7.1 Ein Client hat kein Netzwerk

Wenn nur ein einzelner Client keine Netzwerkverbindung besitzt, sollte die Fehlersuche schnell feststellen, auf welcher Ebene die Verbindung unterbrochen ist:

1. Netzwerkadapter,
2. physische oder drahtlose Verbindung,
3. IP-Konfiguration,
4. lokales Netzwerk,
5. Routing,
6. DNS,
7. Zielsystem oder Anwendung.

Dieser Entscheidungsbaum dient der schnellen Eingrenzung. Die ausführliche Ende-zu-Ende-Analyse befindet sich auf der Seite **6.1 Client ohne Netzwerkverbindung – systematische Ende-zu-Ende-Analyse**.

---

1. Störungsumfang bestimmen

Zuerst prüfen:

- ist wirklich nur ein Client betroffen,
- funktionieren andere Clients am selben Switch oder Access Point,
- betrifft der Fehler Ethernet, WLAN oder beide Verbindungsarten,
- sind interne Ziele, das Internet oder nur einzelne Dienste nicht erreichbar,
- begann die Störung nach einer Änderung,
- funktioniert der Client an einem anderen Anschluss oder in einem anderen WLAN?

Beobachtung	Nächster Untersuchungsbereich
nur ein Client betroffen	Client, Anschluss, Kabel, WLAN oder lokale Konfiguration
mehrere Clients betroffen	Switch, Access Point, VLAN, DHCP, Gateway oder Standortverbindung
nur eine Anwendung betroffen	Anwendung, Proxy, Dienst, Port oder Zertifikat
IP-Ziele erreichbar, Namen nicht	DNS
interne Ziele erreichbar, Internet nicht	Gateway, Firewall, Proxy oder Internetübergang
Internet erreichbar, interne Ziele nicht	Routing, VPN, interne DNS-Zone oder Zugriffskontrolle
Ethernet betroffen, WLAN funktioniert	Kabel, Switchport, Ethernetadapter oder VLAN
WLAN betroffen, Ethernet funktioniert	WLAN-Profil, Authentifizierung, Signal oder Access Point
beide Verbindungsarten betroffen	Clientkonfiguration, VPN, Firewall, Routing oder Betriebssystem

Wenn mehrere Clients betroffen sind, zum Entscheidungsbaum für Standort- oder Bereichsstörungen wechseln.

---

2. Besteht eine Verbindung zum Netzwerkmedium?

Ethernet

Prüfen:

- ist das Netzwerkkabel vollständig eingesteckt,
- leuchten oder blinken die Link-LEDs,
- ist der Adapter aktiviert,
- erkennt Windows eine Verbindung,
- funktioniert ein geprüftes Ersatzkabel,
- funktioniert derselbe Anschluss mit einem Vergleichsgerät,
- funktioniert der Client an einem anderen freigegebenen Switchport?

Adapterstatus anzeigen:

```
Get-NetAdapter
```

Nur physische Adapter anzeigen:

```
Get-NetAdapter -Physical
```

Ausführliche Adapterinformationen:

```
Get-NetAdapter | Format-List Name, InterfaceDescription, Status, LinkSpeed, MacAddress
```

Entscheidung

- Status `Up` → mit der IP-Konfiguration fortfahren.
- Status `Disconnected` → Kabel, Dose, Patchfeld, Switchport und Adapter prüfen.
- Status `Disabled` → klären, warum der Adapter deaktiviert ist.
- Adapter fehlt vollständig → Geräteerkennung, Treiber, Hardware oder BIOS/UEFI prüfen.
- Link besteht nur mit einem anderen Kabel → ursprüngliches Kabel austauschen.
- Link besteht nur an einem anderen Port → ursprünglichen Anschluss und dessen Konfiguration untersuchen.

Ein leuchtendes Link-Signal bestätigt nur die physische Verbindung. Es beweist nicht, dass VLAN, DHCP, Routing, DNS oder Anwendungen funktionieren.

