20.6 Trainer – Schicht 4 / TCP, UDP, Ports und Schicht 4

Diese Trainer-Seite wiederholt die OSI-Schicht 4, TCP, UDP, Ports und typische Fehlerbilder auf der Transportschicht.

Ziel ist, Prüfungsfragen zu zuverlässiger Übertragung, verbindungsloser Übertragung, Portnummern, Dienstzuordnung und Firewall-Fehlersuche sicher zu beantworten.

Merksatz:

```
Schicht 4 fragt:
Ist der richtige Dienst über den richtigen Port erreichbar?
```

Lernziele

Nach dieser Seite solltest du sicher können:

```
- OSI-Schicht 4 einordnen
- TCP und UDP unterscheiden
- Ports erklären
- Quellport und Zielport unterscheiden
- wichtige Standardports nennen
- TCP-Verbindungsaufbau erklären
- typische TCP-Status einordnen
- Portprobleme erkennen
- erklären,
  warum ping keinen Porttest ersetzt
```

Kurzüberblick: OSI-Schicht 4

OSI-Schicht 4 heißt:

```
Transportschicht
```

Aufgabe:

Ende-zu-Ende-Kommunikation zwischen Anwendungen ermöglichen.

Typische Begriffe:

TCP

UDP

Port

Segment

Datagramm

Verbindungsaufbau

Three-Way Handshake

LISTEN

ESTABLISHED

Merksatz:

Schicht 4 ordnet Netzwerkverkehr dem richtigen Dienst zu.

TCP kurz erklärt

TCP steht für:

Transmission Control Protocol

Eigenschaften:

verbindungsorientiert

zuverlässig

```
bestätigt Daten

stellt Reihenfolge sicher

sendet verlorene Daten erneut

nutzt Ports
```

Typische Dienste:

```
HTTPS

SSH

SMTP

IMAP

SMB

RDP
```

Merksatz:

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

UDP kurz erklärt

UDP steht für:

```
User Datagram Protocol
```

Eigenschaften:

```
verbindungslos

schnell
```

```
wenig Overhead

keine eingebaute Zustellgarantie

keine eingebaute Reihenfolgegarantie

nutzt Ports
```

Typische Dienste:

```
DNS

DHCP

NTP

SNMP

VoIP

Streaming
```

Merksatz:

```
UDP = schnell,
schlank
und verbindungslos.
```

Aufgabe 1

Wie heißt OSI-Schicht 4?

Antwort anzeigen

OSI-Schicht 4 heißt:

Transportschicht

Englisch:

Transport Layer

Aufgabe:

Kommunikation zwischen Anwendungen oder Prozessen über Ports ermöglichen.

Merksatz:

Schicht 4 = TCP,
UDP
und Ports.

Aufgabe 2

Welche Protokolle gehören typisch zu OSI-Schicht 4?

A: TCP und UDP

B: IP und ICMP

C: Ethernet und ARP

D: HTTP und DNS

Antwort anzeigen

Richtig ist:

A: TCP und UDP

Begründung:

```
TCP und UDP sind Transportprotokolle
und gehören zur OSI-Schicht 4.
```

Merksatz:

```
TCP und UDP = Transportschicht.
```

Aufgabe 3

Was ist ein Port?

Antwort anzeigen

Ein Port ist eine logische Nummer, mit der ein Dienst oder Prozess auf einem Host angesprochen wird.

Beispiel:

```
192.168.1.10:443
```

Bedeutung:

```
Host:
192.168.1.10

Dienst:
Port 443
```

Merksatz:

```
IP findet den Host.
Port findet den Dienst.
```

Aufgabe 4

Welche OSI-Schicht ist für Portnummern zuständig?

Antwort anzeigen

Portnummern gehören zu:

```
OSI-Schicht 4
```

Begründung:

```
Ports werden von TCP und UDP genutzt,
um Daten dem richtigen Dienst oder Prozess zuzuordnen.
```

Merksatz:

```
Ports = Schicht 4.
```

Aufgabe 5

Was ist der Unterschied zwischen IP-Adresse und Port?

