ICMP	106	Echo (ping) reply id=0x0001, seq=7/1792, ttl=254
2650	94.0574540	192.168.77.45	192.168.77.1	ICMP	106	Echo (ping) request id=0x0001, seq=8/2048, ttl=1
2651	94.0597480	192.168.77.1	192.168.77.45	ICMP	106	Echo (ping) reply id=0x0001, seq=8/2048, ttl=254

Frame 2626: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
Ethernet II, Src: ZyxelCom_fd:7a:80 (00:13:49:fd:7a:80), Dst: IntelCor_6a:7d:d8 (10:0b:a9:6a:7d:d8)
Internet Protocol Version 4, Src: 192.168.77.1 (192.168.77.1), Dst: 192.168.77.45 (192.168.77.45)
Internet Control Message Protocol
Type: 0 (Echo (ping) reply)
Code: 0
Checksum: 0x5559 [correct]
Identifier (BE): 1 (0x0001)
Identifier (LE): 256 (0x0100)
Sequence number (BE): 2 (0x0002)
Sequence number (LE): 512 (0x0200)
[\[Response To: 2625\]](#)
[Response Time: 2.491 ms]
Data (32 bytes)
Data: 6162636465666768696a6b6c6d6e6f707172737475767761...
[Length: 32]

0000 10 0b a9 6a 7d d8 00 13 49 fd 7a 80 08 00 45 00 ...j}... I.Z...E.
0010 00 3c 3e 7b 00 00 fe 01 62 c6 c0 a8 4d 01 c0 a8 ..<>{... b...M..
0020 4d 2d 00 00 55 59 00 01 00 02 61 62 63 64 65 66 M--UY... ..abcdef
0030 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 ghijklmn opqrstuv
0040 77 61 62 63 64 65 66 67 68 69 71 72 73 74 75 76 wabcdefg hi

Ready to load or capture Packets: 2716 Displayed: 14 Marked: 0 Dropped: 0 Load time: 0:00.093 Profile: Default

Selber aufzeichnen / ICMP Traceroute Traceroute-Aufzeichnung mit Wireshark

The screenshot shows a Wireshark capture of an ICMP traceroute. The packet list pane displays 33 packets. Packets 9, 11, 13, 15, 17, 19, 21, 23, 25, 27, 29, 31, and 33 are Echo (ping) requests. Packets 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, and 34 are 'Time-to-live exceeded' messages, indicating packet loss at various hops. The packet details pane for packet 8 shows an Ethernet II frame from IntelCor_6a:7d:d8 to Zyxelcom_fd:7a:80, an Internet Protocol Version 4 packet from 192.168.77.45 to 82.195.250.38, and an Internet Control Message Protocol Echo (ping) request with ID 1, sequence number 9, and TTL 1. The packet bytes pane shows the raw data of the packet.

No.	Time	Source	Destination	Protocol	Length	Info
8	9.85615700	192.168.77.45	82.195.250.38	ICMP	106	Echo (ping) request id=0x0001, seq=9/2304, ttl=1
9	9.85894700	192.168.77.1	192.168.77.45	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
10	9.85950900	192.168.77.45	82.195.250.38	ICMP	106	Echo (ping) request id=0x0001, seq=10/2560, ttl=1
11	9.86243000	192.168.77.1	192.168.77.45	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
12	9.86292500	192.168.77.45	82.195.250.38	ICMP	106	Echo (ping) request id=0x0001, seq=11/2816, ttl=1
13	9.86622700	192.168.77.1	192.168.77.45	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
23	15.7364590	192.168.77.45	82.195.250.38	ICMP	106	Echo (ping) request id=0x0001, seq=12/3072, ttl=2
24	19.6055090	192.168.77.45	82.195.250.38	ICMP	106	Echo (ping) request id=0x0001, seq=13/3328, ttl=2
25	19.6229800	80.254.161.240	192.168.77.45	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
26	19.6235180	192.168.77.45	82.195.250.38	ICMP	106	Echo (ping) request id=0x0001, seq=14/3584, ttl=2
27	19.6417680	80.254.161.240	192.168.77.45	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
30	20.6348450	192.168.77.45	82.195.250.38	ICMP	106	Echo (ping) request id=0x0001, seq=15/3840, ttl=3
31	20.6530300	146.228.3.65	192.168.77.45	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
32	20.6535720	192.168.77.45	82.195.250.38	ICMP	106	Echo (ping) request id=0x0001, seq=16/4096, ttl=3
33	20.6740560	146.228.3.65	192.168.77.45	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)

Frame 8: 106 bytes on wire (848 bits), 106 bytes captured (848 bits) on interface 0
Ethernet II, Src: IntelCor_6a:7d:d8 (10:0b:a9:6a:7d:d8), Dst: Zyxelcom_fd:7a:80 (00:13:49:fd:7a:80)
Internet Protocol Version 4, Src: 192.168.77.45 (192.168.77.45), Dst: 82.195.250.38 (82.195.250.38)
Internet Control Message Protocol
Type: 8 (Echo (ping) request)
Code: 0
Checksum: 0xf7f5 [correct]
Identifier (BE): 1 (0x0001)
Identifier (LE): 256 (0x0100)
Sequence number (BE): 9 (0x0009)
Sequence number (LE): 2304 (0x0900)
Data (64 bytes)
Data: 00...
[Length: 64]

0000 00 13 49 fd 7a 80 10 0b a9 6a 7d d8 08 00 45 00 ..I.Z... .j}...E.
0010 00 5c 10 c2 00 00 01 01 4e 20 c0 a8 4d 2d 52 c3 .\..... N...M-R.
0020 fa 26 08 00 f7 f5 00 01 00 09 00 00 00 00 00 00 .&.....
0030 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0040 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0050 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Ready to load or capture Packets: 70 Displayed: 37 Marked: 0 Dropped: 0 Load time: 0:00.000 Profile: Default

Agenda

«Grundlagen Routing»

CCNA1 Buch Kapitel 3 «Fundamentals of WANs and IP Routing»

