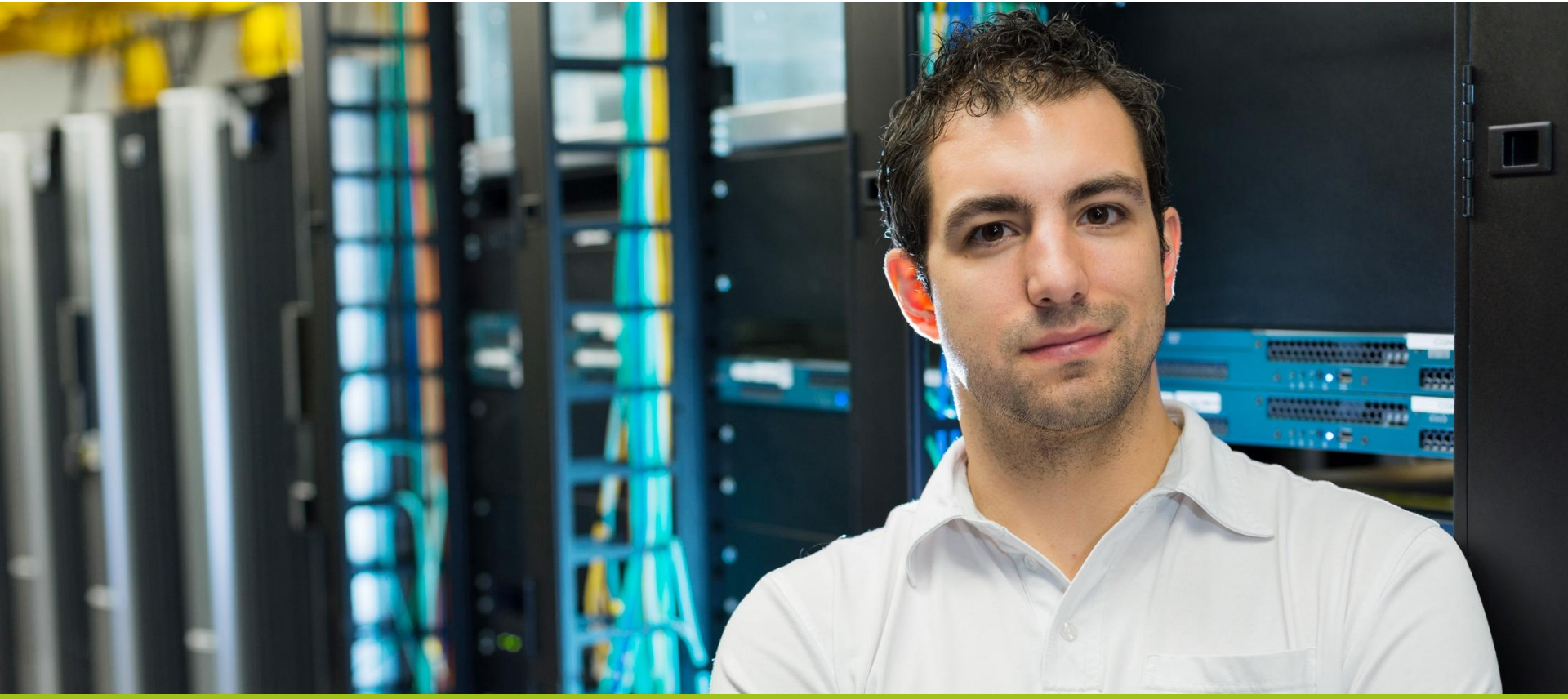
ipso! Bildung seit 1876



Kommunikationstechnik KOTE / Netzwerkgrundlagen
4. 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	Netzwerkkommunikation 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

ipso!

Lernziele des 4. Modulblocks

- **Du kannst..**
  1. …grundlegende technische Funktionen von IPv4 einordnen.
  2. …selbstständig IPv4 Netze in Subnetze unterteilen.

Agenda

«Repetition und Hausaufgabenbesprechung»

Gruppenarbeit
Repetition Block 3

Auftrag: Jede Gruppe bereitet eines der folgenden 4 Themen soweit vor, dass sie es den Kollegen im Anschluss erklären kann.

Form: keine Vorgabe

Zeit: Vorbereitung 30 Minuten

Themen:

1. Namensauflösung (DNS-Anfrage) und anschliessender Aufruf einer Website
2. Auf- und Abbau einer TCP-Verbindungen
3. Erklärung Transportschicht Protokoll-Header (UDP und TCP)
4. Erklären der TCP/IP Standards (Organisationen, RFC, technische Standards)

Zeit: 30 Minuten

Repetition Block 3

Fragen zur Vertiefung:

- CCNA2 Kapitel 1 «Introduction to TCP/IP Transport and Applications»
- «https://de.wikipedia.org/wiki/Transmission_Control_Protocol»
- «https://de.wikipedia.org/wiki/User_Datagram_Protocol»
- «https://de.wikipedia.org/wiki/Domain_Name_System»

Praxistransfer: Besprechung in den Gruppen

Zeit: 20 Minuten

Agenda

«Kurztest»

Ablauf Kurztest

- Versuche die Aufgaben bestmöglich zu lösen. Du hast jeweils **3 Minuten Zeit pro Folie**. Danach kommt die nächste Aufgabe.
- Schreibe die Grundlagen sinnvoll auf ein Blatt, so dass eine Korrektur möglich ist.
- **Es handelt sich hier um eine Einzelarbeit!**
- **Es gibt keine Note!**

ipso!

1. Aufgabe zur Netzwerktechnik

- Welche verschiedenen Adressierungen (Source und Destination) befinden sich auf den jeweiligen OSI Layern 2, 3 und 4?

2. Aufgabe zur Netzwerktechnik

- Beschreibe den TCP Verbindungsaufbau und den TCP Verbindungsabbau. Was läuft genau ab?

3. Aufgabe zur Netzwerktechnik

- Welches sind die wichtigsten Netzwerkdienste und deren Protokolle und Ports?

