Netzwerk

Ziel dieser Zusammenfassung

Diese Zusammenfassung führt Schritt für Schritt durch zentrale Themen der Netzwerktechnik.

Behandelte Themen:

- Grundlagen von Netzwerken
- OSI-Schichtenmodell
- Schicht 0: Übertragungsmedien
- Ethernet-Frame
- Sniffer
- Schicht 1: Netzwerkkarte und Hub
- Schicht 2: MAC-Adresse, Switch, VLAN
- Schicht 3: IPv4, IPv6, DHCP, DNS, Routing
- Schicht 4: Ports, TCP, UDP, NAT
- Firewall-Grundlagen
- SPI-Firewall
- DMZ

---

1. Grundlagen der Netzwerktechnik

Ein Netzwerk verbindet mehrere Geräte miteinander, damit diese Daten austauschen und gemeinsame Ressourcen verwenden können.

Typische Geräte in einem Netzwerk:

- PC
- Notebook
- Smartphone
- Server
- Drucker
- NAS
- Switch
- Router
- Firewall
- Access Point

Ein Netzwerk besteht also nicht nur aus Computern, sondern aus allen Geräten, die miteinander kommunizieren können.

1.1 Vorteile von Netzwerken

Netzwerke werden eingesetzt, weil sie viele praktische Vorteile bieten:

- schneller Datenaustausch
- gemeinsame Nutzung von Druckern und Servern
- zentrale Datenspeicherung
- zentrale Benutzerverwaltung
- gemeinsame Internetnutzung
- einfachere Sicherung von Daten
- bessere Zusammenarbeit im Unternehmen

Beispiel:

In einem Unternehmen müssen nicht alle Mitarbeiter eigene Drucker besitzen. Alle können über das Netzwerk denselben Netzwerkdrucker verwenden.

1.2 Nachteile und Risiken von Netzwerken

Netzwerke bringen auch Risiken mit sich:

- Schadsoftware kann sich schneller verbreiten
- Angriffe von innen und außen sind möglich
- falsche Konfiguration kann Sicherheitslücken erzeugen
- Ausfall zentraler Systeme kann viele Benutzer betreffen
- Wartung und Administration verursachen Kosten

Deshalb sind Schutzmaßnahmen wie Firewalls, VLANs, Benutzerrechte, Updates und Backups wichtig.

1.3 Netzwerkgrößen

Netzwerke werden oft nach ihrer räumlichen Ausdehnung unterschieden.

Begriff	Bedeutung	Beispiel
LAN	Local Area Network	Netzwerk in einem Büro, Schule oder Zuhause
MAN	Metropolitan Area Network	Netzwerk innerhalb einer Stadt
WAN	Wide Area Network	Netzwerk über große Entfernungen, z. B. Internet

---

1.4 Topologien

Eine Topologie beschreibt, wie Geräte in einem Netzwerk miteinander verbunden sind.

Topologie	Erklärung
Bus	Alle Geräte hängen an einer gemeinsamen Leitung. Heute veraltet.
Ring	Geräte sind ringförmig verbunden. Daten laufen im Kreis.
Stern	Alle Geräte sind mit einem zentralen Gerät verbunden, meistens einem Switch.
Mesh	Geräte sind mehrfach miteinander verbunden. Dadurch entsteht Redundanz.

Grafik: Sterntopologie

```
flowchart TD
    SW[Switch]
    PC1[PC 1]
    PC2[PC 2]
    PC3[PC 3]
    PR[Drucker]
    NAS[NAS / Server]

    SW --- PC1
    SW --- PC2
    SW --- PC3
    SW --- PR
    SW --- NAS
```

Die Sterntopologie ist heute im LAN am häufigsten. Fällt ein einzelnes Kabel aus, ist meist nur ein Gerät betroffen. Fällt aber der zentrale Switch aus, sind alle daran angeschlossenen Geräte betroffen.

1.5 Simplex, Halbduplex und Vollduplex

Begriff	Bedeutung	Beispiel
Simplex	Kommunikation nur in eine Richtung	Radio, Fernsehsendung
Halbduplex	Kommunikation in beide Richtungen, aber nicht gleichzeitig	Funkgerät
Vollduplex	Kommunikation gleichzeitig in beide Richtungen	modernes Ethernet mit Switch

Merksatz:

- Hub = meistens Halbduplex
- Switch = Vollduplex möglich

---

2. OSI-Schichtenmodell

Das OSI-Modell teilt Netzwerkkommunikation in 7 Schichten ein. Jede Schicht hat eine bestimmte Aufgabe.

Der Vorteil: Netzwerkprobleme lassen sich besser eingrenzen.

Beispiel:

Wenn ein PC keine Webseite öffnen kann, kann man schrittweise prüfen:

- Ist das Kabel verbunden?
- Hat der PC eine IP-Adresse?
- Funktioniert DNS?
- Ist der Webserver erreichbar?
- Blockiert eine Firewall?

2.1 Die 7 OSI-Schichten

Schicht	Name	Aufgabe	Beispiele
7	Anwendung	Dienste für Anwendungen	HTTP, HTTPS, DNS, SMTP
6	Darstellung	Datenformat, Codierung, Verschlüsselung	TLS, Zeichencodierung
5	Sitzung	Verbindungen zwischen Anwendungen verwalten	Sitzungen, Logins
4	Transport	Ende-zu-Ende-Kommunikation	TCP, UDP, Ports
3	Vermittlung	logische Adressierung und Routing	IP, Router
2	Sicherung	lokale Zustellung im LAN	MAC-Adresse, Switch, Ethernet
1	Bitübertragung	elektrische, optische oder Funk-Signale	Netzwerkkarte, Kabel
0	Übertragungsmedium	physisches Medium selbst	Kupfer, Glasfaser, Funk

Hinweis:

Schicht 0 gehört nicht offiziell zum OSI-Modell, wird im Unterricht aber oft als praktische Ergänzung verwendet.

