7.5 Merksätze und Prüfungswissen zu OSI-Schicht 4

Diese Seite fasst die wichtigsten Inhalte zur OSI-Schicht 4 zusammen.

OSI-Schicht 4 heißt:

```
Transportschicht
```

Die Hauptaufgabe von Schicht 4 ist:

```
Daten zwischen Anwendungen auf Endgeräten transportieren.
```

Dabei sind besonders wichtig:

```
- TCP
- UDP
- Ports
- Verbindungsaufbau
- Zuverlässigkeit
- Dienst-Erreichbarkeit
- Firewall-Regeln nach Port
- NAT/PAT mit Port-Zuordnung
```

Merksatz:

```
Schicht 4 = TCP, UDP und Ports.
```

Grundidee von Schicht 4

Schicht 3 bringt Daten zum richtigen Gerät.

Schicht 4 bringt Daten zur richtigen Anwendung auf diesem Gerät.

Beispiel:

```
IP-Adresse:
192.168.10.50

Port:
443
```

Zusammen:

```
192.168.10.50:443
```

Das bedeutet:

```
Gerät 192.168.10.50
Dienst auf Port 443
```

Merksatz:

```
IP bringt zum Gerät.
Port bringt zum Dienst.
```

Schicht 3 und Schicht 4 unterscheiden

Frage	Schicht
Welche IP-Adresse hat das Ziel?	3
Gibt es eine Route zum Ziel?	3
Ist das Gateway erreichbar?	3
Funktioniert Ping auf die IP?	3
Ist TCP 443 erreichbar?	4
Ist UDP 53 erreichbar?	4
Kommt der TCP-Handshake zustande?	4
Läuft die Webanwendung korrekt?	7

Merksatz:

```
IP-Erreichbarkeit = Schicht 3.
Port-Erreichbarkeit = Schicht 4.
```

TCP

TCP steht für:

```
Transmission Control Protocol
```

TCP ist:

```
verbindungsorientiert
zuverlässig
reihenfolgetreu
bestätigungsbasiert
```

TCP sorgt dafür, dass Daten vollständig und in richtiger Reihenfolge bei der Anwendung ankommen.

Merksatz:

```
TCP = zuverlässig und verbindungsorientiert.
```

UDP

UDP steht für:

```
User Datagram Protocol
```

UDP ist:

```
verbindungslos
schlank
schnell
ohne eingebaute Zustellgarantie
```

UDP sendet Datagramme ohne vorherigen Verbindungsaufbau.

Merksatz:

> UDP = schnell und verbindungslos.

TCP und UDP vergleichen

Merkmal	TCP	UDP
Verbindungsaufbau	ja	nein
Verbindung	verbindungsorientiert	verbindungslos
Zustellgarantie	ja	nein
Reihenfolge	wird sichergestellt	nicht sichergestellt
Bestätigungen	ja	nein
erneute Übertragung	ja	nein
Overhead	höher	geringer
Datenform	Segment	Datagramm

Merksatz:

> TCP kontrolliert.
> UDP sendet schlank.

Verbindungsorientiert

Verbindungsorientiert bedeutet:

> Vor der Datenübertragung wird eine Verbindung aufgebaut.

TCP arbeitet verbindungsorientiert.

Der Verbindungsaufbau erfolgt mit:

> SYN
> SYN-ACK
> ACK

Merksatz:

Verbindungsorientiert = Verbindung vor Datenübertragung.

Verbindungslos

Verbindungslos bedeutet:

Es wird keine feste Verbindung aufgebaut.

UDP sendet direkt ein Datagramm an Ziel-IP und Ziel-Port.

UDP prüft nicht selbst:

ob das Datagramm angekommen ist
ob die Reihenfolge stimmt
ob eine erneute Übertragung nötig ist

Merksatz:

Verbindungslos = senden ohne Handshake.

TCP-Drei-Wege-Handshake

Der TCP-Verbindungsaufbau besteht aus drei Schritten.

Schritt	Richtung	Bedeutung
1	Client → Server	SYN
2	Server → Client	SYN-ACK
3	Client → Server	ACK

Nach dem dritten Schritt ist die TCP-Verbindung aufgebaut.

