6.7 Fehlersuche auf Schicht 3

Fehler auf OSI-Schicht 3 betreffen die logische IP-Kommunikation.

Dabei geht es vor allem um:

```
- IP-Adresse
- Subnetzmaske
- Standard-Gateway
- Routing
- Routing-Tabelle
- ICMP
- NAT
- IPv4
- IPv6
- Firewall-Regeln auf IP-Ebene
```

Schicht 3 liegt zwischen der lokalen Frame-Weiterleitung auf Schicht 2 und der Transportkommunikation auf Schicht 4.

Merksatz:

```
Schicht-3-Fehlersuche = IP, Subnetz, Gateway und Routing prüfen.
```

Grundidee der Schicht-3-Fehlersuche

Auf Schicht 3 prüft man, ob IP-Pakete den richtigen Weg finden.

Typische Fragen:

```
Hat das Gerät eine passende IP-Adresse?
Passt die Subnetzmaske?
Liegt das Gateway im eigenen Subnetz?
Gibt es eine Route zum Ziel?
Gibt es eine Rückroute?
Wird NAT benötigt?
Blockiert eine Firewall?
Funktioniert ICMP?
Ist IPv4 oder IPv6 betroffen?
```

Merksatz:

```
Auf Schicht 3 wird geprüft,
ob IP-Pakete korrekt weitergeleitet werden.
```

Reihenfolge bei der Fehlersuche

Eine sinnvolle Reihenfolge ist:

```
1. Schicht 1 prüfen:
   Link, Kabel, Signal, Port

2. Schicht 2 prüfen:
   MAC-Adresse, VLAN, ARP, Switch-Port

3. Schicht 3 prüfen:
   IP-Adresse, Subnetzmaske, Gateway, Routing

4. Schicht 4 prüfen:
   TCP-/UDP-Port

5. Schicht 7 prüfen:
   DNS, Anwendung, Dienst
```

Wichtig:

```
Schicht 3 kann nur funktionieren,
wenn Schicht 1 und Schicht 2 grundsätzlich funktionieren.
```

Merksatz:

```
Erst Link,
dann MAC/VLAN,
dann IP/Routing.
```

Typische Schicht-3-Fehler

Typische Fehler auf Schicht 3 sind:

- falsche IP-Adresse
- falsche Subnetzmaske
- falsches Standard-Gateway
- Gateway nicht erreichbar
- fehlende Route
- falsche Route
- fehlende Default Route
- doppelte IP-Adresse
- falsches VLAN-Subnetz-Zusammenspiel
- NAT fehlt oder ist falsch
- Rückroute fehlt
- Firewall blockiert IP-Verkehr
- Routing-Schleife
- IPv6 falsch konfiguriert

Merksatz:

Schicht-3-Fehler betreffen IP-Konfiguration und Wege zwischen Netzen.

Fehlerbild: Keine IP-Adresse

Wenn ein Gerät keine IP-Adresse hat, kann es nicht sinnvoll auf Schicht 3 kommunizieren.

Mögliche Ursachen:

- DHCP-Server nicht erreichbar
- DHCP-Server ausgeschaltet
- falsches VLAN
- Trunk-Fehler
- DHCP-Relay fehlt
- Netzwerkkarte deaktiviert
- Schicht-1-Problem
- Schicht-2-Problem
- manuelle IP-Konfiguration fehlt

Wichtig:

Keine IP-Adresse ist nicht immer ein reines Schicht-3-Problem.
Die Ursache kann auch auf Schicht 1 oder Schicht 2 liegen.

Merksatz:

Keine IP-Adresse:
DHCP, VLAN und Link prüfen.

Fehlerbild: APIPA-Adresse

APIPA-Adressen liegen im Bereich:

```
169.254.0.0/16
```

Beispiel:

```
169.254.23.80
```

Eine APIPA-Adresse bedeutet häufig:

Das Gerät konnte keine IP-Adresse per DHCP erhalten.

Mögliche Ursachen:

- DHCP-Server nicht erreichbar
- falsches VLAN
- DHCP-Relay fehlt
- Switch-Port falsch konfiguriert
- Netzwerkverbindung gestört

Merksatz:

169.254.x.x weist oft auf DHCP-Probleme hin.

Fehlerbild: Falsche IP-Adresse

Eine falsche IP-Adresse kann dazu führen, dass ein Gerät im falschen Netz landet.