2.2 Merksatz für das OSI-Modell

Von oben nach unten:

Alle Deutschen Schüler Trinken Verschiedene Sorten Brause

Wort	Schicht
Alle	Anwendung
Deutschen	Darstellung
Schüler	Sitzung
Trinken	Transport
Verschiedene	Vermittlung
Sorten	Sicherung
Brause	Bitübertragung

2.3 OSI-Modell als Grafik

```
flowchart TB
    L7["7 Anwendung<br>HTTP, HTTPS, DNS"]
    L6["6 Darstellung<br>Format, Verschlüsselung"]
    L5["5 Sitzung<br>Sitzungen, Verbindungen"]
    L4["4 Transport<br>TCP, UDP, Ports"]
    L3["3 Vermittlung<br>IP, Routing"]
    L2["2 Sicherung<br>MAC, Switch, Ethernet"]
    L1["1 Bitübertragung<br>Signale, Netzwerkkarte"]
    L0["0 Medium<br>Kabel, Glasfaser, Funk"]

    L7 --> L6 --> L5 --> L4 --> L3 --> L2 --> L1 --> L0
```

2.4 TCP/IP-Modell

In der Praxis wird häufig das TCP/IP-Modell verwendet. Es ist weniger theoretisch als das OSI-Modell und orientiert sich stärker an realen Netzwerken.

TCP/IP-Schicht	Entspricht ungefähr OSI	Beispiele
Anwendung	OSI 5–7	HTTP, HTTPS, DNS, SMTP
Transport	OSI 4	TCP, UDP
Internet	OSI 3	IPv4, IPv6, ICMP

TCP/IP-Schicht	Entspricht ungefähr OSI	Beispiele
Netzzugang	OSI 1–2	Ethernet, WLAN, MAC

2.5 Datenkapselung

Beim Senden werden Daten auf jeder Schicht verpackt. Jede Schicht fügt eigene Steuerinformationen hinzu.

Beispiel beim Aufruf einer Webseite:

```
flowchart TD
    A["HTTP-Daten<br>Webseiteninhalt"]
    B["TCP-Header + HTTP-Daten<br>Port 80/443"]
    C["IP-Header + TCP + Daten<br>Quell-IP / Ziel-IP"]
    D["Ethernet-Header + IP + TCP + Daten<br>Quell-MAC / Ziel-MAC"]
    E["Bits auf Kabel / Glasfaser / Funk"]

    A --> B --> C --> D --> E
```

Wichtig für die IHK:

- MAC-Adresse arbeitet auf Schicht 2
- IP-Adresse arbeitet auf Schicht 3
- Ports arbeiten auf Schicht 4
- Anwendungen wie HTTP oder DNS liegen oben im Modell

---

3. Schicht 0 – Übertragungsmedien

Schicht 0 beschreibt das Medium, über das Daten übertragen werden.

Typische Medien:

- Koaxialkabel
- Twisted-Pair-Kabel
- Lichtwellenleiter
- Funk bei WLAN

3.1 Koaxialkabel

Koaxialkabel wurden früher häufig in Bus-Netzwerken verwendet. Heute sind sie in klassischen LANs veraltet.

Merkmale:

- früher für Ethernet verwendet
- Bus-Topologie
- störanfällig bei schlechter Verkabelung
- heute kaum noch relevant für moderne LANs

3.2 Twisted-Pair-Kabel

Twisted-Pair-Kabel sind die typischen Netzwerkkabel mit RJ45-Stecker.

Die Adernpaare sind verdrillt. Dadurch werden Störungen reduziert.

Kategorie	Typische Verwendung
Cat 5e	bis 1 Gbit/s
Cat 6	1 Gbit/s, teilweise 2,5/5 Gbit/s
Cat 6A	bis 10 Gbit/s
Cat 7	hochwertige Gebäudeverkabelung
Cat 8	sehr hohe Datenraten im kurzen Bereich

Faustregel:

Für normale Büro- und Heimnetzwerke ist Cat 6 oder Cat 6A meistens ausreichend.

3.3 Lichtwellenleiter

Lichtwellenleiter übertragen Daten mit Licht statt mit elektrischen Signalen.

Vorteile:

- hohe Reichweite
- hohe Geschwindigkeit
- unempfindlicher gegen elektromagnetische Störungen
- gut für Gebäudeverbindungen und Rechenzentren

Nachteile:

- empfindlicher gegen Knicken
- teurer in Installation und Technik
- Spleißen und Messung benötigen Fachwissen

3.4 Multimode und Singlemode

Typ	Erklärung	Einsatz
Multimode	Licht läuft auf mehreren Wegen durch die Faser	kurze bis mittlere Strecken
Singlemode	Licht läuft auf einem sehr engen Weg	lange Strecken

Merksatz:

- Multimode = kürzere Strecken
- Singlemode = lange Strecken

3.5 Verkabelungsregel

Eine einfache praktische Regel:

Entfernung	Medium
bis ca. 100 m	Twisted-Pair-Kupferkabel
bis mehrere hundert Meter	Multimode-LWL
größere Entfernungen	Singlemode-LWL

3.6 WLAN

WLAN überträgt Daten per Funk.

Wichtige Frequenzbereiche:

Frequenz	Eigenschaften
2,4 GHz	hohe Reichweite, aber oft stärker belegt
5 GHz	schneller, weniger Reichweite
6 GHz	modern, hohe Geschwindigkeit, kürzere Reichweite

Wichtige WLAN-Generationen:

Name	Standard
Wi-Fi 4	IEEE 802.11n
Wi-Fi 5	IEEE 802.11ac
Wi-Fi 6	IEEE 802.11ax
Wi-Fi 6E	IEEE 802.11ax mit 6 GHz
Wi-Fi 7	IEEE 802.11be

3.7 WLAN-Sicherheit

Für die IHK wichtig:

- WLAN sollte verschlüsselt sein
- WPA2 ist Mindeststandard
- WPA3 ist empfohlen
- Gastnetz getrennt vom internen Netz betreiben
- unsichere alte Standards vermeiden
- starke Passwörter verwenden

---

4. Ethernet-Frame

Ethernet arbeitet auf Schicht 2. Die Daten werden in Frames übertragen.

Ein Ethernet-Frame enthält unter anderem:

- Ziel-MAC-Adresse
- Quell-MAC-Adresse
- Typfeld
- Nutzdaten
- Prüfsumme

4.1 Ethernet-Frame als Grafik

```
flowchart LR
    A["Präambel"]
    B["Ziel-MAC"]
    C["Quell-MAC"]
    D["Typ"]
    E["Daten<br>z. B. IP + TCP + HTTP"]
    F["FCS / Prüfsumme"]

    A --> B --> C --> D --> E --> F
```

4.2 MAC-Adresse

Eine MAC-Adresse ist die Hardwareadresse einer Netzwerkschnittstelle.

Eigenschaften:

- 48 Bit lang

- hexadezimale Schreibweise
- Beispiel: `00:1A:2B:3C:4D:5E`
- arbeitet auf OSI-Schicht 2
- wird im lokalen Netzwerk verwendet

Wichtig:

Eine MAC-Adresse wird nur im lokalen Netzwerksegment verwendet. Sobald ein Paket über einen Router weitergeleitet wird, ändern sich die MAC-Adressen auf dem Weg. Die IP-Adressen bleiben dagegen im Normalfall gleich.