Merksatz:

TCP-Handshake = SYN, SYN-ACK, ACK.

SYN

SYN steht für:

```
Synchronize
```

SYN startet den TCP-Verbindungsaufbau.

Vereinfacht sagt der Client:

```
Ich möchte eine Verbindung aufbauen.
```

Merksatz:

```
SYN = Start der TCP-Verbindung.
```

SYN-ACK

SYN-ACK ist die Antwort des Servers auf das SYN.

Der Server sagt vereinfacht:

```
Ich habe deine Anfrage erhalten
und bin bereit.
```

Merksatz:

```
SYN-ACK = Antwort und Bestätigung.
```

ACK

ACK steht für:

```
Acknowledgement
```

ACK bedeutet:

```
Bestätigung
```

Der Client bestätigt damit das SYN-ACK des Servers.

Merksatz:

```
ACK = Bestätigung.
```

TCP-Zuverlässigkeit

TCP bietet Zuverlässigkeit durch:

```
- Sequenznummern
- Bestätigungsnummern
- ACKs
- erneute Übertragung
- Reihenfolgesicherung
- Flusskontrolle
- Staukontrolle
```

Dadurch eignet sich TCP gut für Daten, die vollständig und korrekt ankommen müssen.

Merksatz:

```
TCP nutzt mehrere Mechanismen für zuverlässigen Transport.
```

Sequenznummern

Sequenznummern helfen TCP, Daten in die richtige Reihenfolge zu bringen.

Sie zeigen:

```
an welcher Stelle im Datenstrom ein Teil gehört.
```

Damit kann TCP erkennen:

```
Daten fehlen.
Daten kamen doppelt.
Daten kamen in falscher Reihenfolge.
```

Merksatz:

```
Sequenznummer = Position im TCP-Datenstrom.
```

Bestätigungen

TCP bestätigt empfangene Daten mit ACKs.

Der Empfänger teilt dem Sender mit:

```
welche Daten angekommen sind
und
welche Daten als Nächstes erwartet werden.
```

Wenn eine Bestätigung fehlt, können Daten erneut gesendet werden.

Merksatz:

```
TCP bestätigt empfangene Daten.
```

Retransmission

Retransmission bedeutet:

```
erneute Übertragung
```

TCP sendet Daten erneut, wenn sie vermutlich verloren gegangen sind.

Mögliche Ursachen:

```
- Paketverlust
- Timeout
- beschädigte Daten
- Überlastung
- schlechte Verbindung
```

Merksatz:

```
Retransmission = TCP sendet erneut.
```

Flusskontrolle

Flusskontrolle schützt den Empfänger.

Der Empfänger signalisiert, wie viele Daten er aufnehmen kann.

Dadurch soll der Sender den Empfänger nicht überlasten.

Merksatz:

```
Flusskontrolle schützt den Empfänger.
```

Staukontrolle

Staukontrolle schützt das Netzwerk.

TCP kann die Sendeleistung anpassen, wenn Paketverlust oder Überlastung erkannt wird.

Ziel:

```
Das Netzwerk soll nicht weiter überlastet werden.
```

Merksatz:

```
Staukontrolle schützt das Netzwerk.
```

TCP-Verbindungsabbau

TCP-Verbindungen können geordnet beendet werden.

Wichtige Steuerbits:

```
FIN
ACK
```

FIN bedeutet:

```
Verbindung geordnet beenden.
```

RST bedeutet:

Verbindung sofort abbrechen.

Merksatz:

FIN beendet geordnet.
RST bricht sofort ab.

TCP-Zustände

Wichtige TCP-Zustände:

Zustand	Bedeutung
LISTEN	Dienst wartet auf eingehende Verbindung
SYN-SENT	Client hat SYN gesendet
SYN-RECEIVED	Server hat SYN erhalten und SYN-ACK gesendet
ESTABLISHED	Verbindung besteht
FIN-WAIT	Verbindung wird beendet
TIME-WAIT	Wartephase nach Verbindungsende
CLOSED	Verbindung ist geschlossen

Merksatz:

LISTEN = Dienst wartet.
ESTABLISHED = Verbindung steht.