Antwort anzeigen

IP-Adresse:

```
identifiziert den Host logisch im Netzwerk
```

Port:

```
identifiziert den Dienst oder Prozess auf diesem Host
```

Beispiel:

```
192.168.1.10:22

192.168.1.10 = Host
```

```
22 = SSH-Dienst
```

Merksatz:

```
IP = welcher Rechner?
Port = welcher Dienst?
```

Aufgabe 6

Was ist der Unterschied zwischen Quellport und Zielport?

Antwort anzeigen

Quellport:

```
Port auf dem sendenden System

beim Client oft dynamisch
```

Zielport:

```
Port des angesprochenen Dienstes auf dem Server
```

Beispiel:

```
Client:
192.168.1.50:52344

Server:
93.184.216.34:443
```

Hier ist 52344 der Quellport und 443 der Zielport.

Merksatz:

```
Zielport zeigt meistens den Dienst.
```

Aufgabe 7

Welche Aussage ist richtig?

A: TCP ist verbindungslos.

B: UDP garantiert die Reihenfolge der Pakete.

C: TCP ist verbindungsorientiert und zuverlässig.

D: Ports gehören zu OSI-Schicht 3.

Antwort anzeigen

Richtig ist:

C: TCP ist verbindungsorientiert und zuverlässig.

Begründung:

TCP baut eine Verbindung auf,
bestätigt Daten
und kann verlorene Daten erneut übertragen.

Merksatz:

TCP = zuverlässig.

Aufgabe 8

Welche Aussage ist richtig?

A: UDP ist immer besser als TCP.

B: UDP ist verbindungslos und hat wenig Overhead.

C: UDP baut immer einen Three-Way Handshake auf.

D: UDP nutzt keine Ports.

Antwort anzeigen

Richtig ist:

B: UDP ist verbindungslos und hat wenig Overhead.

Begründung:

UDP verzichtet auf einen Verbindungsaufbau
und auf eingebaute Zustellgarantien.
Dadurch ist es schlanker und schneller,
aber weniger zuverlässig als TCP.

Merksatz:

UDP = verbindungslos und schlank.

Aufgabe 9

Vergleiche TCP und UDP.

Merkmal	TCP	UDP
Verbindung	?	?
Zuverlässigkeit	?	?
Overhead	?	?
Beispiel	?	?

Antwort anzeigen

Merkmal	TCP	UDP
Verbindung	verbindungsorientiert	verbindungslos

Merkmal	TCP	UDP
Zuverlässigkeit	eingebaut	keine eingebaute Garantie
Overhead	höher	geringer
Beispiel	HTTPS, SSH, SMB	DNS, DHCP, VoIP

Merksatz:

```
TCP für zuverlässige Übertragung.
UDP für schnelle und schlanke Kommunikation.
```

Aufgabe 10

Was ist der TCP Three-Way Handshake?

Antwort anzeigen

Der TCP Three-Way Handshake ist der Verbindungsaufbau bei TCP.

Ablauf:

```
1. SYN

2. SYN-ACK

3. ACK
```

Bedeutung:

```
Client fragt Verbindung an.

Server bestätigt und antwortet.

Client bestätigt die Verbindung.
```

Merksatz:

```
TCP startet mit SYN,
SYN-ACK,
ACK.
```

Aufgabe 11

Warum hat TCP mehr Overhead als UDP?

Antwort anzeigen

TCP hat mehr Overhead, weil es zusätzliche Funktionen bietet.

Dazu gehören:

```
Verbindungsaufbau

Bestätigungen

Sequenznummern

erneute Übertragung

Reihenfolgeprüfung

Flusskontrolle
```

Merksatz:

```
TCP ist aufwendiger,
weil es Zuverlässigkeit bietet.
```

Aufgabe 12

Warum wird UDP häufig für DNS verwendet?

Antwort anzeigen

DNS-Anfragen sind oft klein und sollen schnell beantwortet werden.

UDP ist dafür geeignet, weil es wenig Overhead hat und keinen TCP-Verbindungsaufbau benötigt.

Wichtig:

```
DNS kann bei Bedarf auch TCP 53 nutzen.
```

Merksatz:

```
DNS nutzt häufig UDP 53,
aber TCP 53 nicht vergessen.
```

Aufgabe 13

Warum eignet sich UDP für VoIP?

Antwort anzeigen

Bei VoIP ist geringe Verzögerung wichtig.

Ein verlorenes Sprachpaket ist meist weniger schlimm als eine stark verspätete Übertragung.