4.3 FCS / CRC

Die Prüfsumme dient zur Fehlererkennung.

Wenn ein Frame beschädigt ist, kann dies erkannt werden. Der Frame wird dann verworfen.

Wichtig:

Ethernet korrigiert Fehler nicht selbst. Fehlerhafte Frames werden verworfen. Höhere Schichten, zum Beispiel TCP, können dann eine erneute Übertragung auslösen.

4.4 MTU und Nutzdaten

Die übliche MTU bei Ethernet beträgt 1500 Byte.

Das bedeutet:

Ein Ethernet-Frame kann typischerweise 1500 Byte Nutzdaten für die nächsthöhere Schicht transportieren.

Da IP- und TCP-Header ebenfalls Platz benötigen, bleiben für reine Anwendungsdaten weniger als 1500 Byte übrig.

---

5. Sniffer

Ein Sniffer ist ein Werkzeug zur Analyse von Netzwerkverkehr.

Beispiele:

- Wireshark
- tcpdump
- Windump

Sniffer werden zur Fehlersuche eingesetzt.

Beispiele:

- Warum bekommt ein Client keine IP-Adresse?
- Wird DNS korrekt aufgelöst?
- Sendet ein Gerät ARP-Anfragen?
- Kommt eine TCP-Verbindung zustande?

5.1 Rechtlicher Hinweis

Sniffing darf nur erlaubt und kontrolliert eingesetzt werden.

In Unternehmen gilt:

- Vorgesetzte informieren
- Datenschutz beachten
- Betriebsrat einbeziehen, falls vorhanden
- nicht heimlich fremde Daten mitschneiden

Für Ausbildung und Laborumgebungen ist Sniffing sinnvoll, solange keine fremden Daten ausspioniert werden.

---

6. Schicht 1 – Bitübertragung

Schicht 1 beschreibt die technische Übertragung der Bits.

Dazu gehören:

- elektrische Signale
- optische Signale
- Funkwellen
- Netzwerkkarten
- physische Anschlüsse

6.1 Netzwerkkarte

Die Netzwerkkarte verbindet den Computer mit dem Netzwerk.

Aufgaben:

- Daten senden und empfangen
- Signale erzeugen
- Prüfsummen prüfen
- Zugriff auf das Medium steuern
- MAC-Adresse bereitstellen

6.2 CSMA/CD und CSMA/CA

Verfahren	Bedeutung	Einsatz
CSMA/CD	Kollisionserkennung	alte kabelgebundene Netze mit Hub
CSMA/CA	Kollisionsvermeidung	WLAN

Merksatz:

- CD = Collision Detection = Kollision erkennen
- CA = Collision Avoidance = Kollision vermeiden

6.3 Hub

Ein Hub ist ein veraltetes Netzwerkgerät.

Eigenschaften:

- verteilt Daten an alle Ports
- kennt keine MAC-Adressen
- erzeugt unnötigen Datenverkehr
- Sniffing ist leicht möglich
- nur Halbduplex
- praktisch durch Switches ersetzt

---

7. Schicht 2 – Sicherungsschicht

Schicht 2 ist für die lokale Kommunikation im gleichen Netzwerk zuständig.

Wichtige Begriffe:

- MAC-Adresse
- Ethernet-Frame
- Switch
- VLAN
- ARP
- Broadcast

7.1 Switch

Ein Switch verbindet Geräte in einem LAN.

Er arbeitet hauptsächlich auf Schicht 2 und leitet Frames anhand der MAC-Adresse weiter.

Vorteile gegenüber einem Hub:

- sendet Frames gezielt an den richtigen Port
- weniger unnötiger Datenverkehr
- Vollduplex möglich
- höhere Geschwindigkeit
- bessere Sicherheit

7.2 Switch-Tabelle

Ein Switch merkt sich, welche MAC-Adresse an welchem Port erreichbar ist.

Diese Tabelle wird oft MAC Address Table, SAT-Tabelle oder Forwarding Table genannt.

Ablauf:

1. Ein Frame kommt am Switch an.
2. Der Switch liest die Quell-MAC-Adresse.
3. Er merkt sich: Diese MAC-Adresse befindet sich an diesem Port.
4. Bei späteren Frames zur gleichen MAC-Adresse kann der Switch gezielt weiterleiten.

7.3 ARP

ARP bedeutet Address Resolution Protocol.

ARP wird bei IPv4 verwendet, um zu einer IP-Adresse die passende MAC-Adresse zu finden.

Beispiel:

Ein PC möchte an `192.168.1.20` senden, kennt aber nur die IP-Adresse.

Dann fragt er per Broadcast:

„Wer hat 192.168.1.20?“

Das Zielgerät antwortet:

„Ich habe 192.168.1.20, meine MAC-Adresse ist …“

7.4 ARP als Grafik

```
sequenceDiagram
    participant PC1 as PC 1
    participant LAN as LAN / Switch
    participant PC2 as PC 2
```

```
PC1->>LAN: ARP Request: Wer hat 192.168.1.20?
LAN->>PC2: Broadcast wird weitergeleitet
PC2->>PC1: ARP Reply: Ich habe die IP, meine MAC ist AA:BB:CC...
```

7.5 Managed und unmanaged Switch

Typ	Erklärung
Unmanaged Switch	keine Konfiguration nötig, einfache Nutzung
Managed Switch	konfigurierbar, z. B. VLAN, Port-Mirroring, STP, PoE

Für Unternehmen sind managed Switches wichtig, weil sie mehr Kontrolle und Sicherheit bieten.

7.6 Port-Mirroring

Beim Port-Mirroring wird der Datenverkehr eines Ports auf einen anderen Port kopiert.

Einsatz:

- Analyse mit Wireshark
- Fehlersuche
- Sicherheitsanalyse

7.7 Link Aggregation

Bei Link Aggregation werden mehrere physische Netzwerkverbindungen zu einer logischen Verbindung zusammengefasst.

Vorteile:

- höhere Gesamtbandbreite
- Redundanz
- bessere Auslastung

Wichtig:

Eine einzelne Verbindung wird nicht automatisch doppelt so schnell. Die Last wird meistens auf mehrere Verbindungen verteilt.

7.8 Power over Ethernet

Power over Ethernet, kurz PoE, überträgt Daten und Strom über dasselbe Netzwerkkabel.