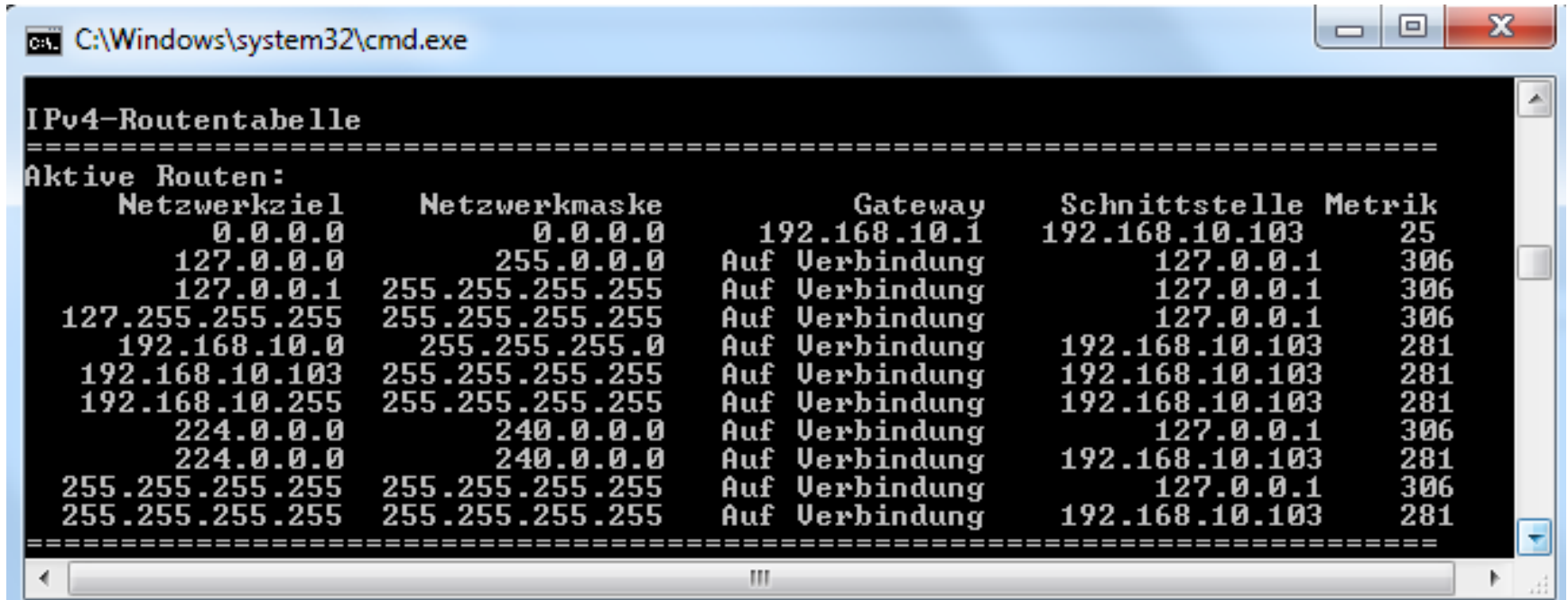
Der Router (Layer 3)

Bezeichnung	Beschreibung
Routingtabelle (statisch oder dynamisch)	Um den Verkehr an den nächsten Router (Hop) zu senden.
Funktion	Routing (meist IP-Routing) Verbindet Netzwerke miteinander
Schicht	Bis Layer 3
Was passiert mit Broadcasts?	Werden blockiert resp. nicht weitergeleitet.
Routingprotokolle	RIP, RIPv2, RIPv6 (Routing Information Protocol) IGRP, EIGRP (Enhanced Interior Gateway Routing Protocol) OSPF (Open Shortest Path First) IS-IS (Intermediate System-to-Intermediate System) BGP (Border Gateway Protocol)

Übersicht Einträge Routingtabelle

Eintrag Routingtabelle	Erklärung
Netzadresse	IP-Adresse
Subnetzmaske	Subnetzadresse des Netzes (Bildet zusammen mit Netzadresse die Möglichkeit zum bestimmen des Netzes.)
Gateway (next hop)	Nächster Router, an den die Pakete gesandt werden
Metrik	Bestimmt die Reihenfolge bei mehreren Routern im gleichen Netz. (Tiefere Zahl = höhere Priorität)

Beispiel lokale Routingtabelle (route print)



```
C:\Windows\system32\cmd.exe

IPv4-Routentabelle
=====
Aktive Routen:
  Netzwerkziel      Netzwerkmaske      Gateway      Schnittstelle      Metrik
  0.0.0.0           0.0.0.0           192.168.10.1 192.168.10.103      25
  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
  192.168.10.0      255.255.255.0     Auf Verbindung 192.168.10.103     281
  192.168.10.103    255.255.255.255   Auf Verbindung 192.168.10.103     281
  192.168.10.255    255.255.255.255   Auf Verbindung 192.168.10.103     281
  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 192.168.10.103     281
  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 192.168.10.103     281
=====
```

Wichtig:

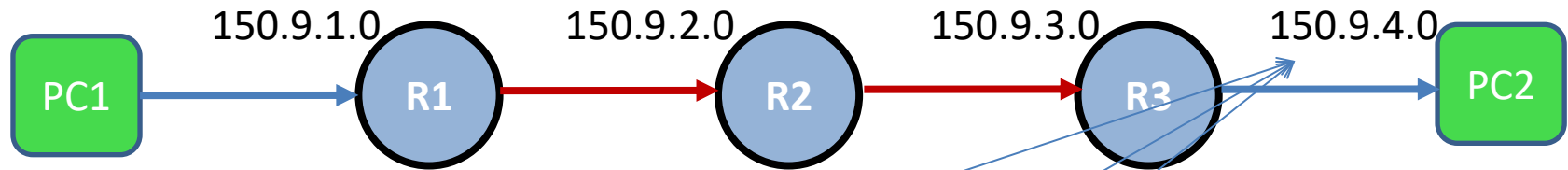
Auch ein Client braucht seine eigene Routingtabelle!

Beispiel Routingtabelle PC (route print)

Netzwerkziel	Netzwerkmaske	Gateway	Schnittstelle	Metrik	Bemerkungen
0.0.0.0	0.0.0.0	192.168.1.1	192.168.1.10	25	Standardgateway
127.0.0.0	255.0.0.0	Auf Verbindung	127.0.0.1	306	Loopback-Netz
127.0.0.1	255.255.255.255	Auf Verbindung	127.0.0.1	306	Localhost-Adresse
127.255.255.255	255.255.255.255	Auf Verbindung	127.0.0.1	306	Broadcast
192.168.1.0	255.255.255.0	Auf Verbindung	192.168.1.10	281	Lokale Subnetadresse
192.168.1.10	255.255.255.255	Auf Verbindung	192.168.1.10	281	Eigene IP Adresse
192.168.1.255	255.255.255.255	Auf Verbindung	192.168.1.10	281	Subnetbroadcast
224.0.0.0	240.0.0.0	Auf Verbindung	127.0.0.1	306	Multicast-Adressen
224.0.0.0	240.0.0.0	Auf Verbindung	192.168.1.10	281	Multicast-Adressen
255.255.255.255	255.255.255.255	Auf Verbindung	127.0.0.1	306	Broadcast
255.255.255.255	255.255.255.255	Auf Verbindung	192.168.1.10	281	Broadcast

Quelle: <http://support.microsoft.com/kb/140859/de>

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 CCNA Vol 1, Seite 71 für ein Beispiel mit der korrekten Cisco Notation.

