12.5 Typische Netzwerkfehler und ihre Ursachen

Netzwerkfehler können auf vielen verschiedenen Schichten entstehen.

Ein sichtbares Problem ist oft nur ein Symptom.

Beispiel:

```
Webseite öffnet nicht.
```

Das kann viele Ursachen haben:

```
- DNS falsch
- Server nicht erreichbar
- Port blockiert
- Zertifikat ungültig
- Webserver down
- Reverse Proxy falsch
- Benutzer nicht berechtigt
```

Merksatz:

```
Ein Fehlerbild zeigt nur das Symptom,
nicht automatisch die Ursache.
```

Warum Fehlerbilder wichtig sind

Fehlerbilder helfen, die Suche einzugrenzen.

Man fragt:

```
Was genau funktioniert nicht?
Was funktioniert noch?
Wer ist betroffen?
Seit wann?
Wurde etwas geändert?
Ist der Fehler dauerhaft oder sporadisch?
Gibt es eine Fehlermeldung?
```

Je genauer das Fehlerbild, desto schneller findet man die Ursache.

Merksatz:

```
Gute Fehlerbeschreibung ist der erste Diagnoseschritt.
```

Fehlerbild: Kein Netzwerklink

Typische Anzeichen:

```
- keine Link-LED
- Netzwerkadapter zeigt getrennt
- Switchport down
- keine Verbindung über Kabel
- keine Pakete sichtbar
- kein DHCP Discover
```

Mögliche Ursachen:

```
- Kabel defekt
- Kabel nicht richtig gesteckt
- falscher Port
- Switchport deaktiviert
- Netzwerkkarte deaktiviert
- SFP-Modul defekt
- falsches Glasfasermodul
- Stromversorgung fehlt
```

Wahrscheinliche Schicht:

```
Schicht 1
```

Merksatz:

```
Kein Link ist meistens ein physisches Problem.
```

Fehlerbild: Link vorhanden, aber keine IP-Adresse

Typische Anzeichen:

```
- Netzwerk verbunden
- aber keine gültige IP-Adresse
- Windows zeigt 169.254.x.x
- DHCP schlägt fehl
- keine Verbindung zum Gateway
- Client meldet eingeschränkte Konnektivität
```

Mögliche Ursachen:

```
- DHCP-Server nicht erreichbar
- DHCP-Scope voll
- DHCP-Relay fehlt
- falsches VLAN
- Firewall blockiert UDP 67/68
- Switchport falsch konfiguriert
- Client im falschen Netz
- DHCP-Dienst gestoppt
```

Wahrscheinliche Schichten:

```
Schicht 2
Schicht 3
Schicht 7 wegen DHCP
```

Merksatz:

```
169.254.x.x deutet häufig auf DHCP-Probleme hin.
```

Fehlerbild: Falsche IP-Adresse

Typische Anzeichen:

```
- Client hat IP aus falschem Netz
- Gateway passt nicht
- DNS passt nicht
- Zugriff auf interne Dienste funktioniert nicht
```

- nur manche Dienste erreichbar

Mögliche Ursachen:

- falsches VLAN
- falscher DHCP-Scope
- Rogue-DHCP-Server
- statische IP falsch gesetzt
- falsches WLAN
- falsche Netzwerkdose
- DHCP-Reservierung falsch

Wahrscheinliche Schichten:

Schicht 2
Schicht 3
Schicht 7 wegen DHCP

Merksatz:

Falsche IP bedeutet oft:
falsches Netz oder falsche DHCP-Konfiguration.

Fehlerbild: Gateway nicht erreichbar

Typische Anzeichen:

- lokale IP vorhanden
- andere Geräte im Netz eventuell erreichbar
- Internet nicht erreichbar
- Ping zum Gateway schlägt fehl
- Routing funktioniert nicht

Mögliche Ursachen:

- falsches Gateway eingetragen
- Gateway offline

- VLAN falsch
- falsche Netzmaske
- ARP funktioniert nicht
- Firewall blockiert ICMP
- Switchport im falschen VLAN
- IP-Konflikt

Wahrscheinliche Schichten:

Schicht 2
Schicht 3

Merksatz:

Ohne Gateway keine Kommunikation in andere Netze.

