7.4 Fehlersuche auf Schicht 4

Fehler auf OSI-Schicht 4 betreffen den Transport zwischen Anwendungen.

Dabei geht es vor allem um:

```
- TCP
- UDP
- Ports
- Verbindungsaufbau
- Verbindungszustände
- Firewall-Regeln
- Portweiterleitungen
- NAT/PAT
- Timeouts
- Resets
- Dienst-Erreichbarkeit
```

Schicht 4 liegt zwischen:

```
Schicht 3:
IP, Routing, Gateway

und

Schicht 5 bis 7:
Sitzung, Darstellung, Anwendung
```

Merksatz:

```
Schicht-4-Fehlersuche = TCP, UDP und Ports prüfen.
```

Grundidee der Schicht-4-Fehlersuche

Auf Schicht 3 prüft man:

```
Ist das Zielgerät per IP erreichbar?
```

Auf Schicht 4 prüft man:

```
Ist der gewünschte Dienst-Port erreichbar?
```

Beispiel:

```
Server per Ping erreichbar:
ja

HTTPS auf TCP 443 erreichbar:
nein
```

Dann ist die reine IP-Erreichbarkeit nicht das Problem.

Man muss TCP-Port, Firewall, Dienst oder Portweiterleitung prüfen.

Merksatz:

```
IP erreichbar heißt nicht automatisch:
Port erreichbar.
```

Schicht 3 und Schicht 4 unterscheiden

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

Merksatz:

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

Dienstinhalt = Schicht 7.

Typische Schicht-4-Fehler

Typische Fehler auf Schicht 4 sind:

- falscher Ziel-Port
- falsches Protokoll TCP statt UDP
- falsches Protokoll UDP statt TCP
- Dienst lauscht nicht
- Dienst lauscht auf anderer IP-Adresse
- Dienst lauscht auf anderem Port
- Firewall blockiert TCP oder UDP
- TCP-Handshake scheitert
- TCP Reset
- Timeout
- NAT/PAT-Zuordnung falsch
- Portweiterleitung falsch
- Rückweg fehlt
- UDP-Antwort kommt nicht zurück

Merksatz:

Schicht-4-Fehler betreffen Erreichbarkeit von TCP- oder UDP-Diensten.

Reihenfolge bei der Fehlersuche

Eine sinnvolle Reihenfolge ist:

1. Schicht 1 prüfen:
   Link, Kabel, Signal

2. Schicht 2 prüfen:
   MAC, VLAN, ARP

3. Schicht 3 prüfen:
   IP, Gateway, Routing

```
4. Schicht 4 prüfen:
   TCP, UDP, Port

5. Schicht 7 prüfen:
   Anwendung, DNS, Authentifizierung, Zertifikat
```

Merksatz:

```
Erst IP-Erreichbarkeit prüfen,
dann Port-Erreichbarkeit prüfen.
```

Fehlerbild: Ping funktioniert, Dienst funktioniert nicht

Beispiel:

```
ping server funktioniert
```

Aber:

```
Webseite über HTTPS funktioniert nicht.
```

Dann ist das Zielgerät grundsätzlich per IP erreichbar.

Mögliche Ursachen:

```
- TCP 443 geschlossen
- Firewall blockiert TCP 443
- Webserver läuft nicht
- Webserver hört auf anderem Port
- Dienst hört nur auf localhost
- Reverse Proxy falsch
- TLS-Zertifikat fehlerhaft
- Anwendung abgestürzt
```

Merksatz:

```
Ping geht,
Dienst nicht:
```

Schicht 4 und Schicht 7 prüfen.

Fehlerbild: Port geschlossen

Ein Port ist geschlossen, wenn kein Dienst auf diesem Port lauscht.

Beispiel:

```
Server erreichbar,
aber TCP 22 geschlossen.
```

Bedeutung:

```
Der Host ist erreichbar,
aber SSH läuft dort nicht
oder SSH nutzt einen anderen Port.
```

Mögliche Ursachen:

```
- Dienst nicht gestartet
- Dienst deaktiviert
- falscher Port
- Dienst hört nur auf anderer Schnittstelle
- Konfigurationsfehler
- Dienst abgestürzt
```

Merksatz:

```
Geschlossener Port heißt:
Host kann erreichbar sein,
Dienst aber nicht.
```

Fehlerbild: Port gefiltert

Ein Port wirkt gefiltert, wenn keine klare Antwort kommt.

