

# Matura

## NWES-SESD

Höhere Technische Bundeslehr- und Versuchsanstalt Anichstraße

---

Abteilung für Wirtschaftsingenieure/Betriebsinformatik

Ausgeführt im Schuljahr 2024 von:  
Gwercher

# Inhaltsverzeichnis

<b>I 4BHWII</b>	<b>1</b>
<b>1 IPv4 (Internet Protocol Version 4):</b>	<b>2</b>
<b>2 Netzwerke im Alltag und Grundbegriffe</b>	<b>4</b>
2.1 Referenzmodell (OSI und TCP/IP) . . . . .	6
2.1.1 Layer 1 (Physical) . . . . .	8
2.1.2 Layer 2 (Data Link) . . . . .	10
2.1.3 Layer 3 (Network) . . . . .	14
2.1.4 Layer 4 (Transport) . . . . .	18
2.1.5 Layer 5, 6, 7 (Session, Presentation, Application) . . . . .	22
2.2 VLANs . . . . .	26
<b>II 5BHWII</b>	<b>29</b>
<b>3 Routing</b>	<b>30</b>
<b>4 Aufbau des Internets</b>	<b>33</b>
<b>5 IPv6</b>	<b>34</b>
<b>I Quellcodeverzeichnis</b>	<b>III</b>

## Teil I

# 4BHWII

# 1 IPv4 (Internet Protocol Version 4):

Eine IPv4-Adresse ist eine 32-Bit Zahl. Es gibt also  $2^{32} \approx 4,3$  Milliarden IPv4-Adressen.

**Bsp:**

11000000	10101000	00001010	00001010
192	168	10	10
→ 192.168.10.10			

**Schreibweise:**

Die IPv4-Adresse wird in Dotted Decimal Notation geschrieben. Die IP-Adresse wird in 8-Bit Blöcke (Oktetten) geteilt, dezimal übersetzt und durch Punkte getrennt.

**Verwendung**

Jedes Gerät soll durch eine Adresse (IP-Adresse) eindeutig identifiziert werden. Zusätzlich sollten auch Gruppen (Netze) von Computern erstellt werden (mit Subnetzmasken). Ein Gerät mit IP-Adresse nennt man Host.

**Subnetmask**

Ist eine 32-Bit Zahl, die in Dotted Decimal Notation beschrieben wird. Es kommen zuerst alles Einsen und nach der ersten Null nur noch Nullen.

**Typische Subnetmasken:**

	Präfix	Hosts
255.0.0.0	8	$2^{24} - 2 = 16.777.214$
255.255.0.0	16	$2^{16} - 2 = 65.534$
255.255.255.0	24	$2^8 - 2 = 254$

**Bsp:**

Telefonnummer	IP-Adresse	
+43 664 123456	172.16.	20.25
Netz	einzigartig	255.255. 0.0
		Netzteil Hostteil

Die Subnetzmaske trennt die IP-Adresse in Netzteil und Hostteil. IP-Adresse und Subnetzmaske gehören immer zusammen.

1) 2 IP-Adressen im gleichen Netz

10.10.226.120 / 24

10.10.226.80 / 24

2) 2 IP-Adressen nicht im gleichen Netz

11.40.30.124 / 24

14.8.50.100 / 24

3) Anzahl der Hosts

$2^8 - 2$  10.10.226.0 (Netzadresse)

10.10.226.255 (Broadcastadresse)

192.168.20.100 / 8

Netz: 192.0.0.0

Broad: 192.255.255.255

## 2 Netzwerke im Alltag und Grundbegriffe

### Netzwerk Komponenten

- Endgeräte (PC, Handy, Uhr, TV, Server,...)
- Intermediary Devices (Router, Repeater, Switch, Hub, Access Point)
- Übertragungsmedien (Drahtlos, Kupfer, Glasfaser)

### Host-Aufgaben

- Client-Server-Modell
- Peer-to-Peer Modell
  - + Komplexität
  - + Leichter zum Aufsetzen
  - Security
  - Erweiterbarkeit

### Netzwerk Dokumentation

- Physische Topologie (Räume, ...)
- Logische Topologie (Netze, ...)

### Netzwerke nach Größe

- SOHO ... small office home office
- LAN ... local area network
- MAN ... metropolitan area network
- WAN ... wide area network
- Internet

### Netzwerke nach Funktion

- SAN ... storage area network
- Intranet, Extranet

## Internetzugang

- Kabel (Glasfaser)
- DSL / Dial Up
- Mobilfunknetz
- Satellit

## Trends

- Video / Streaming
- Cloud
- Drahtlos (5G)
- BYOD (bring your own device)
- Online Collaboration
- Powerline Method

## Netzwerkarchitektur

- Quality of Service QoS
- Erweiterbarkeit
- Security
- Fehlertoleranz

## Security

- Ransomware
- DoS / DDoS
- Virus, Wurm, Trojaner
- Social Engineering
- Zero-Day-Attack

## 2.1 Referenzmodell (OSI und TCP/IP)

OSI		Protokolle	TCP/IP
7	Application Layer	HTTPS, FTP, Telnet, SSH	Application Layer
6	Presentation Layer	POP, SMTP, IMAP	
5	Session Layer	DHCP, NTP, DNS	
4	Transport Layer	TCP, UDP	
3	Netzwerk Layer	IP, ICMP; OSPF, BGP, RIP	
2	Data Link Layer	Wifi, Ethernet, ARP	
1	Physical Layer		Network Access Layer