Fehlerbild: Lokales Netz funktioniert, Internet nicht

Typische Anzeichen:

- interne Server erreichbar
- Gateway erreichbar
- externe Webseiten nicht erreichbar
- DNS oder Routing auffällig
- nur Internetzugriff betroffen

Mögliche Ursachen:

- Standardroute fehlt
- Internetrouter down
- Firewall blockiert WAN
- DNS falsch
- NAT funktioniert nicht
- Providerstörung
- Proxy falsch
- VPN verändert Routing
- öffentliche Verbindung gestört

Wahrscheinliche Schichten:

```
Schicht 3
Schicht 4
Schicht 7
```

Merksatz:

```
Intern geht,
extern nicht:
Gateway,
DNS,
NAT
und Provider prüfen.
```

Fehlerbild: IP funktioniert, Name nicht

Typische Anzeichen:

```
- Zugriff per IP funktioniert
- Zugriff per DNS-Name funktioniert nicht
- Browser meldet DNS-Fehler
- nslookup liefert keine oder falsche Antwort
- nur bestimmte Namen betroffen
```

Mögliche Ursachen:

```
- falscher DNS-Server
- DNS-Eintrag fehlt
- DNS-Eintrag zeigt falsch
- DNS-Cache veraltet
- Split DNS falsch
- Suchsuffix falsch
- interne Zone fehlt
- IPv6-Record zeigt auf falsches Ziel
```

Wahrscheinliche Schicht:

Schicht 7 wegen DNS

Merksatz:

IP geht,
Name nicht:
DNS prüfen.

Fehlerbild: Name löst auf falsche IP auf

Typische Anzeichen:

- DNS liefert Antwort
- aber falscher Server wird erreicht
- falsches Zertifikat erscheint
- falsche Webseite wird angezeigt
- intern und extern unterschiedliche Ergebnisse

Mögliche Ursachen:

- falscher A-Record
- falscher AAAA-Record
- falscher CNAME
- Split DNS falsch
- DNS-Cache alt
- falscher DNS-Server
- alte öffentliche IP
- interne Zone überschreibt externe Zone

Wahrscheinliche Schicht:

Schicht 7

Merksatz:

Falsche DNS-Antwort führt zum falschen Ziel.

Fehlerbild: Ping funktioniert, Dienst nicht

Typische Anzeichen:

- Ziel antwortet auf Ping
- aber Webseite, SSH, SMB oder RDP funktioniert nicht
- Porttest schlägt fehl
- Anwendung meldet Verbindungsfehler

Mögliche Ursachen:

- Dienst läuft nicht
- Port blockiert
- Host-Firewall blockiert
- zentrale Firewall blockiert
- Dienst lauscht auf falscher IP
- falscher Port
- falsches Protokoll
- Anwendung falsch konfiguriert

Wahrscheinliche Schichten:

Schicht 4
Schicht 7

Merksatz:

Ping beweist nicht,
dass ein Dienst funktioniert.

Fehlerbild: Port offen, Anwendung funktioniert nicht

Typische Anzeichen:

- Porttest erfolgreich
- TCP-Verbindung möglich
- aber Anwendung liefert Fehler
- HTTP 500 oder 502

- Login schlägt fehl
- API antwortet mit Fehler
- Dienst bricht Verbindung ab

Mögliche Ursachen:

- Anwendung defekt
- Backend nicht erreichbar
- Datenbankfehler
- falsche Konfiguration
- Authentifizierungsproblem
- Berechtigung fehlt
- falsches Datenformat
- Zertifikatsproblem
- Reverse Proxy falsch

Wahrscheinliche Schichten:

Schicht 5
Schicht 6
Schicht 7

Merksatz:

Offener Port ist nur Verbindung,
nicht Anwendungserfolg.

Fehlerbild: Timeout

Timeout bedeutet:

Es kommt keine Antwort innerhalb der erwarteten Zeit.

Typische Anzeichen:

- Verbindung hängt
- Browser lädt lange

- SSH wartet und bricht ab
- Porttest läuft ins Timeout
- SYN-Wiederholungen im Mitschnitt

Mögliche Ursachen:

- Firewall droppt Pakete
- Ziel nicht erreichbar
- Routingproblem
- Rückweg fehlt
- Dienst antwortet nicht
- falsche IP
- NAT falsch
- Provider blockiert

Wahrscheinliche Schichten:

Schicht 3
Schicht 4
Schicht 7

Merksatz:

Timeout bedeutet meistens:
keine passende Antwort kommt zurück.

Fehlerbild: Connection Refused

Connection Refused bedeutet:

Das Zielsystem lehnt die Verbindung aktiv ab.