WLAN

WLAN-Schnittstelle und Verbindungszustand anzeigen:

```
netsh wlan show interfaces
```

Sichtbare WLAN-Netze anzeigen:

```
netsh wlan show networks
```

Gespeicherte WLAN-Profile anzeigen:

```
netsh wlan show profiles
```

Prüfen:

- ist WLAN eingeschaltet,
- ist der Flugmodus ausgeschaltet,
- wird die vorgesehene SSID angezeigt,
- ist der Client tatsächlich mit dieser SSID verbunden,
- stimmt die BSSID beziehungsweise der verbundene Access Point,
- ist die Signalqualität ausreichend,
- wurde die WLAN-Authentifizierung erfolgreich abgeschlossen,
- verwendet der Client das vorgesehene Benutzer- oder Computerzertifikat,
- greift eine zentrale WLAN-Richtlinie,
- wurde der Client in das richtige VLAN eingeordnet?

Entscheidung

- SSID nicht sichtbar → Reichweite, Access Point, Funkband, Kanal, Treiber oder Richtlinie prüfen.
- SSID sichtbar, Verbindung scheitert → Profil, Schlüssel, 802.1X, Zertifikat oder RADIUS untersuchen.
- WLAN verbunden, aber keine gültige IP-Konfiguration → DHCP oder VLAN prüfen.
- Verbindung besteht mit falscher SSID → mit dem vorgesehenen Netz verbinden.
- sehr schwaches oder stark schwankendes Signal → Abstand, Störungen, Funkabdeckung und Roaming prüfen.

Ein angezeigter WLAN-Status „Verbunden“ bestätigt noch keine funktionierende IP-Verbindung.

---

3. Besitzt der Client eine gültige IP-Konfiguration?

Vollständige Konfiguration erfassen:

```
ipconfig /all
```

Alternativ mit PowerShell:

```
Get-NetIPConfiguration
```

Zu dokumentieren sind:

- verwendeter Netzwerkadapter,
- IPv4- und gegebenenfalls IPv6-Adresse,
- Subnetzmaske beziehungsweise Präfixlänge,
- Standardgateway,
- DHCP aktiviert oder deaktiviert,
- DHCP-Server,
- Lease-Zeiten,
- DNS-Server,
- DNS-Suffix,
- Medienstatus,
- eventuell vorhandene virtuelle Adapter.

Entscheidungsbaum zur IPv4-Adresse

```
Besitzt der aktive Adapter eine IPv4-Adresse?
|
+-- Nein
|   |
|   +-- DHCP vorgesehen?
|       |
|       +-- Ja  -> DHCP-Client, VLAN, Switchport, Access Point,
|       |          DHCP-Server und DHCP-Relay prüfen
|       |
|       +-- Nein -> statische Konfiguration mit Netzwerkplan vergleichen
|
+-- Ja
    |
    +-- Adresse beginnt mit 169.254?
    |   |
    |   +-- Ja  -> keine verwendbare DHCP-Konfiguration erhalten
    |              DHCP-Pfad untersuchen
    |
```

```
  +-- Adresse 0.0.0.0 oder unvollständig?
| |
| +-- Ja  -> Adapter-, DHCP- oder Konfigurationsfehler
|
+-- Adresse aus erwartetem Subnetz?
  |
  +-- Nein -> falsches VLAN, falscher DHCP-Bereich,
  |         statische Fehlkonfiguration oder fremdes Netz
  |
  +-- Ja  -> Gateway und lokale Erreichbarkeit prüfen
```

Eine Adresse aus `169.254.0.0/16` ist eine automatisch vergebene Link-Local-Adresse. Sie zeigt typischerweise, dass der Client keine verwendbare IPv4-Konfiguration per DHCP erhalten hat. Sie beweist allein jedoch noch nicht, ob DHCP-Server, Relay, VLAN, Kabel, WLAN oder der lokale Client die Ursache ist.

---

4. DHCP-Pfad prüfen

Wenn DHCP vorgesehen ist, zunächst den bestehenden Zustand dokumentieren.

DHCP-Clientdienst prüfen:

```
Get-Service -Name Dhcp
```

Adapterkonfiguration prüfen:

```
Get-NetIPInterface
```

Mögliche Ursachen:

- keine physische Verbindung,
- falsches VLAN,
- Switchport falsch konfiguriert,
- WLAN-Authentifizierung nicht vollständig,
- DHCP-Server nicht erreichbar,
- DHCP-Relay fehlt oder ist falsch konfiguriert,
- DHCP-Bereich ausgeschöpft,
- DHCP-Richtlinie oder Filter lehnt den Client ab,
- UDP 67 oder 68 wird blockiert,
- DHCP-Clientdienst funktioniert nicht,
- fremder DHCP-Server liefert eine falsche Konfiguration,

- Network Access Control weist ein Quarantäne-VLAN zu.