Typische Geräte:

- IP-Telefone
- Access Points
- Überwachungskameras
- kleine Netzwerkgeräte

Vorteil:

Man braucht nicht an jedem Gerät eine eigene Steckdose.

7.9 Spanning Tree Protocol

Das Spanning Tree Protocol verhindert Schleifen zwischen Switches.

Warum ist das wichtig?

Wenn Switches mehrfach miteinander verbunden sind, kann ein Broadcast endlos im Kreis laufen. Dadurch kann das Netzwerk stark überlastet werden.

STP blockiert bestimmte Verbindungen logisch und aktiviert sie bei Bedarf wieder, wenn eine andere Verbindung ausfällt.

7.10 Spanning Tree als Grafik

```
flowchart TD
    SW1[Switch 1]
    SW2[Switch 2]
    SW3[Switch 3]
    SW4[Switch 4]

    SW1 --- SW2
    SW2 --- SW3
    SW3 -. blockiert durch STP .- SW4
    SW4 --- SW1
```

Die gestrichelte Verbindung ist vorhanden, wird aber logisch blockiert. Fällt eine andere Verbindung aus, kann STP neu berechnen und die blockierte Verbindung wieder aktivieren.

7.11 VLAN

VLAN bedeutet Virtual Local Area Network.

Ein VLAN teilt ein physisches Netzwerk in mehrere logische Netzwerke auf.

Beispiel:

Ein Switch kann gleichzeitig mehrere getrennte Netze bereitstellen:

- VLAN 10 = Verwaltung
- VLAN 20 = Schüler / Mitarbeiter
- VLAN 30 = Gäste
- VLAN 40 = Server

Vorteile:

- bessere Sicherheit
- weniger Broadcast-Verkehr
- klare Trennung von Bereichen
- einfachere Netzwerkstruktur

7.12 VLAN als Grafik

```
flowchart TD
    SW[Managed Switch]

    PC1[PC Verwaltung<br>VLAN 10]
    PC2[PC Verwaltung<br>VLAN 10]
    PC3[Gastgerät<br>VLAN 30]
    PC4[Server<br>VLAN 40]

    SW --- PC1
    SW --- PC2
    SW --- PC3
    SW --- PC4
```

Geräte im gleichen VLAN können direkt miteinander kommunizieren. Geräte in unterschiedlichen VLANs benötigen Routing, meist über einen Router, Layer-3-Switch oder eine Firewall.

7.13 Tagged und Untagged VLAN

Begriff	Erklärung
Untagged Port	Port gehört fest zu einem VLAN, z. B. Endgerät

Begriff	Erklärung
Tagged Port	VLAN-Information wird im Frame mitgesendet, z. B. Verbindung zwischen Switches
Trunk	Verbindung, die mehrere VLANs transportiert

Beispiel:

Ein PC-Port ist meistens untagged. Eine Verbindung zwischen zwei Switches ist meistens tagged.

---

8. Schicht 3 – Vermittlungsschicht

Schicht 3 ist für logische Adressierung und Routing zuständig.

Wichtige Themen:

- IPv4
- IPv6
- Subnetzmaske
- Routing
- DHCP
- DNS
- Router
- Layer-3-Switch

8.1 IPv4-Adresse

Eine IPv4-Adresse ist 32 Bit lang.

Sie wird in vier Oktette aufgeteilt.

Beispiel:

`192.168.1.10`

Binär:

`11000000.10101000.00000001.00001010`

Jedes Oktett hat 8 Bit und kann Werte von 0 bis 255 enthalten.

8.2 Subnetzmaske

Die Subnetzmaske trennt eine IP-Adresse in Netzanteil und Hostanteil.

Beispiel:

IP-Adresse:

`192.168.1.10`

Subnetzmaske:

`255.255.255.0`

CIDR-Schreibweise:

`/24`

Das bedeutet:

- die ersten 24 Bit gehören zum Netzanteil
- die restlichen 8 Bit gehören zum Hostanteil

Netz:

`192.168.1.0/24`

Hostbereich:

`192.168.1.1` bis `192.168.1.254`

Broadcast:

`192.168.1.255`

8.3 IPv4-Netz als Grafik

```
flowchart LR
    A["192.168.1.0<br>Netzadresse"]
    B["192.168.1.1<br>erster Host"]
    C["192.168.1.10<br>Host"]
    D["192.168.1.254<br>letzter Host"]
    E["192.168.1.255<br>Broadcast"]

    A --> B --> C --> D --> E
```

8.4 Netzadresse und Broadcast

In jedem IPv4-Netz gibt es zwei besondere Adressen:

Adresse	Bedeutung
erste Adresse	Netzadresse
letzte Adresse	Broadcast-Adresse

Diese beiden Adressen können nicht als normale Hostadresse verwendet werden.

Beispiel bei `192.168.1.0/24`:

Typ	Adresse
Netzadresse	192.168.1.0
erster Host	192.168.1.1
letzter Host	192.168.1.254
Broadcast	192.168.1.255

8.5 Private IPv4-Adressbereiche

Private IP-Adressen werden in lokalen Netzwerken verwendet und nicht direkt im Internet geroutet.

Bereich	CIDR
10.0.0.0 bis 10.255.255.255	10.0.0.0/8
172.16.0.0 bis 172.31.255.255	172.16.0.0/12
192.168.0.0 bis 192.168.255.255	192.168.0.0/16

Diese Bereiche sind besonders wichtig für Heimnetzwerke, Firmennetze, Labore und virtuelle Umgebungen.

8.6 Besondere IPv4-Adressen

Adresse	Bedeutung
0.0.0.0	unspezifizierte Adresse
127.0.0.1	localhost / Loopback
169.254.0.0/16	APIPA / Link Local
255.255.255.255	lokaler Broadcast

APIPA sieht man häufig, wenn ein Client keine Adresse vom DHCP-Server bekommt.

8.7 Subnetting

Subnetting bedeutet, ein größeres Netzwerk in kleinere Teilnetze aufzuteilen.

Warum macht man Subnetting?