Nützliche Windows CMD-Befehle um die Vermittlungsschicht zu testen

CMD-Befehl	Zweck
route print	Lokale Routingtabelle anzeigen
ping 127.0.0.1	Loopback-Ping um lokalen Stack zu testen
ping 192.168.1.1	Testen der Konnektivität zu einem Host (z.B. zum Gateway oder einem Remote-Host)
tracert www.domain.ch tracert 192.168.2.1	RTT (Round-Trip Time) für jeden Hop auf dem Pfad wird ausgegeben. Tracert verwendet dazu die TTL.

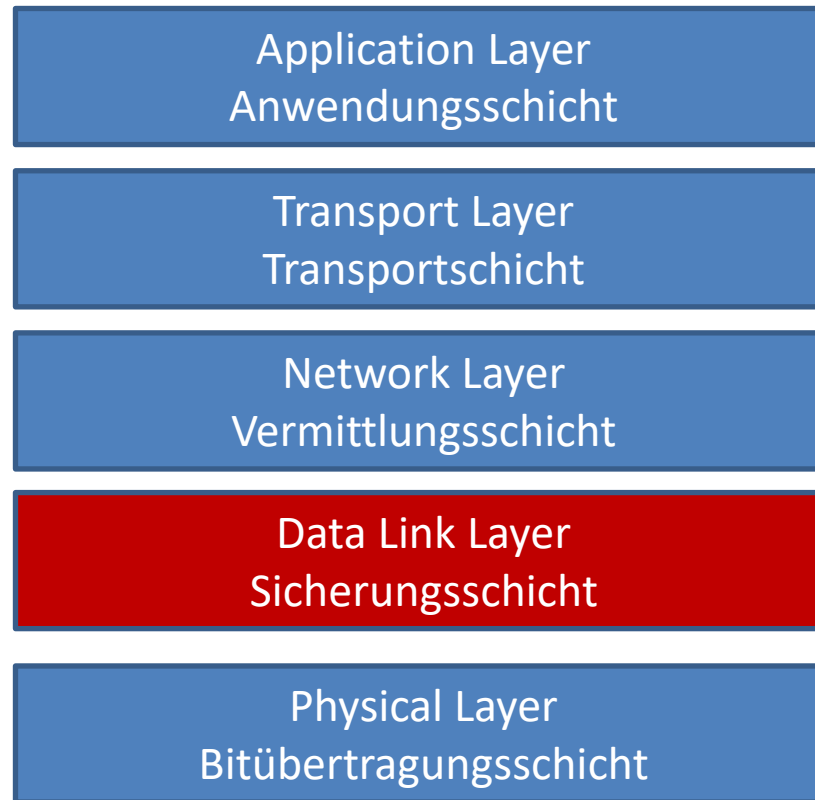
Agenda



«Vertiefung Sicherungsschicht»

CCNA1, Kapitel 5

Einordnung der Sicherungsschicht Layer 2

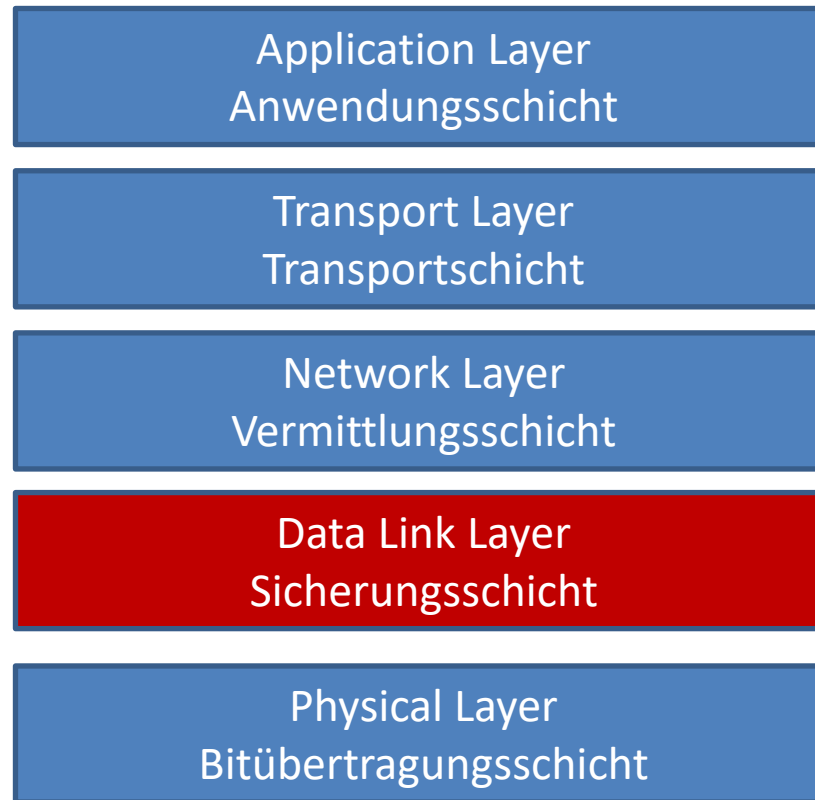


TCP/IP				
OSI-Schicht	Einordnung	DoD-Schicht	Protokollbeispiel	Einheiten
7 Anwendungen (Application)	Anwendungs- orientiert	Anwendung	HTTP FTP	Daten
6 Darstellung (Presentation)			HTTPS SMTP LDAP NCP	
5 Sitzung (Session)				
4 Transport (Transport)	Transport- orientiert	Transport	TCP UDP SCTP SPX	TCP = 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