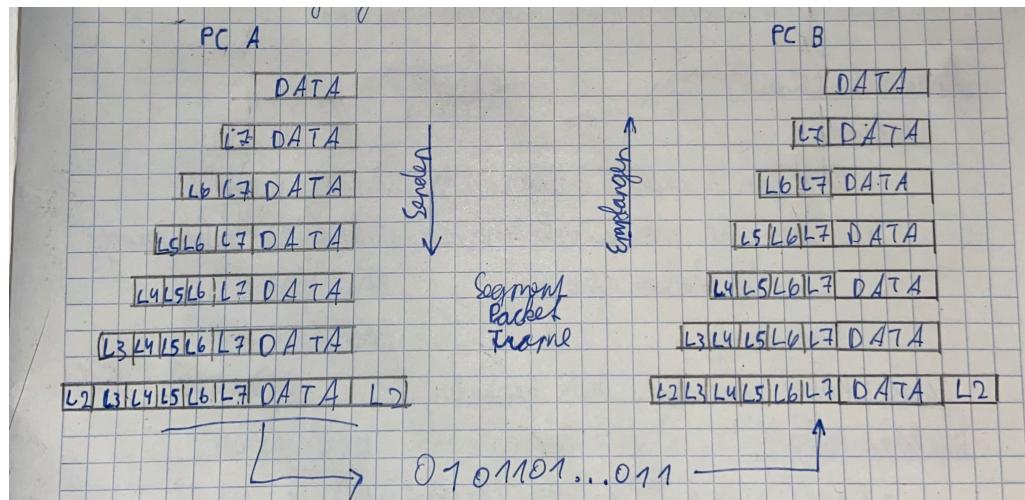


Abbildung 2.1: OSI-Modell Datenübertragung

**Layer 1 (Physical):** Bits übertragen

**Layer 2 (Data Link):** Lokale Adressierung, Fehlererkennung

**Layer 3 (Network):** Globale Adressierung, Routing

**Layer 4 (Transport):** Datenpaketazuordnung, Segmentierung, Datenfluss steuern

**Layer 5 (Session):** Session Verwalten, Verschlüsselung

**Layer 6 (Presentation):** Darstellung der Daten

**Layer 7 (Application):** Funktionen für die Application

Cisco CLI

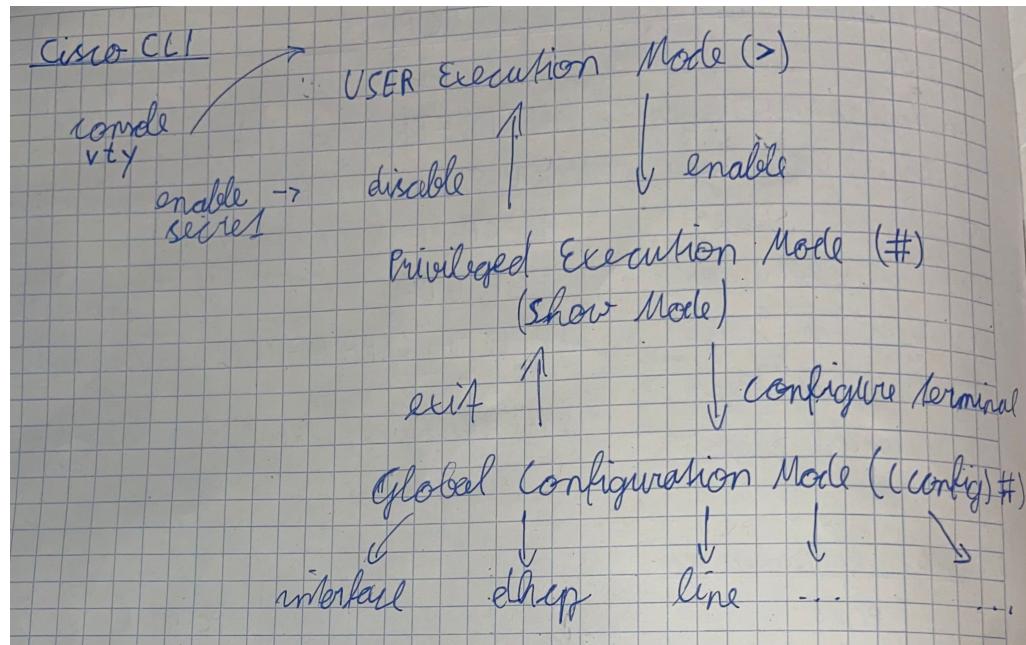


Abbildung 2.2: Cisco CLI

## 2.1.1 Layer 1 (Physical)

### Aufgaben

- Bits von A nach B bringen
- elektrische, mechanische oder andere physische Verbindung zwischen zwei Geräten
- Kodierung

**Geräte:** Kabel, Antenne, Hub, Repeater,...

### Wichtige Begriffe

- Bandbreite (bits/s → theoretisch)
- Durchsatz (bits/s → praktisch)
- Latenz (Dauer der Daten von A bis B in ms)

### Typische Medien

- Kupferkabel (Twisted-Pair-Kabel)
  - + Günstig
  - + einfache Handhabung
  - ≈ Distanz (ca 100m)
  - ≈ Geschwindigkeit
  - Interferenzen (Störungen)

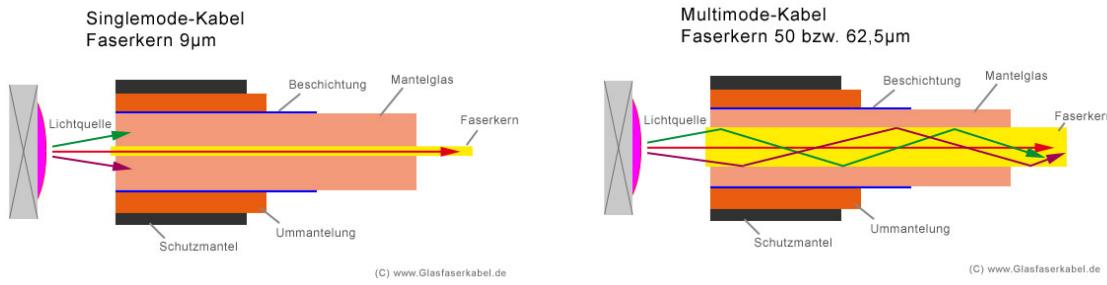
Straight Through (beide Enden gleich)

Crossover (verschiedene Enden)

(durch Auto MDIX werden Enden automatisch konfiguriert)

- Koaxialkabel
- Glasfaserkabel

Arten: Single-Mode (Senden Laser, Reichweite 1-10km)  
Multi-Mode (Senden LED, Reichweite ca 600m)



(a) Single-Mode

(b) Multi-Mode

Abbildung 2.3: Glasfaserkabelarten

- |  |                         |
|--|-------------------------|
| + Speed<br>+ Reichweite<br>+ Störungen | - Teuer<br>- Handhabung |
|--|-------------------------|

- Drahtlos

Übertragung: elektromagnetische Wellen über Luft

- |   |
|---|
| + Flexibel<br><br>- Störungen<br>- Shared Medium<br>- Reichweite (ca 100m), Hindernisse<br>- Security |
|---|

## 2.1.2 Layer 2 (Data Link)

### Aufgaben

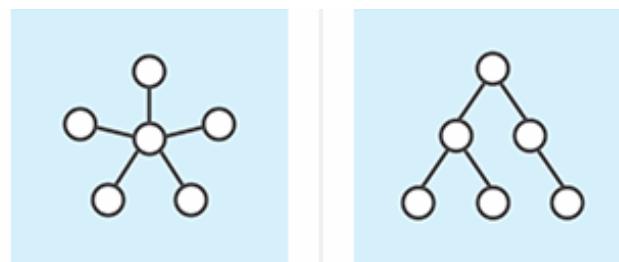
- lokale Adressierung
- Fehlererkennung
- Zugang zum Medium herstellen
- Kommunikation mit Layer 3

**Geräte:** Netzwerkkarte, Switch, Bridge,...

**Standards:** Wifi (802.11), Ethernet (802.2, 802.3)

### Topologie

- Sterntopologie
- Baumtopologie
- Punkt-zu-Punkt



<p><b>Stern</b>            Verfügt über ein zentrales Gerät, das Daten an andere Knoten im System überträgt.</p>	<p><b>Baum</b>            Verbindet Geräte in einer Struktur, die einem Baum ähnelt, bei dem übergeordnete Knoten mit untergeordneten Knoten verbunden sind.</p>
--	--

Abbildung 2.4: Baum- und Stern Topologie

### Ethernet



Abbildung 2.5: Ethernet Frame

### MAC-Adresse

Die MAC-Adresse ist eine 48-Bit Zahl und wird in hexadecimal dargestellt.

Bsp:

Hersteller für den Hersteller einzigartig  
DC F5 05 |17 9A 69

Jede Netzwerkkarte besitzt eine weltweit einzigartige (theoretisch) MAC-Adresse.

### Type

Kodierung für Layer 3  
0x800 → IP  
0x806 → ARP

### Fehlerkennung

Frame Checksum (CRC)  
Polynomdivision mit einem Polynom von Grad 32

### Funktion eines Switches

Der Switch baut mit der Source-MAC seine MAC-Tabelle auf. Dort steht zu jeder MAC-Adresse der passende Port. Falls die MAC-Adresse schon eingetragen ist, wird ein Timer aktualisiert. Sollte es noch keinen Eintrag geben wird er hinzugefügt und bleibt dort eine gewisse Zeit (5 Minuten) bevor er gelöscht wird. Der Switch vergleicht die Destination-MAC mit seiner MAC-Tabelle. Falls der Switch keinen Eintrag findet sendet er an alle Ports (Flooding, Unknown Unicast). Sonst sendet er an den Port, wo er den Frame bekommen hat.

Layer 2 Broadcast Adresse: FF:FF:FF:FF:FF:FF

### L2, L3 Adressierung

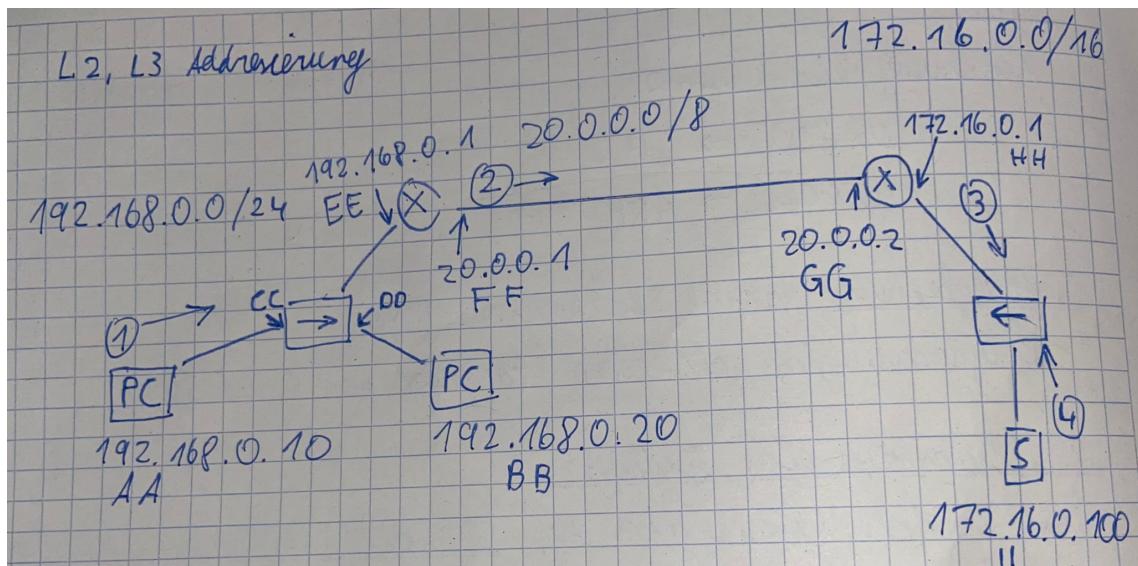


Abbildung 2.6: Layer 2 &amp; 3 Adressierung

	Source MAC	Destination MAC	Source IP	Destination IP
1	AA	EE	192.168.0.10	172.16.0.100
2	FF	GG	192.168.0.10	172.16.0.100
3	HH	II	192.168.0.10	172.16.0.100
4	II	HH	172.16.0.100	192.168.0.10