- bessere Struktur
- weniger Broadcast-Verkehr
- bessere Sicherheit
- Trennung von Abteilungen
- effizientere Adressvergabe

Beispiel:

Aus `192.168.1.0/24` werden zwei Subnetze:

Subnetz	Bereich
192.168.1.0/25	192.168.1.0 bis 192.168.1.127
192.168.1.128/25	192.168.1.128 bis 192.168.1.255

Nutzbare Hosts:

Subnetz	nutzbare Hosts
192.168.1.0/25	192.168.1.1 bis 192.168.1.126
192.168.1.128/25	192.168.1.129 bis 192.168.1.254

8.8 Subnetting-Regel

Formel:

`Anzahl Adressen = 2^(Hostbits)`

`nutzbare Hosts = 2^(Hostbits) - 2`

Beispiel `/24`:

- 32 Bit insgesamt
- 24 Bit Netzanteil
- 8 Bit Hostanteil
- $2^8 = 256$ Adressen
- 256 - 2 = 254 nutzbare Hosts

8.9 Häufige CIDR-Werte

CIDR	Subnetzmaske	Adressen	nutzbare Hosts

/24	255.255.255.0	256	254
/25	255.255.255.128	128	126
/26	255.255.255.192	64	62
/27	255.255.255.224	32	30
/28	255.255.255.240	16	14
/29	255.255.255.248	8	6
/30	255.255.255.252	4	2

Für IHK-Aufgaben sind diese Werte sehr wichtig.

8.10 IPv6

IPv6 ist der Nachfolger von IPv4.

Eigenschaften:

- 128 Bit lang
- hexadezimale Schreibweise
- sehr großer Adressraum
- kein klassisches Broadcast wie bei IPv4
- nutzt Multicast und Neighbor Discovery

Beispiel:

`2001:0db8:0000:0000:0000:ff00:0042:8329`

Gekürzt:

`2001:db8::ff00:42:8329`

8.11 IPv6 kürzen

Regeln:

- führende Nullen in einem Block dürfen weggelassen werden
- eine zusammenhängende Folge von Null-Blöcken darf einmal durch `::` ersetzt werden

Beispiel:

Lang:

`2001:0db8:0000:0000:0000:0000:0000:0001`

Kurz:

`2001:db8::1`

Wichtig:

`::` darf nur einmal in einer IPv6-Adresse verwendet werden, sonst wäre die Adresse nicht eindeutig.

8.12 Besondere IPv6-Adressen

Adresse / Bereich	Bedeutung
`::`	unspezifizierte Adresse
`::1`	Loopback
`fe80::/10`	Link Local
`fc00::/7`	Unique Local Address
`ff00::/8`	Multicast

8.13 DHCP

DHCP vergibt automatisch Netzwerkkonfigurationen an Clients.

Typische DHCP-Informationen:

- IP-Adresse
- Subnetzmaske
- Standardgateway
- DNS-Server
- Lease-Zeit

8.14 DHCP-Ablauf

Der typische DHCP-Ablauf besteht aus vier Schritten:

Schritt	Bedeutung
Discover	Client sucht DHCP-Server
Offer	Server bietet Adresse an
Request	Client fordert Adresse an
Acknowledge	Server bestätigt die Vergabe

Merksatz:

DORA

- Discover
- Offer
- Request
- Acknowledge

8.15 DHCP als Grafik

```
sequenceDiagram
    participant C as Client
    participant S as DHCP-Server

    C->>S: DHCP Discover
    S->>C: DHCP Offer
    C->>S: DHCP Request
    S->>C: DHCP Acknowledge
```

8.16 DNS

DNS bedeutet Domain Name System.

DNS übersetzt Namen in IP-Adressen.

Beispiel:

`www.example.com`

wird zu einer IP-Adresse aufgelöst.

Warum ist DNS wichtig?

Menschen merken sich Namen leichter als IP-Adressen.

8.17 FQDN

FQDN bedeutet Fully Qualified Domain Name.

Beispiel:

`server01.firma.local`

Bestandteile:

Teil	Bedeutung

server01	Hostname
firma	Domain
local	Top-Level oder interner Namensraum

8.18 Routing

Routing bedeutet, Datenpakete zwischen verschiedenen Netzwerken weiterzuleiten.

Ein Router verbindet mehrere IP-Netze.

Beispiel:

- Netz A: `192.168.1.0/24`
- Netz B: `192.168.2.0/24`

Damit Geräte aus beiden Netzen kommunizieren können, braucht man einen Router oder Layer-3-Switch.

8.19 Routing als Grafik

```
flowchart LR
    A["PC A<br>192.168.1.10/24"]
    R["Router<br>192.168.1.1 / 192.168.2.1"]
    B["PC B<br>192.168.2.10/24"]

    A --- R --- B
```

Wenn PC A mit PC B kommunizieren möchte, erkennt PC A:

PC B liegt nicht im eigenen Netz. Deshalb sendet PC A das Paket an sein Standardgateway.

8.20 Statisches und dynamisches Routing

Art	Erklärung
statisches Routing	Routen werden manuell eingetragen
dynamisches Routing	Router tauschen Routen automatisch aus

Für kleinere Netze reichen statische Routen oft aus. In größeren Netzen verwendet man dynamische Routing-Protokolle.

8.21 Layer-3-Switch

Ein Layer-3-Switch kann zusätzlich zum Switching auch Routing übernehmen.

Typischer Einsatz:

- VLANs miteinander verbinden
- schnelles Routing im LAN
- Entlastung eines Routers

Beispiel:

VLAN 10 und VLAN 20 können über einen Layer-3-Switch miteinander kommunizieren, wenn Routing erlaubt ist.

---

9. Schicht 4 – Transportschicht

Schicht 4 ist für die Kommunikation zwischen Anwendungen zuständig.

Wichtige Themen:

- TCP
- UDP
- Ports
- Verbindungsaufbau
- Verbindungsabbau
- NAT
- Portweiterleitung

9.1 Ports

Ports dienen dazu, Anwendungen auf einem Gerät zu unterscheiden.

Ein Gerät kann eine IP-Adresse haben, aber viele Dienste gleichzeitig anbieten.

Beispiel:

Dienst	Port
HTTP	80
HTTPS	443
DNS	53
SSH	22
SMTP	25

Dienst	Port
IMAP	143
RDP	3389

Die IP-Adresse sagt, welches Gerät gemeint ist. Der Port sagt, welche Anwendung auf dem Gerät gemeint ist.

9.2 Schreibweise IP-Adresse mit Port

Beispiele:

- `192.168.1.10:80`
- `10.0.0.5:22`
- `https://example.com:443`

9.3 Portbereiche

Bereich	Name	Bedeutung
0–1023	System Ports / Well-known Ports	bekannte Standarddienste
1024–49151	User Ports	registrierte Anwendungen
49152–65535	Dynamic / Private Ports	temporäre Client-Ports

9.4 TCP

TCP ist verbindungsorientiert.