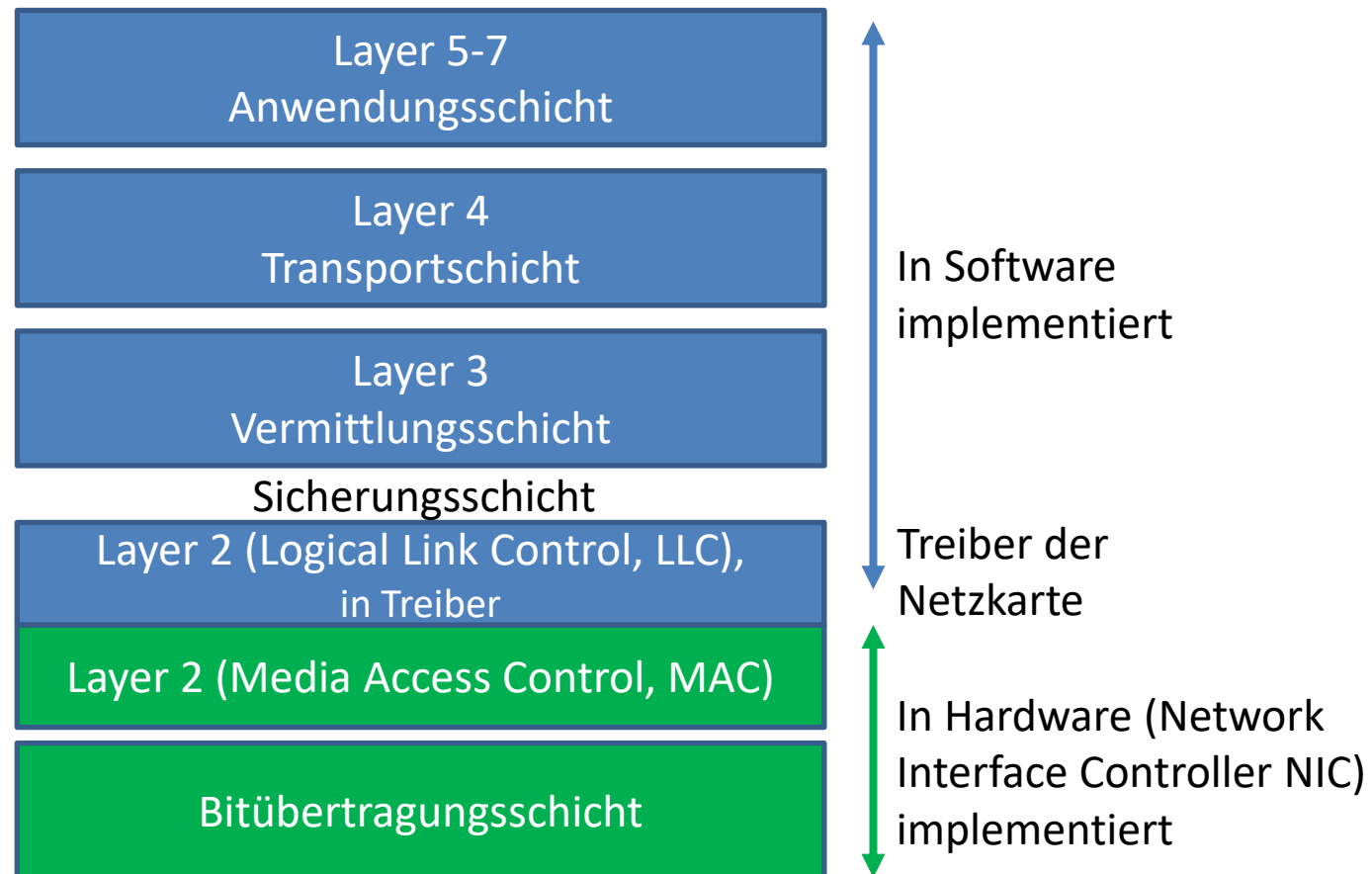
Wichtige IEEE 802.x-Reihe in der Übersicht

IEEE 802.x-Reihe	Standard für
IEEE 802.1	Bridging & Management
IEEE 802.1Q	Tagged VLANs
IEEE 802.2	Logical Link Control
IEEE 802.3	CSMA/CD Access Method
IEEE 802.5	Token Ring Access Method
IEEE 802.6	ANSI-Standard für MAN mit DQDB
IEEE 802.11	Wireless
IEEE 802.15	Wireless Personal Area Network
IEEE 802.16	Broadband Wireless Metropolitan Area Networks
IEEE 802.17	Resilient Packet Rings

Einordnung der Vermittlungsschicht



Unterteilung und Implementierung der Sicherungsschicht

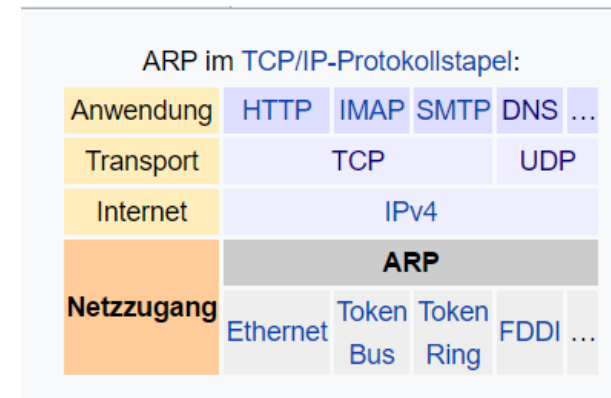


Unterteilung der Sicherungsschicht in die Teilschichten MAC und LLC (Ethernet)

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 = 1010101 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>	

Kurzaufgabe Aufzeichnung Frame in Gruppen

- Zeichnet mit dem Tool Wireshark den ARP-Prozess* auf.
- Beantwortet aus den Aufzeichnungen zu zweit folgende Fragen:
 - An welche physische Destination Adresse wird das Frame geleitet?
 - Welche Informationen findet Ihr im Ethernet Header.
 - Welche Informationen der L2-PDU sind nicht zu finden?
 - Welche konkreten ARP-Abfragen und ARP-Antworten findet ihr?
- Macht dazu z.B. einen Ping an den Router oder an einen Client welcher sich im gleichen Netz befindet.
- **Zeit: 15 Minuten**



* Das **Address Resolution Protocol (ARP)** ist ein Netzwerkprotokoll, das zu einer Netzwerkadresse der Internetschicht die physikalische Adresse (Hardwareadresse) der Netzzugangsschicht ermittelt und diese Zuordnung gegebenenfalls in den so genannten ARP-Tabellen der beteiligten Rechner hinterlegt. Es wird fast ausschließlich im Zusammenhang mit IPv4-Adressierung auf Ethernet-Netzen, **also zur Ermittlung von MAC-Adressen zu gegebenen IP-Adressen verwendet.**