Beispiel:

```
erwartet:
192.168.10.20/24

tatsächlich:
192.168.20.20/24
```

Mögliche Ursachen:

```
- falsches VLAN
- falscher DHCP-Bereich
- falsche manuelle Konfiguration
- falsche SSID-VLAN-Zuordnung
- falscher Standort oder Switch-Port
```

Merksatz:

```
Falsche IP-Adresse kann auf falsches VLAN oder falschen DHCP-Bereich hinweisen.
```

Fehlerbild: Falsche Subnetzmaske

Eine falsche Subnetzmaske kann dazu führen, dass ein Gerät falsch entscheidet:

```
Ziel ist lokal
oder
Ziel muss über das Gateway erreicht werden
```

Beispiel:

```
PC A:
192.168.10.20/24

PC B:
192.168.10.130/25
```

Diese Geräte können unterschiedlich bewerten, ob sie im gleichen Netz liegen.

Mögliche Folgen:

```
- einseitige Kommunikation
- Gateway wird falsch genutzt
- ARP-Anfragen laufen ins Leere
- Ziele wirken unerreichbar
```

Merksatz:

```
IP-Adresse und Subnetzmaske müssen zusammenpassen.
```

Fehlerbild: Falsches Standard-Gateway

Das Standard-Gateway ist der Weg in andere Netze.

Wenn es falsch eingetragen ist, funktionieren Ziele außerhalb des eigenen Subnetzes nicht.

Beispiel falsch:

```
Client:
192.168.10.20/24

Gateway:
192.168.20.1
```

Problem:

```
Das Gateway liegt nicht im eigenen Subnetz.
```

Richtig wäre zum Beispiel:

```
192.168.10.1
```

Merksatz:

```
Gateway muss im eigenen Subnetz erreichbar sein.
```

Fehlerbild: Gateway nicht erreichbar

Wenn das Gateway nicht erreichbar ist, kann der Client keine anderen Netze erreichen.

Mögliche Ursachen:

- falsche Gateway-IP
- Router-Interface down
- falsches VLAN
- ARP zum Gateway funktioniert nicht
- Schicht-1-Problem
- Schicht-2-Problem
- Firewall blockiert ICMP
- Gateway antwortet nicht auf Ping

Prüfung:

IP-Konfiguration prüfen.
Subnetzmaske prüfen.
VLAN prüfen.
ARP-Eintrag prüfen.
Ping zum Gateway testen.
Switch-Port prüfen.

Merksatz:

Gateway-Probleme können Schicht 2 und Schicht 3 betreffen.

Fehlerbild: Gleiches Netz funktioniert, anderes Netz nicht

Wenn Geräte im gleichen Subnetz erreichbar sind, aber andere Netze nicht, liegt das Problem häufig bei Gateway oder Routing.

Beispiel:

PC erreicht Drucker im gleichen VLAN.
PC erreicht Server in anderem VLAN nicht.

Mögliche Ursachen:

```
- Standard-Gateway fehlt
- falsches Gateway
- Inter-VLAN-Routing fehlt
- Firewall blockiert
- Route fehlt
- Rückroute fehlt
```

Merksatz:

```
Gleiches Netz geht,
anderes Netz nicht:
Gateway und Routing prüfen.
```

Fehlerbild: Ein Zielnetz ist nicht erreichbar

Wenn nur ein bestimmtes Zielnetz nicht erreichbar ist, kann eine Route fehlen.

Beispiel:

```
192.168.10.0/24 erreicht 192.168.20.0/24.
192.168.10.0/24 erreicht 10.10.30.0/24 nicht.
```

Mögliche Ursachen:

```
- Route zum Zielnetz fehlt
- falscher nächster Hop
- Rückroute fehlt
- Firewall-Regel blockiert
- Zielnetz existiert nicht
- Router-Interface down
- falsche Subnetzmaske
```

Merksatz:

```
Einzelnes Netz nicht erreichbar:
Routing-Tabelle und Rückroute prüfen.
```

Fehlerbild: Internet funktioniert nicht

Wenn ein Client nicht ins Internet kommt, können mehrere Schichten beteiligt sein.