4. Aufgabe zur Netzwerktechnik

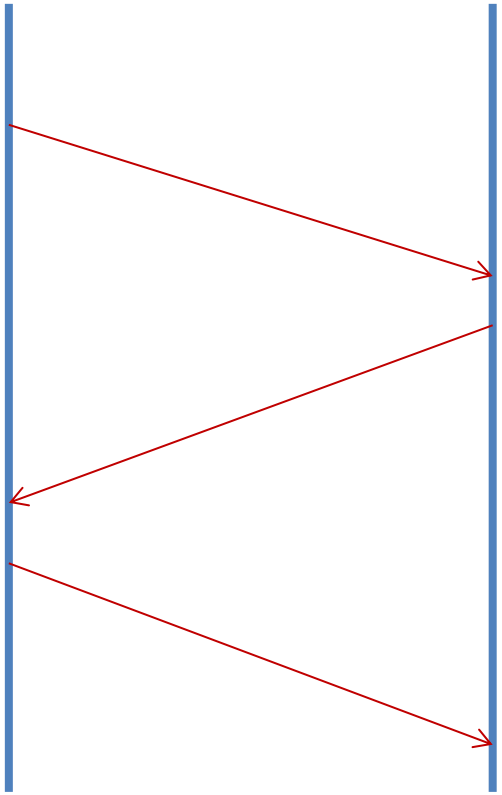
1. Was verstehen wir in der Netzwerktechnik unter einem Socket oder einer API?
2. Was ist ein Peer-to-Peer Netzwerk?
3. Wie funktioniert die Kommunikation mit Protokollen im Netzwerk? Beschreibe das **Vorgehen** anhand eines Schichtenmodells z.B. OSI oder TCP/IP.

Musterantwort zur 1. Aufgabe

OSI-Layer	Adressierung (Source / Destination)
Layer 4	TCP- oder UDP-Port
Layer 3	IP-Adresse
Layer 2	MAC-Adresse

Musterantwort zur 2. Aufgabe
TCP Verbindung aufbauen (three-way-handshake)

1.
Sende SYN
(SEQ=100, CTL=SYN)

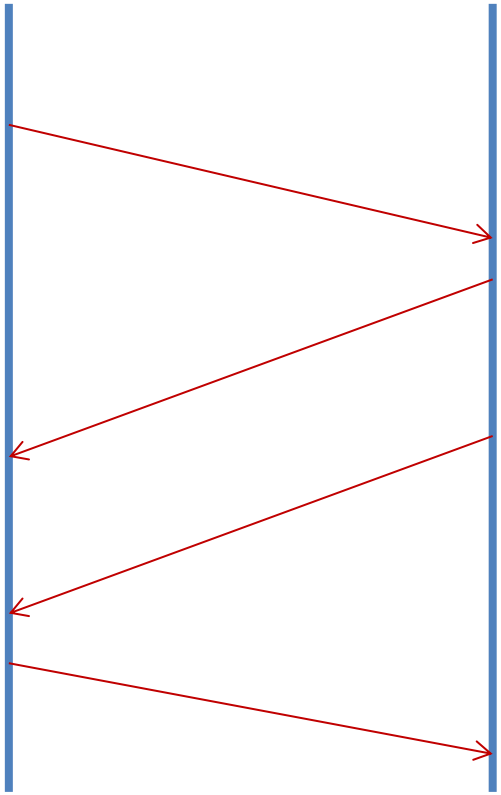


2.
Empfange SYN
Sende SYN-ACK
(SEQ=300, ACK=101,
CTL=SYN, ACK)

3.
SYN wurde empfangen
Verbindung aufgebaut
Sende ACK
(SEQ=101, ACK=301,
CTL=ACK)

Musterantwort zur 2. Aufgabe
TCP Verbindung abbauen teardown process

FIN/ACK
(SEQ=X, CTL=FIN, ACK)



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

FIN/ACK
(SEQ=Y, CTL=FIN, ACK)

ACK
(SEQ=Y+1, CTL=ACK)

Musterantwort zur 3. Aufgabe

Dienstbezeichnung	Protokoll	Ports
Dateifreigabe	SMB 2.1 (Win 7 / Win Server 2008 R2) SMB 3.0 (Win 8 / Win Server 2012)	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