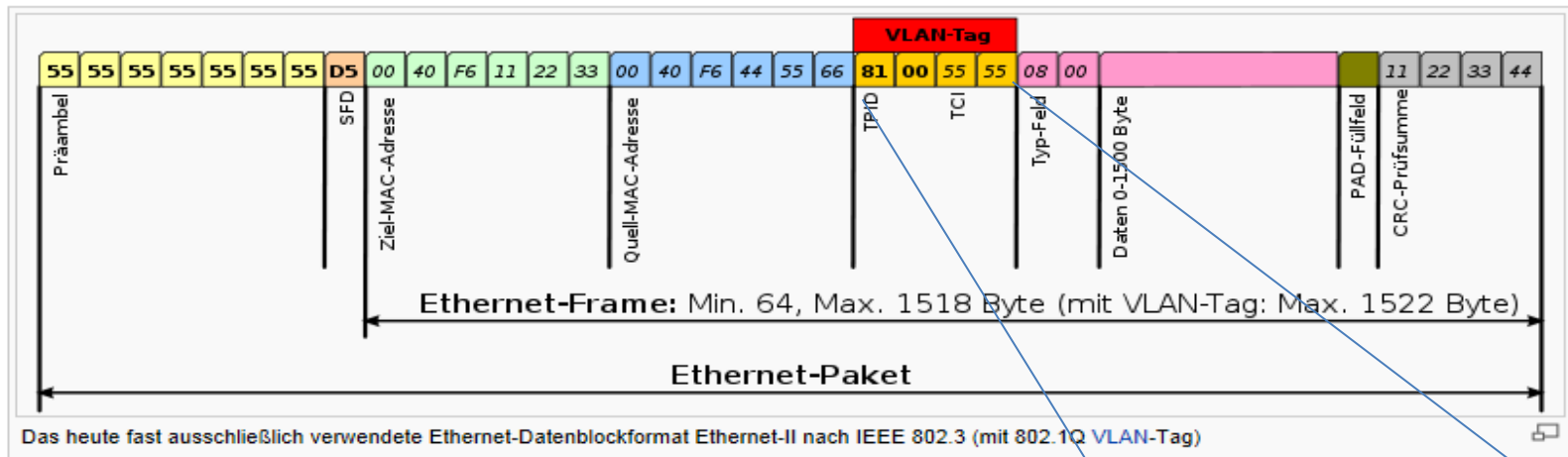
Musterantworten

- Beantwortet aus den Aufzeichnungen folgende Fragen:
 - An welche physische Destination Adresse wird das Frame geleitet? (**ff:ff:ff:ff:ff:ff – Broadcastadresse**)
 - Welche Informationen findet Ihr im Ethernet Header. (**siehe nächste Folie**)
 - Welche Informationen der L2-PDU sind nicht zu finden? **Der Trailer (FCS-Feld)**
 - Welche ARP-Abfrage und ARP-Antwort erhaltet ihr? (**ARP Request, ARP Response**)

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}))

Address Resolution Protocol

ARP-Aufzeichnung mit Wireshark

Wireshark_Capture_Beiispiel_Metadaten.pcapng [Wireshark 1.8.4 (SVN Rev 46250 from /trunk-1.8)] DE Deutsch (Schweiz) Hilfe

Filter: arp Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
2624	73.0308830	ZyxelCom_fd:7a:80	Broadcast	ARP	60	who has 192.168.77.40? Tell 192.168.77.1
2655	97.0407660	IntelCor_6a:7d:d8	ZyxelCom_fd:7a:80	ARP	42	who has 192.168.77.1? Tell 192.168.77.45
2656	97.0428580	ZyxelCom_fd:7a:80	IntelCor_6a:7d:d8	ARP	60	192.168.77.1 is at 00:13:49:fd:7a:80
2714	127.537931	IntelCor_6a:7d:d8	ZyxelCom_fd:7a:80	ARP	42	who has 192.168.77.1? Tell 192.168.77.45
2715	127.541710	ZyxelCom_fd:7a:80	IntelCor_6a:7d:d8	ARP	60	192.168.77.1 is at 00:13:49:fd:7a:80

Frame 2624: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
Ethernet II, Src: ZyxelCom_fd:7a:80 (00:13:49:fd:7a:80), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Destination: Broadcast (ff:ff:ff:ff:ff:ff)
Source: ZyxelCom_fd:7a:80 (00:13:49:fd:7a:80)
Type: ARP (0x0806)
Padding: 4d2cc0a84dff00890089003af152a1260110
Address Resolution Protocol (request)
Hardware type: Ethernet (1)
Protocol type: IP (0x0800)
Hardware size: 6
Protocol size: 4
Opcode: request (1)
Sender MAC address: ZyxelCom_fd:7a:80 (00:13:49:fd:7a:80)
Sender IP address: 192.168.77.1 (192.168.77.1)
Target MAC address: 00:00:00:00:00:00 (00:00:00:00:00:00)
Target IP address: 192.168.77.40 (192.168.77.40)

0000 ff ff ff ff ff ff 00 13 49 fd 7a 80 08 06 00 01 I.Z....
0010 08 00 06 04 00 01 00 13 49 fd 7a 80 c0 a8 4d 01 I.Z...M.
0020 00 00 00 00 00 00 c0 a8 4d 28 4d 2c c0 a8 4d ff M(M...M.
0030 00 89 00 89 00 3a f1 52 a1 26 01 10R .&..

Destination Hardware Address (eth.dst), 6 by... Packets: 2716 Displayed: 5 Marked: 0 Dropped: 0 Load time: 0:00.093 Profile: Default

ARP-Tabelle / ARP-Cache auf Windows auslesen

- Befehl in CMD: **arp -a**

Ermittlung von MAC-Adressen zu gegebenen IP-Adressen

Internetadresse	Physische Adresse	Typ	Beschreibung
192.168.1.1	00-13-49-34-8b-20	dynamisch	Standardgateway
192.168.1.255	ff-ff-ff-ff-ff-ff	statisch	Broadcast Adresse des Netzes
224.0.0.251	01-00-5e-00-00-fb	statisch	Multicast DNS, .local
224.0.0.252	01-00-5e-00-00-fc	statisch	Link Local Multicast Name Resolution (LLMNR), DNS
239.255.255.250	01-00-5e-7f-ff-fa	statisch	Simple Service Discovery Protocol (SSDP), Multicast für UPnP Geräte
255.255.255.255	ff-ff-ff-ff-ff-ff	statisch	Limitierter Broadcast