UDP ist dafür geeignet, weil es schnell und verbindungslos arbeitet.

Merksatz:

```
VoIP braucht geringe Latenz,
daher ist UDP sinnvoll.
```

Aufgabe 14

Ordne zu.

Dienst	TCP oder UDP?	Port

SSH	?	?
HTTPS	?	?
DNS	?	?
DHCP Server	?	?
RDP	?	?
SMB	?	?

Antwort anzeigen

Dienst	TCP oder UDP?	Port
SSH	TCP	22
HTTPS	TCP	443
DNS	UDP/TCP	53
DHCP Server	UDP	67
RDP	TCP	3389
SMB	TCP	445

Merksatz:

> Portnummer immer mit TCP oder UDP lernen.

Aufgabe 15

Welchen Port nutzt SSH typischerweise?

Antwort anzeigen

SSH nutzt typischerweise:

> TCP 22

SSH steht für:

> Secure Shell

Merksatz:

```
SSH = TCP 22.
```

Aufgabe 16

Welchen Port nutzt HTTPS typischerweise?

Antwort anzeigen

HTTPS nutzt typischerweise:

```
TCP 443
```

HTTPS bedeutet:

```
HTTP über TLS
```

Merksatz:

```
HTTPS = TCP 443.
```

Aufgabe 17

Welche Ports nutzt DHCP?

Antwort anzeigen

DHCP nutzt:

```
UDP 67 für den DHCP-Server

UDP 68 für den DHCP-Client
```

Merksatz:

```
DHCP = UDP 67 und 68.
```

Aufgabe 18

Welchen Port nutzt DNS?

Antwort anzeigen

DNS nutzt:

```
UDP 53
```

und bei Bedarf:

```
TCP 53
```

Merksatz:

```
DNS = UDP/TCP 53.
```

Aufgabe 19

Welchen Port nutzt SMB typischerweise?

Antwort anzeigen

SMB nutzt typischerweise:

```
TCP 445
```

SMB wird genutzt für:

```
Datei- und Druckfreigaben
```

```
Netzlaufwerke
```

Merksatz:

```
SMB = TCP 445.
```

Aufgabe 20

Welchen Port nutzt RDP typischerweise?

Antwort anzeigen

RDP nutzt typischerweise:

```
TCP 3389
```

RDP steht für:

```
Remote Desktop Protocol
```

Merksatz:

```
RDP = TCP 3389.
```

Aufgabe 21

Was bedeutet LISTEN bei TCP?

Antwort anzeigen

LISTEN bedeutet:

```
Ein Dienst wartet auf eingehende Verbindungen.
```

Beispiel:

```
Ein Webserver lauscht auf TCP 443.
```

Merksatz:

```
LISTEN = Dienst wartet auf Verbindung.
```

Aufgabe 22

Was bedeutet ESTABLISHED bei TCP?

Antwort anzeigen

ESTABLISHED bedeutet:

```
Eine TCP-Verbindung besteht.
```

Client und Server haben eine aktive Verbindung aufgebaut.

Merksatz:

```
ESTABLISHED = Verbindung besteht.
```

Aufgabe 23

Was bedeutet SYN_SENT?

Antwort anzeigen

SYN_SENT bedeutet:

```
Der Client hat einen Verbindungsaufbau gestartet
und wartet auf eine Antwort.
```

Mögliche Ursache, wenn es hängen bleibt:

```
Ziel antwortet nicht

Firewall blockiert

Dienst läuft nicht

Routingproblem
```

Merksatz:

```
SYN_SENT hängt oft bei fehlender Antwort.
```

Aufgabe 24

Ein Host ist per ping erreichbar, aber SSH funktioniert nicht.

Was ist wahrscheinlich?

Antwort anzeigen

Ping prüft ICMP. SSH nutzt TCP 22.

Mögliche Ursachen:

```
TCP 22 blockiert

SSH-Dienst läuft nicht

SSH lauscht auf anderem Port

Firewall blockiert

Zugriff nur aus bestimmten Netzen erlaubt

Benutzer oder Schlüssel falsch
```

Merksatz:

Host erreichbar heißt nicht,
dass der Dienst erreichbar ist.

Aufgabe 25

Ein Webserver antwortet nicht auf HTTPS, ping funktioniert aber.

Was sollte geprüft werden?