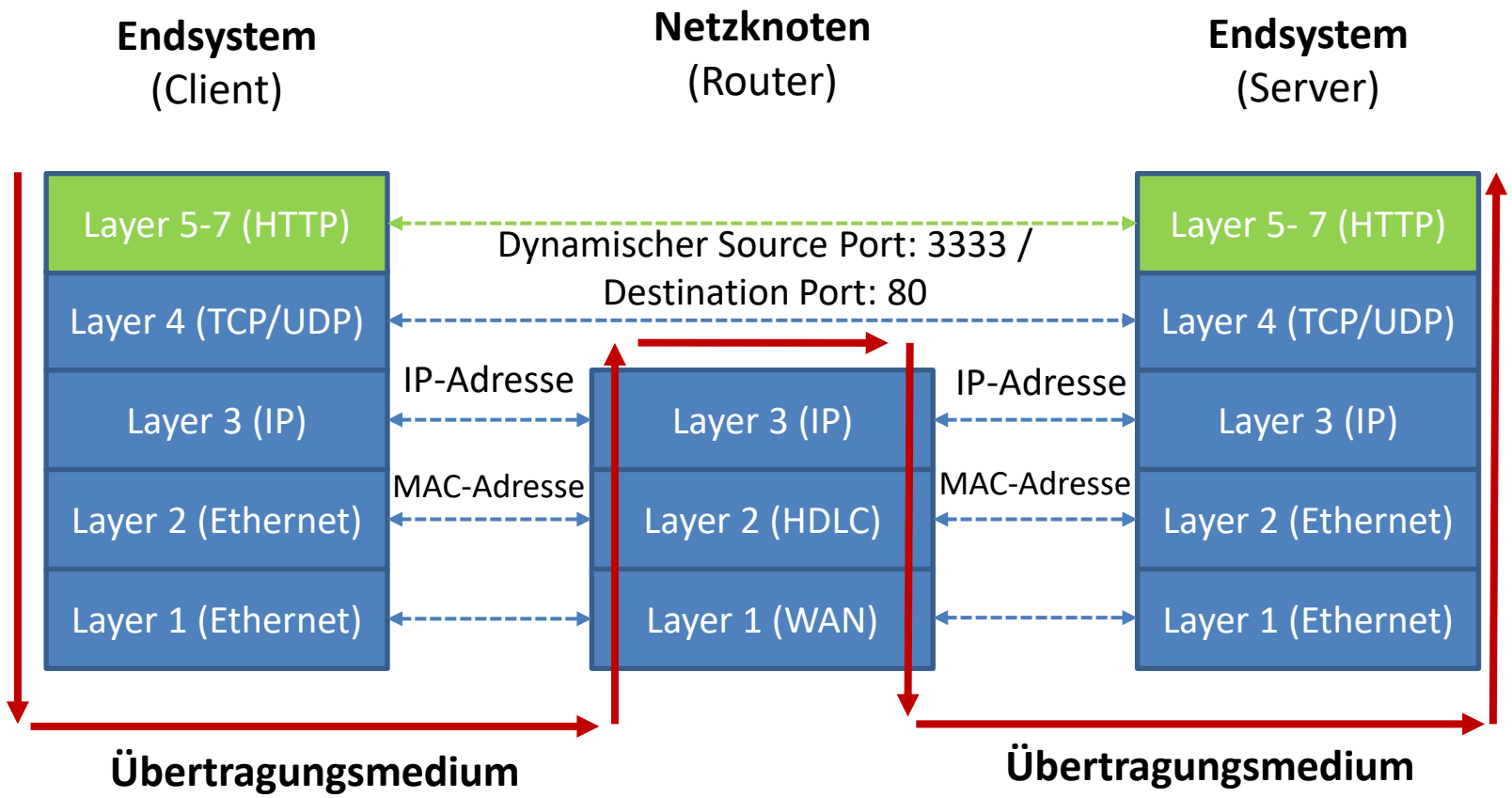
Musterantwort zur 3. Aufgabe

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

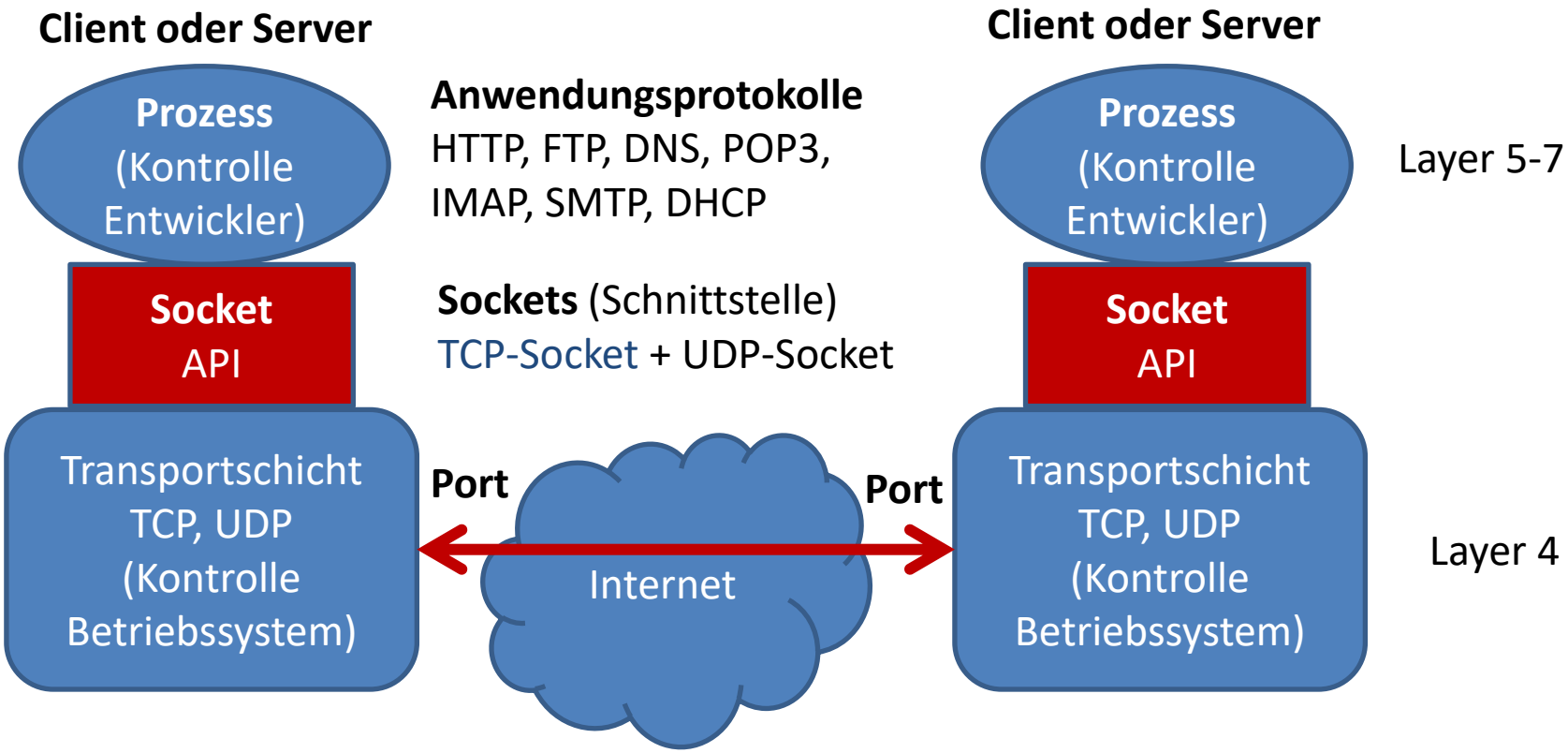
Musterantworten zur 4. Aufgabe

1. Prozesse auf unterschiedlichen Computern kommunizieren in dem sie Nachrichten durch **Sockets (IP und Port)** übermitteln. Dazu wird eine standardisierte Schnittstelle namens **API** verwendet, welche die Anwendung mit der Netzwerkprotokollimplementierung (z.B. TCP/IP) des Betriebssystems verbindet.
2. Bei einem Peer-to-Peer Netzwerk kommunizieren die Workstations direkt miteinander. Jeder Computer kann Client, sowie auch Server sein, also Ressourcen (z.B. Datenspeicher, Drucker,..) verwenden und anbieten.
3. Jede Schicht des ISO/OSI-Modells, bis auf die Bitübertragungsschicht verwendet **Header** für Steuerinformationen. Auf der Sicherungsschicht wird zusätzlich ein Trailer mit Checksumme verwendet.