Weitere Multicastbezeichnungen findet Ihr auf:

http://en.wikipedia.org/wiki/Multicast_address

Agenda



«Grundlagen Ethernet LAN-Switching»

CCNA1, Kapitel 5

Wichtige Funktionen eines Switches

Funktion oder Bezeichnung	Beschreibung
Multiport-Bridging	Jeder Port wird dadurch zu einer eigenen Kollisionsdomäne (nicht für Broad- und Multicasts) Vollduplex möglich
Switching	Arbeitet mittels einer MAC-Adresstabelle (CAM – Content Addressable Memory). Hier werden MAC-Adressen gespeichert. Die Weiterleitung eines Unicast erfolgt daher nur an den entsprechenden Ziel-Port.
OSI-Layer	Meist OSI Layer 2 aber auch höher (Sicherheitsschicht)
Durchleitungsmethode	Store and forward (komplett empfangen und erst dann weiterleiten) Cut-trough (möglichst schnelles Weiterleiten, erkennt Fehler nicht) Fragment-Free-Switching (Weiterleiten nach 64Byte)
VLANs (Virtual Local Area Network)	Das lokale Netzwerk kann in VLANs unterteilt (802.1Q) werden.
Trunking (Link Aggregation)	Mehrere Ports werden auf einem Switch gebündelt.
Sicherheit	Port-Security durch IEEE 802.1X
Netzwerk-Schlaufen (flooding) verhindern mit STP resp. neu R-STP Rapid-Spanning Tree Protocol	Ein Switch wird Master (logischer Baum). Durch Multicasts (BPDU) werden Parallelstrecken erkannt und Schleifen unterbunden. (Kein Loop möglich wenn MAC-Adressen nicht vorhanden sind)

Das hierarchische Netzwerkmodell

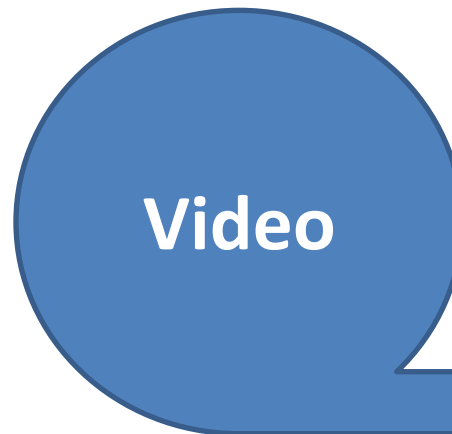
Auswahl der richtigen Switches

Hierarchie	Beschreibung
Access-Layer (Zugangsschicht)	Verbindung zwischen Endgeräten (PCs, Druckern, IP-Telefonen. Umfasst Router, Switches, Access-Points, Server).
Distribution-Layer (Verteilerschicht)	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.

Video anschauen

- CCENT/CCNA ICND1 100-105 Video
– **Switch Basics / 1. Teil**



Dauer: 10 Minuten

Einzelarbeit Cisco Networking Academy (optional)

- Bearbeitet und überfliegt das Kapitel 7.3 Switch-Grundlagen in der Cisco Network Academy und ergänzt euer bereits erworbenes Wissen selbstständig.

<https://www.netacad.com>

<https://contenthub.netacad.com/itn/7.3.1>

- **Zeit: 20 Minuten**

Agenda



«CLI Grundlagen»