TCP-Segment

Die Datenform von TCP auf Schicht 4 heißt:

Segment

Ein TCP-Segment enthält unter anderem:

- Quell-Port
- Ziel-Port
- Sequenznummer

- Bestätigungsnummer
- Steuerbits
- Prüfsumme
- Nutzdaten

Merksatz:

TCP arbeitet mit Segmenten.

UDP-Datagramm

Die Datenform von UDP auf Schicht 4 heißt:

Datagramm

Ein UDP-Datagramm enthält unter anderem:

- Quell-Port
- Ziel-Port
- Länge
- Prüfsumme
- Nutzdaten

Merksatz:

UDP arbeitet mit Datagrammen.

Segment und Datagramm unterscheiden

Protokoll	Datenform
TCP	Segment
UDP	Datagramm

Prüfungsfalle:

In der Umgangssprache sagt man oft „Paket“.
Fachlich ist TCP auf Schicht 4 ein Segment.

UDP auf Schicht 4 ist ein Datagramm.

Merksatz:

TCP = Segment.
UDP = Datagramm.

Ports

Ein Port ist eine logische Dienstnummer auf Schicht 4.

Ports unterscheiden Dienste auf einem Gerät.

Beispiel:

192.168.10.50:22
192.168.10.50:80
192.168.10.50:443

Gleiche IP-Adresse, aber unterschiedliche Dienste.

Merksatz:

Port = Dienstnummer.

Port ist nicht gleich Switch-Port

Begriff	Bedeutung	Schicht
Switch-Port	physischer Anschluss	1 / 2
TCP-Port	logische Dienstnummer	4
UDP-Port	logische Dienstnummer	4

Merksatz:

Switch-Port = physisch.
TCP-/UDP-Port = logisch.

Portnummern

Portnummern gehen von:

```
0
```

bis:

```
65535
```

Grund:

```
Ports sind 16 Bit groß.
```

16 Bit ermöglichen:

```
65536 Werte
```

Merksatz:

```
Portnummern = 0 bis 65535.
```

Portbereiche

Bereich	Portnummern	Bedeutung
Well-Known Ports	0 – 1023	bekannte Standarddienste
Registered Ports	1024 – 49151	registrierte Anwendungsports
Dynamic / Ephemeral Ports	49152 – 65535	temporäre Client-Ports

Merksatz:

```
Well-Known = bekannt.
Ephemeral = temporär.
```

Quell-Port und Ziel-Port

Ein TCP- oder UDP-Header enthält:

```
Quell-Port
Ziel-Port
```

Beispiel HTTPS:

```
Client:
192.168.10.20:52344

Server:
93.184.216.34:443
```

Dabei gilt:

```
Ziel-Port 443 = HTTPS-Dienst
Quell-Port 52344 = temporärer Client-Port
```

Merksatz:

```
Ziel-Port zeigt den Dienst.
Quell-Port hilft bei der Rückzuordnung.
```

Socket

Ein Socket besteht aus:

```
IP-Adresse
und
Port
```

Beispiel:

```
192.168.10.20:52344
```

Eine TCP-Verbindung wird eindeutig durch folgende Kombination:

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

Merksatz:

```
Socket = IP-Adresse plus Port.
```

TCP-Port und UDP-Port getrennt betrachten

Die gleiche Portnummer kann bei TCP und UDP getrennt existieren.

Beispiel:

```
TCP 53
UDP 53
```

Beide können DNS betreffen, sind aber technisch unterschiedliche Transportwege.

Eine Firewall-Regel für TCP 53 erlaubt nicht automatisch UDP 53.

Merksatz:

```
Portnummer immer mit TCP oder UDP nennen.
```

Wichtige Standardports

Dienst	Protokoll	Port
FTP Steuerverbindung	TCP	21
SSH	TCP	22
Telnet	TCP	23
SMTP	TCP	25
DNS	TCP / UDP	53
DHCP Server	UDP	67
DHCP Client	UDP	68

Dienst	Protokoll	Port
HTTP	TCP	80
POP3	TCP	110
NTP	UDP	123
IMAP	TCP	143
HTTPS	TCP	443
IMAPS	TCP	993
POP3S	TCP	995
RDP	TCP	3389

Merksatz:

```
HTTP 80,
HTTPS 443,
SSH 22,
DNS 53,
DHCP 67/68.
```

DNS

DNS nutzt häufig:

```
UDP 53
```

DNS kann aber auch nutzen:

```
TCP 53
```

Beispiele für TCP bei DNS:

```
- große Antworten
- Zonentransfers
- bestimmte DNSSEC-Fälle
```

Merksatz:

DNS = UDP 53 häufig,
TCP 53 ebenfalls möglich.