Typisches Verhalten:

```
Timeout
keine Rückmeldung
Verbindung bleibt hängen
```

Mögliche Ursachen:

```
- Firewall verwirft Pakete
- Paketfilter blockiert
- Security-Gruppe blockiert
- NAT-Regel fehlt
- Rückroute fehlt
- Provider blockiert Port
```

Merksatz:

```
Gefilterter Port bedeutet oft:
Firewall oder Filter im Weg.
```

Fehlerbild: Port offen, Anwendung funktioniert trotzdem nicht

Ein offener Port bedeutet nur:

```
Ein Dienst nimmt Verbindungen an
oder antwortet auf Anfragen.
```

Das bedeutet nicht automatisch:

```
Anwendung ist korrekt konfiguriert.
Anmeldung funktioniert.
Zertifikat ist gültig.
Datenbank ist erreichbar.
Webanwendung läuft fehlerfrei.
```

Beispiel:

```
TCP 443 offen,
aber Webseite zeigt Fehler 500.
```

Dann ist Schicht 4 grundsätzlich erreichbar, aber die Anwendung auf höherer Schicht hat ein Problem.

Merksatz:

```
Port offen heißt nicht:
Anwendung korrekt.
```

Fehlerbild: TCP-Handshake scheitert

Der TCP-Verbindungsaufbau besteht aus:

```
SYN
SYN-ACK
ACK
```

Wenn dieser Handshake nicht vollständig zustande kommt, kann keine TCP-Verbindung aufgebaut werden.

Mögliche Ursachen:

```
- SYN kommt nicht beim Server an
- Server antwortet nicht mit SYN-ACK
- SYN-ACK kommt nicht zum Client zurück
- Firewall blockiert eine Richtung
- NAT oder Portweiterleitung falsch
- Dienst lauscht nicht
- Rückroute fehlt
```

Merksatz:

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

Fehlerbild: SYN ohne SYN-ACK

Wenn der Client SYN sendet, aber kein SYN-ACK zurückkommt, gibt es mehrere Möglichkeiten.

Mögliche Ursachen:

```
- Server nicht erreichbar
- Firewall blockiert SYN
- Firewall blockiert SYN-ACK
- Dienst lauscht nicht
- Paket geht auf dem Weg verloren
- NAT-Regel fehlt
- Rückroute fehlt
```

Wichtig:

```
Ohne Mitschnitt oder Logs sieht man oft nur einen Timeout.
```

Merksatz:

```
SYN ohne Antwort deutet oft auf Filter, Routing oder Dienstproblem hin.
```

Fehlerbild: TCP Reset

TCP Reset wird mit RST gekennzeichnet.

RST bedeutet:

```
Verbindung sofort abbrechen.
```

Mögliche Ursachen:

```
- Port geschlossen
- Dienst lehnt Verbindung ab
- Anwendung beendet Verbindung
- Firewall sendet Reset
- falsches Protokoll auf richtigem Port
- Server akzeptiert Verbindung nicht
```

Merksatz:

```
RST = Verbindung wird aktiv zurückgesetzt.
```

Fehlerbild: TCP Timeout

Timeout bedeutet:

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

Mögliche Ursachen:

```
- Firewall verwirft still
- Server antwortet nicht
- Rückweg fehlt
- NAT-Zuordnung fehlt
- Netzwerkverlust
- Dienst überlastet
- falsche Zieladresse
- falscher Port
```

Merksatz:

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

Fehlerbild: Verbindung wird langsam

Eine TCP-Verbindung kann funktionieren, aber sehr langsam sein.

Mögliche Ursachen:

```
- Paketverlust
- viele Retransmissions
- hohe Latenz
- MTU-Probleme
- Überlastung
- zu kleine TCP-Fenstergröße
- Staukontrolle greift
- Firewall oder Proxy bremst
```

Merksatz:

```
Langsame TCP-Verbindung kann Paketverlust oder MTU-Problem bedeuten.
```

Fehlerbild: TCP Retransmissions

Retransmission bedeutet:

```
TCP sendet Daten erneut.
```

Das passiert, wenn TCP annimmt, dass Daten verloren gegangen sind.

