6.1 Client ohne Netzwerkverbindung – systematische Ende-zu-Ende-Analyse

Ein Client meldet „Kein Internet“, erreicht keine internen Systeme oder kann einzelne Netzwerkdienste nicht verwenden. Diese Beschreibung benennt zunächst nur das sichtbare Symptom. Sie beweist weder einen Kabeldefekt noch einen Ausfall des Routers oder Internetzugangs.

Die Ursache kann an unterschiedlichen Stellen liegen:

- physische Verbindung,
- WLAN-Verbindung,
- Netzwerkadapter,
- VLAN-Zuordnung,
- IP-Konfiguration,
- DHCP,
- ARP beziehungsweise IPv6 Neighbor Discovery,
- Standardgateway,
- Routing,
- DNS,
- Firewall,
- Proxy,
- VPN,
- Authentifizierung,
- Zielsystem,
- Anwendung,
- Internetzugang.

Die Fehleranalyse muss deshalb vom betroffenen Client schrittweise bis zum Ziel erfolgen.

---

1. Lernziele

Nach dieser Seite kannst du:

- eine ungenaue Störungsmeldung in ein prüfbares Fehlerbild übersetzen,
- den betroffenen Umfang bestimmen,
- physische Verbindung und logische Erreichbarkeit unterscheiden,
- IPv4- und IPv6-Konfigurationen bewerten,
- DHCP-, Gateway-, Routing- und DNS-Probleme auseinanderhalten,
- lokale und entfernte Fehler voneinander abgrenzen,
- geeignete Vergleichstests durchführen,
- typische Fehlinterpretationen vermeiden,
- Maßnahmen kontrolliert ausführen,

- Ursache, Lösung und Nachprüfung dokumentieren.

---

2. Ausgangssituation

Ein Benutzer meldet:

> „Mein Computer hat kein Netzwerk.“

Diese Aussage lässt entscheidende Fragen offen:

- Ist Ethernet oder WLAN betroffen?
- Besteht überhaupt eine Verbindung zum lokalen Netzwerk?
- Funktioniert nur das Internet nicht?
- Sind interne Systeme erreichbar?
- Ist nur eine Anwendung betroffen?
- Funktionieren Ziele über IP-Adresse, aber nicht über Namen?
- Sind weitere Benutzer oder Geräte betroffen?
- Trat das Problem plötzlich oder nach einer Änderung auf?
- Ist der Fehler dauerhaft oder nur zeitweise vorhanden?
- Funktioniert eine andere Netzwerkverbindung?
- Ist ein VPN aktiv?
- Wird ein Proxy verwendet?
- betrifft das Problem IPv4, IPv6 oder beide Protokolle?

Vor technischen Eingriffen muss aus der allgemeinen Meldung ein eindeutig prüfbares Symptom entstehen.

---

3. Fehlerbild präzisieren

Geeignete Fragen sind:

- Welche konkrete Anwendung funktioniert nicht?
- Welche Adresse oder welcher Dienst soll erreicht werden?
- Welche Fehlermeldung wird angezeigt?
- Seit wann besteht der Fehler?
- Funktionierte die Verbindung zuvor?
- Was wurde unmittelbar vorher verändert?
- Sind interne und externe Ziele gleichermaßen betroffen?
- Funktioniert der Zugriff über eine IP-Adresse?
- Funktioniert der Zugriff über einen DNS-Namen?
- Sind andere Geräte am selben Standort betroffen?
- Funktioniert der Client über ein anderes Netzwerk?
- Tritt der Fehler mit einem anderen Benutzerkonto ebenfalls auf?

- Besteht der Fehler nur bei aktivem VPN?
- Ist ein bestimmtes WLAN, Kabel, Dock oder VLAN beteiligt?

Beispiel für ein präzisiertes Fehlerbild

```
Client: Notebook NB-204
Verbindung: Ethernet über USB-C-Dockingstation
Standort: Gebäude B, Raum 204
Beginn: heute nach dem Wechsel des Arbeitsplatzes
Lokale Linkanzeige: aktiv
IPv4-Adresse: 169.254.37.18/16
Standardgateway: nicht vorhanden
Interne und externe Ziele: nicht erreichbar
Weitere Clients an derselben Datendose: ebenfalls ohne DHCP-Adresse
WLAN-Verbindung des Notebooks: funktioniert
```

Damit ist die Untersuchung wesentlich stärker eingegrenzt als durch die ursprüngliche Aussage „Kein Netzwerk“.

---

4. Zuerst den Umfang bestimmen

Beobachtung	wahrscheinlicher Untersuchungsbereich
nur eine Anwendung betroffen	Anwendung, Dienst, Port, Proxy, Zertifikat oder Berechtigung
nur ein Ziel betroffen	Zielsystem, Zielnetz, DNS-Eintrag oder Route
nur ein Client betroffen	Client, Adapter, Kabel, Port oder lokale Konfiguration
mehrere Clients an einem Switch betroffen	Switch, Uplink, VLAN, Stromversorgung oder zentrale Dienste
nur ein VLAN betroffen	VLAN-Konfiguration, Trunk, Gateway, DHCP-Relay oder ACL
nur WLAN betroffen	Access Point, Authentifizierung, Funkversorgung oder WLAN-Konfiguration
interne Ziele erreichbar, Internet nicht	Gateway, Firewall, NAT, Proxy oder Provider
Internet erreichbar, interne Ziele nicht	internes Routing, VPN, DNS, Firewall oder Berechtigung
IP-Adressen funktionieren, Namen nicht	DNS-Konfiguration oder Namensauflösung
Namen werden aufgelöst, Verbindung scheitert	Routing, Firewall, Dienst, Port oder Anwendung
nur ein Standort betroffen	Standortanbindung, lokales Gateway, WAN oder Standort-Firewall
alle Systeme betroffen	zentrale Netzwerkkomponente, DNS, DHCP, Firewall, WAN oder Stromversorgung

> Der Umfang ist einer der wichtigsten Hinweise auf die Fehlerdomäne. Ein lokaler Eingriff am Client ist nicht sinnvoll, wenn gleichzeitig ein vollständiges VLAN oder ein ganzer Standort betroffen ist.

---

5. Ausgangszustand sichern

Vor Änderungen sollten mindestens dokumentiert werden:

- Datum und Uhrzeit,
- betroffener Client,
- Benutzerkontext, soweit erforderlich,
- Standort,
- Anschlussart,
- Dockingstation oder Adapter,
- Switchport, sofern bekannt,
- SSID bei WLAN,
- IP-Adressen,
- Präfix beziehungsweise Subnetzmaske,
- Standardgateway,
- DNS-Server,
- DHCP-Status,
- Routingtabelle,
- Proxy- und VPN-Status,
- genaue Fehlermeldung,
- erreichbare und nicht erreichbare Ziele,
- bereits ausgeführte Maßnahmen,
- letzte bekannte funktionierende Nutzung,
- vorausgegangene Änderungen.

Windows

```
Get-Date
Get-NetAdapter
Get-NetIPConfiguration
Get-NetIPAddress
Get-NetRoute
Get-DnsClientServerAddress
ipconfig /all
route print
```

Linux

```
date
ip link
ip address
ip route
resolvectl status
nmcli device status
```

macOS

```
date
networksetup -listallhardwareports
ifconfig
route -n get default
scutil --dns
```

Je nach Betriebssystem, Version und Netzwerkkonfiguration können einzelne Befehle oder Ausgaben abweichen.

---

6. Prüfreihenfolge

```
Fehlerbild präzisieren
→ Umfang bestimmen
→ Ausgangszustand dokumentieren
→ physische Verbindung prüfen
→ Netzwerkadapter prüfen
→ IP-Konfiguration bewerten
→ lokales Protokoll prüfen
→ Standardgateway testen
→ Routing untersuchen
→ DNS getrennt testen
→ Zielport und Dienst prüfen
→ Firewall, Proxy und VPN berücksichtigen
→ kontrollierten Vergleichstest durchführen
→ Maßnahme umsetzen
→ erneut messen
→ Funktion und Nebenwirkungen prüfen
→ Ursache und Lösung dokumentieren
```

Diese Reihenfolge ist kein starres Schema. Sie verhindert jedoch, dass ohne ausreichende Eingrenzung gleichzeitig Kabel, Einstellungen, Treiber und Netzwerkkomponenten verändert werden.