Repetition
Musterlösung des Übertragungsprozesses



Repetition
Verbindung Anwendung mit Transportschicht



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

ipso!

Agenda

«Vertiefung Vermittlungsschicht»

CCNA2 Buch Kapitel 1
«Introduction to TCP/IP Transport and Applications»

Einordnung der Vermittlungsschicht

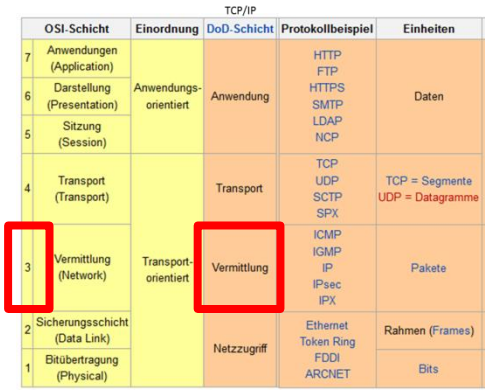
Application Layer
Anwendungsschicht

Transport Layer
Transportschicht

Network Layer
Vermittlungsschicht

Data Link Layer
Sicherungsschicht

Physical Layer
Bitübertragungsschicht



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

Aufgaben der Netzwerkschicht
OSI-Vermittlungsschicht

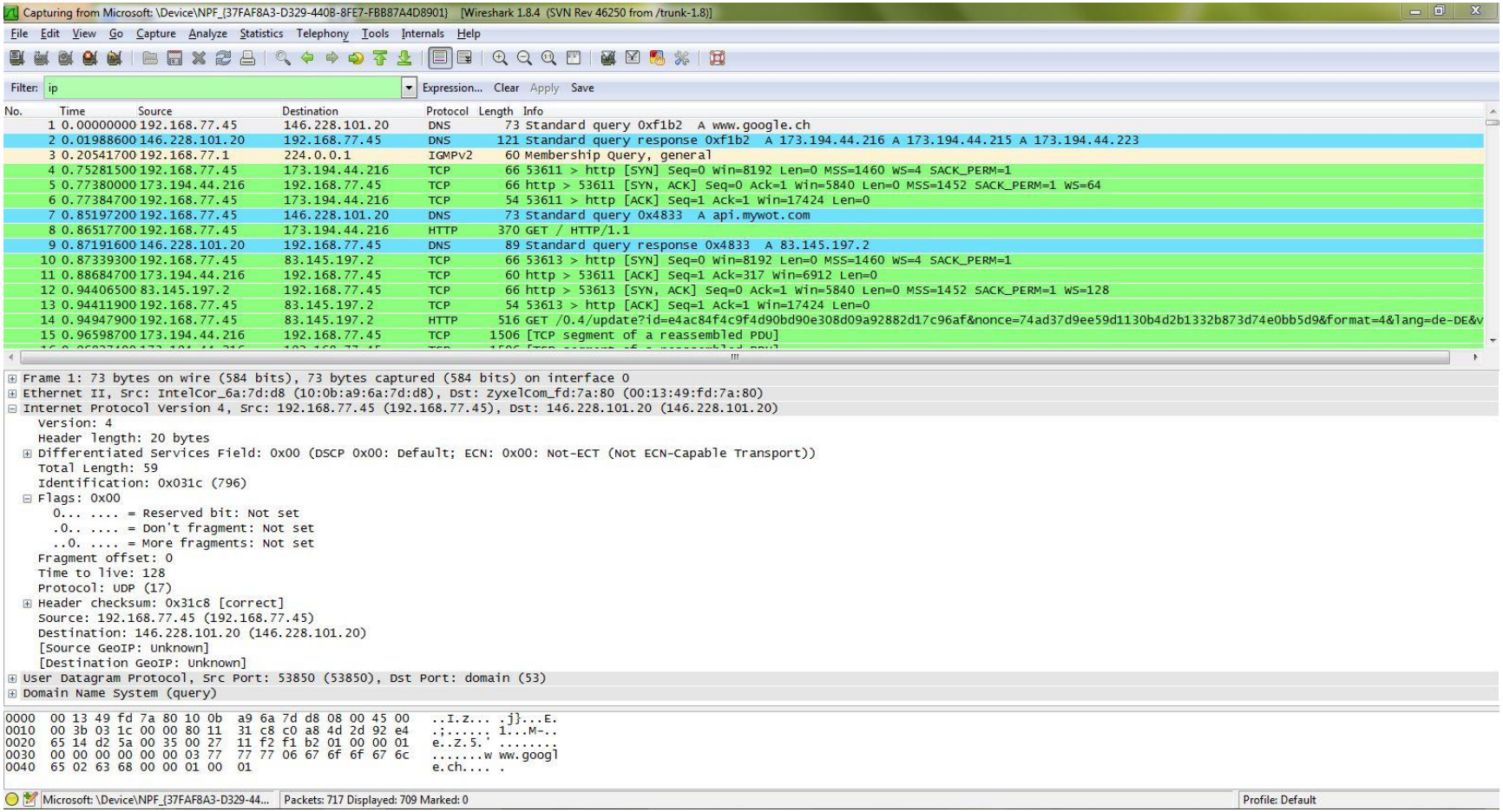
- Übernimmt Segmente der Transportschicht
- Fügt IP-Header der PDU hinzu
- Stellt Host zu Host Verbindung her
  - Source- und Destination-Adresse
- Leitet die Pakete ins Zielnetzwerk weiter (Routing)
- Die Netzwerkschicht (IP) ist verbindungslos und ungesichert, dies übernimmt die Transportschicht (TCP)

Kurzaufgabe in Gruppen

- Zeichnet mit dem Tool Wireshark den IP-Header auf.
- Beantwortet aus den Aufzeichnungen folgende Fragen:
  - Wie sieht der Header aus?
  - Welche wichtige Information verhindert ein Dauersenden eines IP-Datagramms?