Mögliche Ursachen:

```
- Paketverlust
- Überlastung
- schlechte Verbindung
- fehlerhafte Netzkomponente
- MTU-Probleme
- Funkprobleme
- Duplex- oder Linkproblem
```

Merksatz:

```
Viele Retransmissions deuten auf Übertragungsprobleme hin.
```

Fehlerbild: UDP-Dienst antwortet nicht

UDP hat keinen Verbindungsaufbau.

Wenn ein UDP-Dienst nicht antwortet, ist die Ursache oft schwerer zu erkennen.

Mögliche Ursachen:

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

```
- Dienst antwortet nur auf bestimmte Quellen
- Paketverlust
```

Merksatz:

```
UDP-Probleme brauchen oft Logs oder Mitschnitt.
```

TCP und UDP bei Firewalls

Firewalls unterscheiden zwischen TCP und UDP.

Beispiel DNS:

```
UDP 53
TCP 53
```

Wenn nur TCP 53 erlaubt ist, funktionieren normale DNS-Anfragen über UDP möglicherweise nicht.

Wenn nur UDP 53 erlaubt ist, können große DNS-Antworten oder Zonentransfers scheitern.

Merksatz:

```
Firewall-Regel muss Protokoll und Port korrekt enthalten.
```

Fehlerbild: Falsches Protokoll

Ein häufiger Fehler ist:

```
TCP erlaubt,
aber Dienst nutzt UDP
```

Oder:

```
UDP weitergeleitet,
aber Dienst nutzt TCP
```

Beispiel:

DNS benötigt häufig UDP 53.
Nur TCP 53 wurde freigegeben.

Folge:

DNS funktioniert nicht oder nur teilweise.

Merksatz:

Richtige Portnummer reicht nicht,
TCP oder UDP muss ebenfalls stimmen.

Fehlerbild: Portweiterleitung funktioniert nicht

Eine Portweiterleitung leitet einen externen Port an ein internes Ziel weiter.

Mögliche Fehler:

- falscher externer Port
- falscher interner Port
- falsche interne IP-Adresse
- falsches Protokoll TCP/UDP
- Dienst läuft intern nicht
- Firewall blockiert am Router
- Firewall blockiert am Server
- CGNAT beim Provider
- DNS zeigt auf falsche öffentliche IP
- Hairpin NAT fehlt bei internem Test

Merksatz:

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

Fehlerbild: Dienst hört nur auf localhost

Ein Dienst kann so konfiguriert sein, dass er nur lokal erreichbar ist.

Beispiel:

```
Dienst hört auf:
127.0.0.1:8080
```

Dann ist er nur vom eigenen Gerät aus erreichbar.

Von anderen Geräten im Netzwerk funktioniert der Zugriff nicht.

Richtig wäre je nach Bedarf zum Beispiel:

```
0.0.0.0:8080
oder
konkrete Server-IP:8080
```

Merksatz:

```
localhost bedeutet:
nur lokal auf dem eigenen Gerät.
```

Fehlerbild: Dienst hört auf falscher Schnittstelle

Ein Server kann mehrere IP-Adressen haben.

Beispiel:

```
192.168.10.50
10.0.0.50
```

Ein Dienst kann nur auf einer dieser Adressen lauschen.

Wenn Clients die andere IP-Adresse nutzen, ist der Dienst dort nicht erreichbar.

Merksatz:

```
Dienst muss auf der richtigen IP-Adresse lauschen.
```

Fehlerbild: Dienst nutzt anderen Port

Ein Dienst kann auf einem anderen Port konfiguriert sein als erwartet.

Beispiele:

```
Weboberfläche auf TCP 8080 statt TCP 80
HTTPS auf TCP 8443 statt TCP 443
SSH auf TCP 2222 statt TCP 22
```

Dann schlägt der Zugriff auf den Standardport fehl.

Merksatz:

```
Standardport prüfen,
aber tatsächliche Dienstkonfiguration beachten.
```

Fehlerbild: Firewall auf dem Server blockiert

Auch wenn Netzwerk und Router korrekt sind, kann die lokale Firewall auf dem Server blockieren.