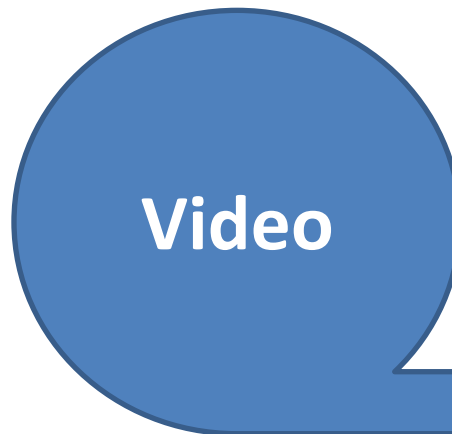
CCNA1 Kapitel 4

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

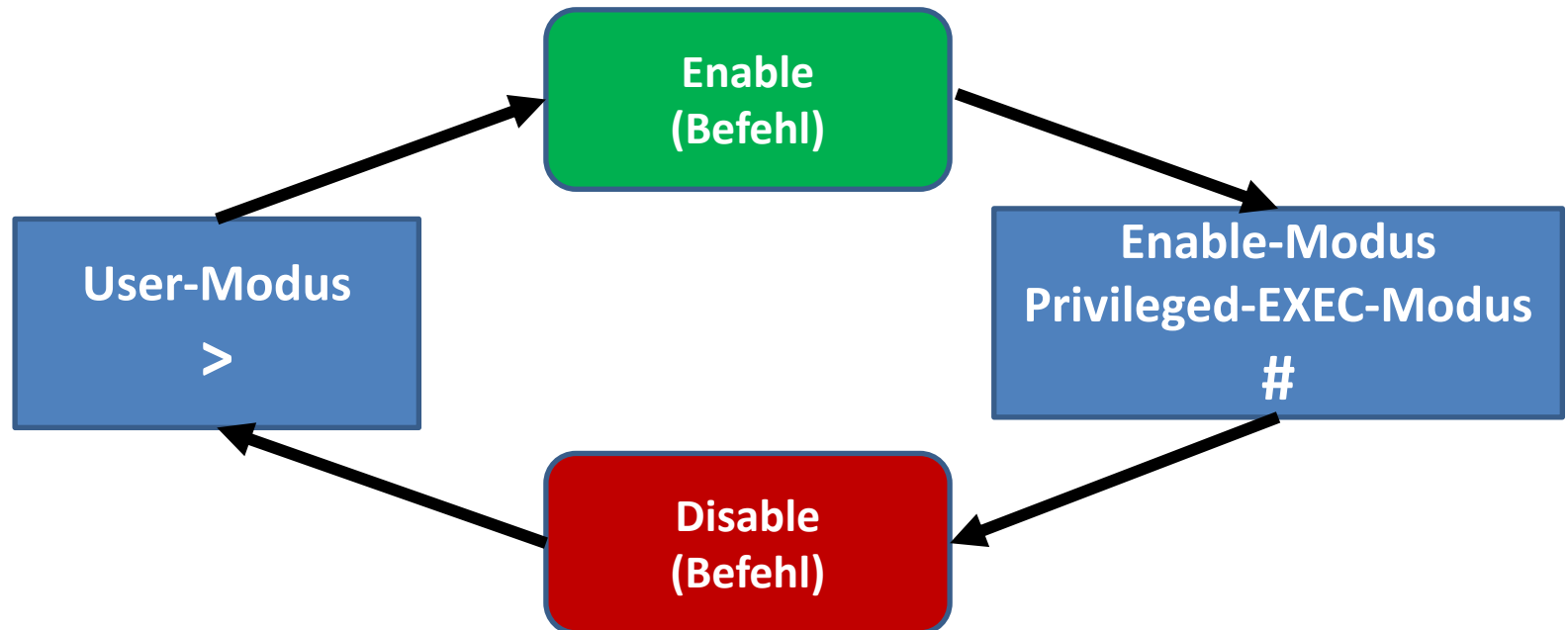
Video anschauen

- CCENT/CCNA ICND1 100-105 Video
– CLI Navigation



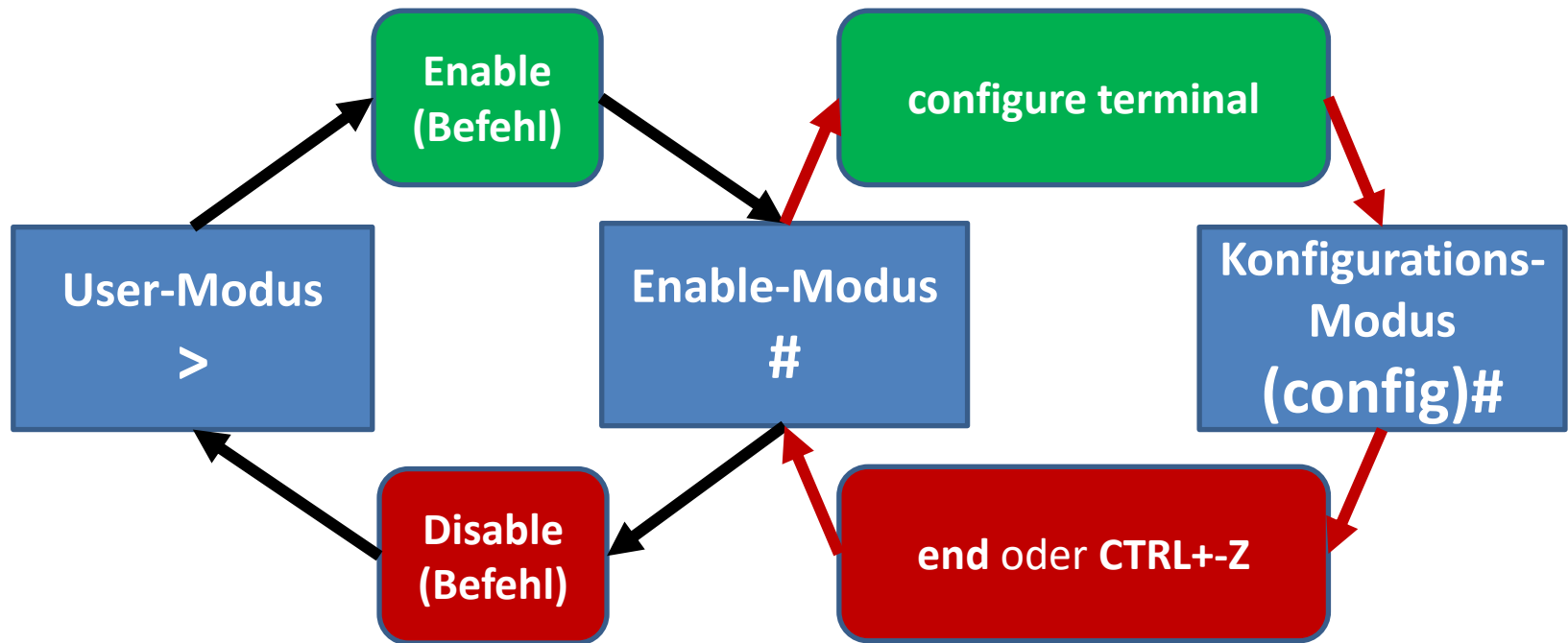
Dauer: 13 Minuten

CLI-Berechtigungskonzept



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

Der Konfigurationsmodus



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

Enable Modus und Konfigurations Modus

LAB>_

Höheren Modus erlangen:

```
R1> enable  
R1# configure terminal  
R1(config)#
```

Modus verlassen:

```
R1(config)# end oder CTRL+Z  
R1# disable  
R1>
```

Nützliche Grundbefehle CLI

LAB>_

HELP und nützliche Commands

R1# show ? (Zeigt weitere Befehlsergänzungen an)

R1# show run (Mit **TAB** ergänzen)

R1# show running-config

R1# show ip route

R1# show interfaces

R1(config)# **do** show ip interface brief

R1# show run | begin hostname (Pipe ist case sensitive, sonst nicht)

R1# show run | in int

R1# show run | section bgp

Nützliche Grundbefehle CLI

LAB>_

Weitere nützliche Commands

R1# reload (Neustart)

R1# write (Konfiguration speichern)

S1# write erase (in Werkzustand zurücksetzen Vorsicht!)

R1> ping 192.168.10.1

Eine IP Adresse zuweisen

LAB>_

Erstes Router Interfaces konfigurieren:

```
R1(config)# interface gigabitEthernet 0/0  
R1(config-if)# ip address 10.10.10.1 255.255.255.0  
R1(config-if)# no shutdown
```

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 Zugriff „Konsole“

LAB>_

Konsolen Access konfigurieren:

```
S1(config)# line con 0
```

```
S1(config-line)# password console
```

```
S1(config-line)# login
```

```
S1(config-line)# logging synchronous
```

```
S1(config-line)# history size 15
```

```
S1(config-line)# exec-timeout 10
```

CLI Zugriff „Telnet“

LAB>_

Telnet Access konfigurieren (Port TCP 23):

```
S1(config)# line vty 0 15
S1(config-line)# exec-timeout 10
S1(config-line)# password telnet
S1(config-line)# logging synchronous
S1(config-line)# login
S1(config-line)# history size 15
```

Telnet sollte aus Sicherheitsgründen nicht mehr verwendet werden!

Verwende wann immer möglich SSH. (Hier nur aus theoretischer Sicht noch erläutert.)