---

7. Physische Verbindung prüfen

Bei Ethernet sind zu prüfen:

- sitzt das Kabel an beiden Seiten vollständig?
- zeigt der Netzwerkadapter einen Link?
- zeigt der Switchport einen Link?
- ist das Kabel sichtbar beschädigt?
- wird eine Dockingstation oder ein USB-Netzwerkadapter verwendet?
- wird der richtige Anschluss verwendet?
- ist der Switchport aktiviert?
- stimmt die ausgehandelte Geschwindigkeit?
- steigen Fehler- oder Verwerfungszähler?
- befindet sich der Anschluss im erwarteten VLAN?
- liefert die Dockingstation zuverlässig Strom?
- funktioniert ein geprüftes Vergleichskabel?
- funktioniert ein bekanntermaßen geeigneter Vergleichsport?

Windows

```
Get-NetAdapter
Get-NetAdapterStatistics
```

Linux

```
ip -s link
ethtool <schnittstelle>
```

macOS

```
ifconfig <schnittstelle>
networksetup -getMedia <netzwerkdienst>
```

`<schnittstelle>` muss durch den tatsächlichen Schnittstellennamen ersetzt werden.

Mögliche Beobachtungen

Beobachtung	mögliche Einordnung

kein Link auf beiden Seiten	Kabel, Port, Adapter, Stromversorgung oder deaktivierte Schnittstelle
Link nur mit 100 Mbit/s statt 1 Gbit/s	Adernpaar, Auflegung, Kabelqualität oder Aushandlung
Link wechselt wiederholt	Kontaktproblem, Kabel, Adapter, Dock, Port oder Stromversorgung
hohe CRC- beziehungsweise FCS-Fehler	physische Signalstörung, Kabel, Stecker oder Port
viele Drops ohne physische Fehler	Überlastung, Puffer, QoS oder Systemressourcen
anderer Switchport funktioniert	ursprünglicher Port oder dessen Konfiguration
anderes Kabel funktioniert	ursprüngliches Kabel oder veränderter Steckkontakt verdächtig
direkte Verbindung funktioniert, Dock nicht	Dock, USB-Verbindung, Treiber oder Stromversorgung

> Dass der Link aktiv ist, bestätigt nur eine Verbindung auf der Bitübertragungsschicht. Eine richtige IP-Konfiguration, VLAN-Zuordnung oder Ende-zu-Ende-Erreichbarkeit ist damit nicht bewiesen.

---

8. WLAN-Verbindung prüfen

Bei WLAN sind zusätzlich zu prüfen:

- ist WLAN aktiviert?
- befindet sich das Gerät im Flugmodus?
- ist die richtige SSID ausgewählt?
- wurde die Authentifizierung erfolgreich abgeschlossen?
- besitzt das Gerät eine IP-Konfiguration?
- ist das Signal ausreichend?
- ist der Signal-Rausch-Abstand ausreichend?
- besteht eine Captive-Portal-Anmeldung?
- ist das Gerät im richtigen VLAN?
- greift eine Geräte- oder Benutzerzulassung?
- besteht eine auffällige Kanalnutzung?
- funktioniert derselbe Client an einem anderen Standort?
- funktioniert ein Vergleichsclient am betroffenen Standort?
- wird zwischen verschiedenen Access Points oder Frequenzbändern gewechselt?

Windows

```
netsh wlan show interfaces
netsh wlan show networks mode=bssid
```

Linux mit NetworkManager

```
nmcli device status
nmcli device wifi list
nmcli connection show --active
```

macOS

```
networksetup -getairportnetwork en0
system_profiler SPAirPortDataType
```

Der tatsächliche Schnittstellenname kann abweichen.

Wichtige Unterscheidung

```
mit SSID verbunden
≠ erfolgreich authentifiziert
≠ richtige VLAN-Zuordnung
≠ gültige IP-Konfiguration
≠ erreichbares Standardgateway
≠ funktionsfähiger DNS-Dienst
≠ erreichbares Internet
```

---

9. Zustand des Netzwerkadapters prüfen

Ein Netzwerkadapter kann vorhanden, aber nicht funktionsfähig sein.

Zu prüfen sind:

- Schnittstelle aktiviert oder deaktiviert,
- administrativer Zustand,
- operativer Zustand,
- Treiberstatus,
- Firmwarestatus,
- Hardwareerkennung,
- MAC-Adresse,
- Geschwindigkeit und Duplex,
- Energieverwaltung,
- virtuelle Netzwerkadapter,
- VPN-Adapter,
- Bridging,

- Teaming oder Bonding,
- auffällige Fehlerzähler,
- wiederholte Trennung und Neuverbindung.

Windows

```
Get-NetAdapter
Get-NetAdapterAdvancedProperty
Get-NetAdapterPowerManagement
Get-PnpDevice -Class Net
```

Linux

```
ip link
ip -s link
lspci -k
lsusb
ethtool <schnittstelle>
```

macOS

```
networksetup -listallhardwareports
ifconfig
system_profiler SPNetworkDataType
```

> Ein Treiberupdate oder eine Neuinstallation sollte nicht die erste Maßnahme sein, solange der aktuelle Zustand noch nicht ausreichend dokumentiert und eingegrenzt wurde.

---

10. IPv4-Konfiguration bewerten

Eine vollständige IPv4-Konfiguration umfasst normalerweise:

- IPv4-Adresse,
- Subnetzmaske beziehungsweise Präfixlänge,
- Standardgateway,
- DNS-Server,
- gegebenenfalls DHCP-Server,
- Lease-Zeiten,

- verbindungsspezifisches DNS-Suffix,
- zusätzliche statische Routen.

Beispiel

```
IPv4-Adresse: 192.168.10.24
Präfix: /24
Standardgateway: 192.168.10.1
DNS-Server: 192.168.10.10 und 192.168.10.11
DHCP-Server: 192.168.10.5
```

Bei `/24` gehören beispielsweise `192.168.10.24` und `192.168.10.1` zum selben IPv4-Subnetz.

Typische Auffälligkeiten

Beobachtung	mögliche Ursache
keine IPv4-Adresse	Adapter, DHCP, VLAN oder Konfiguration
Adresse aus `169.254.0.0/16`	keine nutzbare DHCP-Antwort oder bewusst verwendete Link-Local-Adresse
Adresse `0.0.0.0`	Initialisierung oder Adresszuweisung fehlgeschlagen
falsches Subnetz	statische Fehlkonfiguration oder falscher DHCP-Bereich
kein Standardgateway	DHCP-Option fehlt oder statische Konfiguration unvollständig
falscher DNS-Server	DHCP-Option, VPN, manuelle Konfiguration oder Richtlinie
doppelte IP-Adresse	Adresskonflikt
sehr kurze Lease-Zeit	DHCP-Konfiguration oder Sondernetz
mehrere Gateways	mehrdeutiges Routing oder mehrere aktive Adapter
gültige Adresse, Gateway nicht erreichbar	VLAN, Layer 2, Gateway, ARP oder Firewall
Gateway erreichbar, entfernte IP nicht	Routing, Firewall, NAT oder Zielpfad

---

11. Automatische private IPv4-Adresse richtig einordnen

Erhält ein Windows-Client keine geeignete DHCP-Konfiguration, kann er automatisch eine Adresse aus `169.254.0.0/16` verwenden. Dieser Bereich ist für IPv4 Link-Local-Adressen vorgesehen.

Eine solche Adresse bedeutet nicht automatisch:

- dass der DHCP-Server ausgeschaltet ist,
- dass das Netzwerkkabel defekt ist,
- dass der Switch ausgefallen ist,

- dass der Client überhaupt keine Verbindung besitzt.