Mögliche Systeme:

```
Windows Defender Firewall
Linux-Firewall
Host-Firewall
Sicherheitssoftware
Cloud-Security-Groups
```

Typische Prüfung:

```
Ist der Dienst lokal erreichbar?
Ist der Port auf dem Server erlaubt?
Darf die Client-Quelle zugreifen?
```

Merksatz:

```
Nicht nur Netzwerk-Firewall prüfen,
auch Host-Firewall prüfen.
```

Fehlerbild: Stateful Firewall blockiert

Eine Stateful Firewall merkt sich Verbindungszustände.

Bei TCP kann sie den Handshake und bestehende Verbindungen verfolgen.

Probleme entstehen bei:

```
- asymmetrischem Routing
- fehlender Rückroute
- NAT über anderen Weg
- ungültigen TCP-Zuständen
- Verbindung läuft über andere Firewall zurück
```

Merksatz:

```
Stateful Firewall muss Hin- und Rückrichtung richtig sehen.
```

Fehlerbild: NAT/PAT-Zuordnung fehlt

Bei PAT werden Verbindungen über Ports zugeordnet.

Wenn die Zuordnung fehlt oder abläuft, kann Rückverkehr nicht richtig zugestellt werden.

Besonders bei UDP kann das auftreten, weil UDP keinen echten Verbindungszustand hat.

Mögliche Folgen:

```
- Antwort kommt nicht an
- Verbindung bricht ab
- Dienst wirkt instabil
```

Merksatz:

```
PAT braucht passende Port-Zuordnung für den Rückverkehr.
```

Fehlerbild: MTU-Problem wirkt wie Schicht-4-Problem

Manchmal funktionieren kleine Verbindungen, aber größere Datenübertragungen hängen.

Mögliche Ursache:

MTU-Problem

Symptome:

Ping mit kleiner Größe funktioniert.
Webseite lädt teilweise.
VPN funktioniert instabil.
Dateiübertragung bleibt hängen.
TLS-Verbindung hängt beim Aufbau.

Obwohl die Ursache tiefer liegen kann, sieht es oft wie ein TCP- oder Anwendungsproblem aus.

Merksatz:

Teilweise funktionierende Verbindungen können auf MTU-Probleme hinweisen.

Werkzeuge für Schicht-4-Fehlersuche

Typische Werkzeuge und Informationen:

Werkzeug / Anzeige	Nutzen
Porttest	prüft TCP- oder UDP-Port
netstat / ss	zeigt lauschende Dienste und Verbindungen
Firewall-Logs	zeigt erlaubte oder blockierte Verbindungen
Dienststatus	zeigt, ob Dienst läuft
Packet Capture	zeigt SYN, ACK, RST, UDP-Anfragen
NAT-Tabelle	zeigt Port-Zuordnungen
Portscan	zeigt offene Ports, nur mit Berechtigung
Anwendungslog	zeigt Fehler des Dienstes

Merksatz:

Schicht 4 prüft man mit Porttests, Logs und Mitschnitten.

Porttest

Ein Porttest prüft, ob ein bestimmter TCP- oder UDP-Port erreichbar ist.

Beispielhafte Prüffragen:

```
Ist TCP 443 erreichbar?
Ist TCP 22 erreichbar?
Ist UDP 53 erreichbar?
Antwortet der Dienst?
Kommt ein Timeout?
Kommt ein Reset?
```

Wichtig:

```
Ping ist kein Porttest.
```

Merksatz:

```
Porttest prüft Schicht 4,
Ping prüft ICMP auf Schicht 3.
```

Lauschende Dienste prüfen

Auf einem Server sollte man prüfen:

```
Lauscht der Dienst?
Auf welchem Port lauscht er?
Auf welcher IP-Adresse lauscht er?
Nutzt er TCP oder UDP?
Ist er nur lokal erreichbar?
Ist der Dienst wirklich gestartet?
```

Typische Zustände:

```
LISTEN
ESTABLISHED
```

Merksatz:

Dienst muss laufen und auf der richtigen Adresse lauschen.