### ARP (Address Resolution Protocol)

Nutzt ein Host um zu einer gegebenen IP-Adresse die passende MAC-Adresse zu finden

#### ARP-Request (Broadcast)

Source MAC: eigene MAC-Adresse

Destination MAC: FF-FF-FF-FF-FF-FF

Type: 0x806 Danach ARP-Header (IP, MAC, Protokoll)

#### ARP-Reply Unicast (auch als Broadcast möglich)

Source MAC: eigene MAC-Adresse (gesucht)

Destination MAC: MAC-Adresse (Anfrage)

Type: 0x806

Danach ARP-Header

#### ARP-Cache

Die Einträge werden im ARP-Cache gespeichert (ca 5 min)

IP MAC Time

#### ARP-Spoofing

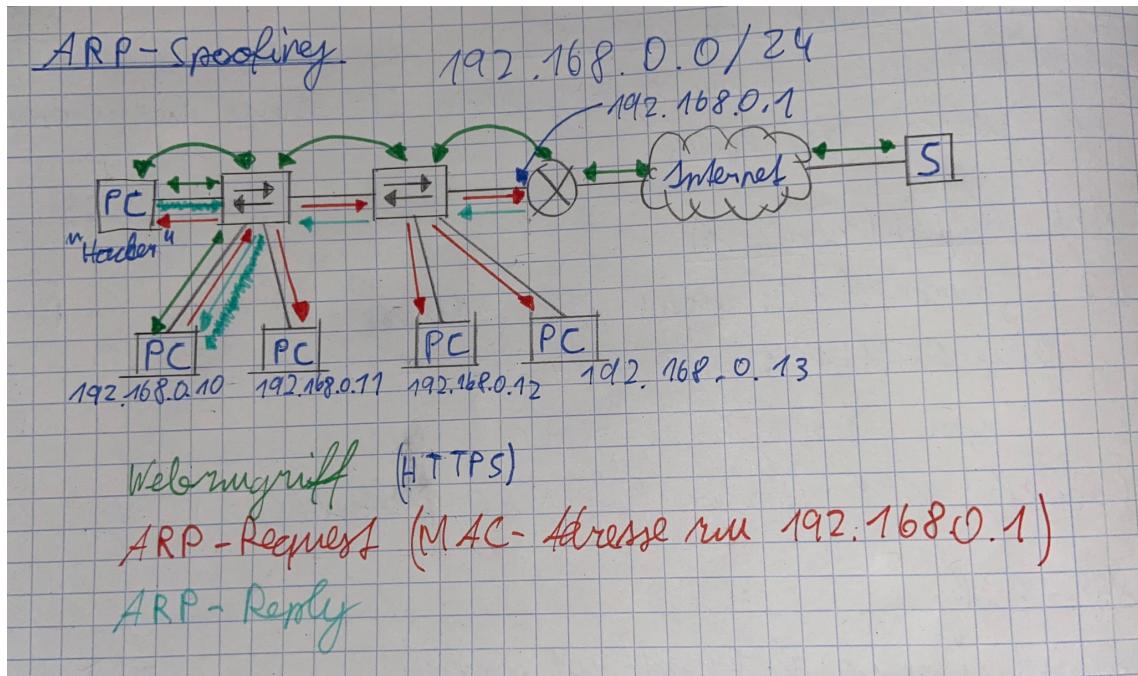


Abbildung 2.7: ARP-Spoofing

## 2.1.3 Layer 3 (Network)

### Aufgaben

- Routing
- Globale Adressierung
- Kommunikation mit L2 & L4

**Protokolle:** IPv4, IPv6, ICMP, RIP, OSPF, EIGRP, IS-IS, BGP

### IPv4

Eigenschaften von IP

- Verbindungslos
- Best Effort
- Medium unabhängig

**IP-Header (8.2.2)** Wichtige Felder: Source & Destination IP, Time-to-Live

### Kommunikationsart

- Unicast (IP des Host)
- Multicast (224.0.0.0 - 239.255.255.255)
- Broadcast (letzte IP im Netz, 255.255.255.255)

### Spezielle IP-Adressen

- 127.0.0.0 / 8 ... localhost
- 10.0.0.0 / 8
- 172.16.0.0 / 12
- 192.168.0.0 / 16 ... private IP-Adressen (NAT)
- 169.254.0.0 / 16 ... APIPA
- 192.0.2.0 / 24 ... Testnetz

**Fazit:** Zu wenig IPv4-Adressen!

### Deshalb

- VLSM (variable length subnet mask)
- NAT

- IPv6

### **Classful Addressing (uralt)**

Das erste Oktett bestimmt die Subnetzmaske (/8, /16, /24)

Klasse A	0-127	(0...)	/8
Klasse B	128-191	(10...)	/16
Klasse C	192-223	(110...)	/24
Klasse D	224-239	(1110...)	Multicast
Klasse E	240-255	(11110...)	für spätere Verwendung

### **Classless Addressing (veraltet!)**

Die Subnetzmasken /8, /16, /24 können beliebig verwendet werden

### **CIDR (Classless Inter-Domain Routing)**

Es können beliebige Subnetzmasken (z.B. /25, /26, ...) verwendet werden. Alle Subnetze werden gleich groß.

### **VLSM (variable length subnet mask)**

Alle Subnetzmasken können beliebig verwendet werden. Die Netzte dürfen sich nicht überschneiden.

### **Subnetzmasken**

Präfix Notation	Dotted Decimal Notation	Hosts	Subnetz von /24
/25	255.255.255.128	$2^7 - 2 = 126$	2
/26	255.255.255.192	$2^6 - 2 = 62$	4
/27	255.255.255.224	$2^5 - 2 = 30$	8
/28	255.255.255.240	$2^4 - 2 = 14$	16
/29	255.255.255.248	$2^3 - 2 = 6$	32
/30	255.255.255.252	$2^2 - 2 = 2$	64
/31	255.255.255.254	$2^1 - 2 = 0$	für spezielle Anwendung
/20	255.255.240.0	$2^{12} - 2 = 4.094$	/

### **Bsp 1 (CIDR):**

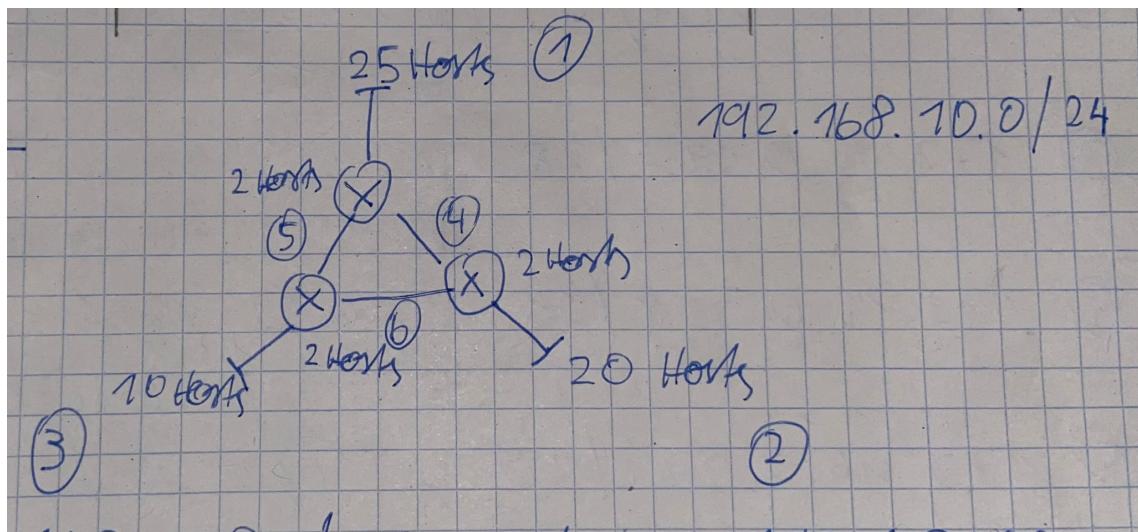
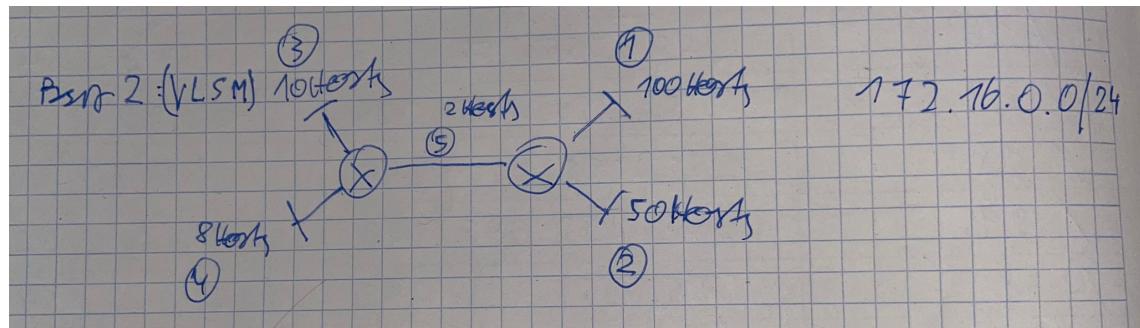