Mögliche Ursachen sind:

- DHCP-Server nicht erreichbar,
- DHCP-Dienst ausgefallen,
- falsches VLAN,
- fehlerhafter DHCP-Relay-Agent,
- erschöpfter DHCP-Adressbereich,
- DHCP-Antwort durch Sicherheitsfunktion blockiert,
- fehlerhafte Portkonfiguration,
- beschädigte Verbindung,
- Clientfehler,
- verzögerte Adressvergabe.

Zu prüfen sind

```
physischer Link
→ VLAN-Zuordnung
→ DHCP-Anforderung
→ DHCP-Weiterleitung
→ DHCP-Server
→ verfügbarer Adressbereich
→ DHCP-Angebot
→ Clientannahme
```

---

12. DHCP systematisch untersuchen

Der vereinfachte IPv4-DHCP-Ablauf wird häufig als DORA bezeichnet:

```
DHCPDISCOVER
→ DHCPOFFER
→ DHCPREQUEST
→ DHCPACK
```

Je nach Zustand und Erneuerung eines Leases können andere DHCP-Nachrichten auftreten.

Windows

```
ipconfig /all
ipconfig /release
```

```
ipconfig /renew
```

Linux mit NetworkManager

```
nmcli device show
nmcli connection show --active
```

macOS

```
ipconfig getpacket <schnittstelle>
networksetup -getinfo <netzwerkdienst>
```

Eine Lease-Erneuerung verändert den Zustand und sollte nur kontrolliert ausgeführt werden.

Mögliche Fehlerstellen

Phase	mögliche Ursache
Discover verlässt Client nicht	Schnittstelle, Clientdienst, lokale Firewall oder Treiber
Discover erreicht Server nicht	VLAN, Switch, DHCP Snooping, Relay oder Routing
Server sendet kein Offer	Dienst, Bereich, Reservierung, Richtlinie oder Adressmangel
Offer erreicht Client nicht	Relay, VLAN, Sicherheitsfunktion oder Rückweg
Client sendet keinen Request	Clientzustand oder ungeeignetes Angebot
Server sendet kein ACK	Konflikt, Richtlinie, Bereich oder Serverfehler
ACK erreicht Client nicht	Netzwerkpfad oder Sicherheitsfunktion
Adresse vorhanden, Optionen fehlen	DHCP-Optionen oder Gültigkeitsbereich fehlerhaft

Bei DHCP zusätzlich prüfen

- ist der richtige DHCP-Bereich aktiv?
- sind freie Adressen vorhanden?
- bestehen Ausschlüsse oder Reservierungen?
- stimmt die Subnetzmaske?
- wird das richtige Gateway verteilt?
- werden geeignete DNS-Server verteilt?
- stimmt der DHCP-Relay-Eintrag?
- ist DHCP Snooping korrekt konfiguriert?
- existiert ein nicht autorisierter DHCP-Server?
- erscheinen Fehler oder Konflikte im DHCP-Protokoll?

---

13. IPv6 nicht übersehen

Ein Client kann gleichzeitig IPv4 und IPv6 verwenden. Daher können Fehler nur eines Protokollstapels zu scheinbar widersprüchlichen Ergebnissen führen.

Zu prüfen sind:

- Link-Local-Adresse,
- globale oder lokale IPv6-Adresse,
- Präfixlänge,
- Standardroute,
- Router Advertisement,
- DNS-Server,
- DHCPv6, sofern eingesetzt,
- Duplicate Address Detection,
- Neighbor Discovery,
- Übergangs- oder Tunnelmechanismen,
- IPv6-Firewallregeln.

Windows

```
Get-NetIPAddress -AddressFamily IPv6
Get-NetRoute -AddressFamily IPv6
ipconfig /all
```

Linux

```
ip -6 address
ip -6 route
ip -6 neighbor
```

macOS

```
ifconfig
netstat -rn -f inet6
```

Wichtige Einordnung

- Eine Adresse aus `fe80::/10` ist eine IPv6-Link-Local-Adresse.
- Link-Local-Adressen gelten nur auf dem jeweiligen Link.
- Bei der Verwendung einer Link-Local-Adresse kann eine Schnittstellenangabe erforderlich sein.

- Ein funktionierendes IPv6 kann einen defekten IPv4-Pfad teilweise verdecken.
- Ein fehlerhafter IPv6-Pfad kann Verzögerungen erzeugen, obwohl IPv4 funktioniert.
- IPv6 sollte nicht allein zur Fehlerumgehung pauschal deaktiviert werden.

---

14. Lokalen Protokollstapel prüfen

Vor externen Zielen kann zunächst der lokale TCP/IP-Stapel geprüft werden.

IPv4

```
127.0.0.1
```

IPv6

```
::1
```

Windows

```
ping 127.0.0.1
ping ::1
```

Linux und macOS

```
ping 127.0.0.1
ping6 ::1
```

Abhängig vom Betriebssystem kann der IPv6-Befehl auch über `ping -6` erfolgen.

Ein erfolgreicher Loopback-Test bestätigt Teile des lokalen Protokollstapels. Er bestätigt nicht:

- den Netzwerkadapter,
- das Kabel,
- die WLAN-Verbindung,
- die VLAN-Zuordnung,
- das Standardgateway,
- den DNS-Dienst,
- die Erreichbarkeit anderer Systeme.

---

15. Eigene Adresse prüfen

Danach kann die eigene zugewiesene Adresse geprüft werden.

```
Loopback-Adresse
→ eigene IP-Adresse
→ Nachbar im selben Netz
→ Standardgateway
→ entferntes Ziel per IP
→ DNS-Server
→ Ziel per DNS-Namen
→ konkreter Dienst und Port
```

Auch ein erfolgreicher Ping auf die eigene Adresse bestätigt nicht automatisch, dass Pakete den physischen Netzwerkadapter tatsächlich verlassen.

---

16. ARP und Neighbor Discovery untersuchen

Für IPv4 wird ARP verwendet, um IPv4-Adressen auf MAC-Adressen im lokalen Netz abzubilden. IPv6 verwendet Neighbor Discovery über ICMPv6.

Windows

```
arp -a
Get-NetNeighbor
```

Linux

```
ip neighbor
```

macOS

```
arp -a
ndp -a
```

Mögliche Zustände

Beobachtung	mögliche Einordnung
Gateway besitzt gültigen Nachbareintrag	lokale Auflösung war grundsätzlich möglich
Eintrag bleibt unvollständig	Gegenstelle antwortet nicht oder Layer-2-Pfad fehlerhaft

Beobachtung	mögliche Einordnung
MAC-Adresse ändert sich unerwartet	Redundanz, Gatewaywechsel, Fehlkonfiguration oder Sicherheitsproblem
falsche MAC-Adresse	doppelter Adressgebrauch, ARP-Spoofing oder falsche Netzstruktur
viele unvollständige Einträge	Layer-2-, VLAN- oder Erreichbarkeitsproblem
Nachbareintrag vorhanden, Ping scheitert	ICMP kann blockiert sein oder Gegenstelle antwortet nicht

Ein vorhandener ARP- oder Neighbor-Eintrag beweist nicht die vollständige Erreichbarkeit eines Dienstes.

---

17. Standardgateway prüfen

Das Standardgateway leitet Daten zu Zielen außerhalb des lokalen Netzes weiter.

Zu prüfen sind:

- ist ein Gateway eingetragen?
- gehört das Gateway zum direkt erreichbaren Netz?
- ist eine passende Standardroute vorhanden?
- wird die richtige Schnittstelle verwendet?
- stimmt die Metrik beziehungsweise Priorität?
- ist das Gateway über ARP oder Neighbor Discovery erreichbar?
- antwortet es auf zulässige Tests?
- betrifft das Problem nur ein VLAN?
- ist die Gateway-Schnittstelle aktiv?
- bestehen redundante Gateways?
- funktionieren Hin- und Rückweg?