Eigenschaften:

- zuverlässige Übertragung
- Reihenfolge der Daten wird sichergestellt
- verlorene Daten werden erneut gesendet
- Verbindung wird aufgebaut und beendet
- mehr Verwaltungsaufwand als UDP

Typische TCP-Dienste:

- HTTP
- HTTPS
- SSH
- SMTP
- IMAP
- FTP

9.5 TCP-Verbindungsaufbau

TCP nutzt den Three-Way-Handshake.

```
sequenceDiagram
    participant C as Client
    participant S as Server

    C->>S: SYN
    S->>C: SYN/ACK
    C->>S: ACK
```

Danach ist die Verbindung aufgebaut.

9.6 TCP-Verbindungsabbau

Eine TCP-Verbindung wird kontrolliert beendet.

Vereinfacht:

```
sequenceDiagram
    participant C as Client
    participant S as Server

    C->>S: FIN
    S->>C: ACK
    S->>C: FIN
    C->>S: ACK
```

9.7 UDP

UDP ist verbindungslos.

Eigenschaften:

- kein Verbindungsaufbau
- keine Garantie für Zustellung
- keine automatische Wiederholung
- schneller und schlanker als TCP

Typische UDP-Dienste:

- DNS
- DHCP
- VoIP
- Streaming
- Gaming

9.8 TCP und UDP Vergleich

Merkmal	TCP	UDP
Verbindung	verbindungsorientiert	verbindungslos
Zuverlässigkeit	hoch	keine Garantie
Reihenfolge	wird sichergestellt	nicht garantiert
Geschwindigkeit	mehr Overhead	weniger Overhead
Beispiele	HTTPS, SSH, SMTP	DNS, DHCP, VoIP

9.9 NAT

NAT bedeutet Network Address Translation.

NAT übersetzt IP-Adressen.

Typischer Fall:

Viele private Geräte im LAN nutzen eine gemeinsame öffentliche IP-Adresse für den Zugriff ins Internet.

Beispiel:

- PC intern: `192.168.1.10`
- Router öffentlich: `84.x.x.x`

Der Router ersetzt beim Senden ins Internet die private Quelladresse durch seine öffentliche Adresse.

9.10 NAT als Grafik

```
flowchart LR
    PC["PC<br>192.168.1.10"]
    R["Router / NAT<br>innen: 192.168.1.1<br>außen: öffentliche IP"]
```

```
INET["Internet<br>Webserver"]

PC --> R --> INET
INET --> R --> PC
```

9.11 PAT

PAT bedeutet Port Address Translation.

PAT ist eine Form von NAT, bei der zusätzlich Ports genutzt werden.

Dadurch können viele interne Geräte gleichzeitig über eine öffentliche IP-Adresse kommunizieren.

Beispiel:

Intern	Extern
192.168.1.10:50001	öffentliche-IP:61001
192.168.1.11:50002	öffentliche-IP:61002

Der Router merkt sich diese Zuordnung in einer NAT-Tabelle.

9.12 Portforwarding

Portforwarding wird auch Destination NAT genannt.

Dabei wird eine Anfrage von außen an ein internes Gerät weitergeleitet.

Beispiel:

Anfrage aus dem Internet an:

`öffentliche-IP:443`

wird weitergeleitet an:

`192.168.1.20:443`

Typische Verwendung:

- Webserver im internen Netzwerk
- VPN-Server
- Spieleserver
- Remote-Zugriff

Sicherheitswarnung:

Portforwarding öffnet Dienste nach außen. Deshalb sollte man nur notwendige Ports freigeben und Dienste aktuell halten.

9.13 Portforwarding als Grafik

```
flowchart LR
    I["Client im Internet"]
    R["Router / Firewall<br>Port 443 offen"]
    S["Interner Webserver<br>192.168.1.20:443"]

    I --> R --> S
```

9.14 Allowlist und Blocklist

Begriff	Bedeutung
Allowlist	Nur ausdrücklich erlaubte Dinge sind erlaubt
Blocklist	Nur ausdrücklich verbotene Dinge sind blockiert

Sicherer ist meistens das Allowlist-Prinzip:

Alles ist verboten, außer es wurde ausdrücklich erlaubt.

---

10. Firewalls

Eine Firewall kontrolliert Netzwerkverkehr anhand von Regeln.

Sie entscheidet:

- Wer darf wohin?
- Von welcher Quelle?
- Zu welchem Ziel?
- Über welches Protokoll?
- Über welchen Port?
- In welche Richtung?

Eine Firewall schützt nicht automatisch vor allem. Sie ist nur so gut wie ihre Regeln und ihre Platzierung im Netzwerk.

10.1 Aufgaben einer Firewall

Eine Firewall kann:

- unerwünschten Datenverkehr blockieren
- erlaubte Kommunikation zulassen
- Netze voneinander trennen
- Server in einer DMZ schützen
- Zugriffe protokollieren
- Angriffsfläche reduzieren
- Regeln für ein- und ausgehenden Verkehr erzwingen

10.2 Personal Firewall und Unternehmens-Firewall

Typ	Erklärung
Personal Firewall	läuft direkt auf einem einzelnen PC oder Server
Unternehmens-Firewall	schützt ein gesamtes Netzwerk oder mehrere Netzbereiche

Beispiel:

Die Windows Defender Firewall ist eine Personal Firewall.

Eine Firewall zwischen LAN und Internet ist eine Unternehmens-Firewall.

10.3 Paketfilter-Firewall

Eine einfache Paketfilter-Firewall prüft einzelne Pakete anhand von Regeln.

Sie betrachtet zum Beispiel:

- Quell-IP
- Ziel-IP
- Protokoll
- Port

Nachteil:

Klassische Paketfilter kennen oft keinen Verbindungszustand. Hin- und Rückweg müssen dann separat erlaubt werden.

Für die IHK wichtig:

Paketfilter-Firewalls sind weiterhin prüfungsrelevant, auch wenn moderne Firewalls meist zustandsorientiert arbeiten.

10.4 Stateful Packet Inspection Firewall

Eine SPI-Firewall ist zustandsorientiert.

SPI bedeutet Stateful Packet Inspection.

Das bedeutet:

Die Firewall merkt sich bestehende Verbindungen.

Vorteil:

Wenn ein Client aus dem LAN eine Verbindung nach außen aufbaut, kann die Antwort automatisch wieder zurückgelassen werden.

Der Rückweg muss nicht extra als neue Regel eingerichtet werden.