DHCP

DHCP nutzt UDP.

Wichtige Ports:

Rolle	Protokoll	Port
DHCP-Server	UDP	67
DHCP-Client	UDP	68

Merksatz:

DHCP = UDP 67 und 68.

HTTP und HTTPS

HTTP nutzt typischerweise:

TCP 80

HTTPS nutzt typischerweise:

TCP 443

HTTPS nutzt zusätzlich TLS für Verschlüsselung.

Merksatz:

HTTP = TCP 80.
HTTPS = TCP 443.

SSH und Telnet

SSH nutzt:

TCP 22

Telnet nutzt:

TCP 23

Wichtiger Unterschied:

SSH ist verschlüsselt.
Telnet ist unverschlüsselt.

Merksatz:

SSH statt Telnet verwenden.

E-Mail-Protokolle

Protokoll	Zweck	typischer Port
SMTP	E-Mail senden / transportieren	TCP 25
POP3	E-Mail abrufen	TCP 110
IMAP	E-Mail abrufen und verwalten	TCP 143
IMAPS	IMAP verschlüsselt	TCP 993
POP3S	POP3 verschlüsselt	TCP 995

Merksatz:

SMTP sendet.
POP3 und IMAP holen ab.

NTP

NTP steht für:

Network Time Protocol

Typischer Port:

```
UDP 123
```

NTP dient der Zeitsynchronisation.

Wichtig für:

```
- Zertifikate
- Kerberos
- Logs
- Monitoring
- Fehlersuche
```

Merksatz:

```
NTP = UDP 123.
```

RDP

RDP steht für:

```
Remote Desktop Protocol
```

Typischer Port:

```
TCP 3389
```

RDP dient dem grafischen Fernzugriff auf Windows-Systeme.

Wichtig:

```
RDP nicht ungeschützt direkt ins Internet öffnen.
```

Merksatz:

```
RDP = TCP 3389,
sorgfältig absichern.
```

Portstatus

Ein Port kann aus Sicht eines Clients unterschiedlich wirken.

Status	Bedeutung
offen	Dienst nimmt Verbindung an oder antwortet
geschlossen	kein Dienst lauscht auf diesem Port
gefiltert	Firewall oder Paketfilter blockiert
offen, aber Anwendung fehlerhaft	Schicht 4 erreichbar, höhere Schicht fehlerhaft

Merksatz:

> Portstatus hilft bei der Eingrenzung.

Offener Port

Ein offener Port bedeutet:

> Ein Dienst ist grundsätzlich erreichbar.

Aber ein offener Port beweist nicht:

> dass die Anwendung korrekt funktioniert
> dass Login klappt
> dass Zertifikate stimmen
> dass keine Fehler in der Anwendung bestehen

Merksatz:

> Offener Port = Transport zum Dienst möglich.

Geschlossener Port

Ein geschlossener Port bedeutet:

> Kein Dienst lauscht auf diesem Port.

Der Host kann trotzdem erreichbar sein.

Beispiel:

```
Ping funktioniert.
TCP 22 geschlossen.
```

Dann ist der Host erreichbar, aber SSH läuft dort nicht oder nicht auf Port 22.

Merksatz:

```
Geschlossener Port heißt nicht:
Gerät offline.
```

Gefilterter Port

Ein gefilterter Port bedeutet häufig:

```
Firewall oder Paketfilter blockiert.
```

Typisches Verhalten:

```
Timeout
keine klare Antwort
Verbindung hängt
```

Merksatz:

```
Gefiltert = oft Firewall im Weg.
```

Firewall-Regeln auf Schicht 4

Firewalls nutzen häufig Ports.