Windows

```
Get-NetRoute -DestinationPrefix "0.0.0.0/0"
Get-NetRoute -AddressFamily IPv6
route print
```

Linux

```
ip route
ip -6 route
```

macOS

```
route -n get default
netstat -rn
```

> Ein Gateway muss nicht auf ICMP-Echo-Anfragen antworten. Ein fehlgeschlagener Ping allein beweist deshalb keinen Gateway-Ausfall.

---

18. Lokales und entferntes Ziel unterscheiden

Ob ein Ziel lokal oder entfernt ist, ergibt sich aus:

- eigener IP-Adresse,
- Präfix beziehungsweise Subnetzmaske,
- Zieladresse,
- Routingtabelle.

Beispiel

```
Client: 192.168.10.24/24
Ziel A: 192.168.10.80
Ziel B: 192.168.20.80
```

`Ziel A` liegt im selben `/24`-Netz und wird normalerweise direkt über die lokale Verbindung erreicht.

`Ziel B` liegt in einem anderen Netz und benötigt eine passende Route, häufig über das Standardgateway.

Eine falsche Subnetzmaske kann dazu führen, dass der Client ein entferntes Ziel fälschlich als lokal behandelt oder ein lokales Ziel unnötig an ein Gateway sendet.

---

19. Routingtabelle auswerten

Die Routingentscheidung berücksichtigt unter anderem:

- Zielpräfix,
- Präfixlänge,
- Gateway,
- Schnittstelle,
- Metrik,
- Richtlinien,
- VPN-Routen,

- statische Routen,
- mehrere aktive Netzwerkadapter.

Grundsätzlich gewinnt die spezifischste passende Route, also die Route mit dem längsten passenden Präfix.

Beispiel

```
0.0.0.0/0          über 192.168.10.1
10.0.0.0/8         über VPN
10.20.30.0/24      über 192.168.10.254
```

Für ein Ziel in `10.20.30.0/24` ist die `/24`-Route spezifischer als die `/8`-Route und die Standardroute.

Typische Routingfehler

- keine Standardroute,
- falsches Gateway,
- falsche Präfixlänge,
- unerwünschte VPN-Route,
- gleiche Netze auf beiden Seiten eines VPN,
- mehrere Standardrouten,
- ungeeignete Metrik,
- fehlende Rückroute,
- asymmetrisches Routing,
- veraltete statische Route,
- falsche Schnittstellenbindung.

---

20. Erreichbarkeit schrittweise testen

Eine sinnvolle Testfolge lautet:

```
1. Loopback
2. eigene Adresse
3. Gegenstelle im selben Subnetz
4. Standardgateway
5. entferntes internes Ziel per IP
6. externer Dienst per IP
7. DNS-Server
8. Name eines internen Ziels
9. Name eines externen Ziels
10. konkreter TCP- oder UDP-Dienst
```

Die Ziele müssen bewusst ausgewählt werden. Eine beliebige öffentliche IP-Adresse oder Website ist nicht automatisch ein geeigneter Referenzpunkt.

Beispielhafte Dokumentation

Test	Ergebnis	Einordnung
Loopback erreichbar	erfolgreich	lokaler Protokollstapel grundsätzlich aktiv
eigene Adresse erreichbar	erfolgreich	lokale Adressbindung vorhanden
Gateway nicht erreichbar	fehlgeschlagen	Layer 2, VLAN, Gateway oder ICMP-Regel untersuchen
internes Ziel per IP erreichbar	erfolgreich	grundlegendes Routing vorhanden
interner Name nicht auflösbar	fehlgeschlagen	DNS gezielt untersuchen
Name wird aufgelöst, Port 443 nicht erreichbar	fehlgeschlagen	Dienst, Firewall, Route oder Zielsystem
Port 443 erreichbar, Browser scheitert	fehlgeschlagen	TLS, Proxy, Anwendung oder Authentifizierung

---

21. Ping richtig interpretieren

`ping` verwendet ICMP-Echo-Anfragen und kann Hinweise auf Erreichbarkeit und Laufzeit geben.

Ein erfolgreicher Ping kann bestätigen:

- das Ziel beziehungsweise eine antwortende Komponente ist erreichbar,
- ein Hin- und Rückweg für diese ICMP-Pakete besteht,
- die verwendete Zieladresse war grundsätzlich erreichbar.

Ein erfolgreicher Ping bestätigt nicht:

- dass DNS funktioniert,
- dass ein bestimmter TCP- oder UDP-Port erreichbar ist,
- dass die Anwendung funktioniert,
- dass keine Paketverluste bei anderer Last auftreten,
- dass der gesamte Pfad fehlerfrei ist,
- dass die Antwort tatsächlich vom erwarteten Anwendungsdienst stammt.

Ein fehlgeschlagener Ping beweist nicht automatisch:

- dass das Ziel ausgefallen ist,
- dass keine Route besteht,
- dass eine Firewall vollständig blockiert,
- dass das Netzwerk unterbrochen ist.

ICMP kann gefiltert, begrenzt oder vom Ziel nicht beantwortet werden.

---

22. Pfad mit Traceroute untersuchen

Windows

```
tracert <ziel>
Test-NetConnection <ziel> -TraceRoute
```

Linux

```
traceroute <ziel>
tracepath <ziel>
```

macOS

```
traceroute <ziel>
```

Traceroute-Werkzeuge senden Pakete mit schrittweise erhöhtem Hop Limit beziehungsweise TTL-Wert. Zwischenrouter können daraufhin ICMP-Meldungen zurückgeben.

Grenzen

- Router müssen nicht antworten.
- Ein Sternchen beweist keinen Ausfall.
- Hin- und Rückweg können unterschiedlich sein.
- Firewalls können die verwendeten Probe-Pakete filtern.
- Load Balancing kann unterschiedliche Pfade anzeigen.
- Der letzte sichtbare Hop ist nicht automatisch die Fehlerstelle.
- Hohe Antwortzeit eines Zwischenrouters beweist keine Weiterleitungsverzögerung.
- Unterschiedliche Implementierungen verwenden unterschiedliche Protokolle.

> Entscheidend ist nicht nur, welcher Hop antwortet, sondern ob nachfolgende Hops und der eigentliche Zieldienst erreichbar sind.

---

23. DNS getrennt von der Netzwerkverbindung prüfen

Wenn ein Ziel per IP-Adresse erreichbar ist, aber nicht über seinen Namen, liegt der Untersuchungsbereich häufig bei der Namensauflösung.

Zu prüfen sind:

- konfigurierte DNS-Server,
- Erreichbarkeit der DNS-Server,
- Suchdomänen,
- DNS-Suffix,
- Record-Typ,
- Name und Schreibweise,
- DNS-Cache,
- Split-DNS,
- VPN-DNS,
- Weiterleitungen,
- Rekursion,
- lokale Hosts-Datei,
- DNSSEC, sofern relevant,
- Ablaufzeit und Replikation,
- Filter- oder Sicherheitsdienst.

Windows

```
Resolve-DnsName <name>
nslookup <name>
Get-DnsClientServerAddress
Get-DnsClientCache
```

Linux

```
resolvectl query <name>
resolvectl status
dig <name>
```

macOS

```
scutil --dns
dig <name>
nslookup <name>
```

Gezielte Abfrage eines bestimmten DNS-Servers

```
dig @<dns-server> <name>
```

Mögliche Ergebnisse

Ergebnis	mögliche Einordnung
Name wird korrekt aufgelöst	DNS-Auflösung grundsätzlich erfolgreich
`NXDOMAIN`	Name existiert aus Sicht des antwortenden DNS-Systems nicht
Zeitüberschreitung	DNS-Server, Netzwerkpfad oder Firewall
falsche Adresse	veralteter oder fehlerhafter Eintrag, Cache oder Split-DNS
interner Name nur ohne VPN auflösbar	DNS-Zuweisung oder VPN-Routing untersuchen
externer Name funktioniert, interner nicht	interne Zone, Suchdomäne oder Split-DNS
ein DNS-Server antwortet, der andere nicht	Serverzustand, Pfad oder Konfiguration
AAAA vorhanden, IPv6-Pfad fehlerhaft	IPv6 und Anwendungsauswahl untersuchen

> `nslookup`, `dig`, `Resolve-DnsName` und die Namensauflösung einer Anwendung können unterschiedliche Auflösungswege oder Bibliotheken verwenden. Ergebnisse müssen im Kontext des Betriebssystems und der Anwendung bewertet werden.