- **Zeit: 10 Minuten**

Selber aufzeichnen / IPv4-Header
IPv4-Aufzeichnung mit Wireshark



Grundlagen IPv4

- IPv4 Paket Header

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

Version = V4/V6 IHL= IP Header Length

Paketlänge = gesamtes Paket inkl. Kopfdaten

Flags = 0,1,2 Fragementierung Kontroll-Schalter

TTL = Lebensdauer des Pakets (Max. 255)

Header Checksumme = sichert Header

TOS = Type of Service (Priorität)

Kennung = Fragmente erkennen

Fragmentoffset = Aufteilung

Protokoll = Folgeprotokoll (TCP/UDP)

Optionen/Füllbits = Zusatzinfos

Die IP-Netzklassen (Historisch nur klassenbezogen)

Klasse	IP-Adressbereich	Anzahl Host/Netz
A	0.0.0.0 – 127.255.255.255	16’777’214
B	128.0.0.0 – 191.255.255.255	65’534
C	192.0.0.0 – 223.255.255.255	254
D (Multicast)	224.0.0.0 – 239.255.255.255	
E (Reserviert)	240.0.0.0 – 255.255.255.255	

Zur Verteilung bestimmte IPv4 Netzklassen

Netzklasse	Präfix	Adressbereich	Verwendung	CIDR Suffix
Klasse A	**0..**	**0.0.0.0 – 127.255.255.255**	**Verteilung**	**/8**
Klasse B	**10..**	**128.0.0.0 – 191.255.255.255**	**Verteilung**	**/16**
Klasse C	**110..**	**192.0.0.0 – 223.255.255.255**	**Verteilung**	**/24**
Klasse D	1110..	224.0.0.0 – 239.255.255.255	Multicast	
Klasse E	1111..	240.0.0.0 – 255.255.255.255	Reserviert	

CDIR = Classless Inter-Domain Routing

Beispiel der IP-Subnettierung (klassenbezogenes Subnetze)

Nr.	Subnetz	IP-Adressen	Anzahl Host
1	150.9.1.0	150.9.1.1 – 150.9.1.254	254
2	150.9.2.0	150.9.2.1 – 150.9.2.254	254
3	150.9.3.0	150.9.3.1 – 150.9.3.254	254
4	150.9.4.0	150.9.4.1 – 150.9.4.254	254
5	150.9.5.0	150.9.5.1 – 150.9.5.254	254

Subnettierung
In welchem Subnetz bin ich?

```
source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
allow-hotplug enp0s3
#iface enp0s3 inet dhcp
iface enp0s3 inet static
        address 10.10.10.100
        netmask 255.255.255.0
        gateway 10.10.10.1
user@debian:~$ _
```

255 255 255

Binär: 11111111 11111111 11111111 00000000

- Der Computer vergleicht den Teil der **IP-Adresse** bis dort wo die 1en (Einsen) der **Subnetzmaske** aufhören. Ist der Wert gleich, dann befindet sich der gewünschte Client im gleichen Netz. Wenn nicht werden die Pakete an den **Standardgateway** (Router) gesandt.

Commands:

Ipconfig /all

ncpa.cpl Netzwerk auswählen + Details

ipso!

IP-Adressen Vergabe

IP-Vergabestellen	Zuständigkeit
IANA – Internet Assigned Numbers Authority	Regelt die Vergabe von IP-Netzen im Internet
RIR – Regional Internet Registries	Seit Februar 2005 gibt es 5 RIR für die verschiedenen weltweiten Regionen Für die **Schweiz ist RIPE NCC** zuständig http://www.ripe.net/
LIR – Local Internet Registry	Internet Service Provider geben IP an Kunden
Private Netze nach RFC 1918	Können selbst vergeben werden.

Eine IP muss EINMALIG sein!

ipso!

Berechnungen im Binärsystem (siehe auch Tabelle A.1 im Buch)

Umrechnung Binär zu Dezimal:

Ein Oktett

Wert	1. Stelle	2. Stelle	3. Stelle	4. Stelle	5. Stelle	6. Stelle	7. Stelle	8. Stelle
Potenz	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
Dezimal	128	64	32	16	8	4	2	1
Binär	1	1	1	1	1	1	1	1
Wert	128	64	32	16	8	4	2	1

Berechnung dezimal = 128 + 64 + 32 + 16 + 8 + 4 + 2 + 1 = 255 (1111 1111)

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

Berechnung dezimal = 128 + 16 + 8 + 2 + 1 = 155 (1001 1011)

ipso!

Übung macht den Meister
Berechne selbständig

Umrechnung Binär zu Dezimal:

Wert								
Dezimal	128	64	32	16	8	4	2	1
Binär	1	1	0	1	1	1	1	1
Wert	128	64	0	16	8	4	3	1

Berechnung = 223

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

Berechnung = ?

ipso!

Lösung
(vergleiche mit Tabelle A.1 im Buch)

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 = 64 + 32 + 8 + 4 = 108

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

Berechnung = 16 + 1 = 17

ipso!

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.

Erörterung (RFC 1918) warum /12
172.16.0.0/12 bis 172.31.255.255/12

2. Oktett

Netz-Teil ⟷ Host-Teil

Wert								
Dezimal	128	64	32	16	8	4	2	1
IP	0	0	0	**1**	**0**	**0**	**0**	**0**
Subnetmaske	**1**	**1**	**1**	**1**	0	0	0	0
Subnetz	**0**	**0**	**0**	**1**	**0**	**0**	**0**	**0**

Subnetz = 172.16.0.0 / 255.240.0.0 (/12)

1. IP-Adresse = 172.**16**.0.1 (10101100 0001000 00000000 00000001)

Wert								
Dezimal	128	64	32	16	8	4	2	1
IP	0	0	0	**1**	**1**	**1**	**1**	**1**
Subnetmaske	**1**	**1**	**1**	**1**	0	0	0	0
Subnetz	**0**	**0**	**0**	**1**	**0**	**0**	**0**	**0**

Broadcast-Adresse = 172.**31**.255.255 (10101100 0001111 11111111 11111111)

nächstes Subnetz = 172.32.0.0 / 255.240.0.0 (/12)

ipso!