Mögliche Schicht-3-Ursachen:

```
- falsches Gateway
- Gateway nicht erreichbar
- Default Route fehlt
- NAT fehlt
- Firewall blockiert
- Provider-Routing gestört
- falsche IP-Adresse
- falsche Subnetzmaske
```

Prüfidee:

```
Gateway testen.
externe IP testen.
DNS-Namen testen.
```

Merksatz:

```
Internetproblem:
erst Gateway,
dann externe IP,
dann DNS prüfen.
```

Fehlerbild: IP funktioniert, Name funktioniert nicht

Beispiel:

```
ping 8.8.8.8 funktioniert.
ping www.example.com funktioniert nicht.
```

Dann ist IP-Kommunikation grundsätzlich möglich.

Wahrscheinliche Ursache:

```
DNS-Problem
```

Mögliche DNS-Ursachen:

```
- falscher DNS-Server
- DNS-Server nicht erreichbar
- Firewall blockiert DNS
- falsche Suchdomäne
- lokaler DNS-Cache fehlerhaft
```

Merksatz:

```
IP geht,
Name nicht:
DNS prüfen.
```

Fehlerbild: Ping funktioniert, Anwendung nicht

Beispiel:

```
ping server funktioniert.
Webseite lädt nicht.
```

Dann ist Schicht 3 wahrscheinlich grundsätzlich erreichbar.

Mögliche Ursachen auf höheren Schichten:

```
- TCP-Port blockiert
- Webserver läuft nicht
- Firewall blockiert Port 80 oder 443
- Zertifikatsproblem
- Reverse Proxy falsch
- Anwendung abgestürzt
```

Merksatz:

```
Ping-Erfolg beweist nicht,
dass der Dienst funktioniert.
```

Fehlerbild: Ping funktioniert nicht, Dienst funktioniert aber

Beispiel:

```
Webseite funktioniert.
Ping funktioniert nicht.
```

Mögliche Ursache:

```
ICMP wird blockiert.
```

Viele Firewalls erlauben TCP 443, blockieren aber ICMP Echo.

Deshalb bedeutet ein fehlgeschlagener Ping nicht automatisch, dass das Ziel nicht erreichbar ist.

Merksatz:

```
Kein Ping heißt nicht automatisch:
Ziel offline.
```

Fehlerbild: Rückroute fehlt

Kommunikation braucht Hinweg und Rückweg.

Beispiel:

```
Netz A kann Paket zu Netz B senden.
Netz B kennt aber keinen Weg zurück zu Netz A.
```

Dann kommt keine Antwort an.

Mögliche Ursachen:

```
- Rückroute fehlt
- falsche Default Route
```

- NAT fehlt oder falsch
- asymmetrisches Routing
- Firewall blockiert Antwortverkehr

Merksatz:

Ohne Rückroute keine Antwort.

Fehlerbild: Asymmetrisches Routing

Asymmetrisches Routing bedeutet:

Hinweg und Rückweg nehmen unterschiedliche Pfade.

Das ist nicht immer falsch.

Problematisch wird es oft bei:

- Firewalls
- NAT
- zustandsbehafteter Paketprüfung
- VPN-Verbindungen
- mehreren Internetanschlüssen

Warum?

Eine Firewall erwartet häufig,
beide Richtungen einer Verbindung zu sehen.

Merksatz:

Asymmetrisches Routing kann Firewalls und NAT stören.

Fehlerbild: NAT funktioniert nicht

Wenn NAT nicht funktioniert, können interne Geräte eventuell keine externen Ziele erreichen.

Mögliche Ursachen:

```
- NAT-Regel fehlt
- falsches Interface
- falsches Quellnetz
- Firewall blockiert
- Default Route fehlt
- Rückroute fehlt
- Provider-Verbindung gestört
```

Prüfung:

```
interne IP prüfen.
Gateway prüfen.
NAT-Regel prüfen.
Firewall-Regel prüfen.
externe IP testen.
```

Merksatz:

```
NAT-Fehler wirken oft wie Internet- oder Routing-Probleme.
```

Fehlerbild: Portweiterleitung funktioniert nicht

Wenn ein interner Dienst von außen nicht erreichbar ist, kann das mehrere Ursachen haben.

Mögliche Ursachen:

```
- keine öffentliche IPv4-Adresse
- CGNAT beim Provider
- falscher externer Port
- falsche interne Ziel-IP
- Dienst läuft nicht
- Firewall blockiert am Router
- Firewall blockiert am Server
- DNS zeigt auf falsche IP
- Hairpin NAT fehlt bei internem Test
```

Merksatz:

Portweiterleitung braucht öffentliche Erreichbarkeit,
NAT-Regel,
Firewall-Freigabe
und laufenden Dienst.