Abbildung 2.8: CIDR Beispiel

1	192.168.10.0 / 27	Netzadresse	192.168.100.0
		Broadcast	192.168.100.31
2	192.168.10.32 / 27	Netzadresse	192.168.100.32
		Broadcast	192.168.100.63
3	192.168.10.64 / 27	Netzadresse	192.168.100.64
		Broadcast	192.168.100.95
4	192.168.10.96 / 27	Netzadresse	192.168.100.96
		Broadcast	192.168.100.127
5	192.168.10.128 / 27	Netzadresse	192.168.100.128
		Broadcast	192.168.100.159
6	192.168.10.160 / 27	Netzadresse	192.168.100.160
		Broadcast	192.168.100.191

**Bsp 2 (VLSM):**



1	172.16.0.0 / 25	Netzadresse	172.16.0.0
		Broadcast	172.16.0.127
2	172.16.0.128 / 26	Netzadresse	172.16.0.128
		Broadcast	172.16.0.191
3	172.16.0.192 / 28	Netzadresse	172.16.0.192
		Broadcast	172.16.0.207
4	172.16.0.208 / 28	Netzadresse	172.16.0.208
		Broadcast	172.16.0.223
5	172.16.0.224 / 30	Netzadresse	172.16.0.224
		Broadcast	172.16.0.227

(PT: 10.4.3, 11.5.5, 11.9.3, 11.10.1)

## 2.1.4 Layer 4 (Transport)

### Aufgaben

- Anwendungen identifizieren
- Segmentierung
- ev. Flusskontrolle, Verbindungsauflösung & abbau
- Kommunikation mit L3 & L5

### Protokolle:

- TCP (Transmission Control Protocol)
- UDP (User Datagram Protocol)

TCP	UDP
Anwendungen identifizieren (Ports) Segmentierung Verbindungen auf- bzw abbauen Segmente ordnen wiederholtes Senden Flusskontrolle	Anwendungen identifizieren (Ports) Segmentierung

TCP: HTTP (80)/HTTPS (443), SMTP (25), POP (110), IMAP (143), Telnet (23), SSH (22), FTP (20/21),...  
 UDP: DNS (53), DHCP (67/68), VoIP, Streaming,...

### Ports

Der Port ist eine 16-Bit Zahl  $\rightarrow 2^{16} = 65.536$

Der Port identifiziert die Anwendung, sowohl beim Server als auch beim Client.

### Gruppe von Ports

Well-Known-Ports	0 - 1.023
Registered-Ports	1.024 - 49.151
Private Ports	49.152 - 65.535

### L4-Adressierung

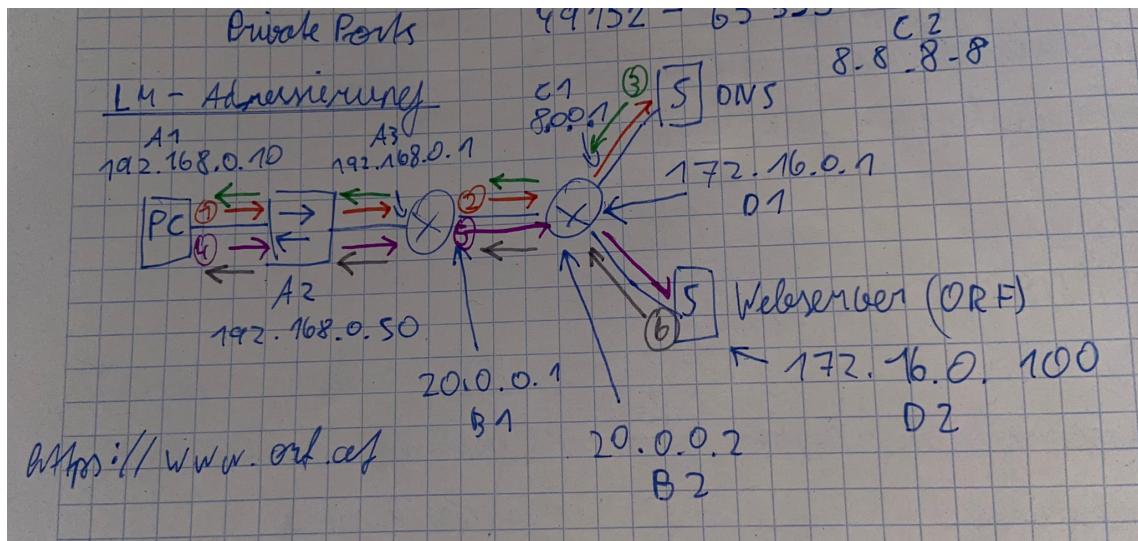


Abbildung 2.10: L4-Adressierung

	L2 (MAC)		L3 (IP)		L4 (Ports)	
	Source	Destination	Source	Destination	Source	Destination
1	A1	A3	192.168.0.10	8.8.8.8	53.722	53
2	B1	B2	192.168.0.10	8.8.8.8	53.722	53
3	C2	C1	8.8.8.8	192.168.0.10	53	53.722
4	A1	A3	192.168.0.10	172.16.0.100	60.112	443
5	B1	B2	192.168.0.10	172.16.0.100	60.112	443
6	D2	D1	172.16.0.100	192.168.0.10	443	60.112