Packet Capture bei TCP

In einem Mitschnitt kann man erkennen:

- SYN
- SYN-ACK
- ACK
- RST
- FIN
- Retransmissions
- Timeouts
- Quell-Port
- Ziel-Port

Typische Interpretation:

SYN geht raus,
keine Antwort:
Filter, Routing oder Dienstproblem.

SYN, SYN-ACK, ACK:
Verbindung aufgebaut.

RST:
Verbindung wird zurückgesetzt.

Merksatz:

TCP-Mitschnitt zeigt den Verbindungsaufbau sehr gut.

Packet Capture bei UDP

Bei UDP sieht man keinen Handshake.

Man prüft:

- geht Anfrage raus?
- ist Ziel-Port korrekt?
- kommt Antwort zurück?
- ist Quell-Port passend?
- blockiert Firewall?
- antwortet Dienst überhaupt?

Beispiel DNS:

Anfrage an UDP 53
Antwort von UDP 53 zurück

Merksatz:

Bei UDP vergleicht man Anfrage und Antwort.

Firewall-Logs prüfen

Firewall-Logs können zeigen:

- Quelle
- Ziel
- Protokoll
- Port
- Aktion
- Zeit
- Regelname
- Interface oder Zone

Wichtige Fragen:

Wird die Verbindung erlaubt?
Wird sie blockiert?
Welche Regel greift?
Ist TCP oder UDP betroffen?
Gibt es Rückverkehr?

Merksatz:

```
Firewall-Logs zeigen oft,
ob Schicht 4 blockiert wird.
```

NAT- und Portweiterleitungsprüfung

Bei NAT oder Portweiterleitung prüft man:

```
- externe IP korrekt?
- kein CGNAT?
- externer Port korrekt?
- internes Ziel korrekt?
- internes Ziel erreichbar?
- TCP oder UDP korrekt?
- Firewall erlaubt?
- Dienst läuft?
- Rückweg vorhanden?
- Hairpin NAT nötig?
```

Merksatz:

```
NAT-Fehlersuche braucht Port,
Protokoll,
Ziel-IP
und Rückweg.
```

Typische Prüf-Reihenfolge bei Dienstproblemen

Eine einfache Reihenfolge:

```
1. Ziel-IP erreichbar?
2. Route und Gateway korrekt?
3. richtiger Port?
4. richtiges Protokoll TCP oder UDP?
5. Dienst läuft?
6. Dienst lauscht auf richtiger IP?
7. lokale Server-Firewall erlaubt?
8. Netzwerk-Firewall erlaubt?
```

9. NAT oder Portweiterleitung korrekt?
10. Anwendung selbst prüfen

Merksatz:

Erst IP,
dann Port,
dann Dienst.

Beispiel: HTTPS intern nicht erreichbar

Fehlerbild:

Client erreicht Server-IP per Ping.
HTTPS auf TCP 443 funktioniert nicht.

Prüfung:

1. Hört der Webserver auf TCP 443?
2. Ist TCP 443 auf der Server-Firewall erlaubt?
3. Ist Netzwerk-Firewall im Weg?
4. Nutzt der Dienst vielleicht TCP 8443?
5. Gibt es TLS- oder Anwendungsfehler?
6. Funktioniert Zugriff lokal auf dem Server?

Merksatz:

Ping geht,
HTTPS nicht:
TCP 443 und Dienst prüfen.

Beispiel: DNS antwortet nicht

Fehlerbild:

Client kann externe IPs erreichen,
aber Namen werden nicht aufgelöst.

Prüfung:

```
1. DNS-Server-IP korrekt?
2. DNS-Server per IP erreichbar?
3. UDP 53 erlaubt?
4. TCP 53 bei Bedarf erlaubt?
5. DNS-Dienst läuft?
6. DNS-Zone korrekt?
7. Firewall-Logs prüfen.
```

Merksatz:

```
DNS-Fehler können Port- und Dienstfehler sein.
```

Beispiel: SSH von außen nicht erreichbar

Fehlerbild:

```
SSH funktioniert intern,
aber nicht von außen.
```

Mögliche Ursachen:

```
- Portweiterleitung fehlt
- falscher externer Port
- falsches Ziel intern
- CGNAT
- Firewall blockiert
- SSH hört nur intern
- Zugriff nur von bestimmten IPs erlaubt
- Provider blockiert
- DNS zeigt falsch
```

Merksatz:

```
Von außen braucht man öffentliche Erreichbarkeit,
NAT-Regel,
Firewall
```

und laufenden Dienst.