Antwort anzeigen

Zu prüfen:

TCP 443 erreichbar?

Webserver läuft?

Dienst lauscht auf Port 443?

Firewall erlaubt TCP 443?

Reverse Proxy korrekt?

TLS-Zertifikat korrekt?

Anwendung fehlerfrei?

Merksatz:

ping geht,
HTTPS nicht:
TCP 443,
Dienst
und Firewall prüfen.

Aufgabe 26

Warum ersetzt ping keinen Porttest?

Antwort anzeigen

ping prüft ICMP-Erreichbarkeit.

ping prüft nicht:

```
TCP 22

TCP 443

TCP 445

UDP 53

Dienststatus

Anmeldung

Rechte

Anwendung
```

Merksatz:

```
ping prüft Host-Erreichbarkeit,
nicht Dienstfunktion.
```

Aufgabe 27

Welche Angaben braucht man für eine saubere Firewall-Regel?

Antwort anzeigen

Eine saubere Firewall-Regel enthält:

Quelle

Ziel

Protokoll

Port

Richtung

Aktion

Zweck

Beispiel:

Quelle:
Adminnetz

Ziel:
Server

Protokoll:
TCP

Port:
22

Aktion:
erlauben

Zweck:
SSH-Administration

Merksatz:

```
Firewall-Regeln brauchen Quelle,
Ziel,
Port
und Protokoll.
```

Aufgabe 28

Warum ist die Angabe „Port 53 erlauben“ ungenau?

Antwort anzeigen

Die Angabe ist ungenau, weil nicht klar ist, ob TCP 53, UDP 53 oder beides gemeint ist.

Bei DNS ist wichtig:

```
UDP 53 für normale Abfragen

TCP 53 für große Antworten,
Zonentransfers
oder bestimmte Spezialfälle
```

Merksatz:

```
Portnummer ohne TCP oder UDP ist unvollständig.
```

Aufgabe 29

Was ist ein Well-Known Port?

Antwort anzeigen

Well-Known Ports sind bekannte Standardports.

Bereich:

```
0 bis 1023
```

Beispiele:

```
TCP 22 SSH

TCP 80 HTTP

TCP 443 HTTPS

UDP/TCP 53 DNS
```

Merksatz:

```
Well-Known Ports sind bekannte Dienstports.
```

Aufgabe 30

Was sind dynamische oder ephemeral Ports?

Antwort anzeigen

Dynamische Ports werden häufig von Clients als Quellports verwendet.

Bereich:

```
49152 bis 65535
```

Beispiel:

```
Client nutzt Quellport 52344
und verbindet sich zu Server TCP 443.
```

Merksatz:

```
Server hat bekannten Zielport.
Client nutzt oft dynamischen Quellport.
```

Aufgabe 31

Ein Client verbindet sich zu einem Webserver.

```
Client:
192.168.1.50:52344

Server:
93.184.216.34:443
```

Welcher Port zeigt den Webdienst?

Antwort anzeigen

Der Webdienst wird durch den Zielport angezeigt:

```
TCP 443
```

Der Quellport 52344 ist ein dynamischer Clientport.

Merksatz:

```
Zielport zeigt den Dienst.
```

Aufgabe 32

Warum sollte RDP nicht direkt aus dem Internet erreichbar sein?

Antwort anzeigen

RDP ist ein häufiges Angriffsziel.

Risiken:

```
Brute-Force-Angriffe

Credential Stuffing

Exploits

unberechtigter Fernzugriff
```

Sicherer:

```
VPN

RDP-Gateway

MFA

Firewall-Beschränkung auf bekannte Quellnetze

Logging
```

Merksatz:

```
RDP nicht offen ins Internet stellen.
```

Aufgabe 33

Warum sollte SMB nicht direkt aus dem Internet erreichbar sein?

Antwort anzeigen

SMB ist für Datei- und Druckfreigaben gedacht und sollte nicht öffentlich erreichbar sein.

Risiken:

```
Datenabfluss
```

Malware-Ausbreitung

Brute Force

Ausnutzung von Schwachstellen

Zugriff auf interne Freigaben

Merksatz:

SMB gehört nicht offen ins Internet.

Aufgabe 34

Was ist der Unterschied zwischen FTP, FTPS und SFTP?