## TCP

Verbindungsaufbau: Drei-Wege-Handshake

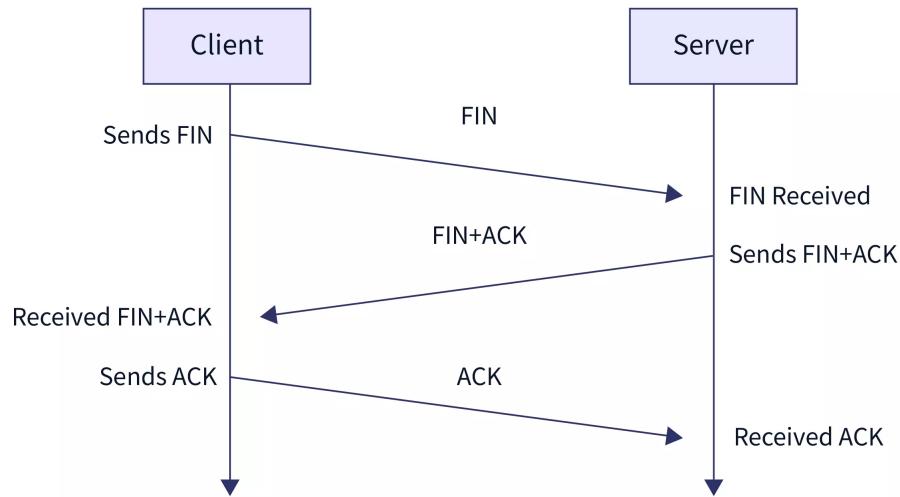


Abbildung 2.11: TCP 3-Way-Handshake

Verbindungsabbau: Zwei-Wege-Handshake

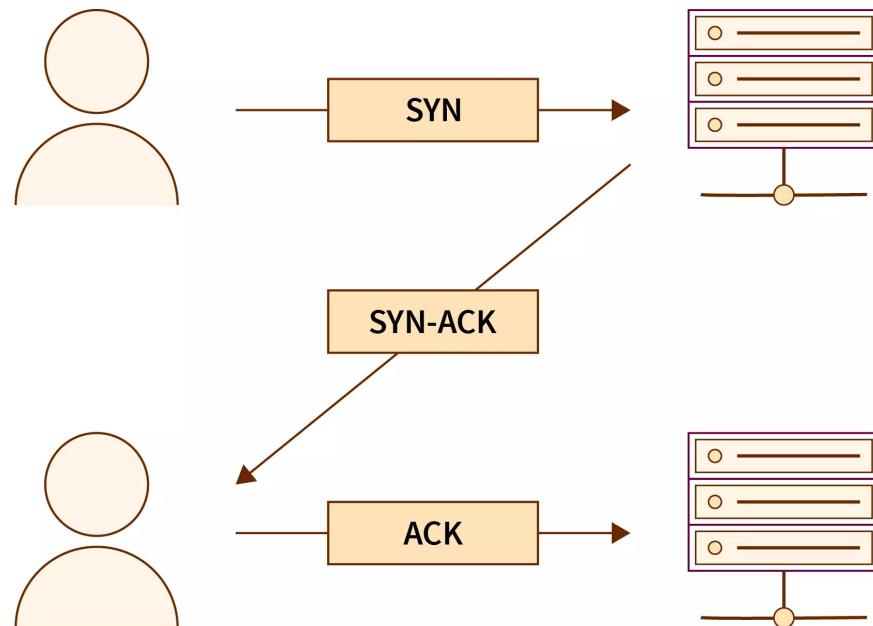


Abbildung 2.12: TCP 2-Way-Handshake

### Segmentierung

Es wird eine SEQUENCENUMBER mitgeschickt. Diese gibt die Reihenfolge an. Der Client bestätigt die Segmente mit ACK-Segmenten. Die ACK-NUMBER gibt an, welches Segment als nächstes kommen soll.

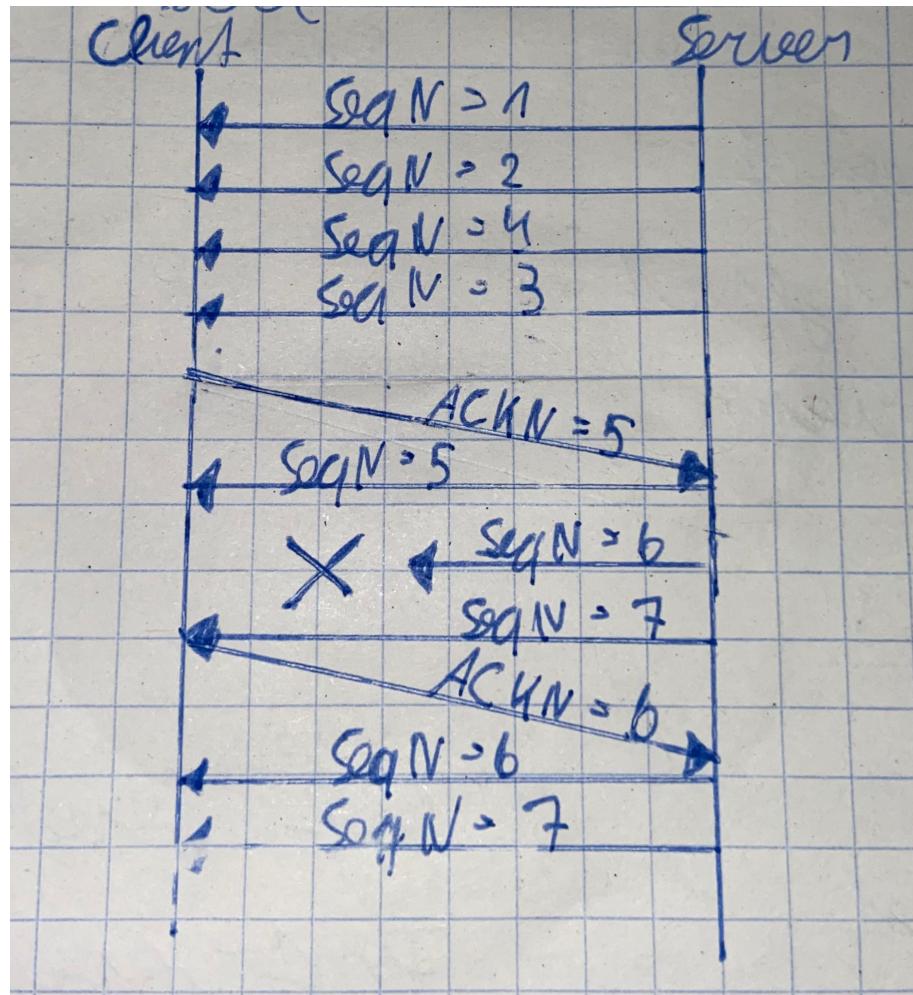


Abbildung 2.13: Layer 4 Segmentierung

### Flow-Control

Die Window Size gibt an wann das nächste ACK-Segment erwartet wird.

## 2.1.5 Layer 5, 6, 7 (Session, Presentation, Application)

### Aufgaben

- Session erstellen und halten
- Regelung der Session, Restart, Exchange, Idle
- Format und Präsentation der Daten
- Verschlüsselung und Komprimierung der Daten
- Anwendungsspezifische Informationen

**Protokolle:** HTTP/HTTPS, FTP, Telnet/SSH, DHCP, DNS, SMTP, POP, IMAP

### DNS (Port 53, UDP)

Um zu einer Domain die passende IP-Adresse zu finden. Typische DNS-Server: 8.8.8.8

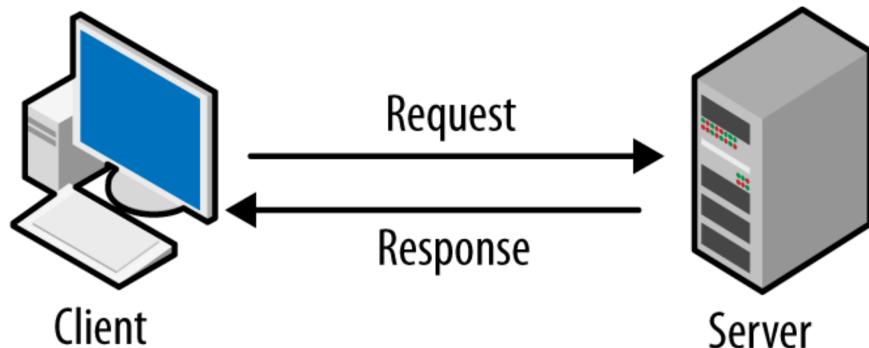


Abbildung 2.14: Request/Response Modell

### Einträge

A ... IPv4-Endgerät AAAA ... IPv6-Endgerät MX ... Mail-Server

### Hierarchisches DNS-Modell

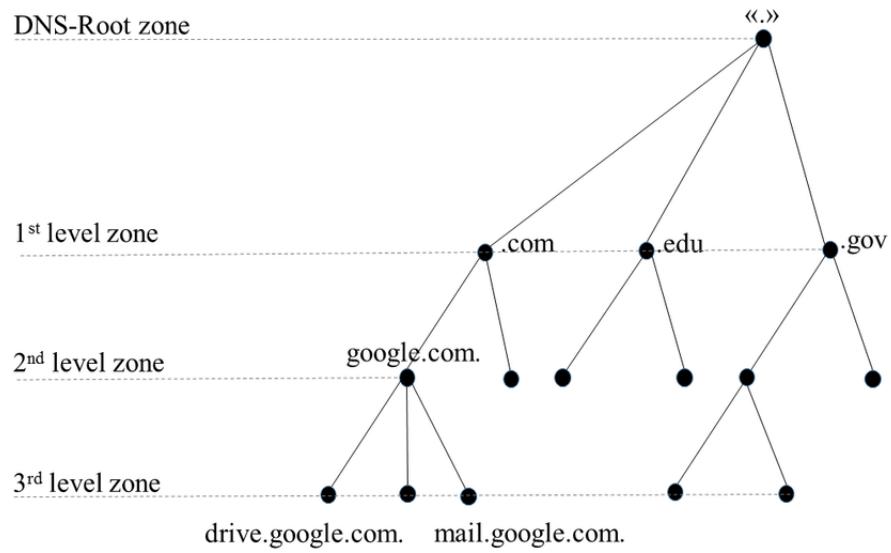


Abbildung 2.15: DNS-Hierarchie

Falls der DNS-Server keinen Eintrag findet, wird das Paket weitergeleitet. Der Client speichert die erhaltenen DNS-Einträge.