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: • 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

Agenda

«Die Subnettierung»

CCNA1 Buch Kapitel 11 «Perspectives on IPv4 Subnetting»

Grundlagen Subnettierung

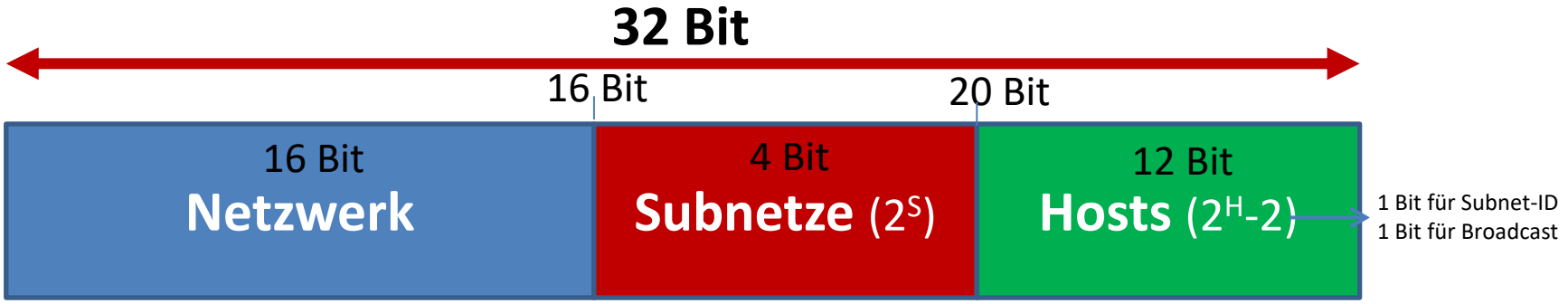
- Die Subnettierung ist notwendig um Netze zu teilen, meist aus..
  - ..Ressourcen Gründen (Broadcast eindämmen)
  - ..aus Sicherheitsgründen
- Die Subnettierung erfolgt durch die **Subnetz Maske:**
  - **z.B. 255.255.255.0**
  - **oder 11111111. 11111111. 11111111.00000000**
  - **oder /24 (Präfix)**

Klassenbezogene A-, B- und C-Netze

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

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

Klassenbezogene IPv4-Netzwerke analysieren

Arbeit zu zweit:

Übung Anhang D (2017):

Einige IP-Adressen analysieren

Zeit: 15 Minuten

ipso!

Masken analysieren

Beispiel:

- Problem: 10.66.5.99
- Maske: 255.255.254.0
- Präfix: /23
- Netzwerkbits: 8 (Class A)
- Subnetbits: 15
- Anzahl der Subnetze im Netzwerk: $2^{15} = 32768$
- Anzahl Host pro Subnetz: $2^9 - 2 = 510$

Arbeit zu zweit:

Übung Anhang E: einige Masken analysieren
(ab Seite 1118, 2. Hälfte des Anhangs)

Zeit: 15 Minuten

ipso!

Bestimmung des Subnetzes

- Es wird dazu das **Boolesche UND** verwendet
  - 1 UND 1 = 1
  - 0 UND 1 = 0
  - 1 UND 0 = 0
  - 0 UND 0 = 0

- Der Hostanteil bei einem Subnet besteht aus Nullen.

Subnetze Vergleichen /26 (letztes Oktett ist von Interesse)
Gleiches Subnet im letzten Oktett?

Letztes Oktett

Wert								
Dezimal	128	64	32	16	8	4	2	1
IP	1	1	1	0	1	0	1	0
Maske	1	1	0	0	0	0	0	0
	1 UND 1=1	1 UND 1=1	1 UND 0	0 UND 0				
Netz	**1**	**1**	**0**	**0**	**0**	**0**	**0**	**0**

234

192

IP = 192.168.1.234 / Subnetz = 192.168.1.192 / Maske = (1111 1111 1111 1111 1111 1111 1100 0000 / P=26)

Wert								
Dezimal	128	64	32	16	8	4	2	1
IP	0	0	0	0	0	0	1	0
Maske	1	1	0	0	0	0	0	0
Netz	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**

2

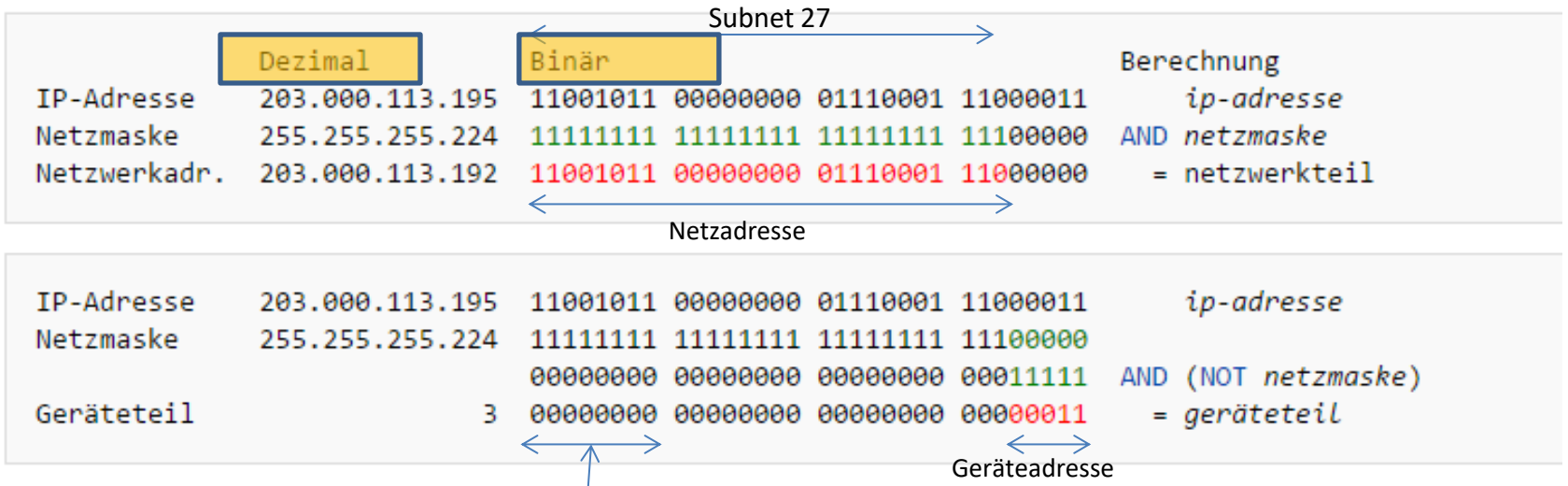
0

IP = 192.168.1.2 / Subnetz = 192.168.1.0

ipso!