Eine vollständige Regel enthält idealerweise:

```
- Quelle
- Ziel
```

- Protokoll
- Port
- Richtung
- Aktion
- Kommentar oder Zweck

Beispiel:

Quelle:
Mitarbeiter-Netz

Ziel:
Internet

Protokoll:
TCP

Port:
443

Aktion:
erlauben

Merksatz:

Firewall-Regel = Quelle, Ziel, Protokoll, Port, Aktion.

Portweiterleitung

Portweiterleitung bedeutet:

Ein externer Port wird an ein internes Ziel weitergeleitet.

Beispiel:

öffentlich:
93.184.100.10:443

intern:
192.168.10.50:443

Wichtig:

Protokoll muss stimmen.
Ziel-IP muss stimmen.
Dienst muss laufen.
Firewall muss erlauben.

Merksatz:

Portweiterleitung braucht richtige IP,
richtigen Port,
richtiges Protokoll
und laufenden Dienst.

NAT/PAT und Ports

PAT nutzt Ports, um Verbindungen zu unterscheiden.

Beispiel:

Intern	Extern
192.168.10.20:52344	93.184.100.10:40001
192.168.10.30:52344	93.184.100.10:40002

Dadurch können mehrere interne Geräte dieselbe öffentliche IP-Adresse nutzen.

Merksatz:

PAT unterscheidet Verbindungen über Ports.

TCP und UDP bei NAT/PAT

Bei TCP kann ein NAT-Gerät Verbindungszustände gut verfolgen.

Bei UDP gibt es keinen echten Verbindungsaufbau.

Deshalb arbeitet NAT bei UDP häufig mit Zeitfenstern und Zuordnungstabellen.

Wenn eine Zuordnung abläuft, können Antworten verloren gehen.

Merksatz:

```
NAT verfolgt TCP leichter als UDP.
```

Ping und Porttest unterscheiden

Ping nutzt ICMP.

ICMP nutzt keine TCP- oder UDP-Ports.

Deshalb gilt:

```
Ping prüft IP-Erreichbarkeit,
aber keinen Dienst-Port.
```

Beispiel:

```
Ping funktioniert.
```

Das beweist nicht:

```
TCP 443 ist offen.
```

Merksatz:

```
Ping prüft Schicht 3.
Porttest prüft Schicht 4.
```

Typische Schicht-4-Fehler

Typische Fehler sind:

```
- falscher Port
- falsches Protokoll TCP oder UDP
```

- Dienst läuft nicht
- Dienst lauscht auf falscher IP
- Dienst lauscht nur auf localhost
- Firewall blockiert
- TCP-Handshake scheitert
- RST
- Timeout
- Portweiterleitung falsch
- NAT/PAT-Zuordnung fehlt
- Rückweg fehlt
- UDP-Antwort kommt nicht zurück

Merksatz:

Schicht-4-Fehler betreffen Transport zum Dienst.

Fehlerbild: Ping geht, Dienst nicht

Beispiel:

ping server funktioniert.
HTTPS funktioniert nicht.

Mögliche Ursachen:

- TCP 443 geschlossen
- Firewall blockiert TCP 443
- Webserver läuft nicht
- Webserver hört auf anderem Port
- TLS- oder Anwendungsproblem
- Reverse Proxy falsch

Merksatz:

Ping geht,
Dienst nicht:
Schicht 4 und 7 prüfen.

Fehlerbild: TCP-Handshake scheitert

Der TCP-Handshake lautet:

```
SYN
SYN-ACK
ACK
```

Wenn der Handshake nicht vollständig ist, entsteht keine TCP-Verbindung.

Mögliche Ursachen:

```
- Dienst lauscht nicht
- Firewall blockiert
- Rückroute fehlt
- NAT falsch
- Server lehnt ab
- Netzwerkverlust
```

Merksatz:

```
Kein vollständiger Handshake = keine TCP-Verbindung.
```

Fehlerbild: RST

RST bedeutet:

```
Reset
```

Ein RST bricht eine TCP-Verbindung sofort ab.