Beispiel: UDP-VPN instabil

Fehlerbild:

```
VPN verbindet manchmal,
bricht aber ab oder bleibt instabil.
```

Mögliche Ursachen:

```
- UDP wird gefiltert
- NAT-Zuordnung läuft ab
- MTU-Problem
- Paketverlust
- Firewall-Zeitlimit
- falscher Port
- Provider filtert
- asymmetrisches Routing
```

Merksatz:

```
UDP-VPN-Probleme können NAT-, Firewall- oder MTU-Ursachen haben.
```

Schicht 4 oder Schicht 7?

Nicht jedes Dienstproblem ist ein Portproblem.

Beobachtung	eher Ursache
TCP-Verbindung kommt nicht zustande	Schicht 4 / Firewall
TCP 443 offen, aber Zertifikatsfehler	Schicht 6 / 7
TCP 443 offen, aber HTTP 500	Anwendung
DNS-Port erreichbar, aber falsche Antwort	DNS-Konfiguration
SSH-Port offen, aber Login scheitert	Benutzer, Schlüssel, Rechte
Datenbank-Port offen, aber Anmeldung scheitert	Anwendung / Rechte

Merksatz:

Port erreichbar bedeutet nur:
Transportweg zum Dienst ist möglich.

Schicht 4 oder Firewall?

Firewalls können auf Schicht 3 und 4 filtern.

Typische Regelbestandteile:

Quelle
Ziel
Protokoll
Port
Richtung
Aktion

Beispiel:

Quelle:
Mitarbeiter-Netz

Ziel:
Server-Netz

Protokoll:
TCP

Port:
443

Aktion:
erlauben

Merksatz:

Firewall-Regeln müssen Quelle, Ziel, Protokoll und Port passend erlauben.

Schicht 4 oder NAT?

Wenn ein Dienst intern funktioniert, aber extern nicht, ist NAT oder Portweiterleitung ein häufiger Prüfpunkte.

Typische Unterscheidung:

Beobachtung	mögliche Ursache
intern geht, extern nicht	NAT, Firewall, CGNAT, DNS
extern kommt falscher Dienst	falsche Portweiterleitung
nur TCP geht, UDP nicht	falsches Protokoll freigegeben
Rückverkehr fehlt	NAT oder Rückroute
Test intern über Domain geht nicht	Hairpin NAT oder Split DNS

Merksatz:

```
Externe Dienstprobleme oft mit NAT und Firewall prüfen.
```

Was Schicht-4-Fehlersuche nicht löst

Wenn TCP oder UDP korrekt funktioniert, können trotzdem Anwendungsfehler bestehen.

Dann prüft man:

```
- Anwendungskonfiguration
- Benutzerrechte
- Zertifikate
- TLS-Version
- Datenbankverbindung
- Reverse Proxy
- DNS-Inhalte
- API-Endpunkte
- Logs der Anwendung
```

Merksatz:

```
Schicht 4 transportiert,
Schicht 7 verarbeitet.
```

Einordnung in das OSI-Modell

Thema	Schicht
Kabel und Link	1
MAC und VLAN	2
IP und Routing	3
TCP und UDP	4
Ports	4
TCP-Handshake	4
Firewall nach IP	3
Firewall nach Port	4
TLS-Zertifikat	6 / 7
DNS-Dienst	7
Webanwendung	7

Merksatz:

```
Schicht 4 sagt:
Kommt der Transport zum Dienst zustande?
```

Typische IHK-Fragen

In AP1 und AP2 kann zum Beispiel gefragt werden:

```
- Was prüft man auf Schicht 4?
- Warum reicht Ping nicht als Diensttest?
- Was bedeutet offener Port?
- Was bedeutet geschlossener Port?
- Was bedeutet gefilterter Port?
- Warum muss man TCP und UDP unterscheiden?
- Warum kann TCP 443 blockiert sein, obwohl Ping funktioniert?
- Was passiert beim TCP-Handshake?
- Was bedeutet RST?
- Was bedeutet Timeout?
- Warum ist UDP-Fehlersuche schwieriger als TCP-Fehlersuche?
- Welche Rolle spielen Firewall-Regeln bei Schicht 4?
- Welche Rolle spielen NAT und Portweiterleitung?
```

Typische Prüfungsfallen

Ping prüft keine TCP- oder UDP-Ports.