### DHCP (Port 67/68, UDP)

Die Hosts erhalten dynamisch eine IP-Konfiguration (IP-Adresse, Subnetzmaske, Default Gateway, DNS-Server, Lease Time,...).

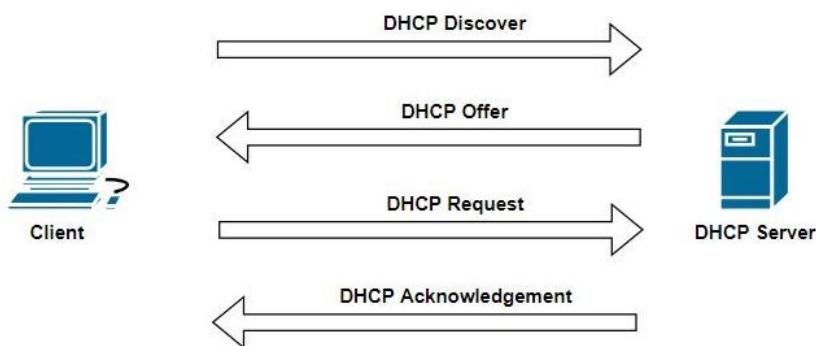


Abbildung 2.16: DHCP-Handshake

DHCP-Discover ... Broadcast

DHCP-Offer ... Unicast

DHCP-Request ... Broadcast

DHCP-ACK ... Unicast

Achtung: DHCP-Spoofing

### HTTP/HTTPS (Port 80/443, TCP)

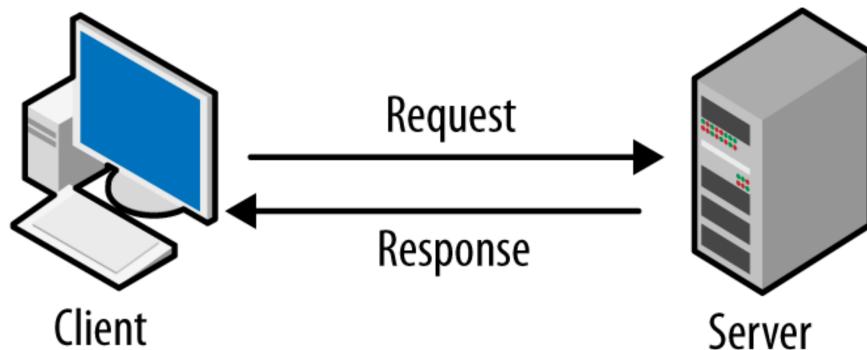


Abbildung 2.17: Request/Response Modell

URL:	https://	www.google.com/	index.html
	Protokoll	Domain IP-Adresse (DNS)	Ordnerstruktur, Datei

### Befehle

Get, Post, Put, Delete,...

Bei HTTP ist alles im Klartext.

Bei HTTPS wird zusätzlich mit SSL/TLS verschlüsselt.

### E-Mail

E-Mail-Adresse:	name	@	gmail.com
	Benutzername		Domain

### SMTP (Port 25, TCP)

Senden von Emails. Wird zum Senden von Mails und dem Weiterleiten zum Zielserver benutzt. SMTP kann zusätzlich Feedback geben (z.B. Ziel nicht erreichbar,...).

### POP (Port 110, TCP)

Empfangen von E-Mails. Man erhält vom Server das Original. Die Mail wird am Server gelöscht (Vorteil: Speicherplatz, Security).

### **IMAP (Port 143, TCP)**

Empfangen von E-Mails. Man erhält vom Server eine Kopie. Das Original bleibt am Server gespeichert (Vorteil: Verbindung mit mehreren Geräten ist praktisch, Backup).

## 2.2 VLANs

Ein physisches Netz wird in mehrere logische Teilnetze (Layer 2) unterteilt.

Vorteile	Nachteile
Kosten	(Konfiguration)
Security	
Flusskontrolle	
Übersicht	
kleinere Broadcast-Domain	
Effizienz & Performance	

### Arten von VLANs

- Daten VLANs
- Default VLAN (bei cisco 1)
- Voice VLAN
- Management VLAN
- Native VLAN (Frames ohne VLAN-Tag kommen in das Native VLAN, kann nur am Trunk passieren)

Access Ports transportieren nur ein VLAN.

Trunk Ports können viele VLANs transportieren.

Die VLAN-Namen werden zusätzlich im Header eingetragen (802.1q → Ethernet)

### ACL

Je nach IP-Adresse (Standard) bzw. Port (Extended) wird ein Packet blockiert oder zugelassen.

### Wildcardmask

Subnetzmaske: Teilt IP-Adresse in Netz- und Hostteil

1 ... Netzteil (relevant für das Netz)

0 ... Hostteil (irrelevant für das Netz)

→ unflexibel

Wildcardmaske '1' & '0' können beliebig gezählt werden

0 ... relevantes Bit der IP-Adresse

1 ... nicht relevantes Bit der IP-Adresse

255.255.255.255      any

0.0.0.0                host

### Position der Wildcardmask

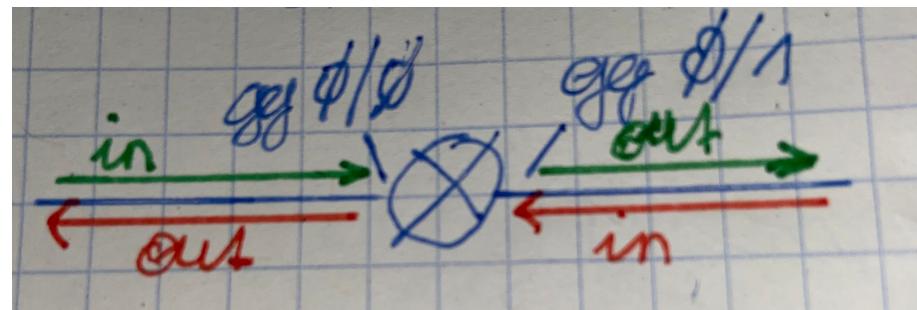


Abbildung 2.18: Position der Wildcardmask

Regeln bei Interfaces: eingehend & ausgehend

**Achtung** Die letzte Zeile in jeder ACL ist 'deny any'.

### Static NAT (1:1 Mapping)

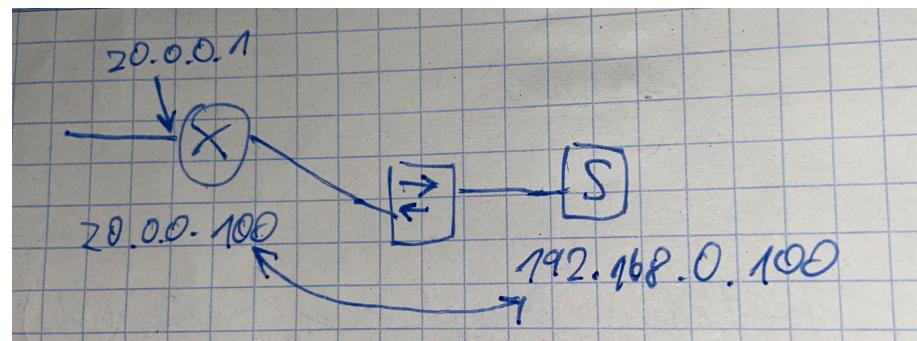


Abbildung 2.19: Static NAT, 1:1 Mapping

### NAT mit PAT (n:1 Mapping)

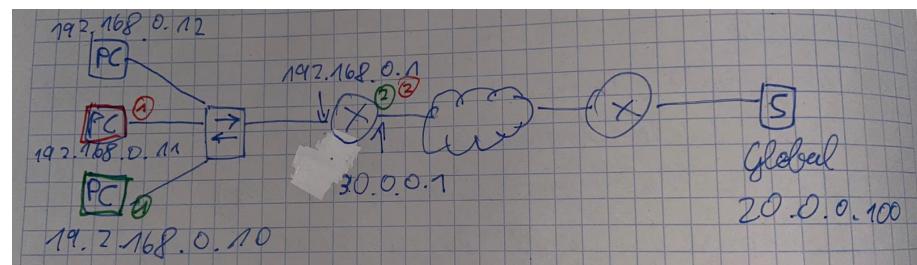


Abbildung 2.20: NAT mit PAT, n:1 Mapping

	Source IP	Destination IP	Source Port	Destination Port
1	192.168.0.10	20.0.0.100	51000	443
1	192.168.0.11	20.0.0.100	51000	443
2	30.0.0.1	20.0.0.100	51000	443
2	30.0.0.1	20.0.0.100	51001	443

Vorteile	Nachteile
<ul style="list-style-type: none"> <li><b>+ IP-Adressen sparen</b></li> <li>+ Security</li> <li>+ IP-Adressen Schema kann frei gewählt werden</li> </ul>	<ul style="list-style-type: none"> <li>- Ende zw. Ende Verbindung geht verloren</li> <li>- Paketverfolgung und Troubleshooting</li> <li>- Performance</li> </ul>

## Teil II

### 5BHWII

## 3 Routing

Router muss entscheiden welcher Weg der 'beste' Weg ist.