Antwort anzeigen

FTP:

klassisches File Transfer Protocol

meist TCP 21

unverschlüsselt

FTPS:

FTP mit TLS-Verschlüsselung

SFTP:

Dateiübertragung über SSH

nutzt TCP 22

Merksatz:

```
FTPS = FTP mit TLS.
SFTP = Dateiübertragung über SSH.
```

Aufgabe 35

Welche Aussage ist richtig?

```
A: SFTP nutzt normalerweise TCP 22.

B: SFTP ist dasselbe wie FTPS.

C: FTP ist immer verschlüsselt.

D: SMB nutzt UDP 53.
```

Antwort anzeigen

Richtig ist:

```
A: SFTP nutzt normalerweise TCP 22.
```

Begründung:

```
SFTP läuft über SSH
und nutzt daher typischerweise TCP 22.
```

Merksatz:

```
SFTP gehört zu SSH,
nicht zu FTPS.
```

Aufgabe 36

Ein Dienst ist auf dem Server installiert, aber von außen nicht erreichbar.

Welche Schicht-4-Prüfungen sind sinnvoll?

Antwort anzeigen

Sinnvolle Prüfungen:

```
Lauscht der Dienst auf dem erwarteten Port?

Nutzt er TCP oder UDP?

Lauscht er auf der richtigen Schnittstelle?

Blockiert die lokale Firewall?

Blockiert eine Netzwerkfirewall?

Ist NAT oder Portweiterleitung korrekt?

Gibt es Logs?
```

Merksatz:

```
Bei Dienstproblemen Port,
Protokoll,
Dienststatus
und Firewall prüfen.
```

Aufgabe 37

Ein DNS-Server antwortet nicht. Welche Portregel könnte fehlen?

Antwort anzeigen

Möglicherweise fehlt:

```
UDP 53
```

und je nach Fall auch:

```
TCP 53
```

Begründung:

```
DNS nutzt meistens UDP 53,
kann aber auch TCP 53 verwenden.
```

Merksatz:

```
DNS-Firewallregel:
UDP 53 nicht vergessen,
TCP 53 mitdenken.
```

Aufgabe 38

Welche Antwort ist besser?

Aufgabe:

```
Ein Server ist pingbar,
aber die Webseite funktioniert nicht.
Nennen Sie eine wahrscheinliche Ursache.
```

Antwort A:

```
Netzwerk kaputt.
```

Antwort B:

```
ICMP-Erreichbarkeit ist vorhanden,
aber der Webdienst auf TCP 80 oder TCP 443 könnte blockiert sein,
nicht laufen
```

oder falsch konfiguriert sein.

Antwort anzeigen

B ist besser.

Begründung:

Die Antwort unterscheidet zwischen Host-Erreichbarkeit per ICMP
und Dienst-Erreichbarkeit über TCP-Port.

Merksatz:

Fehlerbild genau nach Protokoll einordnen.

Aufgabe 39

Welche Antwort ist besser?

Aufgabe:

Warum muss man bei Firewall-Regeln TCP und UDP unterscheiden?

Antwort A:

Weil das immer so ist.

Antwort B:

TCP und UDP sind unterschiedliche Transportprotokolle.
Eine Regel für TCP 53 erlaubt nicht automatisch UDP 53.
Deshalb müssen Protokoll und Port gemeinsam angegeben werden.

Antwort anzeigen

B ist besser.

Begründung:

Die Antwort erklärt,
warum die Protokollangabe technisch relevant ist.

Merksatz:

Port plus Protokoll nennen.

Aufgabe 40

Welche Antwort ist besser?

Aufgabe:

Warum eignet sich TCP für Dateiübertragung?

Antwort A:

Weil TCP halt normal ist.

Antwort B:

TCP eignet sich,
weil es verbindungsorientiert und zuverlässig ist,
Daten bestätigt,
verlorene Daten erneut überträgt
und die Reihenfolge sicherstellt.

Antwort anzeigen

B ist besser.

Begründung:

> Die Antwort nennt die technischen Eigenschaften,
> die bei Dateiübertragung wichtig sind.

Merksatz:

> Bei Begründungen immer die passende Eigenschaft nennen.