Fehlerbild: IPv6 funktioniert nicht

IPv6-Fehler können andere Ursachen haben als IPv4-Fehler.

Mögliche Ursachen:

- keine globale IPv6-Adresse
- nur Link-Local-Adresse vorhanden
- Router Advertisements fehlen
- ICMPv6 wird blockiert
- NDP funktioniert nicht
- falsches Präfix
- falsche Firewall-Regeln
- DNS liefert AAAA-Record, aber IPv6 funktioniert nicht

Merksatz:

IPv6-Fehlersuche:
Adresse, Präfix, Gateway, NDP, ICMPv6 und DNS prüfen.

Fehlerbild: IPv4 geht, IPv6 nicht

Wenn IPv4 funktioniert, aber IPv6 nicht, prüft man gezielt IPv6.

Mögliche Ursachen:

- kein IPv6-Präfix
- Router Advertisement fehlt
- Firewall blockiert ICMPv6
- DHCPv6 oder SLAAC falsch
- kein IPv6-Gateway
- Provider liefert kein IPv6
- DNS bevorzugt IPv6, aber Verbindung scheitert

Merksatz:

> Bei Dual Stack IPv4 und IPv6 getrennt prüfen.

Fehlerbild: IPv6 geht, IPv4 nicht

Auch der umgekehrte Fall ist möglich.

Mögliche Ursachen:

- keine IPv4-Adresse
- DHCPv4 funktioniert nicht
- NAT fehlt
- IPv4-Gateway falsch
- IPv4-Route fehlt
- Firewall blockiert IPv4
- DNS liefert nur IPv6 oder falsche IPv4-Daten

Merksatz:

> Dual Stack bedeutet:
> beide Protokolle separat kontrollieren.

Werkzeuge für Schicht-3-Fehlersuche

Typische Werkzeuge und Informationen:

Werkzeug / Anzeige	Nutzen
IP-Konfiguration	IP, Maske, Gateway, DNS prüfen
Routing-Tabelle	Wege zu Zielnetzen prüfen
Ping	grundlegende IP-Erreichbarkeit prüfen
Traceroute	Weg über Router prüfen
ARP-Tabelle	lokale IP-MAC-Zuordnung prüfen
Neighbor Table	IPv6-Nachbarn prüfen
Firewall-Logs	erlaubte und blockierte Pakete prüfen
NAT-Tabelle	NAT-Zuordnungen prüfen
DNS-Test	Namensauflösung prüfen

Werkzeug / Anzeige	Nutzen
Packet Capture	Pakete genauer analysieren

Merksatz:

```
Schicht-3-Fehlersuche nutzt IP-Konfiguration,
Routing-Tabelle,
Ping
und Traceroute.
```

IP-Konfiguration prüfen

Bei einem Client prüft man zuerst:

```
- IP-Adresse
- Subnetzmaske
- Standard-Gateway
- DNS-Server
- DHCP oder statisch
- IPv4 und IPv6
- richtige Schnittstelle
```

Typische Hinweise:

```
169.254.x.x = häufig DHCP-Problem
falsches Netz = VLAN oder DHCP prüfen
kein Gateway = nur lokales Netz erreichbar
```

Merksatz:

```
IP-Konfiguration ist der erste Schicht-3-Prüfpunkt.
```

Routing-Tabelle prüfen

In der Routing-Tabelle prüft man:

- gibt es eine Route zum Zielnetz?
- gibt es eine Default Route?
- ist der nächste Hop korrekt?
- ist die Ausgangsschnittstelle korrekt?
- gibt es eine genauere Route?
- ist die Metrik sinnvoll?

Wichtig:

Bei mehreren passenden Routen gewinnt die genaueste Route.

Merksatz:

Routing-Tabelle zeigt,
welchen Weg Pakete nehmen sollen.

Ping gezielt verwenden

Ping kann gezielt eingesetzt werden.

Sinnvolle Reihenfolge:

1. Loopback testen
2. eigene IP testen
3. Gateway testen
4. anderes Gerät im gleichen Netz testen
5. Ziel in anderem Netz testen
6. externe IP testen
7. DNS-Namen testen

Merksatz:

Ping von nah nach fern einsetzen.