Typische Anzeichen:

- schnelle Fehlermeldung
- TCP RST im Mitschnitt
- Host erreichbar

- Port nimmt keine Verbindung an

Mögliche Ursachen:

- Dienst läuft nicht
- falscher Port
- Dienst lauscht nur auf localhost
- Host-Firewall lehnt aktiv ab
- Anwendung nimmt keine Verbindung an
- Dienst wurde gestoppt

Wahrscheinliche Schichten:

Schicht 4
Schicht 7

Merksatz:

Connection Refused heißt:
Ziel erreichbar,
aber Dienst nimmt nicht an.

Fehlerbild: Zugriff verweigert

Typische Anzeichen:

- Anmeldung möglich
- aber Ressource nicht zugänglich
- HTTP 403
- SMB Zugriff verweigert
- API meldet Forbidden
- Anwendung zeigt keine Daten

Mögliche Ursachen:

- Gruppe fehlt
- Rolle fehlt

```
- Freigaberecht fehlt
- Dateisystemrecht fehlt
- API-Scope fehlt
- falscher Mandant
- Richtlinie blockiert
- alte Session
- Benutzer nicht autorisiert
```

Wahrscheinliche Schicht:

```
Schicht 7
```

Merksatz:

```
Zugriff verweigert ist meistens ein Autorisierungsproblem.
```

Fehlerbild: Anmeldung schlägt fehl

Typische Anzeichen:

```
- Login nicht möglich
- HTTP 401
- falsche Zugangsdaten
- MFA schlägt fehl
- LDAP-Bind schlägt fehl
- Kerberos-Fehler
- Konto gesperrt
```

Mögliche Ursachen:

```
- Benutzername falsch
- Passwort falsch
- Konto gesperrt
- Konto deaktiviert
- Passwort abgelaufen
- MFA nicht eingerichtet
- Zeitabweichung
- LDAP oder AD nicht erreichbar
```

- falscher Identity Provider

Wahrscheinliche Schicht:

Schicht 7

Merksatz:

Anmeldung fehlgeschlagen:
Authentifizierung prüfen.

Fehlerbild: Zertifikatswarnung

Typische Anzeichen:

- Browser warnt vor Zertifikat
- Mailclient meldet Zertifikatsfehler
- LDAPS oder HTTPS funktioniert nicht
- Name passt nicht
- Zertifikat abgelaufen
- CA nicht vertrauenswürdig

Mögliche Ursachen:

- Zertifikat abgelaufen
- falscher Hostname
- falsches Zertifikat
- Zwischenzertifikat fehlt
- Systemzeit falsch
- interne CA nicht vertraut
- DNS zeigt auf falschen Server
- Reverse Proxy liefert falsches Zertifikat

Wahrscheinliche Schichten:

Schicht 6
Schicht 7

Merksatz:

```
Zertifikatsfehler mit Name,
Zeit,
CA
und DNS prüfen.
```

Fehlerbild: Webseite zeigt 404

404 bedeutet:

```
Ressource nicht gefunden.
```

Typische Ursachen:

```
- falsche URL
- falscher Pfad
- Route fehlt
- Datei fehlt
- Reverse Proxy leitet falsch
- Anwendung erwartet anderen Basis-Pfad
- falscher virtueller Host
```

Wahrscheinliche Schicht:

```
Schicht 7
```

Merksatz:

```
404 bedeutet:
Unter diesem Pfad wurde nichts gefunden.
```

Fehlerbild: Webseite zeigt 500

500 bedeutet:

```
interner Serverfehler.
```

Typische Ursachen:

```
- Fehler in Anwendung
- Datenbank nicht erreichbar
- Konfiguration falsch
- fehlende Rechte
- Anwendung abgestürzt
- Speicherproblem
- Backendfehler
- Abhängigkeit fehlt
```

Wahrscheinliche Schicht:

```
Schicht 7
```

Merksatz:

```
500 ist meist ein Problem der Anwendung oder des Servers.
```

Fehlerbild: Webseite zeigt 502

502 bedeutet:

```
Bad Gateway
```

Typisch bei Reverse Proxys.

Mögliche Ursachen:

```
- Backend nicht erreichbar
- Backend läuft nicht
- falscher Backend-Port
- falsches Backend-Protokoll
- DNS zum Backend falsch
- Firewall blockiert Proxy zu Backend
- Backend antwortet ungültig
```

Wahrscheinliche Schicht:

```
Schicht 7
```

Merksatz:

```
502 bedeutet oft:
Proxy erreicht Backend nicht korrekt.
```

Fehlerbild: Webseite zeigt 503

503 bedeutet:

```
Dienst nicht verfügbar.
```

Mögliche Ursachen:

```
- Dienst gestoppt
- Wartungsmodus
- Server überlastet
- Backend nicht verfügbar
- Ressourcenmangel
- Anwendung startet gerade
- Load Balancer hat keine gesunden Backends
```

Wahrscheinliche Schicht:

```
Schicht 7
```

Merksatz:

```
503 bedeutet:
Dienst ist aktuell nicht verfügbar.
```

Fehlerbild: Webseite zeigt 504

504 bedeutet:

Gateway Timeout

Typisch:

Proxy oder Gateway wartet zu lange auf Antwort vom Backend.