---

24. Port und Dienst statt nur Host testen

Ein erreichbarer Host bestätigt nicht, dass der benötigte Dienst erreichbar ist.

Windows

```
Test-NetConnection <ziel> -Port 443
```

Linux und macOS

```
nc -vz <ziel> 443
```

HTTP beziehungsweise HTTPS

```
curl -I https://<ziel>
curl -v https://<ziel>
```

TLS-Verbindung

```
openssl s_client -connect <ziel>:443 -servername <dns-name>
```

Die Werkzeuge müssen auf dem jeweiligen System vorhanden sein. Vertrauliche Header, Tokens, Cookies und Zertifikatsdaten dürfen nicht ungeprüft in Tickets oder öffentliche Dokumentationen übernommen werden.

Mögliche Ergebnisse

Ergebnis	mögliche Einordnung
Verbindung hergestellt	TCP-Verbindung zum Port grundsätzlich möglich
Verbindung abgelehnt	Ziel erreichbar, aber Dienst nicht aktiv oder Port geschlossen
Zeitüberschreitung	Filterung, Routing, Zielzustand oder Rückweg
TLS-Fehler	Zertifikat, Protokollversion, SNI, Uhrzeit oder Inspektion
HTTP `401` oder `403`	Dienst erreichbar, Authentifizierung oder Berechtigung erforderlich
HTTP `404`	Webdienst erreichbar, angeforderte Ressource nicht gefunden
HTTP `500`	serverseitiger Anwendungsfehler
Umleitungsschleife	Proxy-, Anwendung-, TLS- oder URL-Konfiguration

---

25. Lokale Firewall prüfen

Eine lokale Firewall kann eingehenden oder ausgehenden Verkehr abhängig von folgenden Merkmalen filtern:

- Quell- und Zieladresse,
- Protokoll,
- Port,
- Netzwerkprofil,
- Schnittstelle,
- Anwendung,
- Benutzer,
- Dienst,
- Richtung,
- Sicherheitsrichtlinie.

Windows

```
Get-NetFirewallProfile
Get-NetFirewallRule -Enabled True
```

Linux

Je nach System können unter anderem verwendet werden:

```
nft list ruleset
iptables -S
ufw status verbose
firewall-cmd --state
```

macOS

```
/usr/libexec/ApplicationFirewall/socketfilterfw --getglobalstate
pfctl -s info
```

Zum Auslesen einzelner Firewallinformationen können erhöhte Rechte erforderlich sein.

> Eine Firewall sollte nicht pauschal und dauerhaft deaktiviert werden. Besser ist ein zeitlich begrenzter, dokumentierter Test mit Freigabe oder die gezielte Auswertung von Protokollen und Regeln.

---

26. Netzwerk-Firewalls und ACLs berücksichtigen

Zwischen Client und Ziel können mehrere Filterinstanzen liegen:

- Switch-ACL,
- Router-ACL,
- VLAN-Firewall,
- Host-Firewall,
- Standort-Firewall,
- Cloud-Firewall,
- Security Group,
- Web Application Firewall,
- Proxy,
- VPN-Gateway,
- Netzwerkzugangskontrolle.

Zu prüfen sind:

- Quelle,
- Ziel,
- Protokoll,
- Quellport,
- Zielport,
- Richtung,
- Zeitstempel,
- zustandsbehaftete Sitzung,
- NAT-Übersetzung,
- passende Regel,
- Regelreihenfolge,
- Protokolleintrag,
- Rückweg.

Eine scheinbar passende Freigaberegel kann wirkungslos sein, wenn:

- eine frühere Regel den Verkehr blockiert,
- die falsche Zone verwendet wird,
- die tatsächliche Quelladresse durch NAT verändert wurde,
- die Anwendung einen zusätzlichen Port benötigt,
- der Rückweg fehlt,
- IPv6 anders behandelt wird als IPv4.

---

27. Proxy-Konfiguration untersuchen

Ein Proxy kann nur bestimmte Anwendungen oder Protokolle beeinflussen. Deshalb kann beispielsweise `ping` funktionieren, während der Browser keine Website öffnet.

Zu prüfen sind:

- manueller Proxy,
- automatisch erkannter Proxy,
- PAC-Datei,
- systemweiter Proxy,
- anwendungseigener Proxy,
- Authentifizierung,
- Ausnahmeliste,
- HTTPS-Inspektion,
- Erreichbarkeit des Proxyservers,
- Namensauflösung des Proxys,
- Zertifikatsvertrauen,
- Umgebungsvariablen.

Windows

```
netsh winhttp show proxy
Get-ItemProperty "HKCU:\Software\Microsoft\Windows\CurrentVersion\Internet Settings"
```

Linux und macOS

```
env | grep -i proxy
```

macOS zusätzlich

```
scutil --proxy
```

Sensible Inhalte aus PAC-Dateien, Proxyadressen oder Zugangsdaten dürfen nicht ungeschützt dokumentiert werden.

---

28. VPN als eigene Fehlerdomäne behandeln

Ein VPN verändert möglicherweise:

- Routingtabelle,
- Standardroute,
- DNS-Server,
- Suchdomänen,
- MTU,
- Firewallregeln,
- Proxykonfiguration,
- Quelladresse,
- erreichbare Netze.

Vergleichstests

```
ohne VPN
→ mit VPN
→ internes Ziel
→ externes Ziel
→ Ziel per IP
→ Ziel per Namen
→ Routingtabelle vorher und nachher
→ DNS-Konfiguration vorher und nachher
```

Typische VPN-Probleme

- überlappende lokale und entfernte Netze,
- fehlende Route,
- falsches Split Tunneling,
- gesamter Verkehr unerwartet durch den Tunnel,
- interner DNS-Server nicht erreichbar,
- MTU- oder Fragmentierungsproblem,
- abgelaufenes Zertifikat,
- fehlgeschlagene Authentifizierung,
- lokale Firewallregel,
- instabile Internetverbindung,
- fehlerhafter VPN-Adapter.

---

29. MTU- und Fragmentierungsprobleme

Ein Pfad kann kleine Pakete übertragen, während größere Übertragungen scheitern oder hängen bleiben.

Mögliche Symptome sind:

- Ping mit kleinen Paketen funktioniert,
- Webseiten laden nur teilweise,
- Dateiübertragungen bleiben stehen,
- VPN-Verbindungen sind instabil,
- TLS-Verbindungen brechen ab,
- einzelne Anwendungen funktionieren, andere nicht.

Mögliche Ursachen:

- ungeeignete MTU,
- VPN-Overhead,
- PPPoE-Overhead,
- blockierte ICMP-Meldungen für Path MTU Discovery,
- Tunnel oder Kapselung,
- fehlerhafte Fragmentierungsbehandlung.

Windows – Beispieltest

```
ping <ziel> -f -l <nutzlastgröße>
```

Linux – Beispieltest

```
ping -M do -s <nutzlastgröße> <ziel>
```

Die geeignete Nutzlastgröße hängt vom Protokoll, Betriebssystem und Pfad ab. Ein einzelner Testwert darf nicht ohne Einordnung als allgemeingültige MTU übernommen werden.

---

30. Mehrere aktive Netzwerkadapter

Ein Client kann gleichzeitig verbunden sein über:

- Ethernet,
- WLAN,
- Mobilfunk,
- VPN,
- virtuelle Maschine,
- Container-Bridge,
- USB-Netzwerkadapter,
- Dockingstation,
- Host-only-Netz,
- virtuelle Switches.

Dadurch können entstehen:

- mehrere Standardrouten,
- unerwartete Metriken,
- falscher DNS-Server,
- asymmetrisches Routing,
- Namensauflösung über die falsche Schnittstelle,
- falsche Quelladresse,
- nicht erreichbare lokale Netze,
- VPN-Konflikte.