Traceroute gezielt verwenden

Traceroute hilft, den Weg zum Ziel zu prüfen.

Damit kann man erkennen:

- wie weit Pakete kommen
- bei welchem Hop es stoppt
- ob der Weg ungewöhnlich ist
- ob Routing-Schleifen sichtbar sind
- ob Firewalls Antworten blockieren

Wichtig:

Traceroute-Ausgaben müssen vorsichtig interpretiert werden.

Merksatz:

Traceroute zeigt Hinweise auf den Routing-Weg.

ARP und Schicht 3

ARP gehört zu IPv4 und verbindet Schicht 3 mit Schicht 2.

Bei IPv4 prüft man:

Gibt es einen ARP-Eintrag für das Gateway?
Stimmt die MAC-Adresse?
Ändert sich der Eintrag ständig?
Gibt es doppelte IP-Adressen?

Wenn ARP zum Gateway nicht funktioniert, kann der Client andere Netze nicht erreichen.

Merksatz:

Ohne ARP zum Gateway kein IPv4-Weg ins andere Netz.

NDP und Schicht 3

Bei IPv6 übernimmt NDP ähnliche Aufgaben wie ARP bei IPv4.

NDP basiert auf ICMPv6.

Bei IPv6 prüft man:

- Neighbor Table
- Link-Local-Adresse
- Router Advertisement
- Default Gateway
- ICMPv6-Filterung
- Präfixinformationen

Merksatz:

IPv6 braucht NDP und ICMPv6 für Grundfunktionen.

Firewall als Schicht-3-Fehlerquelle

Eine Firewall kann IP-Verkehr blockieren.

Beispiele:

- bestimmtes Quellnetz blockiert
- bestimmtes Zielnetz blockiert
- ICMP blockiert
- ausgehender Verkehr blockiert
- eingehender Verkehr blockiert
- NAT-Regel fehlt
- falsche Zone

Wichtig:

Firewall-Problem ist nicht immer Schicht 3.
Bei Port- oder Anwendungskontrolle können auch Schicht 4 oder 7 beteiligt sein.

Merksatz:

Firewall kann Routing erlauben oder verhindern.

Schicht 3 oder Schicht 4?

Eine einfache Unterscheidung:

Frage	eher Schicht
Hat der Client eine passende IP-Adresse?	3
Ist das Gateway erreichbar?	3
Gibt es eine Route zum Zielnetz?	3
Funktioniert Ping auf eine IP?	3
Ist TCP-Port 443 offen?	4
Ist UDP-Port 53 erreichbar?	4
Läuft der Webdienst?	7
Löst der DNS-Name korrekt auf?	7

Merksatz:

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

Schicht 3 oder DNS?

DNS gehört zur Anwendungsschicht, wird aber oft bei IP-Problemen vermutet.

Unterscheidung:

Test	Bedeutung
IP-Adresse erreichbar, Name nicht	DNS prüfen
IP-Adresse nicht erreichbar	Routing, Gateway, Firewall, Link prüfen
Name zeigt auf falsche IP	DNS-Zone oder DNS-Cache prüfen
interner Name geht extern nicht	Split DNS oder öffentliche DNS-Zone prüfen

Merksatz:

```
Erst IP testen,
dann Namen testen.
```

Schicht 3 oder VLAN?

VLAN gehört zu Schicht 2.

Subnetz gehört zu Schicht 3.

Beide hängen in der Praxis eng zusammen.

Beispiel:

> Client bekommt IP aus falschem Subnetz.

Mögliche Ursache:

> Switch-Port im falschen VLAN.

Deshalb gilt:

> Bei falscher IP-Adresse auch VLAN prüfen.

Merksatz:

> VLAN-Fehler können wie Schicht-3-Fehler aussehen.

Schicht 3 oder NAT?

Wenn interne Kommunikation funktioniert, aber Internet nicht, kann NAT beteiligt sein.

Unterscheidung:

Beobachtung	mögliche Ursache
Gateway erreichbar, externe IP nicht	Routing, NAT, Firewall, Provider
externe IP erreichbar, Name nicht	DNS
intern erreichbar, extern nicht	Portweiterleitung, CGNAT, Firewall
nur Rückverkehr fehlt	NAT oder Rückroute

Merksatz:

> NAT-Probleme zeigen sich oft beim Übergang ins Internet.