Mögliche Ursachen:

- Backend zu langsam
- Backend hängt
- Firewall blockiert Rückweg
- Datenbank langsam
- Timeout zu kurz
- Netzwerkproblem zwischen Proxy und Backend

Wahrscheinliche Schichten:

Schicht 4
Schicht 7

Merksatz:

504 bedeutet:
Gateway wartet vergeblich auf Backend-Antwort.

Fehlerbild: Mail kommt nicht an

Typische Anzeichen:

- Absender erhält Bounce
- Empfänger sieht keine Mail
- Mail landet im Spam
- Mail verzögert sich
- SMTP-Fehler
- NDR wird erzeugt

Mögliche Ursachen:

```
- MX-Record falsch
- SMTP-Port blockiert
- Mailserver nicht zuständig
- Spamfilter blockiert
- SPF, DKIM oder DMARC falsch
- Postfach voll
- Domain falsch
- TLS-Problem
- Blacklisting
```

Wahrscheinliche Schicht:

```
Schicht 7
```

Merksatz:

```
Mailfehler mit DNS,
SMTP,
Spamfilter
und Logs prüfen.
```

Fehlerbild: SMB-Freigabe nicht erreichbar

Typische Anzeichen:

```
- Netzlaufwerk verbindet nicht
- `\\server\freigabe` funktioniert nicht
- Zugriff verweigert
- Freigabe nicht gefunden
- Benutzer sieht Netzlaufwerk nicht
```

Mögliche Ursachen:

```
- DNS-Name falsch
- TCP 445 blockiert
- SMB-Dienst läuft nicht
- Freigabe existiert nicht
```

- Benutzer nicht berechtigt
- Freigabe- oder Dateisystemrechte falsch
- gespeicherte Zugangsdaten falsch
- SMB-Version inkompatibel

Wahrscheinliche Schichten:

Schicht 4
Schicht 7

Merksatz:

SMB-Probleme mit Name,
Port,
Dienst
und Rechten prüfen.

Fehlerbild: VPN verbunden, aber keine internen Dienste

Typische Anzeichen:

- VPN zeigt verbunden
- interne Server nicht erreichbar
- DNS intern funktioniert nicht
- nur Internet geht
- bestimmte Netze fehlen

Mögliche Ursachen:

- Route fehlt
- Split Tunnel falsch
- interne DNS-Server fehlen
- Firewall-Regel VPN → LAN fehlt
- Benutzergruppe nicht berechtigt
- Rückweg fehlt
- Zielserver-Firewall blockiert
- falscher VPN-Adresspool

Wahrscheinliche Schichten:

```
Schicht 3
Schicht 4
Schicht 7
```

Merksatz:

```
VPN verbunden heißt nicht automatisch:
interne Ressourcen erlaubt.
```

Fehlerbild: Nur manche Webseiten gehen nicht

Typische Anzeichen:

```
- viele Webseiten funktionieren
- einzelne Seiten nicht
- bestimmte Domains nicht erreichbar
- Zertifikatsfehler nur bei bestimmten Seiten
- DNS oder Proxy auffällig
```

Mögliche Ursachen:

```
- DNS-Problem für bestimmte Domain
- Proxy blockiert
- Firewall-Kategorie blockiert
- Zertifikatsproblem
- IPv6-Problem
- MTU-Problem
- CDN-Störung
- Geoblocking
- Browsercache
- HSTS-Problem
```

Wahrscheinliche Schichten:

```
Schicht 3
Schicht 6
```

Schicht 7

Merksatz:

Einzelne Webseiten betroffen:
DNS,
Proxy,
Zertifikat
und IPv6 prüfen.