Mögliche Ursachen:

```
- Port geschlossen
- Dienst lehnt Verbindung ab
- Firewall sendet Reset
- Anwendung bricht ab
- falsches Protokoll
```

Merksatz:

```
RST = aktiver TCP-Abbruch.
```

Fehlerbild: Timeout

Timeout bedeutet:

```
Eine erwartete Antwort kommt nicht rechtzeitig.
```

Mögliche Ursachen:

```
- Firewall verwirft still
- Server antwortet nicht
- Rückweg fehlt
- NAT-Zuordnung fehlt
- falsches Ziel
- Paketverlust
```

Merksatz:

```
Timeout = keine rechtzeitige Antwort.
```

Fehlerbild: UDP antwortet nicht

UDP hat keinen Handshake.

Wenn keine Antwort kommt, kann das bedeuten:

```
- Dienst läuft nicht
- UDP-Port falsch
- Firewall blockiert
- Anfrage ungültig
- Antwortweg fehlt
- NAT-Zuordnung abgelaufen
- Paketverlust
```

Merksatz:

UDP braucht Anfrage-Antwort-Prüfung.

Schicht 4 oder Schicht 7?

Beobachtung	eher Ursache
TCP-Verbindung kommt nicht zustande	Schicht 4 / Firewall
TCP-Port offen, aber Login scheitert	Anwendung / Authentifizierung
TCP 443 offen, aber Zertifikatsfehler	Darstellung / Anwendung
DNS-Port erreichbar, aber falsche Antwort	DNS-Konfiguration
Webserver antwortet mit Fehler 500	Anwendung
SSH-Port offen, aber Schlüssel abgelehnt	Benutzer / Schlüssel / Rechte

Merksatz:

Port erreichbar bedeutet:
Transport ist möglich,
Anwendung muss trotzdem geprüft werden.

Was Schicht 4 nicht macht

Schicht 4 macht nicht:

- IP-Adressen vergeben
- Routing zwischen Netzen durchführen
- MAC-Adressen auflösen
- DNS-Namen auflösen
- Webseiten bereitstellen
- Benutzer authentifizieren
- Zertifikate prüfen
- Inhalte interpretieren
- Dateirechte verwalten

Merksatz:

Schicht 4 transportiert,
interpretiert aber keine Anwendung.

Prüfungswissen: wichtigste Zuordnungen

Begriff	richtige Einordnung
TCP	Schicht 4
UDP	Schicht 4
Port	Schicht 4
TCP-Handshake	Schicht 4
Segment	TCP auf Schicht 4
Datagramm	UDP auf Schicht 4
Socket	Schicht 4 mit IP-Bezug
ICMP	Schicht 3
IP-Adresse	Schicht 3
Routing	Schicht 3
DNS	Schicht 7, nutzt TCP/UDP 53
HTTP	Schicht 7, nutzt TCP 80
HTTPS	Schicht 7, nutzt TCP 443
DHCP	Schicht 7, nutzt UDP 67/68

Merksatz:

```
TCP, UDP und Ports = Schicht 4.
```

Typische IHK-Fragen

In AP1 und AP2 kann zum Beispiel gefragt werden:

```
- Welche Aufgabe hat die Transportschicht?
- Was ist TCP?
- Was ist UDP?
- Was ist der Unterschied zwischen TCP und UDP?
- Was bedeutet verbindungsorientiert?
- Was bedeutet verbindungslos?
- Wie funktioniert der TCP-Drei-Wege-Handshake?
- Was ist ein Port?
- Warum braucht man Ports?
```

- Was ist ein Socket?
- Welche Portbereiche gibt es?
- Welche Standardports sollte man kennen?
- Warum nutzt DNS TCP und UDP?
- Warum nutzt DHCP UDP?
- Warum reicht Ping nicht als Diensttest?
- Was bedeutet offener, geschlossener oder gefilterter Port?
- Warum muss eine Firewall TCP und UDP unterscheiden?

Typische Prüfungsfallen

TCP gehört zu Schicht 4.

UDP gehört zu Schicht 4.

Ports gehören zu Schicht 4.

ICMP nutzt keine Ports.

Ping ist kein Porttest.

TCP ist verbindungsorientiert.

UDP ist verbindungslos.

TCP-Handshake = SYN, SYN-ACK, ACK.

TCP nutzt Segmente.

UDP nutzt Datagramme.

TCP-Port und UDP-Port sind getrennt.

Gleiche Portnummer bedeutet nicht gleiches Protokoll.