Beispiel: Client erreicht Gateway nicht

Fehlerbild:

```
Client kann Gateway nicht pingen.
```

Prüfung:

```
1. Link vorhanden?
2. Client im richtigen VLAN?
3. IP-Adresse korrekt?
4. Subnetzmaske korrekt?
5. Gateway-IP korrekt?
6. ARP-Eintrag vorhanden?
7. Router-Interface aktiv?
8. Firewall blockiert ICMP?
```

Wahrscheinliche Bereiche:

```
Schicht 1
Schicht 2
Schicht 3
```

Merksatz:

```
Gateway nicht erreichbar:
lokal prüfen.
```

Beispiel: Client erreicht Internet-IP nicht

Fehlerbild:

```
Gateway erreichbar,
aber externe IP nicht.
```

Prüfung:

```
1. Default Route auf Gateway prüfen
2. NAT/PAT prüfen
```

3. Firewall-Regeln prüfen
4. WAN-Verbindung prüfen
5. Provider-Gateway prüfen
6. Rückweg prüfen

Merksatz:

Gateway geht,
Internet-IP nicht:
Routing, NAT und Firewall prüfen.

Beispiel: Client erreicht Server in anderem VLAN nicht

Fehlerbild:

Client in VLAN 10 erreicht Server in VLAN 30 nicht.

Mögliche Ursachen:

- Inter-VLAN-Routing fehlt
- Firewall blockiert zwischen VLANs
- falsches Gateway im VLAN 10
- falsches Gateway im VLAN 30
- Rückroute fehlt
- Server-Firewall blockiert
- Server im falschen VLAN
- falsche Subnetzmaske

Merksatz:

Zwischen VLANs braucht man Routing und erlaubte Regeln.

Beispiel: VPN erreicht internes Netz nicht

Fehlerbild:

VPN-Verbindung steht,
aber interne Systeme sind nicht erreichbar.

Mögliche Ursachen:

- Route ins interne Netz fehlt
- Rückroute zum VPN-Netz fehlt
- Firewall blockiert VPN-Netz
- Split-Tunnel falsch
- NAT-Regel fehlt oder stört
- DNS liefert falsche interne Adresse
- VPN-Client bekommt falsches Netz

Merksatz:

VPN-Probleme sind oft Routing-, Firewall- oder DNS-Probleme.

Typische Prüf-Reihenfolge bei IP-Problemen

Eine einfache Reihenfolge:

1. IP-Adresse prüfen
2. Subnetzmaske prüfen
3. Gateway prüfen
4. eigenes Subnetz testen
5. Gateway pingen
6. ARP oder NDP prüfen
7. Routing-Tabelle prüfen
8. Zielnetzroute prüfen
9. Rückroute prüfen
10. Firewall und NAT prüfen
11. DNS prüfen
12. Dienst prüfen

Merksatz:

IP-Probleme systematisch von lokal nach entfernt prüfen.

Einordnung in das OSI-Modell

Thema	Schicht
Kabel, Link, Signal	1
MAC, VLAN, ARP	2 / 3-Bezug
IP-Adresse	3
Subnetzmaske	3
Gateway	3
Routing-Tabelle	3
ICMP, Ping, Traceroute	3
NAT	3
PAT	3 / 4
TCP-/UDP-Port	4
DNS	7
Anwendung	7

Merksatz:

> Schicht 3 prüft IP-Erreichbarkeit,
> nicht automatisch den Dienst.

Was Schicht-3-Fehlersuche nicht löst

Wenn IP und Routing korrekt funktionieren, können trotzdem Probleme bestehen.

Dann prüft man höhere Schichten:

- TCP-Port offen?
- UDP-Port erreichbar?
- DNS korrekt?
- Zertifikat gültig?
- Anwendung läuft?
- Benutzerrechte korrekt?
- Proxy oder Reverse Proxy korrekt?
- Dienst lauscht auf richtiger Schnittstelle?