Mini-Prüfung: schnelle Zuordnung

Frage	Antwort
Welche OSI-Schicht ist TCP?	Schicht 4
Welche OSI-Schicht ist UDP?	Schicht 4
Welche OSI-Schicht sind Ports?	Schicht 4
Wofür steht TCP?	Transmission Control Protocol
Wofür steht UDP?	User Datagram Protocol
Was ist TCP?	verbindungsorientiert und zuverlässig
Was ist UDP?	verbindungslos und schlank
Wie startet TCP?	SYN, SYN-ACK, ACK
Was bedeutet LISTEN?	Dienst wartet auf Verbindung
Was bedeutet ESTABLISHED?	Verbindung besteht
Welcher Port ist SSH?	TCP 22
Welcher Port ist HTTPS?	TCP 443
Welcher Port ist SMB?	TCP 445
Welcher Port ist RDP?	TCP 3389
Welcher Port ist DNS?	UDP/TCP 53
Welche Ports nutzt DHCP?	UDP 67 und 68

Mini-Prüfung: Fehlerbild erkennen

Fehlerbild	Wahrscheinlichstes Thema
ping geht, SSH nicht	TCP 22, SSH-Dienst, Firewall
ping geht, HTTPS nicht	TCP 443, Webdienst, Firewall, TLS
DNS antwortet nicht	UDP/TCP 53, DNS-Server, Firewall

Fehlerbild	Wahrscheinlichstes Thema
DHCP funktioniert nicht	UDP 67/68, VLAN, Relay, Scope
Dienst lauscht nicht	Dienststatus oder Portkonfiguration
Port offen, Login scheitert	Authentifizierung
Port offen, Zugriff verweigert	Autorisierung
SYN_SENT bleibt stehen	keine Antwort, Firewall, Dienst oder Routing
RDP aus Internet erreichbar	Sicherheitsrisiko
SMB öffentlich erreichbar	hohes Sicherheitsrisiko

IHK-sichere Kurzformulierung

Die OSI-Schicht 4 ist die Transportschicht. Sie sorgt dafür, dass Daten dem richtigen Dienst oder Prozess zugeordnet werden. Dafür nutzen TCP und UDP Portnummern. TCP ist verbindungsorientiert und zuverlässig. Es baut eine Verbindung über den Three-Way Handshake auf, bestätigt Daten und kann verlorene Daten erneut übertragen. UDP ist verbindungslos, schlank und hat keine eingebaute Zustellgarantie. Es eignet sich für schnelle oder zeitkritische Kommunikation wie DNS, DHCP, NTP oder VoIP. Bei der Fehlersuche muss zwischen Host-Erreichbarkeit und Dienst-Erreichbarkeit unterschieden werden. ping prüft ICMP, aber nicht, ob ein TCP- oder UDP-Port erreichbar ist.

Merksätze

Schicht 4 ist die Transportschicht.

TCP und UDP gehören zu Schicht 4.

Ports gehören zu Schicht 4.

IP findet den Host.

Port findet den Dienst.

Zielport zeigt meist den Dienst.

Quellport ist beim Client oft dynamisch.

TCP ist verbindungsorientiert.

TCP ist zuverlässig.

TCP bestätigt Daten.

TCP stellt Reihenfolge sicher.

TCP startet mit SYN,
SYN-ACK,
ACK.

UDP ist verbindungslos.

UDP ist schlank.

UDP hat keine eingebaute Zustellgarantie.

UDP ist nicht schlechter,
sondern für andere Anforderungen gebaut.

SSH nutzt TCP 22.

HTTP nutzt TCP 80.

HTTPS nutzt TCP 443.

DNS nutzt UDP und TCP 53.

DHCP nutzt UDP 67 und 68.

SMB nutzt TCP 445.

RDP nutzt TCP 3389.

LISTEN heißt:
Dienst wartet.

ESTABLISHED heißt:
Verbindung besteht.

ping ist kein Porttest.

Host erreichbar heißt nicht Dienst erreichbar.

Portnummer ohne TCP oder UDP ist unvollständig.

Firewall-Regeln brauchen Quelle,
Ziel,
Port
und Protokoll.

RDP nicht offen ins Internet stellen.

SMB nicht offen ins Internet stellen.

SFTP nutzt SSH und damit TCP 22.

FTPS ist FTP mit TLS.

Bei Dienstproblemen:
Port,
Protokoll,
Dienststatus
und Firewall prüfen.