Fehlerbild: Verbindung ist langsam

Typische Anzeichen:

- Webseiten laden langsam
- Downloads langsam
- RDP verzögert
- VoIP stockt
- Dateiübertragung langsam
- Anwendungen reagieren träge

Mögliche Ursachen:

- hohe Latenz
- Paketverlust
- geringe Bandbreite
- WLAN-Störung
- Duplexproblem
- überlasteter Server
- überlastete Firewall
- DNS-Verzögerung
- VPN-Overhead
- MTU-Problem

Wahrscheinliche Schichten:

alle Schichten möglich

Merksatz:

```
Langsam ist ein eigenes Fehlerbild,
nicht einfach „geht nicht“.
```

Fehlerbild: Verbindung bricht sporadisch ab

Typische Anzeichen:

```
- Verbindung funktioniert zeitweise
- SSH bricht ab
- VPN trennt sich
- WLAN verliert Verbindung
- RDP friert ein
- Downloads brechen ab
```

Mögliche Ursachen:

```
- WLAN-Störungen
- Paketverlust
- DHCP-Lease-Probleme
- instabile Leitung
- MTU-Problem
- Firewall-Timeout
- NAT-Timeout
- Serverüberlastung
- Energieoptionen am Client
- Roaming-Probleme
```

Wahrscheinliche Schichten:

```
Schicht 1 bis 7 möglich
```

Merksatz:

```
Sporadische Fehler brauchen Zeitbezug,
Logs
und Monitoring.
```

Fehlerbild: Nur große Dateien oder große Webseiten brechen ab

Typische Anzeichen:

```
- kleine Webseiten gehen
- große Downloads brechen ab
- VPN instabil
- Uploads hängen
- TLS-Verbindung startet,
  hängt aber später
```

Mögliche Ursachen:

```
- MTU-Problem
- Fragmentierung blockiert
- Paketverlust
- Proxy-Timeout
- Firewall-Timeout
- Upload-Limit
- Speicherproblem
- schlechte Verbindung
```

Wahrscheinliche Schichten:

```
Schicht 3
Schicht 4
Schicht 6
Schicht 7
```

Merksatz:

```
Kleine Daten gehen,
große nicht:
MTU und Paketverlust prüfen.
```

Fehlerbild: Nur ein VLAN hat Probleme

Typische Anzeichen:

- andere Netze funktionieren
- ein Standort oder Netzsegment betroffen
- DHCP nur dort gestört
- Gateway nur dort nicht erreichbar
- bestimmtes WLAN betroffen

Mögliche Ursachen:

- VLAN-ID falsch
- Trunk lässt VLAN nicht durch
- Access-Port falsch
- DHCP-Scope falsch
- DHCP-Relay fehlt
- Gateway des VLANs down
- Firewall-Regel für VLAN fehlt
- Routing für VLAN fehlt

Wahrscheinliche Schichten:

Schicht 2
Schicht 3

Merksatz:

Ein VLAN betroffen:
VLAN,
Gateway,
DHCP
und Routing prüfen.

Fehlerbild: Nur ein Standort hat Probleme

Typische Anzeichen:

- andere Standorte funktionieren
- WAN-Verbindung langsam oder down
- lokale Dienste funktionieren,

zentrale Dienste nicht
- VPN oder MPLS gestört

Mögliche Ursachen:

- Standortleitung gestört
- Router down
- VPN-Tunnel down
- Routingproblem
- DNS lokal falsch
- lokale Firewall blockiert
- Bandbreite ausgelastet
- Providerstörung

Wahrscheinliche Schichten:

Schicht 1 bis 4

Merksatz:

Ein Standort betroffen:
WAN,
Router,
VPN,
DNS
und lokale Infrastruktur prüfen.

Fehlerbild: Nur ein Benutzer hat Probleme

Typische Anzeichen:

- andere Benutzer am gleichen Gerät funktionieren
- Benutzer kann sich nicht anmelden
- bestimmte Berechtigungen fehlen
- Benutzer sieht Daten nicht
- MFA funktioniert nicht

Mögliche Ursachen:

```
- Passwort falsch
- Konto gesperrt
- Gruppenmitgliedschaft fehlt
- Rolle fehlt
- Profilproblem
- MFA falsch eingerichtet
- Lizenz fehlt
- gespeicherte Zugangsdaten falsch
- Session alt
```

Wahrscheinliche Schicht:

```
Schicht 7
```

Merksatz:

```
Einzelner Benutzer:
Konto,
Rechte
und Profil prüfen.
```

Fehlerbild: Nur ein Client hat Probleme

Typische Anzeichen:

```
- andere Clients funktionieren
- gleicher Benutzer auf anderem Gerät funktioniert
- lokaler Browserfehler
- lokales Netzwerkproblem
- falsche IP oder DNS nur auf diesem Client
```

Mögliche Ursachen:

```
- falsche IP-Konfiguration
- falscher DNS
- lokale Firewall
- Proxy-Einstellungen
```

- VPN aktiv oder falsch
- Zertifikatsspeicher
- Browsercache
- Malware oder Sicherheitssoftware
- Treiberproblem
- defektes Kabel oder WLAN

Wahrscheinliche Schichten:

Schicht 1 bis 7

Merksatz:

Einzelner Client:
lokale Konfiguration prüfen.