Beispiel

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



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

Rechnen Sie bitte folgende Subnet-Beispiele Dezimal in Binär

Dezimal	Binär nur letztes Oktett	Anzahl Subnetze	Anzahl gültige Host Adressen
255.255.255.0	0000 0000	$2^0 = 1$	$2^8 - 2 = 254$
255.255.255.128	1000 0000	$2^1 = 2$	$2^7 - 2 = 126$
255.255.255.192	1100 0000		
255.255.255.224	1110 0000		
255.255.255.240	1111 0000		
255.255.255.248	1111 1000		
255.255.255.252	1111 1100	$2^6 = 64$	$2^2 - 2 = 2$

Sucht zu zweit die Lösung.
Was ist der Sinn dahinter?
Zeit: 15 Minuten

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

ipso!

Lösung Subnet Beispiele

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.

ipso!

Subnet-Calculator

- Testet kurz Online die Netzwerkkalkulation:
- http://www.subnet-calculator.com/

Zeit: 10 Minuten

Subnet-Calculator ipcalc in der Linux Bash

```
parallels@ubuntu:~$ ipcalc 10.10.10.10/12
Address:   10.10.10.10          00001010.0000 1010.00001010.00001010
Netmask:   255.240.0.0 = 12     11111111.1111 0000.00000000.00000000
Wildcard:  0.15.255.255         00000000.0000 1111.11111111.11111111
=>
Network:   10.0.0.0/12          00001010.0000 0000.00000000.00000000
HostMin:   10.0.0.1             00001010.0000 0000.00000000.00000001
HostMax:   10.15.255.254        00001010.0000 1111.11111111.11111110
Broadcast: 10.15.255.255        00001010.0000 1111.11111111.11111111
Hosts/Net: 1048574               Class A, Private Internet

parallels@ubuntu:~$
```

Kurze Übung: Probiere diesen Befehl auf Deinem Linux System aus!

apt-get install ipcalc -y (Installation auf Debian)

Einfache Berechnungsgrundlage

- Wie viele Netze werden benötigt
- Wie viele Hosts befinden sich im Netz

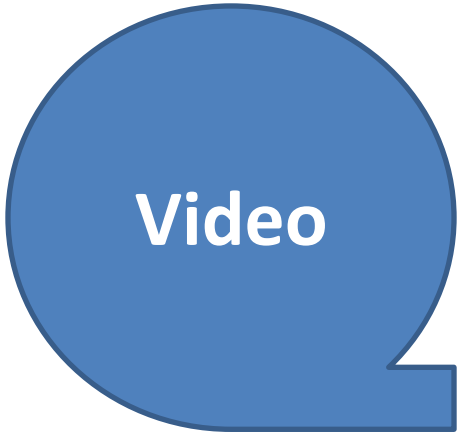
- Berechnung Anzahl Hosts (Hostanteil)
  - 9 Bits Hostanteil = 2^9 = 512 – 2 = 510 Hosts

CIDR – Classless Inter-Domain Routing

- RFCs 1518, 1519, 4632
- Effiziente Nutzung best. 32Bit-IPv4 Adressen
- Netzklassen entfallen damit durch Netzmasken
- Notation durch Suffixe z.B. **/24**
  = 11111111.11111111.11111111.00000000
  = erste 24 Bit sind auf 1 gesetzt

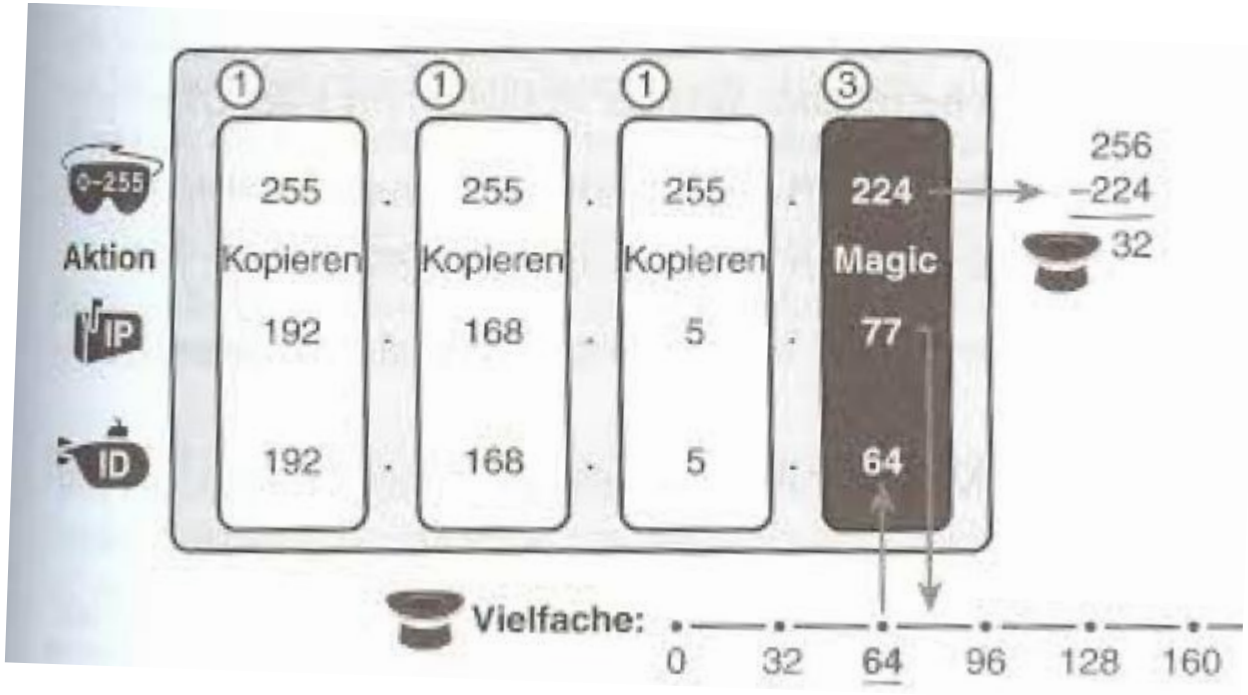
Video anschauen

- CCENT/CCNA ICND1 100-101 Video
  - **5. Finding the Subnet Number – Example 1**
  - **6. Finding the Subnet Number – Example 2**