→ bei welchen Interface (Netz) rauschicken = Routing

Routing Tabelle wird durch ...

- dynamisch (Routingprotokolle)
- statische Einträge

... aufgebaut (in der Praxis meist aus Mischung).

Router wählt Route mit am meisten Bits bei Ziel übereinstimmung (Vergleich von Route & Destination IP).

### 1) Einträge in Routing Tabelle

- Direkt verbundene Netze: Aktive & angeschlossene Netze am Router mit IP-Konfiguration → automatisch (Status Code: C, L)
- Remote Netze: statisch oder dynamisch (vom Routingprotokoll abhängig) einge-tragen (Status Code: S, R, O, E,...)
- Default Route (gateway of last resort): Next Hop falls der Router keine passende Route findet, statisch oder dynamisch.  
Route: 0.0.0.0 / 0 ... 0 Bits müssen übereinstimmen

### 2) Eintrag in Cisco CLI

R	30.0.4.0/24	[120/7]	via 10.0.3.2	00:13:29	Serial 10/1/1
Status	Ziel	AD/Metrik	IP (ausgehendes Interface)	Zeitstempel	Interface

### Status Code

C ... connected Direkt verbundene Netzte

L ... local IP vom Interface, lokale Route

S ... static statisch eingegebene Route

- R ... RIP      entsprechendes Routingprotokoll
- O ... OSPF      entsprechendes Routingprotokoll
- E ... EIGRP      entsprechendes Routingprotokoll

### Ziel

IP-Adresse des Zielnetzes mit Präfix (nicht unbedingt Subnetzmaske). Es müssen die angegebene Anzahl von Bits (Präfix) mit Destination IP-Adresse übereinstimmen (damit Route in Frage kommt). Route mit am meisten übereinstimmenden Bits (von links). Problem: es wird keine Subnetzmaske der Destination IP mitgeschickt → normalerweise auch nicht bekannt.

Dest IP: 172.16.0.10 (letztes Oktett: 00001010)

- 
- 1) 172.16.0.0 /16 Bis Bit 16 übereinstimmend
  - 2) 172.16.0.0 /24 Bis Bit 24 übereinstimmend
  - 3) 172.16.0.0 /26 Bis Bit 26 übereinstimmend
  - 4) 172.16.0.0 /30 Bis Bit 29 nicht übereinstimmend
  - 5) 172.17.0.0 /24 am 2. Oktett stimmt es nicht überein

Router wählt 3. Variante (???). Dort stimmt die angegebene Anzahl an Bits (Präfix) überein

### AD: Administrative Distanz

Router kann Route über mehrere Arten lernen (z.B. statisch, RIP, OSPF,...). AD gibt an wie 'vertrauenswürdig' eine Route ist. Router verwendet Route mit niedrigster AD, andere Routen sind Backups und werden vorerst nicht im Routing Table angezeigt.  
→ wenn 'beste' Route ausfällt wird nächst beste verwendet

Standard Werte bei Cisco Routern

	AD
Direkte Routen	0
Statische Routen	1
EIGRP	90
OSPF	110
RIP	120

### Metrik

Von einem Routingprotokoll kann der Router mehrere Routen zum gleichen Ziel lernen. Die Metrik gibt an, 'wie weit' das Ziel entfernt ist. Der Router verwendet die Route mit der geringsten Metrik. Falls eine Route ausfällt, wird auf Backup-Routen zurückgegriffen.

### 3) Statische Routen

Werden in kleineren Netzen mit geringen Veränderungen, bei speziellen Zielnetzen oder

Router mit nur einen Nachbar (Stub-Network) verwendet.

Problem: Statische Routen werden nicht automatisch aktualisiert und müssen händisch aktualisiert werden.

#### 4) Dynamische Routingprotokolle

Je nach Ablauf des Routingprotokolls unterscheidet man unterschiedliche Kategorien.

- Pfadvektorprotokolle

Diese Protokolle speichern den Pfad/Weg zum Ziel. Sie sind besonders effizient gegen Routing-Schleifen und eignen sich dadurch zum Routen von autonomen Systemen.

Beispiel: BGP (Border Gateway Protocol), Metrik: Anzahl der autonomen Systemen bis zum Ziel (Zusatzinformation IGP-Metrik: wie lange dauert es durch ein autonomes System)

- Distanzvektorprotokolle

Diese Protokolle speichern nur die Distanz zum Ziel

Beispiel: RIP (Routing Information Protocol), Metrik: Anzahl der Hops

EIGRP (Enhanced Interior Gateway Routing Protocol), Metrik: Bandbreite, Auslastung, Delay, Zuverlässigkeit

EIGRP kennt die ganze Topologie im System, speichert diese aber nicht direkt ab.

- Link-State-Protokolle

Diese Protokolle kennen die ganze Topologie im System. Daraus berechnet sich jeder Router die besten Routen zu allen Zielen.

Beispiel: OSPF (Open Shortest Path First), Metrik: Bandbreite

#### 5) Algorithmen zur Bestimmung des kürzesten Weges

- Bellman Ford (RIP)
- Dijkstra (OSPF)
- DUAL (EIGRP)

##### Dijkstra Algorithmus

Ablauf:

1. Startknoten mit 0 markieren, alle anderen mi  $\infty$ : 'Distanz' und 'besucht' merken 2. Solange es unbesuchte Knoten gibt:

- Jenen Knoten mit der kürzesten Distanz wählen
- Als besucht markieren
- Für alle unbesuchten Knoten die Distanz berechnen
- Falls der Wert kleiner ist, als der aktuelle, diese speichern

## 4 Aufbau des Internets

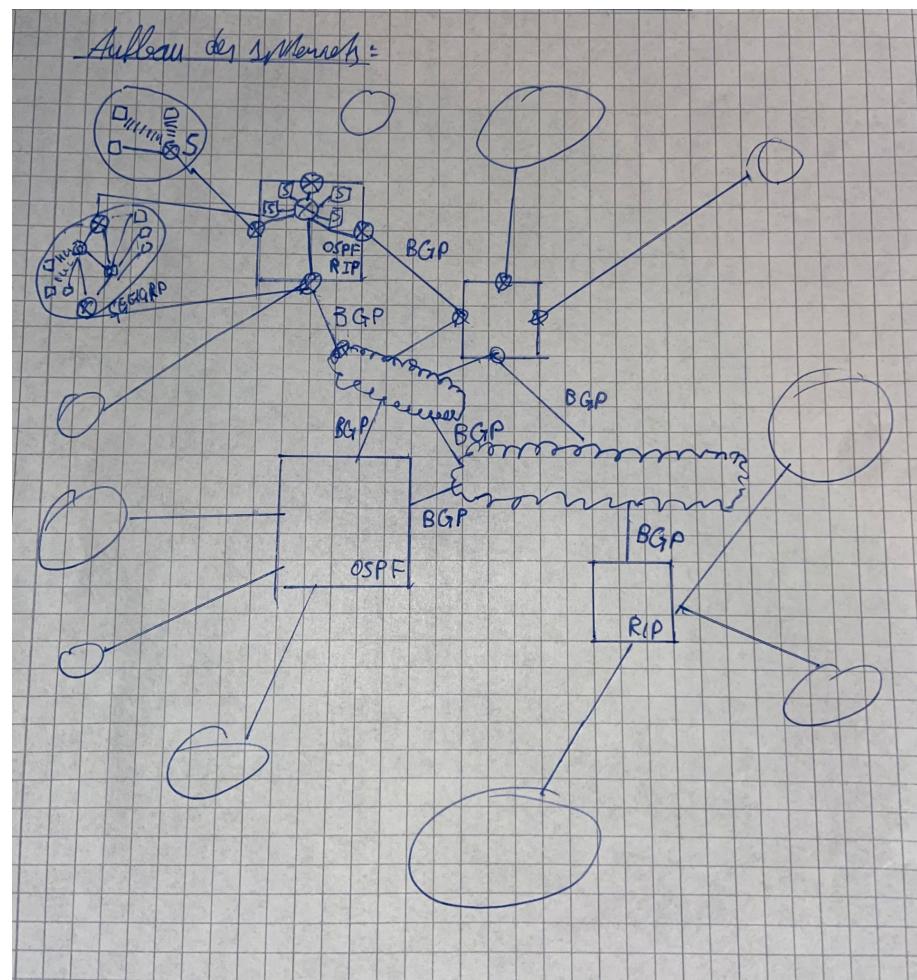


Abbildung 4.1: Static NAT, 1:1 Mapping

## 5 IPv6

Eine IPv6-Adresse ist eine 128 Bit Zahl. Es gibt  $2^{128}$  IPv6-Adressen ( $340 \cdot 10^{36}$ ).