Fehlerbild: Alle Benutzer haben Probleme

Typische Anzeichen:

- mehrere Clients betroffen
- Dienst generell nicht erreichbar
- zentrale Anwendung gestört
- viele Tickets gleichzeitig
- Monitoring schlägt an

Mögliche Ursachen:

- Server down
- DNS-Störung
- DHCP-Störung
- Firewall-Änderung
- Zertifikat abgelaufen
- Datenbank down
- Providerstörung
- zentrales Update fehlerhaft
- Authentifizierungsdienst gestört

Wahrscheinliche Schichten:

```
zentrale Infrastruktur oder Dienst
```

Merksatz:

```
Alle betroffen:
zentralen Dienst und Infrastruktur prüfen.
```

Fehlerbild: Nach Update funktioniert Dienst nicht

Typische Anzeichen:

```
- Fehler begann direkt nach Update
- Anwendung startet nicht
- neue Fehlermeldung
- alte Konfiguration nicht kompatibel
- Abhängigkeiten fehlen
```

Mögliche Ursachen:

```
- Versionskonflikt
- geänderte Konfigurationsoption
- Dienst startet nicht
- Rechte geändert
- Datenbankmigration fehlgeschlagen
- Zertifikat oder TLS geändert
- Firewall- oder Portänderung
- Cacheproblem
```

Wahrscheinliche Schicht:

```
meist Schicht 7,
teilweise Schicht 4 bis 6
```

Merksatz:

Nach Update zuerst Update,
Logs
und Kompatibilität prüfen.

Fehlerbild: Nach Firewall-Änderung funktioniert Dienst nicht

Typische Anzeichen:

- Fehler direkt nach Regeländerung
- bestimmte Verbindungen blockiert
- nur bestimmte Richtung betroffen
- Firewall-Logs zeigen Drops

Mögliche Ursachen:

- falsche Regelreihenfolge
- falsche Quelle
- falsches Ziel
- falscher Port
- TCP/UDP verwechselt
- falsche Zone
- NAT vergessen
- Rückweg blockiert
- temporäre Regel entfernt

Wahrscheinliche Schicht:

Schicht 3 / 4,
je nach Firewall auch Schicht 7

Merksatz:

Nach Firewall-Änderung:
Regel,
Richtung,
NAT
und Logs prüfen.

Fehlerbild: Nach DNS-Änderung falsches Ziel

Typische Anzeichen:

```
- einige Clients erreichen neues Ziel
- andere noch altes Ziel
- Zertifikat passt nicht
- falscher Server antwortet
- interne und externe Antwort unterschiedlich
```

Mögliche Ursachen:

```
- DNS-Cache
- TTL noch aktiv
- falscher Record geändert
- Split DNS vergessen
- CNAME zeigt falsch
- alter Record existiert noch
- Client nutzt anderen DNS-Server
```

Wahrscheinliche Schicht:

```
Schicht 7
```

Merksatz:

```
Nach DNS-Änderung:
Cache,
TTL
und richtigen DNS-Server prüfen.
```

Fehlerbild: Nach Zertifikatserneuerung Fehler

Typische Anzeichen:

```
- Browser warnt
- TLS-Handshake scheitert
```

- App verbindet nicht mehr
- Reverse Proxy liefert altes Zertifikat
- Zwischenzertifikat fehlt

Mögliche Ursachen:

- falsches Zertifikat installiert
- Zertifikatskette unvollständig
- privater Schlüssel passt nicht
- Dienst nicht neu geladen
- SNI falsch
- Zertifikat enthält Namen nicht
- Client vertraut CA nicht

Wahrscheinliche Schichten:

Schicht 6
Schicht 7

Merksatz:

Zertifikatserneuerung braucht richtigen Namen,
Schlüssel,
Kette
und Dienstreload.

Fehlerbild: Nach VLAN-Änderung keine Verbindung

Typische Anzeichen:

- Client bekommt falsche oder keine IP
- Gateway nicht erreichbar
- bestimmter Switchport betroffen
- WLAN-SSID betroffen
- nur ein Netzsegment betroffen

Mögliche Ursachen:

- Access-Port falsches VLAN
- Trunk erlaubt VLAN nicht
- Native VLAN falsch
- DHCP-Relay fehlt
- Gateway für VLAN fehlt
- Firewall-Regel für neues VLAN fehlt
- Routing fehlt

Wahrscheinliche Schichten:

Schicht 2
Schicht 3

Merksatz:

Nach VLAN-Änderung:
VLAN-Zuordnung,
Trunk,
Gateway
und DHCP prüfen.