10.5 Paketfilter vs. SPI-Firewall

Merkmal	Paketfilter	SPI-Firewall
prüft einzelne Pakete	ja	ja
kennt Verbindungszustand	nein oder begrenzt	ja
Rückweg automatisch erlaubt	nein	ja, wenn Verbindung gültig
Sicherheit	geringer	höher
heutige Praxis	eher veraltet	üblich

10.6 Firewall-Regeln nach OSI-Schichten

Eine Firewall kann je nach Typ verschiedene Informationen prüfen.

OSI-Schicht	Prüfkriterium	Beispiel
Schicht 2	MAC-Adresse	Nur Gerät mit bestimmter MAC erlauben
Schicht 3	IP-Adresse	Quelle 192.168.1.10 erlauben
Schicht 4	TCP / UDP und Ports	TCP 443 erlauben
Schicht 7	Anwendung	HTTP, DNS, bestimmte URLs

Wichtig:

Je höher die Schicht, desto genauer kann geprüft werden. Dafür braucht die Firewall aber mehr Leistung und mehr Verständnis des Datenverkehrs.

10.7 Grundprinzip: Default Deny

Ein sicheres Firewall-Konzept arbeitet häufig nach diesem Prinzip:

Alles ist verboten, außer es wurde ausdrücklich erlaubt.

Das nennt man Default Deny.

Beispiel:

Erlaubt:

- LAN → Internet: HTTPS
- LAN → DNS-Server: DNS
- Admin-PC → Server: SSH oder RDP

Verboten:

- Internet → LAN
- Gäste-WLAN → internes Servernetz
- unbekannte Ports
- unnötige Dienste

10.8 Firewall als Grenze zwischen Netzen

```
flowchart LR
    LAN["Internes LAN<br>vertrauenswürdiger Bereich"]
    FW["Firewall<br>Regelprüfung"]
    WAN["Internet<br>nicht vertrauenswürdiger Bereich"]

    LAN --> FW --> WAN
    WAN --> FW --> LAN
```

Die Firewall steht zwischen verschiedenen Sicherheitszonen.

10.9 Typische Firewall-Zonen

Zone	Bedeutung
LAN	internes vertrauenswürdiges Netz
WAN	Internet / externes Netz
DMZ	separates Netz für öffentlich erreichbare Server

Zone	Bedeutung
Gäste-Netz	getrenntes Netz für Besucher
Servernetz	separates Netz für wichtige Server

10.10 DMZ

DMZ bedeutet Demilitarisierte Zone.

Eine DMZ ist ein separates Netzwerk für Server, die aus dem Internet erreichbar sein müssen.

Beispiele:

- Webserver
- Mailserver
- VPN-Gateway
- Reverse Proxy

Warum DMZ?

Wenn ein öffentlich erreichbarer Server kompromittiert wird, soll der Angreifer nicht direkt im internen LAN stehen.

10.11 DMZ als Grafik

```
flowchart LR
    WAN["Internet"]
    FW["Firewall"]
    LAN["Internes LAN<br>Clients, Dateien, interne Server"]
    DMZ["DMZ<br>Webserver / Reverse Proxy"]

    WAN --- FW
    FW --- LAN
    FW --- DMZ
```

Regelbeispiel:

Richtung	Regel
Internet → DMZ	Nur HTTPS zum Webserver erlauben
Internet → LAN	blockieren
DMZ → LAN	nur absolut notwendige Verbindungen

Richtung	Regel
LAN → DMZ	Administration nur von Admin-PCs
LAN → Internet	notwendige Dienste erlauben

10.12 Einstufige und zweistufige DMZ

Einstufige DMZ

Eine Firewall trennt Internet, LAN und DMZ.

Vorteil:

- einfacher Aufbau
- weniger Geräte
- günstiger

Nachteil:

- die Sicherheit hängt stark an einer Firewall

Zweistufige DMZ

Zwei Firewalls trennen Internet, DMZ und LAN.

Vorteil:

- bessere Trennung
- höheres Sicherheitsniveau

Nachteil:

- mehr Aufwand
- höhere Kosten
- komplexere Administration

10.13 Einstufige DMZ

```
flowchart LR
    I["Internet"]
    FW["Firewall mit 3 Schnittstellen"]
    LAN["LAN"]
    DMZ["DMZ"]
```

```
    I --- FW
    FW --- LAN
    FW --- DMZ
```

10.14 Zweistufige DMZ

```
flowchart LR
    I["Internet"]
    FW1["Firewall 1"]
    DMZ["DMZ"]
    FW2["Firewall 2"]
    LAN["Internes LAN"]

    I --- FW1 --- DMZ --- FW2 --- LAN
```

10.15 Firewall-Regeln verstehen

Eine Firewall-Regel besteht typischerweise aus:

Bestandteil	Beispiel
Quelle	192.168.10.0/24
Ziel	8.8.8.8
Protokoll	TCP oder UDP
Port	53, 80, 443
Aktion	erlauben oder blockieren
Richtung	eingehend, ausgehend, weitergeleitet

Beispielregel:

`LAN darf per TCP Port 443 ins Internet.`

Das bedeutet:

- Quelle: LAN
- Ziel: Internet
- Protokoll: TCP
- Port: 443
- Aktion: erlauben

10.16 INPUT, OUTPUT und FORWARD

Bei Linux-Firewalls mit iptables sind drei Richtungen besonders wichtig.

Chain	Bedeutung
INPUT	Verkehr zur Firewall selbst
OUTPUT	Verkehr von der Firewall selbst nach außen
FORWARD	Verkehr durch die Firewall hindurch

Beispiele:

Situation	Chain
Admin greift per SSH auf Firewall zu	INPUT
Firewall macht selbst DNS-Abfrage	OUTPUT
PC im LAN geht über Firewall ins Internet	FORWARD

10.17 INPUT, OUTPUT und FORWARD als Grafik

```
flowchart LR
    LAN["LAN-Client"]
    FW["Firewall-System"]
    NET["Internet"]

    LAN -- "FORWARD<br>durch die Firewall" --> FW
    FW -- "FORWARD" --> NET

    LAN -- "INPUT<br>zur Firewall selbst" --> FW
    FW -- "OUTPUT<br>von der Firewall selbst" --> NET
```

10.18 Beispiel für einfache Firewall-Logik

Ziel:

- LAN darf ins Internet
- Antworten aus dem Internet dürfen zurück
- Internet darf keine neuen Verbindungen ins LAN starten

Regellogik:

1. Erlaube bestehende und zugehörige Verbindungen.

2. Erlaube LAN → Internet für notwendige Dienste.
3. Blockiere neue Verbindungen von Internet → LAN.
4. Protokolliere unerwünschte Zugriffe.
5. Standardregel: blockieren.