DNS nutzt UDP 53 und TCP 53.

DHCP nutzt UDP 67 und 68.

HTTP nutzt TCP 80.

HTTPS nutzt TCP 443.

SSH nutzt TCP 22.

RDP nutzt TCP 3389.

Offener Port heißt nicht automatisch:
Anwendung funktioniert.

Geschlossener Port heißt nicht:
Gerät offline.

Gefilterter Port heißt oft:
Firewall im Weg.

Wichtige Begriffe kurz erklärt

Begriff	Kurze Erklärung
Transportschicht	OSI-Schicht 4
TCP	zuverlässiges, verbindungsorientiertes Transportprotokoll
UDP	verbindungsloses Transportprotokoll
Port	logische Dienstnummer
TCP-Port	Dienstnummer für TCP
UDP-Port	Dienstnummer für UDP
Socket	IP-Adresse plus Port
Segment	TCP-Dateneinheit
Datagramm	UDP-Dateneinheit
SYN	Start des TCP-Verbindungsaufbaus
SYN-ACK	Antwort und Bestätigung auf SYN
ACK	Bestätigung
RST	sofortiger TCP-Abbruch
FIN	geordneter TCP-Abbau
Timeout	Antwort bleibt zu lange aus
Retransmission	erneute Übertragung

Begriff	Kurze Erklärung
LISTEN	Dienst wartet auf Verbindung
ESTABLISHED	Verbindung besteht
Well-Known Port	Port 0 bis 1023
Ephemeral Port	temporärer Client-Port
Portweiterleitung	externer Port wird intern weitergeleitet
gefilterter Port	Firewall oder Paketfilter blockiert

IHK-sichere Gesamtformulierung

Die Transportschicht ist Schicht 4 des OSI-Modells. Sie sorgt für den Transport von Daten zwischen Anwendungen auf Endgeräten. Dafür werden vor allem TCP, UDP und Ports verwendet. TCP ist verbindungsorientiert und zuverlässig, baut eine Verbindung über SYN, SYN-ACK und ACK auf und nutzt Bestätigungen, Sequenznummern und erneute Übertragung. UDP ist verbindungslos, schlanker und bietet keine eingebaute Zustellgarantie. Ports dienen dazu, Dienste auf einem Gerät zu unterscheiden. Eine IP-Adresse zeigt zum Gerät, der Port zeigt zum Dienst. TCP- und UDP-Ports sind getrennt zu betrachten.

Wichtigste Merksätze

```
Schicht 4 = Transportschicht.

Schicht 4 = TCP, UDP und Ports.

IP bringt zum Gerät.

Port bringt zum Dienst.

Port = logische Dienstnummer.

Switch-Port ist physisch.

TCP-Port ist logisch.

TCP = verbindungsorientiert.

UDP = verbindungslos.

TCP = zuverlässig.
```

UDP = schlank und schnell.

TCP-Handshake = SYN, SYN-ACK, ACK.

TCP nutzt ACKs.

TCP nutzt Sequenznummern.

TCP kann erneut übertragen.

TCP stellt Reihenfolge sicher.

UDP hat keinen Handshake.

UDP bietet keine eingebaute Zustellgarantie.

TCP = Segment.

UDP = Datagramm.

Portnummern gehen von 0 bis 65535.

Well-Known Ports = 0 bis 1023.

Ephemeral Ports = temporäre Client-Ports.

Ziel-Port zeigt den Dienst.

Quell-Port hilft bei der Rückzuordnung.

Socket = IP-Adresse plus Port.

HTTP = TCP 80.

HTTPS = TCP 443.

SSH = TCP 22.

DNS = UDP 53 und TCP 53.

DHCP = UDP 67 und 68.

NTP = UDP 123.

RDP = TCP 3389.

Ping nutzt ICMP,
nicht TCP oder UDP.

Ping ist kein Porttest.

IP erreichbar = Schicht 3.

Port erreichbar = Schicht 4.

Anwendung korrekt = höhere Schicht.

Offener Port heißt nicht automatisch sicher.

Firewall-Regel braucht Quelle, Ziel, Protokoll und Port.

Portweiterleitung braucht richtige IP,
richtigen Port
und richtiges Protokoll.