Fehlerbild: Nach Passwortänderung Anwendung kaputt

Typische Anzeichen:

- Dienst startet nicht
- Anwendung kann Datenbank nicht erreichen
- LDAP-Bind schlägt fehl
- API-Zugriff schlägt fehl
- wiederholte Loginfehler im Log

Mögliche Ursachen:

- Dienstkonto-Passwort geändert
- Passwort nicht in Anwendung aktualisiert
- Konto gesperrt
- Secret falsch hinterlegt

- Token abgelaufen
- alte Session ungültig
- gespeicherte Zugangsdaten falsch

Wahrscheinliche Schicht:

Schicht 7

Merksatz:

Dienstkonten und gespeicherte Secrets bei Passwortänderungen beachten.

Erste Einordnung nach Fehlermeldung

Fehlermeldung	erste Richtung
Kein Netzwerk	Schicht 1 bis 3
DNS-Name nicht gefunden	DNS
Zeitüberschreitung	Routing, Firewall, Rückweg, Dienst
Verbindung abgelehnt	Dienst oder Host-Firewall
401 Unauthorized	Authentifizierung
403 Forbidden	Autorisierung
404 Not Found	falscher Pfad oder Ressource fehlt
500 Internal Server Error	Anwendung oder Backend
502 Bad Gateway	Reverse Proxy oder Backend
Zertifikat ungültig	TLS, DNS, Zeit oder CA
Zugriff verweigert	Rechte

Merksatz:

Fehlermeldung gibt Richtung,
aber ersetzt keine Prüfung.

Erste Einordnung nach betroffener Menge

Betroffen	wahrscheinliche Richtung

ein Benutzer	Konto, Rechte, MFA, Profil
ein Client	lokale Konfiguration
ein Raum	Switch, WLAN, VLAN
ein VLAN	VLAN, DHCP, Gateway, Firewall
ein Standort	WAN, Router, Provider, VPN
alle Benutzer	zentraler Dienst oder Infrastruktur
nur extern	DNS extern, NAT, Firewall, Provider
nur intern	DNS intern, Routing, Hairpin NAT, Firewall

Merksatz:

> Betroffene Menge hilft,
> die Fehlerstelle einzugrenzen.

Erste Einordnung nach Änderung

Letzte Änderung	zuerst prüfen
Firewall-Regel	Quelle, Ziel, Port, Richtung, Logs
NAT-Regel	öffentliche IP, Ziel, Port, Protokoll
DNS-Eintrag	Record, TTL, Cache, interner/externer DNS
Zertifikat	Name, Kette, Schlüssel, Dienstreload
VLAN	Access, Trunk, Gateway, DHCP
Update	Logs, Version, Konfiguration, Abhängigkeiten
Passwort	Dienstkonto, Secret, Sperrung
VPN	Route, DNS, Benutzergruppe, Firewall
Rechte	Gruppen, Rollen, ACLs, Session

Merksatz:

> Die letzte Änderung ist oft der wichtigste Hinweis.

Was man vermeiden sollte

Nicht vorschnell:

Firewall ausschalten
alle Ports öffnen
Any-Any erlauben
Rechte auf Vollzugriff setzen
Zertifikatswarnungen ignorieren
DNS wild ändern
mehrere Dinge gleichzeitig ändern
Logs ignorieren
Fehlermeldung nur überfliegen
Workaround als Lösung stehen lassen

Merksatz:

Schnelle unsaubere Änderungen erzeugen neue Probleme.

Typische IHK-Fragen

In AP1 und AP2 kann zum Beispiel gefragt werden:

- Warum ist ein Fehlerbild nur ein Symptom?
- Was deutet auf ein DHCP-Problem hin?
- Was bedeutet 169.254.x.x?
- Warum reicht Ping nicht als Dienstprüfung?
- Was bedeutet Timeout?
- Was bedeutet Connection Refused?
- Was bedeutet HTTP 401?
- Was bedeutet HTTP 403?
- Was bedeutet HTTP 404?
- Was bedeutet HTTP 500?
- Was bedeutet HTTP 502?
- Warum kann DNS wie ein Firewallproblem wirken?
- Warum kann ein Zertifikatsfehler durch DNS entstehen?
- Wie grenzt man Fehler nach betroffenen Benutzern ein?
- Warum ist die letzte Änderung wichtig?