10.19 Beispiel-Regelkonzept

Nr.	Quelle	Ziel	Dienst	Aktion
1	LAN	Internet	DNS	erlauben
2	LAN	Internet	HTTP/HTTPS	erlauben
3	LAN	Internet	NTP	erlauben
4	Internet	LAN	alle	blockieren
5	Admin-PC	Server	SSH/RDP	erlauben
6	Gäste-WLAN	LAN	alle	blockieren

10.20 Firewall und VLAN

VLANs trennen Netze logisch. Eine Firewall kann anschließend regeln, welche VLANs miteinander kommunizieren dürfen.

Beispiel:

```
flowchart TD
    FW["Firewall / Layer-3-Gateway"]

    V10["VLAN 10<br>Verwaltung"]
    V20["VLAN 20<br>Mitarbeiter"]
    V30["VLAN 30<br>Gäste"]
    V40["VLAN 40<br>Server"]

    V10 --- FW
    V20 --- FW
    V30 --- FW
    V40 --- FW
```

Beispielregeln:

Richtung	Erlaubt?
Verwaltung → Server	ja

Richtung	Erlaubt?
Mitarbeiter → Server	teilweise
Gäste → Internet	ja
Gäste → Server	nein
Gäste → Verwaltung	nein

10.21 Typische Prüfungsfragen zur Firewall

Was macht eine Firewall?

Eine Firewall kontrolliert Netzwerkverkehr anhand von Regeln. Sie erlaubt oder blockiert Verbindungen abhängig von Quelle, Ziel, Protokoll, Port und Richtung.

Was ist der Unterschied zwischen Paketfilter und SPI-Firewall?

Ein Paketfilter prüft einzelne Pakete. Eine SPI-Firewall merkt sich zusätzlich den Zustand einer Verbindung und kann Rückverkehr automatisch zuordnen.

Was bedeutet Default Deny?

Alles ist standardmäßig verboten. Nur ausdrücklich erlaubte Verbindungen sind zugelassen.

Warum verwendet man eine DMZ?

Eine DMZ trennt öffentlich erreichbare Server vom internen LAN. Dadurch wird das interne Netzwerk besser geschützt, falls ein öffentlicher Server kompromittiert wird.

Auf welcher OSI-Schicht arbeiten Firewalls?

Einfache Firewalls arbeiten vor allem auf Schicht 3 und 4. Moderne Firewalls können zusätzlich höhere Schichten prüfen, zum Beispiel Anwendungen auf Schicht 7.

---

11. IHK-Merkliste

MAC-Adresse

- Schicht 2
- lokale Zustellung im LAN
- wird vom Switch verwendet

IP-Adresse

- Schicht 3
- logische Adresse

- wird vom Router verwendet

Port

- Schicht 4
- unterscheidet Anwendungen und Dienste

Switch

- arbeitet hauptsächlich auf Schicht 2
- leitet anhand von MAC-Adressen weiter

Router

- arbeitet auf Schicht 3
- verbindet verschiedene IP-Netze

Firewall

- kontrolliert Verkehr zwischen Netzen
- prüft Regeln
- kann auf mehreren Schichten arbeiten

NAT

- übersetzt Adressen
- private Geräte nutzen öffentliche IP

Portforwarding

- leitet externe Anfragen an interne Server weiter
- Sicherheitsrisiko, wenn falsch konfiguriert

VLAN

- logische Trennung in einem physischen Netzwerk
- braucht Routing oder Firewall für Kommunikation zwischen VLANs

DMZ

- separates Netz für öffentlich erreichbare Server
- schützt das interne LAN

---

12. Kurzer Gesamtüberblick als Grafik

```
flowchart TB
    A["Schicht 0<br>Kabel, Glasfaser, Funk"]
    B["Schicht 1<br>Signale, Netzwerkkarte"]
    C["Schicht 2<br>MAC, Switch, Ethernet, VLAN"]
    D["Schicht 3<br>IP, Routing, DHCP, DNS"]
    E["Schicht 4<br>TCP, UDP, Ports, NAT"]
    F["Firewall<br>Regeln zwischen Netzen"]
    G["Anwendungen<br>HTTP, HTTPS, Mail, DNS"]

    A --> B --> C --> D --> E --> F --> G
```

---

13. Beispiel: Webseitenaufruf im Netzwerk

Ein Client ruft eine Webseite auf.

Ablauf vereinfacht:

1. Client prüft seine IP-Konfiguration.
2. Client fragt DNS nach der IP-Adresse der Webseite.
3. Client baut per TCP eine Verbindung zum Webserver auf.
4. Bei HTTPS wird Port 443 verwendet.
5. Daten werden in TCP-Segmente verpackt.
6. TCP wird in IP-Pakete verpackt.
7. IP wird in Ethernet-Frames verpackt.
8. Switch leitet Frames anhand der MAC-Adresse weiter.
9. Router oder Firewall leitet Pakete ins Internet weiter.
10. NAT übersetzt private Adresse in öffentliche Adresse.
11. Antwortpakete kommen zurück.
12. SPI-Firewall erkennt die bestehende Verbindung und lässt die Antwort passieren.

---

14. Webseitenaufruf als Grafik

```
sequenceDiagram
    participant PC as Client-PC
    participant DNS as DNS-Server
    participant FW as Router / Firewall / NAT
    participant WEB as Webserver

    PC->>DNS: Wie lautet die IP von example.com?
    DNS->>PC: Antwort: IP-Adresse
```

```
PC->>FW: TCP SYN an Webserver Port 443
FW->>WEB: Weiterleitung mit NAT
WEB->>FW: SYN/ACK zurück
FW->>PC: Antwort wird wegen SPI erlaubt
PC->>WEB: HTTPS-Datenübertragung
```

---

15. Prüfungsorientierte Zusammenfassung

Für die IHK solltest du besonders sicher beherrschen:

- OSI-Schichten und typische Geräte/Protokolle
- Unterschied zwischen MAC-Adresse, IP-Adresse und Port
- IPv4-Subnetting
- private IP-Bereiche
- DHCP-Ablauf DORA
- DNS-Grundprinzip
- Unterschied TCP und UDP
- NAT und Portforwarding
- VLAN-Grundprinzip
- Firewall-Regeln
- Unterschied Paketfilter und SPI-Firewall
- Zweck einer DMZ

Merksatz:

MAC findet Geräte im lokalen Netz. IP findet Netze. Ports finden Anwendungen. Firewalls entscheiden, was erlaubt ist.

Revision #3
Created 21 May 2026 02:11:39 by Admin
Updated 3 June 2026 06:18:12 by Admin