### Schreibweise einer IPv6-Adresse

- Hexadezimale Schreibweise (32 Zeichen)
- Gruppen von 16 Bit mit : getrennt
- Führende Nullen werden in jeder Gruppe weggelassen
- Einmalig kann der längste Block an Nullen mit :: ersetzt werden

Bsp:

2001:ABAD:0000:0430:0000:0000:00C9:0001

2001:ABAD:0:430:0:0:C9:1

2001:ABAD:0:430::C9:1

### Subnetzmaske

- trennt in Netz- und Hostteil
- nur noch Präfix-Notation
- Es wird fast nur /64 verwendet

### Idee von IPv6

- mehr IP-Adressen
- Problem: alle Protokolle die IPv4 verwenden müssen erneuert werden
- Alte Fehler/Security-Probleme beheben
- leichterer Header

### Übergang von IPv4 zu IPv6

- Dualer Stack
- Translation

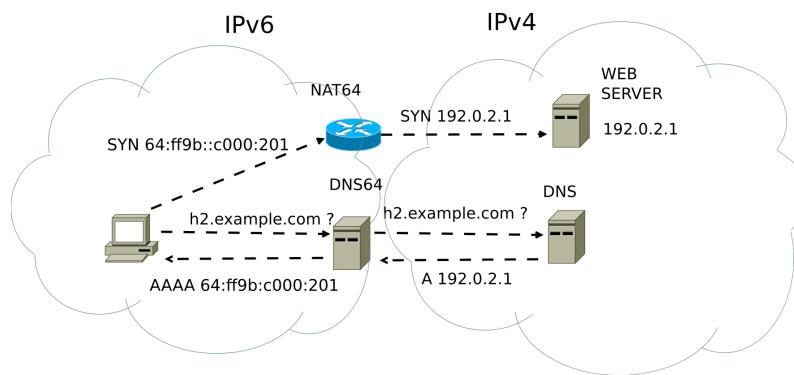


Abbildung 5.1: IPv4-IPv6 Translation mit NAT64

- Tunneling

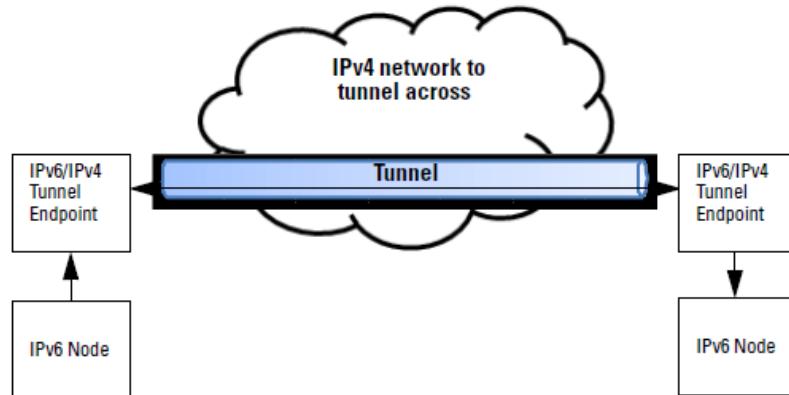


Abbildung 5.2: IPv4-IPv6 Tunneling

## Kommunikationsarten

- Unicast
- Multicast
  - ff02::1 ... all-nodes-multicast (Broadcast)
  - ff02::2 ... all-router-multicast
- Anycast (der 'nägeste' einer Gruppe bekommt den Anycast)

## IPv6-Unicast Adressen

- Global Unicast Adressen 2000-3fff (vgl. öffentliche IP)
- Link Local Adressen fe80-febf (für das lokale Netz, nicht routbar)

- loopback ::1 (vgl. IPv4 127.0.0.1)
- Unspecified Adress :: (vgl. IPv4 0.0.0.0)
- Unique Local fc00-fdff (vgl. IPv4 NAT)
- Embedded IPv4

### IP-Konfiguration

- statisch (GUA, LLA)
- dynamisch
  - SLAAC
  - SLAAC mit stateless DHCPv6 Server
  - DHCPv6

### SLAAC

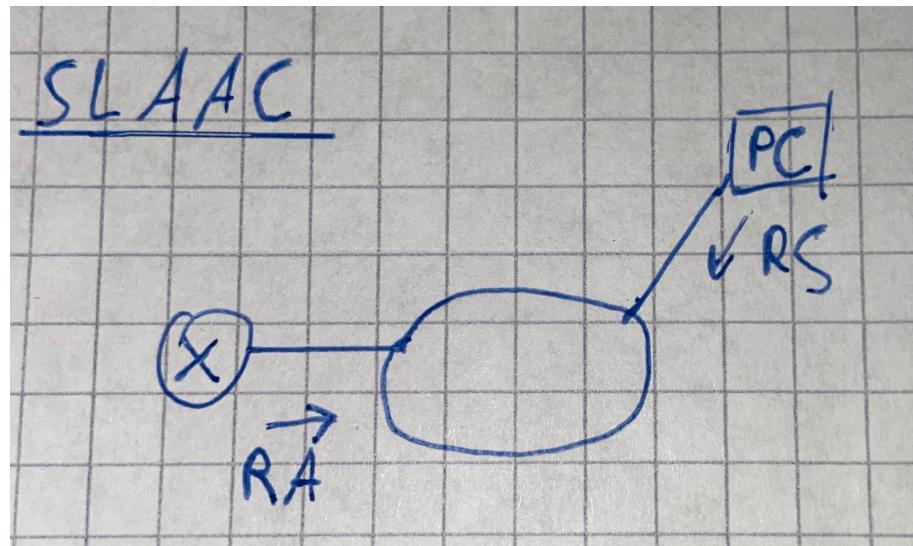


Abbildung 5.3: SLAAC

Router senden (ca. alle 200s) ein RA-Paket (Router Advertisement) aus. Dies enthält die wichtigsten Informationen für die Hosts (Präfix, Präfix-Länge, Default-Gateway). Die Hosts geben sich dann selbst die IPv6-Adresse.

Hostteil

- Zufallszahl (ND-Protokoll)
- EUI-64 (MAC-Adresse)

Die Hosts können RS (Router Solicitation) Pakete aussenden um das RA-Paket anzu fordern.

# Abbildungsverzeichnis

2.1	OSI-Modell Datenübertragung . . . . .	6
2.2	Cisco CLI . . . . .	7
2.3	Glasfaserkabelarten . . . . .	9
2.4	Baum- und Stern topologie . . . . .	10
2.5	Ethernet Frame . . . . .	11
2.6	Layer 2 & 3 Adressierung . . . . .	12
2.7	ARP-Spoofing . . . . .	13
2.8	CIDR Beispiel . . . . .	16
2.9	VLSM Beispiel . . . . .	17
2.10	L4-Adressierung . . . . .	19
2.11	TCP 3-Way-Handshake . . . . .	20
2.12	TCP 2-Way-Handshake . . . . .	20
2.13	Layer 4 Segmentierung . . . . .	21
2.14	Request/Response Modell . . . . .	22
2.15	DNS-Hierarchie . . . . .	23
2.16	DHCP-Handshake . . . . .	23
2.17	Request/Response Modell . . . . .	24
2.18	Position der Wildcardmask . . . . .	27
2.19	Static NAT, 1:1 Mapping . . . . .	27
2.20	NAT mit PAT, n:1 Mapping . . . . .	27
4.1	Static NAT, 1:1 Mapping . . . . .	33
5.1	IPv4-IPv6 Translation mit NAT64 . . . . .	35
5.2	IPv4-IPv6 Tunneling . . . . .	35
5.3	SLAAC . . . . .	36

# Tabellenverzeichnis

# I Quellcodeverzeichnis