Zeit: 15 Minuten

Zugehöriges Subnetz ermitteln (Magic number)



Broadcast Adresse von Subnet finden (Magic number)

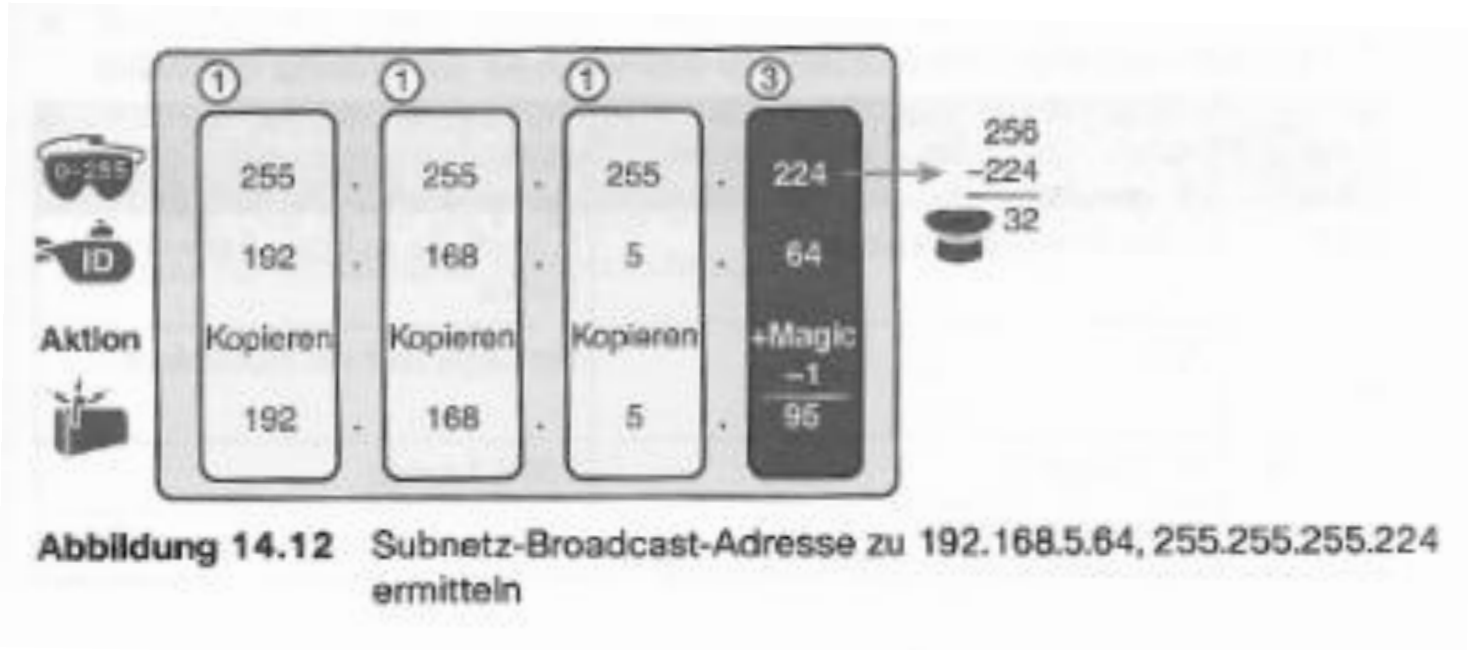


Abbildung 14.12 Subnetz-Broadcast-Adresse zu 192.168.5.64, 255.255.255.224 ermitteln

Maskenanalyse

Arbeit zu zweit:

Übung Anhang F: Jede Gruppe eine Aufgabe, Start bei Aufgabe 1

Zeit: 20 Minuten

NAT (Network Address Translation)

- Warum brauchen wir NAT?
  - Interne IP Adressen werden nicht geroutet.
- Was tut NAT?
  - Durch SNAT wird auf dem Router die SA (Source Address) jeweils durch die externe öffentliche IP-Adresse des Routers ersetzt.
  - Durch die **NAT-Tabelle** weiss der Router bei einem Antwort-Paket an welche interne private IP-Adresse das Paket weitergeleitet werden muss.
  - **Heute meist PAT** oder PNAT (Port Address Translation) dabei werden die Ports umgesetzt.

Zusammenfassende Fragen

Lösen von Fragen CCNA Volume 1: Kapitel 11, 12, 13, 14: in Gruppe

Zeit 30 Minuten

Ende Block 4

«Ende»

Lernziele des 4. Modulblocks

- **Du kannst..**
  1. …grundlegende technische Funktionen von IPv4 einordnen.
  2. …selbstständig IPv4 Netze in Subnetze unterteilen.

Deine Hausaufgaben

Stoff Nachbearbeitung 4. Modul:

- **Repetition der Folieninhalte des Modulblocks**: Ergänzen deiner individuellen Zusammenfassung.
- **Lernstoff 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
  - optional CCNA1 Kapitel 18 «Troubleshooting IPv4 Routing»
- **Löse die Subnetz Aufgaben im CCNA1 Buch Kapitel 12 Seite 296-297**
- **Lernvideos «Youtube»:**
  Suche ein gutes Lernvideo über die IPv4 Subnettierung und nimm deinen Vorschlag in den Unterricht für den gemeinsamen Austausch mit.
- **Praxistransfer:**
  Versuche diese Fragen innerhalb deiner Unternehmung zu klären und nimm die Antworten zur gemeinsamen Besprechung in den Unterricht mit.
  - Wie sieht das IP-Adressenkonzept mit der dazugehörenden Subnettierung aus?
  - Gibt es verbindliche Regeln für die Subnettierung?
  - Welche Routing Protokolle werden in der Unternehmung verwendet (oder statisches Routing)?
- **Vorbereitung auf das nächste Modul:**
  - CCNA1 Buch Kapitel 4 «Using the Command-Line Interface»
  - Installiere den CISCO Pakettracer für den nächsten Modulblock