Merksatz:

```
IP erreichbar heißt nicht:
Anwendung funktioniert.
```

Typische IHK-Fragen

In AP1 und AP2 kann zum Beispiel gefragt werden:

```
- Welche Fehler gehören typischerweise zu Schicht 3?
- Wie prüft man eine IP-Konfiguration?
- Warum muss das Gateway im eigenen Subnetz liegen?
- Was bedeutet 169.254.x.x?
- Was prüft man, wenn das Internet nicht funktioniert?
- Wie unterscheidet man DNS- und Routing-Probleme?
- Was bedeutet fehlende Rückroute?
- Warum kann falsches VLAN wie ein IP-Problem wirken?
- Warum beweist Ping keinen funktionierenden Dienst?
- Was prüft Traceroute?
- Warum kann ICMP blockiert sein?
- Welche Rolle spielt NAT bei Internetproblemen?
```

Typische Prüfungsfallen

```
Keine IP-Adresse kann ein DHCP- oder VLAN-Problem sein.

169.254.x.x weist oft auf DHCP-Probleme hin.

Gateway muss im eigenen Subnetz liegen.

Gleiches Subnetz erreichbar,
anderes nicht:
Gateway und Routing prüfen.

IP geht,
Name nicht:
DNS prüfen.
```

Ping geht,
Anwendung nicht:
Schicht 4 oder 7 prüfen.

Ping geht nicht,
Dienst kann trotzdem funktionieren.

ICMP kann blockiert sein.

Fehlende Rückroute verhindert Antworten.

NAT braucht passenden Hin- und Rückweg.

Falsches VLAN kann falsche IP-Adresse verursachen.

IPv4 und IPv6 getrennt prüfen.

ICMPv6 nicht pauschal blockieren.

Wichtige Begriffe kurz erklärt

Begriff	Kurze Erklärung
Schicht-3-Fehler	Fehler bei IP, Subnetz, Gateway oder Routing
IP-Konfiguration	IP-Adresse, Maske, Gateway, DNS
APIPA	169.254.0.0/16 bei DHCP-Problem
Gateway-Problem	Router ins andere Netz nicht erreichbar
Routing-Problem	Weg zum Zielnetz fehlt oder ist falsch
Rückroute	Weg zurück zum Absendernetz
asymmetrisches Routing	Hin- und Rückweg sind unterschiedlich
NAT-Problem	Adressübersetzung fehlt oder ist falsch
ICMP	Kontrollmeldungen für IP
Ping	Test auf IP-Erreichbarkeit
Traceroute	Wegprüfung über Router
ARP	IPv4-IP-zu-MAC-Auflösung
NDP	IPv6-Nachbarerkennung
DNS-Problem	Name wird nicht korrekt aufgelöst

Begriff	Kurze Erklärung
Dual Stack	IPv4 und IPv6 gleichzeitig

IHK-sichere Kurzformulierung

Fehlersuche auf OSI-Schicht 3 bedeutet, die IP-Kommunikation zu prüfen. Dazu gehören IP-Adresse, Subnetzmaske, Standard-Gateway, Routing-Tabelle, ICMP, NAT und bei IPv6 auch NDP und ICMPv6. Typische Schicht-3-Fehler sind falsche IP-Konfiguration, falsches Gateway, fehlende Routen, fehlende Rückrouten, NAT-Probleme oder falsche Firewall-Regeln. Bei der Fehlersuche prüft man zuerst die lokale IP-Konfiguration, dann das Gateway, anschließend Routing zu externen oder entfernten Netzen und danach DNS oder Dienste auf höheren Schichten.

Merksätze

Schicht-3-Fehlersuche = IP, Gateway und Routing prüfen.

Erst Schicht 1,
dann Schicht 2,
dann Schicht 3.

Keine IP = DHCP, VLAN oder Link prüfen.

169.254.x.x = häufig DHCP-Problem.

Falsche IP kann falsches VLAN bedeuten.

Subnetzmaske muss passen.

Gateway muss im eigenen Subnetz liegen.

Gateway nicht erreichbar = lokal prüfen.

Gleiches Netz geht,
anderes Netz nicht:
Gateway prüfen.

Zielnetz nicht erreichbar:
Route prüfen.

Kommunikation braucht Hinweg und Rückweg.

Ohne Rückroute keine Antwort.

NAT braucht passenden Rückweg.

IP erreichbar,
Name nicht:
DNS prüfen.

Ping erreichbar heißt nicht:
Dienst funktioniert.

Ping nicht erreichbar heißt nicht automatisch:
Ziel offline.

Traceroute zeigt den Routing-Weg.

IPv4 und IPv6 getrennt prüfen.

ICMPv6 ist für IPv6 wichtig.

VLAN-Fehler können wie IP-Probleme aussehen.

Erst lokal,
dann entfernt,
dann DNS,
dann Dienst.