ICMP hat keine Ports.

IP erreichbar heißt nicht:
Dienst erreichbar.

Port erreichbar heißt nicht:
Anwendung korrekt.

TCP und UDP sind getrennt zu betrachten.

Gleiche Portnummer bei TCP und UDP ist nicht dasselbe.

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

Kein SYN-ACK kann Firewall-, Routing- oder Dienstproblem sein.

RST bedeutet aktiver Abbruch.

Timeout bedeutet keine rechtzeitige Antwort.

UDP hat keinen Handshake.

UDP-Fehler sind oft schwerer zu erkennen.

Firewall-Regel braucht Protokoll und Port.

Portweiterleitung braucht richtiges Protokoll.

Dienst muss auf richtiger IP und richtigem Port lauschen.

localhost ist nur lokal.

Wichtige Begriffe kurz erklärt

Begriff	Kurze Erklärung

Schicht-4-Fehler	Fehler bei TCP, UDP oder Ports
Porttest	Prüfung eines TCP- oder UDP-Ports
offener Port	Dienst ist grundsätzlich erreichbar
geschlossener Port	kein Dienst lauscht
gefilterter Port	Firewall oder Filter blockiert
TCP-Handshake	Verbindungsaufbau mit SYN, SYN-ACK, ACK
SYN	TCP-Verbindungsanfrage
SYN-ACK	Antwort und Bestätigung auf SYN
ACK	Bestätigung
RST	sofortiger TCP-Abbruch
Timeout	Antwort kommt nicht rechtzeitig
Retransmission	erneute Übertragung
LISTEN	Dienst wartet auf Verbindung
ESTABLISHED	Verbindung besteht
localhost	eigenes Gerät, 127.0.0.1
Host-Firewall	Firewall direkt auf dem Server
Portweiterleitung	externer Port wird intern weitergeleitet
NAT-Tabelle	Zuordnung übersetzter Verbindungen

IHK-sichere Kurzformulierung

Fehlersuche auf OSI-Schicht 4 bedeutet, TCP, UDP und Ports zu prüfen. Während Schicht 3 die IP-Erreichbarkeit eines Zielgeräts betrachtet, prüft Schicht 4, ob der gewünschte Dienst-Port erreichbar ist. Typische Schicht-4-Probleme sind geschlossene oder gefilterte Ports, fehlgeschlagene TCP-Handshakes, Timeouts, TCP-Resets, falsche TCP-/UDP-Freigaben, blockierende Firewalls oder fehlerhafte NAT- und Portweiterleitungen. Ein erfolgreicher Ping beweist nicht, dass ein TCP- oder UDP-Dienst erreichbar ist, und ein erreichbarer Port beweist nicht automatisch, dass die Anwendung korrekt funktioniert.

Merksätze

Schicht-4-Fehlersuche = TCP, UDP und Ports prüfen.

IP erreichbar heißt nicht:
Port erreichbar.

Ping prüft ICMP,
nicht TCP oder UDP.

Porttest prüft Schicht 4.

Dienstproblem = IP, Port, Protokoll, Firewall und Anwendung prüfen.

TCP und UDP getrennt betrachten.

Gleiche Portnummer bei TCP und UDP ist nicht dasselbe.

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

Kein Handshake = keine TCP-Verbindung.

RST = aktiver Abbruch.

Timeout = keine rechtzeitige Antwort.

Offener Port = Dienst grundsätzlich erreichbar.

Geschlossener Port = kein Dienst lauscht.

Gefilterter Port = Firewall oder Filter im Weg.

UDP hat keinen Handshake.

UDP braucht Anfrage-Antwort-Prüfung.

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

Portweiterleitung braucht richtige IP,
richtigen Port
und richtiges Protokoll.

Dienst muss auf richtiger Schnittstelle lauschen.

localhost ist nur lokal.

Erst IP,

dann Port,

dann Dienst.