Kontrollierter Test

1. aktuelle Adapter und Routen dokumentieren.
2. tatsächlich verwendete Route zum Ziel bestimmen.
3. nicht benötigte Verbindung nur mit Freigabe vorübergehend trennen.
4. Test wiederholen.
5. ursprünglichen Zustand wiederherstellen.
6. Ursache dauerhaft in der Adapter-, Routing- oder VPN-Konfiguration beheben.

---

31. Vergleichstests richtig verwenden

Ein guter Vergleichstest verändert nur eine relevante Komponente.

Mögliche Vergleichskomponenten sind:

- geprüftes Netzwerkkabel,

- anderer Switchport,
- andere Datendose,
- anderer Netzwerkadapter,
- andere Dockingstation,
- anderer Client,
- anderer Benutzer,
- anderes VLAN,
- anderes WLAN,
- anderes Ziel,
- Verbindung ohne VPN,
- Verbindung ohne Proxy,
- direkte Verbindung statt Dockingstation.

Beispiel

```
Ursprünglich:
Client A + Dock A + Kabel A + Dose A → Fehler

Vergleich 1:
Client A + Dock A + geprüftes Kabel B + Dose A → Fehler

Vergleich 2:
Client A + Dock B + geprüftes Kabel B + Dose A → funktioniert
```

Damit wird Dock A zum Hauptverdacht. Vor dem endgültigen Austausch sollte das Ergebnis reproduziert und die übrige Konfiguration verglichen werden.

> Wenn bei einem Test gleichzeitig Kabel, Port, Dock und Benutzer gewechselt werden, lässt sich aus dem Erfolg keine einzelne Ursache ableiten.

---

32. Paketaufzeichnung gezielt einsetzen

Wenn Statusanzeigen und Standardtests keine ausreichende Erklärung liefern, kann eine Paketaufzeichnung zeigen, welche Kommunikation tatsächlich stattfindet.

Geeignete Werkzeuge sind beispielsweise:

- Wireshark,
- `tcpdump`,
- `tshark`,
- Windows-Paketaufzeichnungswerkzeuge,

- Port Mirroring beziehungsweise SPAN,
- Capture-Funktionen auf Firewalls, Routern oder Access Points.

Mögliche Fragestellungen

- verlässt eine DHCP-Anfrage den Client?
- antwortet ein DHCP-Server?
- wird eine ARP-Anfrage beantwortet?
- erfolgt eine DNS-Anfrage?
- welcher DNS-Server antwortet?
- wird ein TCP-SYN gesendet?
- kommt ein SYN-ACK oder RST zurück?
- findet eine TLS-Aushandlung statt?
- treten Wiederholungen oder Zeitüberschreitungen auf?
- wird ICMP zur Fehleranzeige zurückgesendet?
- kommuniziert die Anwendung mit dem erwarteten Ziel?

Beispielhafte Filter

```
arp
dhcp
dns
icmp
icmpv6
tcp.port == 443
ip.addr == 192.0.2.10
```

Datenschutz und Sicherheit

Paketaufzeichnungen können enthalten:

- IP-Adressen,
- Hostnamen,
- Benutzernamen,
- Sitzungsdaten,
- DNS-Anfragen,
- unverschlüsselte Inhalte,
- Authentifizierungsinformationen,
- interne Systemstrukturen.

Aufzeichnungen dürfen nur mit Berechtigung erstellt, auf das erforderliche Zeitfenster begrenzt, sicher gespeichert und kontrolliert weitergegeben werden.

---

33. Typische TCP-Beobachtungen

Erfolgreicher Verbindungsaufbau

```
Client → Server: SYN
Server → Client: SYN, ACK
Client → Server: ACK
```

Port geschlossen

```
Client → Server: SYN
Server → Client: RST, ACK
```

Keine sichtbare Antwort

```
Client → Server: SYN
Client → Server: erneutes SYN
Client → Server: weiteres SYN
```

Mögliche Ursachen für eine ausbleibende Antwort sind:

- Filterung,
- Ziel nicht erreichbar,
- Rückroute fehlt,
- Server antwortet nicht,
- Paket erreicht das Ziel nicht,
- Antwort erreicht den Client nicht.

Eine Paketaufzeichnung an nur einer Stelle zeigt nicht automatisch, an welcher Stelle des gesamten Pfades das Paket verloren geht.

---

34. Ereignisprotokolle gemeinsam auswerten

Relevante Quellen können sein:

- Client-Ereignisprotokolle,
- NetworkManager- oder Systemprotokolle,
- DHCP-Serverprotokolle,
- DNS-Protokolle,
- Switch- und Routerprotokolle,
- Firewallprotokolle,
- VPN-Protokolle,
- Proxyprotokolle,
- Access-Point- und Controllerprotokolle,

- Authentifizierungsserver,
- Zielserverprotokolle,
- Monitoringdaten.

Alle Ereignisse sollten anhand eines möglichst genauen Zeitstempels zusammengeführt werden.

Zeitbezug

```
14:31:02 Client verliert Link
14:31:04 Switchport meldet Down
14:31:09 Switchport meldet Up
14:31:11 DHCP Discover
14:31:11 DHCP Offer
14:31:12 DHCP Request
14:31:12 DHCP ACK
14:31:14 DNS-Anfrage erfolgreich
```

Diese zeitliche Korrelation liefert stärkere Hinweise als voneinander getrennte Einzelmeldungen.

---

35. Praxisfall A: Client erhält eine Adresse aus 169.254.0.0/16

Symptom

- Link ist aktiv.
- Client besitzt `169.254.37.18/16`.
- Standardgateway fehlt.
- interne und externe Ziele sind nicht erreichbar.

Prüfung

1. Adapterstatus dokumentieren.
2. Switchport und VLAN bestimmen.
3. anderes Gerät am selben Anschluss testen.
4. DHCP-Lease und DHCP-Clientprotokoll prüfen.
5. DHCP-Ablauf aufzeichnen.
6. Switch-Sicherheitsfunktionen prüfen.
7. DHCP-Relay kontrollieren.
8. DHCP-Bereich und freie Adressen prüfen.
9. Änderung einzeln durchführen.
10. neue Adressvergabe und Erreichbarkeit kontrollieren.

Mögliche Ursache

Der Switchport wurde nach einem Arbeitsplatzwechsel dem falschen VLAN zugeordnet. Der DHCP-Broadcast erreicht dadurch nicht den DHCP-Relay des vorgesehenen Clientnetzes.

Nachprüfung

- richtige IPv4-Adresse erhalten,
- Gateway vorhanden,
- geeignete DNS-Server vorhanden,
- internes Ziel erreichbar,
- externer Dienst erreichbar,
- erneute Adressvergabe erfolgreich,
- Portkonfiguration dokumentiert.

---

36. Praxisfall B: IP-Ziele funktionieren, DNS-Namen nicht

Symptom

- Standardgateway erreichbar.
- internes Ziel über IP-Adresse erreichbar.
- Name `intranet.example.internal` wird nicht aufgelöst.

Prüfung

1. konfigurierte DNS-Server dokumentieren.
2. DNS-Server per IP testen.
3. Namen über jeden DNS-Server einzeln abfragen.
4. DNS-Suffix und Suchdomäne prüfen.
5. VPN- und Split-DNS-Konfiguration vergleichen.
6. DNS-Zone und Resource Record prüfen.
7. Cache nur bei begründetem Verdacht kontrolliert leeren.
8. Auflösung und Anwendung erneut testen.

Mögliche Ursache

Nach dem Aufbau des VPN wird weiterhin ein öffentlicher DNS-Server verwendet. Dieser kennt die interne Zone nicht.

Nachprüfung

- interner Name wird korrekt aufgelöst,
- erwartete IP-Adresse wird geliefert,
- Anwendung erreicht das Ziel,
- öffentliche Namensauflösung funktioniert weiterhin,
- Verhalten nach erneuter VPN-Verbindung bleibt korrekt.