CLI Zugriff „SSH“

LAB>_

SSH Access konfigurieren (Port TCP 22):

```
S1(config)# line vty 0 15
```

```
S1(config-line)# login local
```

```
S1(config-line)# exit
```

```
S1(config)#username user password cisco
```

```
S1(config)# ip domain-name beispiel.ch
```

```
S1(config)# crypto key generate rsa
```

```
S1(config)# ip ssh version 2
```

Benutzer erstellen

LAB>_

Benutzer erstellen:

```
R1> en
```

```
R1# configure terminal
```

```
R1(config)# username user password cisco (unsicher)
```

```
R1(config)# username user secret cisco
```

```
R1(config)# username admin privilege 15 secret cisco  
                (Volle Adminrechte)
```

```
R1(config)# line console 0
```

```
R1(config-line)# login local
```

```
R1# logout
```

```
R1(config)# no username user password cisco (Benutzer  
löschen)
```

Passwörter setzen und verschlüsseln

LAB>_

Enable Passwort setzen:

```
R1(config)# enable secret cisco (MD5)
```

User Passwort setzen:

```
R1(config)# username user secret cisco (MD5)
```

Passwörter verschlüsseln (WICHTIG):

```
R1(config)# service password-encryption (Encryption  
aktivieren – unsicherer Algorithmus ist knackbar)
```

```
R1# write
```

```
R1# show running-config (Passwörter zu kontrollieren)
```


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

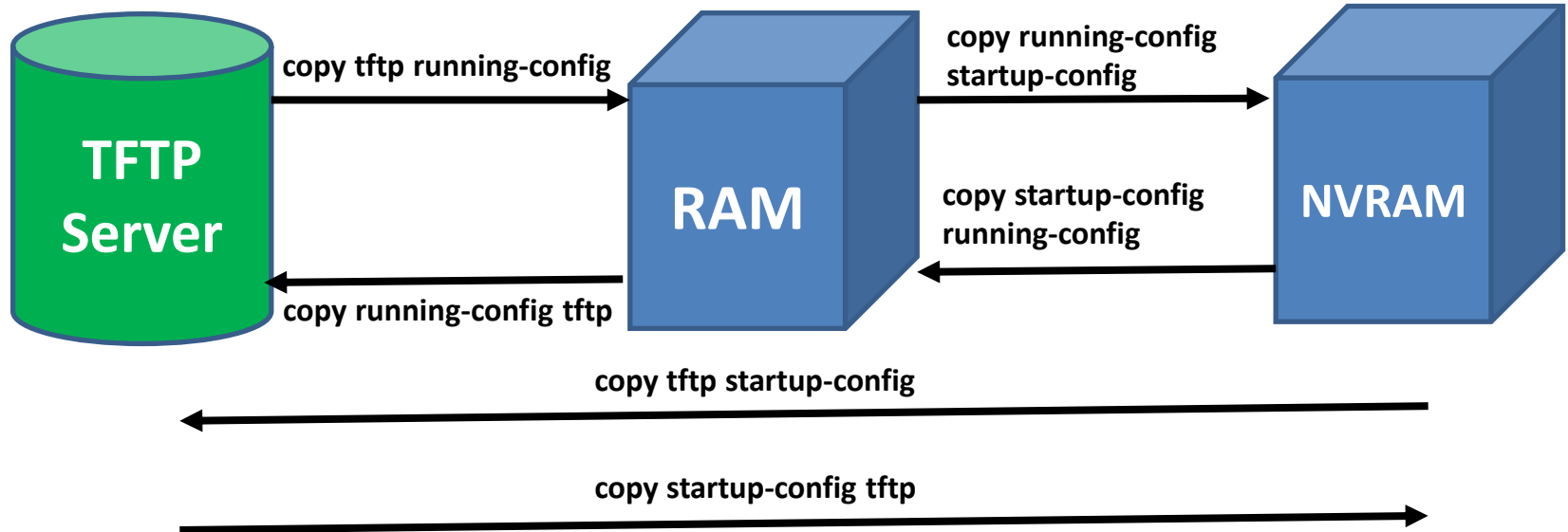
CISCO Switch Konfigurationsdaten speichern

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

Aufgaben aus CCNA-Büchern

Besprechung der Fragen zu
CCNA1 Kapitel 4, 5, 6

Zweiergruppe: Besprechung aller Fragen

Zeit: 15 Minuten

Ende Block 5

«Ende»

Lernziele des 5. Modulblocks

- **Du kannst...**

1. ...die wichtigsten Funktionen von ICMP erklären.
2. ...den Routingprozess anhand des statischen IPv4-Routings erklären.
3. ...die Funktionen der Sicherungsschicht anhand des Ethernet-Protokolls beschreiben.
4. ...die grundlegenden Funktionen und IEEE-Standards des Ethernet LAN-Switching erläutern.
5. ...die grundlegenden Cisco CLI Commands beschreiben.

Deine Hausaufgaben

Stoff Nachbearbeitung 5. Modul:

- **Repetition der Folieninhalte des Modulblocks:** Ergänzen deiner individuellen Zusammenfassung.
- **Lernstoff Vertiefung:**
 - CCNA1 Buch Kapitel 4 «Using the Command-Line Interface»
 - NetAcademy Kapitel 4 und 5
- **Praxistransfer:**

Übe mit dem CISCO Pakettracer die grundlegenden CLI-Befehle aus dem Modulblock 5:

 - Erstelle im Pakettracer einen Cisco 2911 Router
 - Nenne den Router R1. Notiere den dazu verwendeten Befehl
 - Konfiguriere das erste Interface (0/0) mit folgender IP-Adresse 10.10.10.1/30 und notiere die dazu verwendeten Befehle.
 - Erstelle ein sicheres «enable» Passwort. Notiere den dazu verwendeten Befehl.
 - Richte den CLI Zugriff mittels SSH ein. Notiere die dazu verwendeten Befehle.
 - Speichere deine Cisco-Router Konfiguration und notiere den dazu genutzten Befehl.
 - Prüfe in der Cisco Konfigurationsdatei, dass alle Passwörter «gehashed» sind und notiere den zur Anzeige der Konfigurationsdatei genutzten Befehl.
 - Prüfe nun ob alle Passwörter «gehashed» sind. Notiere deine Hashes.
 - Speichere die Notizen und die Pakettracer Lösung für die anschliessende Diskussion im nächsten Modulblock.
- **Vorbereitung auf das nächste Modul:**
 - CCNA1 Buch Kapitel 5 «Analyzing Ethernet LAN Switching»
 - CCNA1 Buch Kapitel 6 «Configuring Basic Switch Management»
 - CCNA1 Buch Kapitel 8 «Implementing Ethernet Virtual LANs»