Typische Prüfungsfallen

Symptom ist nicht Ursache.

169.254.x.x deutet auf DHCP-Problem.

Ping reicht nicht für Dienstprüfung.

Port offen reicht nicht für Anwendungserfolg.

Timeout und Connection Refused unterscheiden.

401 ist Authentifizierung.

403 ist Autorisierung.

404 ist Ressource oder Pfad.

500 ist Anwendung oder Server.

502 ist häufig Proxy zu Backend.

DNS früh prüfen.

Zertifikat hängt mit Name,
Zeit
und Vertrauen zusammen.

Einzelner Benutzer bedeutet oft Konto oder Rechte.

Alle Benutzer bedeutet eher Infrastruktur.

Nur intern oder nur extern getrennt prüfen.

Letzte Änderung zuerst prüfen.

Nicht mehrere Dinge gleichzeitig ändern.

Wichtige Begriffe kurz erklärt

Begriff	Kurze Erklärung

Fehlerbild	sichtbares Symptom eines Problems
Ursache	eigentlicher technischer Grund
Symptom	beobachtbare Auswirkung
Timeout	keine Antwort innerhalb der Zeit
Connection Refused	Ziel lehnt aktiv ab
APIPA	automatische 169.254.x.x-Adresse
NXDOMAIN	DNS-Name existiert nicht
HTTP 401	nicht authentifiziert
HTTP 403	nicht berechtigt
HTTP 404	nicht gefunden
HTTP 500	interner Serverfehler
HTTP 502	Bad Gateway
Rückweg	Antwortweg zurück zur Quelle
Split DNS	intern und extern unterschiedliche DNS-Antwort
Hairpin NAT	interner Zugriff über öffentliche Adresse
Rogue DHCP	unerwünschter DHCP-Server
Dienstkonto	Konto für Anwendung oder Dienst
Workaround	vorübergehende Umgehung
Root Cause	eigentliche Ursache

IHK-sichere Kurzformulierung

Typische Netzwerkfehler müssen anhand ihres Fehlerbildes systematisch eingeordnet werden. Ein Symptom wie „Webseite öffnet nicht“ kann Ursachen auf verschiedenen OSI-Schichten haben, zum Beispiel DNS, Routing, Firewall, Port, TLS, Anwendung oder Berechtigung. Eine Adresse aus dem Bereich 169.254.0.0/16 deutet häufig auf ein DHCP-Problem hin. Ein erfolgreicher Ping beweist nicht, dass ein Dienst funktioniert, und ein offener Port beweist nicht, dass die Anwendung korrekt arbeitet. Timeout, Connection Refused, HTTP-Statuscodes, Zertifikatswarnungen und Zugriff-verweigert-Meldungen geben Hinweise auf die Fehlerursache, müssen aber durch Tests, Logs und Konfigurationsprüfung bestätigt werden.

Merksätze

> Fehlerbild ist Symptom,
> nicht Ursache.

Gute Fehlerbeschreibung spart Zeit.

Kein Link:
Schicht 1 prüfen.

169.254.x.x:
DHCP prüfen.

Gateway nicht erreichbar:
Schicht 2 und 3 prüfen.

IP geht,
Name nicht:
DNS prüfen.

Ping geht,
Dienst nicht:
Port,
Firewall
und Dienst prüfen.

Port offen,
Anwendung kaputt:
Schicht 7 prüfen.

Timeout:
keine passende Antwort.

Connection Refused:
Ziel lehnt aktiv ab.

Zugriff verweigert:
Autorisierung prüfen.

Login fehlgeschlagen:
Authentifizierung prüfen.

Zertifikatsfehler:
Name,
Zeit,

CA
und DNS prüfen.

404:
Pfad oder Ressource fehlt.

500:
Anwendung oder Serverproblem.

502:
Proxy erreicht Backend nicht sauber.

503:
Dienst nicht verfügbar.

504:
Gateway wartet zu lange.

Mailfehler:
DNS,
SMTP
und Logs prüfen.

SMB-Fehler:
TCP 445,
Anmeldung
und Rechte prüfen.

VPN verbunden heißt nicht:
Zugriff erlaubt.

Langsam ist nicht gleich nicht erreichbar.

Kleine Daten gehen,
große nicht:
MTU prüfen.

Ein Benutzer:
Konto und Rechte prüfen.

Ein Client:

lokale Konfiguration prüfen.

Alle Benutzer:

zentrale Infrastruktur prüfen.

Letzte Änderung zuerst prüfen.