---

37. Praxisfall C: Website antwortet nicht, Ping funktioniert

Symptom

- Zielname wird korrekt aufgelöst.
- Ping zum Ziel ist erfolgreich.
- HTTPS-Verbindung scheitert.

Prüfung

1. aufgelöste Zieladresse dokumentieren.
2. TCP-Port 443 testen.
3. Pfad zum Ziel untersuchen.
4. lokale und zentrale Firewallprotokolle prüfen.
5. Proxykonfiguration prüfen.
6. TLS-Verbindung untersuchen.
7. Dienstzustand am Ziel prüfen.
8. Vergleich von internem und externem Zugriff durchführen.

Mögliche Ergebnisse

Ergebnis	Einordnung
TCP-Port 443 abgelehnt	Host erreichbar, Dienst nicht aktiv oder Port geschlossen
TCP-Verbindung läuft in Timeout	Firewall, Routing oder Rückweg
TLS-Zertifikat abgelaufen	Transport funktioniert, TLS-Vertrauen scheitert
Proxy meldet Zugriff verweigert	Proxyregel oder Berechtigung
HTTP `503`	Webdienst oder nachgelagerter Dienst nicht verfügbar
direkter Zugriff funktioniert, Proxyzugriff nicht	Proxykonfiguration oder Proxyzustand

---

38. Praxisfall D: Nur über die Dockingstation kein Netzwerk

Symptom

- WLAN funktioniert.
- integrierter Netzwerkanschluss beziehungsweise anderer Adapter funktioniert.
- Ethernet über die Dockingstation fällt wiederholt aus.

Prüfung

1. Dockmodell und Anschlussart dokumentieren.
2. Linkstatus und Fehlerzähler prüfen.
3. Stromversorgung des Docks kontrollieren.
4. geprüftes Kabel verwenden.

5. anderen USB-C- beziehungsweise Thunderbolt-Anschluss testen.
6. Vergleichsdock verwenden.
7. Treiber- und Firmwarestand nach Herstellerangabe prüfen.
8. Energiesparverhalten untersuchen.
9. Ereignisprotokolle zum Zeitpunkt der Trennung auswerten.
10. Langzeittest nach der Maßnahme durchführen.

Mögliche Ursachen

- instabile Stromversorgung,
- Dock-Firmware,
- Treiber,
- USB-Verbindung,
- defekter Netzwerkcontroller,
- ungeeignetes Kabel,
- Energiesparzustand,
- thermisches Problem.

---

39. Praxisfall E: Interne Systeme funktionieren nur ohne VPN

Symptom

- ohne VPN sind lokale Systeme erreichbar.
- nach dem VPN-Aufbau sind bestimmte lokale Netze nicht erreichbar.
- Internetzugriff funktioniert weiterhin.

Prüfung

1. Routingtabelle vor VPN-Verbindung sichern.
2. Routingtabelle nach VPN-Verbindung sichern.
3. DNS-Konfiguration vergleichen.
4. Zielnetz und lokales Clientnetz vergleichen.
5. überlappende Präfixe suchen.
6. verwendete Route zum Ziel bestimmen.
7. Split-Tunneling-Richtlinie prüfen.
8. VPN-Firewall- und Zugriffsrichtlinien prüfen.
9. kontrollierten Test mit geeignetem nicht überlappendem Netz durchführen.
10. dauerhafte Netz- oder VPN-Konfiguration korrigieren.

Mögliche Ursache

Das lokale Netz und ein entferntes Unternehmensnetz verwenden dasselbe IPv4-Präfix. Der Client kann nicht eindeutig bestimmen, ob das Ziel lokal oder über den VPN-Tunnel erreichbar ist.

---

40. Ungeeignete Sofortmaßnahmen

Folgende Maßnahmen können Spuren vernichten, neue Fehler erzeugen oder den ursprünglichen Zustand unklar machen:

- Client sofort neu starten,
- Switchport ohne Dokumentation umkonfigurieren,
- Netzwerkadapter zurücksetzen,
- alle gespeicherten WLAN-Profile löschen,
- DHCP-Adresse mehrfach ungeprüft erneuern,
- DNS-Cache ohne vorherige Prüfung leeren,
- Firewall vollständig deaktivieren,
- IPv6 pauschal abschalten,
- VPN-Client neu installieren,
- Netzwerkstack zurücksetzen,
- Treiber ungeprüft ersetzen,
- mehrere Kabel und Ports gleichzeitig wechseln,
- statische Adresse als dauerhafte Umgehung eintragen,
- Router oder Switch ohne Freigabe neu starten.

Solche Maßnahmen sind nicht grundsätzlich verboten. Sie müssen jedoch begründet, freigegeben, dokumentiert und anschließend vollständig überprüft werden.

---

41. Häufige Fehlinterpretationen

Aussage	fachliche Einordnung
„Der Link leuchtet, also funktioniert das Netzwerk.“	Ein Link bestätigt keine gültige IP-Konfiguration oder Ende-zu-Ende-Verbindung.
„Der Client hat eine IP-Adresse, also funktioniert DHCP.“	Die Adresse kann statisch, veraltet, link-local oder aus dem falschen Netz sein.
„Das Gateway antwortet nicht auf Ping, also ist es ausgefallen.“	ICMP-Echo kann gefiltert oder deaktiviert sein.
„Ping funktioniert, also liegt es an der Anwendung.“	Der benötigte Dienst, Port, DNS, Proxy oder TLS kann weiterhin fehlerhaft sein.
„Eine Website funktioniert, also funktioniert DNS.“	Die Adresse kann aus einem Cache stammen oder die Anwendung kann einen anderen Resolver verwenden.
„Eine Adresse aus 169.254.0.0/16 beweist einen defekten DHCP-Server.“	VLAN, Relay, Switchport, Client oder Sicherheitsfunktionen können ursächlich sein.
„Traceroute endet an Router X, also ist Router X defekt.“	Router können Antworten filtern, obwohl sie Daten weiterhin übertragen.
„Ohne Firewall funktioniert es, also muss sie dauerhaft deaktiviert bleiben.“	Die konkrete Regel oder Zuordnung muss ermittelt und gezielt korrigiert werden.
„Ein anderes Kabel funktioniert, also ist ausschließlich das ursprüngliche Kabel defekt.“	Auch Kontakte, Position oder mechanische Belastung wurden verändert.

Aussage	fachliche Einordnung
„Nach dem Neustart funktioniert es, also ist der Fehler behoben.“	Ein Neustart kann Symptome beseitigen, ohne die Ursache zu erklären.
„IPv4 funktioniert, also ist die gesamte Netzwerkverbindung in Ordnung.“	Anwendungen können IPv6 bevorzugen oder beide Protokolle verwenden.
„Der Fehler liegt sicher beim Provider.“	Lokale Verbindung, DNS, Routing, Firewall und Zielsystem müssen getrennt geprüft werden.

---

42. Vollständige Prüfreihenfolge

1. genaue Anwendung, Zieladresse und Fehlermeldung bestimmen.
2. Zeitpunkt und letzte bekannte Funktion dokumentieren.
3. betroffene Benutzer, Clients, Netze und Standorte bestimmen.
4. Ethernet, WLAN, VPN und Proxy unterscheiden.
5. Ausgangskonfiguration sichern.
6. physische Verbindung beziehungsweise WLAN-Zustand prüfen.
7. Netzwerkadapter und Fehlerzähler untersuchen.
8. IPv4- und IPv6-Konfiguration bewerten.
9. DHCP-Zustand prüfen.
10. lokale Routingtabelle auswerten.
11. ARP beziehungsweise Neighbor Discovery kontrollieren.
12. Standardgateway und lokales Netz untersuchen.
13. entferntes Ziel gezielt per IP-Adresse testen.
14. DNS-Auflösung separat prüfen.
15. konkreten Zielport und Dienst testen.
16. Pfad bei Bedarf mit Traceroute untersuchen.
17. lokale Firewall, zentrale Firewall und ACLs berücksichtigen.
18. Proxy- und VPN-Konfiguration vergleichen.
19. System-, Netzwerk- und Serverprotokolle zeitlich korrelieren.
20. bei Bedarf eine autorisierte Paketaufzeichnung erstellen.
21. kontrollierten Vergleichstest mit nur einer Änderung durchführen.
22. Hypothese anhand der Ergebnisse bestätigen oder verwerfen.
23. freigegebene Korrektur umsetzen.
24. ursprünglichen Test wiederholen.
25. verwandte Funktionen und mögliche Nebenwirkungen prüfen.
26. Ursache, Maßnahme und Nachweis dokumentieren.

---

43. Dokumentationsbeispiel

```
Ticket: INC-20481
Zeitpunkt: 01.08.2026, 09:18 Uhr
Client: NB-204
```

Standort: Gebäude B, Raum 204

Anschluss: Dockingstation über Ethernet

Symptom: keine internen oder externen Ziele erreichbar

Ausgangszustand:

- physischer Link aktiv
- IPv4-Adresse 169.254.37.18/16
- kein Standardgateway
- kein verwendbarer DNS-Server
- WLAN deaktiviert
- anderer Client an derselben Dose ebenfalls ohne DHCP-Adresse

Hypothese:

Der Switchport befindet sich nach dem Arbeitsplatzwechsel im falschen VLAN.

Prüfung:

- Portbezeichnung mit Dokumentation verglichen
- tatsächliche VLAN-Zuordnung am Switch geprüft
- DHCP-Verkehr im zugewiesenen VLAN kontrolliert
- Port war dem Drucker-VLAN statt dem Client-VLAN zugeordnet

Ursache:

Fehlerhafte VLAN-Zuordnung des Switchports nach einer Portänderung.

Maßnahme:

Switchport nach Freigabe dem vorgesehenen Client-VLAN zugeordnet.

Nachprüfung:

- DHCP-Adresse aus dem vorgesehenen Clientnetz erhalten
- Standardgateway und DNS-Server korrekt
- internes Ziel per IP erreichbar
- interne DNS-Auflösung erfolgreich
- HTTPS-Anwendung erreichbar
- erneute DHCP-Adressvergabe erfolgreich
- Switchport und Dokumentation stimmen überein

Nebenwirkungen:

Keine Auffälligkeiten an benachbarten Ports oder im vorgesehenen VLAN festgestellt.

44. Checkliste Client ohne Netzwerkverbindung

- [ ] konkrete Fehlermeldung wurde erfasst.
- [ ] betroffene Anwendung und Zieladresse sind bekannt.
- [ ] Beginn und letzte bekannte Funktion wurden dokumentiert.
- [ ] vorausgegangene Änderungen wurden erfragt.
- [ ] Umfang der Störung wurde bestimmt.
- [ ] Ethernet, WLAN, VPN und Proxy wurden unterschieden.
- [ ] Ausgangszustand wurde vor Änderungen gesichert.
- [ ] physischer Link beziehungsweise WLAN-Status wurde geprüft.
- [ ] Netzwerkadapter und Treiberstatus wurden kontrolliert.
- [ ] Fehler- und Verwerfungszähler wurden geprüft.
- [ ] IPv4-Adresse und Präfix wurden bewertet.
- [ ] IPv6-Konfiguration wurde berücksichtigt.
- [ ] Standardgateway wurde geprüft.
- [ ] DNS-Server wurden dokumentiert.
- [ ] DHCP-Status und Lease wurden untersucht.
- [ ] ARP beziehungsweise Neighbor Discovery wurde geprüft.
- [ ] Routingtabelle wurde ausgewertet.
- [ ] lokales und entferntes Ziel wurden unterschieden.
- [ ] Ziel wurde kontrolliert per IP-Adresse getestet.
- [ ] DNS-Auflösung wurde separat getestet.
- [ ] benötigter Port und Dienst wurden geprüft.
- [ ] Ping-Ergebnisse wurden nicht überbewertet.
- [ ] Traceroute-Ergebnisse wurden fachlich eingeordnet.
- [ ] lokale Firewall wurde berücksichtigt.
- [ ] zentrale Firewall und ACLs wurden berücksichtigt.
- [ ] Proxykonfiguration wurde geprüft.
- [ ] VPN-Routen und VPN-DNS wurden geprüft.
- [ ] mehrere aktive Adapter wurden berücksichtigt.
- [ ] kontrollierter Vergleichstest veränderte nur eine Komponente.
- [ ] Paketaufzeichnung erfolgte nur mit Berechtigung.
- [ ] Protokolle wurden anhand der Zeitstempel korreliert.
- [ ] Ursache wurde von Symptom und Vermutung getrennt.
- [ ] Änderung wurde freigegeben und dokumentiert.

- [ ] ursprünglicher Test wurde nach der Maßnahme wiederholt.
- [ ] verwandte Funktionen und Nebenwirkungen wurden geprüft.
- [ ] Ursache, Maßnahme und Ergebnis wurden dokumentiert.

---

45. Schnellreferenz

Prüfschritt	geeignete Information	typische Auffälligkeit
Umfang	betroffene Clients, Dienste und Standorte	mehrere Geräte oder nur eine Anwendung
Verbindung	Link, SSID, Authentifizierung	Link down oder falsches WLAN
Adapter	Zustand, Treiber, Fehlerzähler	deaktiviert, instabil oder hohe Fehler
IPv4	Adresse, Präfix, Gateway	`169.254.0.0/16`, falsches Netz oder kein Gateway
IPv6	Adresse, Route, Neighbor	nur Link-Local oder fehlende Standardroute
DHCP	Server, Lease, Optionen	kein Offer, falsche Optionen oder erschöpfter Bereich
Layer 2	ARP, Neighbor, VLAN	unvollständiger Eintrag oder falsches VLAN
Routing	Route, Gateway, Metrik	falsche oder fehlende Route
DNS	Server, Antwort, Record	Timeout, `NXDOMAIN` oder falsche Adresse
Transport	Zielport und TCP-Zustand	Timeout, RST oder TLS-Fehler
Firewall	Regel und Protokoll	Blockierung der tatsächlichen Quelle oder Zone
Proxy	PAC, Authentifizierung, Ausnahme	Browser betroffen, andere Tests erfolgreich
VPN	Routen, DNS und MTU	Netzüberlappung oder falsches Split Tunneling
Zielsystem	Dienst und Protokoll	Port geschlossen oder Anwendung fehlerhaft
Nachprüfung	ursprünglicher Test	Symptom beseitigt und keine Nebenwirkungen

---

Merksatz

> „Kein Netzwerk“ ist keine Ursache, sondern eine ungenaue Symptombeschreibung. Eine belastbare Analyse bestimmt zuerst den Umfang und prüft anschließend kontrolliert Verbindung, Adapter, IP-Konfiguration, DHCP, lokales Netz, Gateway, Routing, DNS, Zielport und Anwendung. Jeder erfolgreiche Test bestätigt nur den tatsächlich geprüften Teil des Kommunikationswegs.

Quellen und weiterführende Dokumentation

- Microsoft Learn – Get-NetIPConfiguration
- Microsoft Learn – Get-NetAdapter
- Microsoft Learn – Get-NetRoute
- Microsoft Learn – Resolve-DnsName
- Microsoft Learn – Test-NetConnection
- Microsoft Learn – Windows-Befehle für TCP/IP-Diagnose
- Red Hat – NetworkManager mit nmcli verwalten
- Apple – networksetup Manual Page
- Wireshark – Benutzerhandbuch
- Wireshark – Display Filter Reference
- RFC 2131 – Dynamic Host Configuration Protocol
- RFC 3927 – Dynamic Configuration of IPv4 Link-Local Addresses
- RFC 8200 – Internet Protocol, Version 6
- RFC 4861 – Neighbor Discovery for IPv6
- RFC 826 – Address Resolution Protocol
- RFC 1034 – Domain Names: Concepts and Facilities
- RFC 1035 – Domain Names: Implementation and Specification