Erst nach Erfassung der ursprünglichen Konfiguration kann eine neue Anforderung kontrolliert ausgelöst werden:

```
ipconfig /release
```

```
ipconfig /renew
```

`ipconfig /release` und `ipconfig /renew` verändern den aktuellen Netzwerkzustand. Sie sollten nicht vor der Dokumentation der vorhandenen Adresse, Lease-Daten und Fehlersituation ausgeführt werden.

Ergebnis bewerten

- gültige Adresse wird vergeben → Lease-Daten und Erreichbarkeit weiterprüfen.
- Zeitüberschreitung → DHCP-Anfrage oder Antwort erreicht ihr Ziel möglicherweise nicht.
- falsches Subnetz wird vergeben → DHCP-Bereich, Relay, VLAN oder fremden DHCP-Server prüfen.
- Adresse wird vergeben, Gateway fehlt → DHCP-Optionen oder Richtlinie prüfen.
- Adresse wird vergeben, DNS-Server fehlen oder sind falsch → DHCP-DNS-Optionen prüfen.

Bei weiterhin unklaren DHCP-Problemen kann ein autorisierter Paketmitschnitt zeigen, ob der DORA-Ablauf vollständig ist:

1. DHCP Discover,
2. DHCP Offer,
3. DHCP Request,
4. DHCP Acknowledge.

---

5. Lokalen TCP/IP-Stack prüfen

Loopback-Adresse testen:

```
ping 127.0.0.1
```

Eigene IPv4-Adresse testen:

```
ping <eigene-ip-adresse>
```

Entscheidung

- Loopback-Test schlägt fehl → lokalen TCP/IP-Stack oder Sicherheitssoftware untersuchen.

- Loopback funktioniert, eigene Adresse nicht → Adapterbindung, IP-Konfiguration oder lokale Filter prüfen.
- beide Tests funktionieren → Verbindung zum lokalen Netz untersuchen.

Ein erfolgreicher Loopback-Test bestätigt nur die lokale TCP/IP-Verarbeitung. Er beweist keine Verbindung zum Switch, WLAN, Gateway oder Internet.

---

6. Standardgateway vorhanden und erreichbar?

Gateway aus der Konfiguration übernehmen:

```
ipconfig
```

Routingtabelle anzeigen:

```
route print
```

Alternativ:

```
Get-NetRoute
```

Gateway testen:

```
ping <gateway-ip>
```

Zusätzliche Verbindungsinformationen:

```
Test-NetConnection -ComputerName <gateway-ip> -InformationLevel Detailed
```

Nachbartabelle anzeigen:

```
arp -a
```

Oder mit PowerShell:

```
Get-NetNeighbor
```

Entscheidungsbaum

```
Ist ein Standardgateway eingetragen?
|
+-- Nein
|   |
|   +-- Nur lokales Subnetz erforderlich?
|   |   |
|   |   +-- Ja  -> lokale Ziele weiterprüfen
|   |   +-- Nein -> DHCP-Option oder statische Konfiguration korrigieren
|   |
+-- Ja
    |
    +-- Gateway im passenden lokalen Subnetz?
        |
        +-- Nein -> IP-Adresse, Maske und Gateway sind inkonsistent
        |
        +-- Ja
            |
            +-- Gateway erreichbar?
                |
                +-- Ja  -> Routing außerhalb des lokalen Netzes prüfen
                |
                +-- Nein -> VLAN, Switchport, WLAN, ARP,
                            lokale Firewall oder Gateway untersuchen
```

Wenn der Gateway-Ping scheitert, kann das Gateway ICMP blockieren. Deshalb zusätzlich prüfen:

- erscheint das Gateway in der ARP- beziehungsweise Nachbartabelle,
- erreichen Vergleichsclients das Gateway,
- funktioniert der Zugriff auf ein anderes System im selben Subnetz,
- zeigen Switch und Access Point den Client im erwarteten VLAN,
- bestehen Port-Security-, NAC- oder MAC-Filterregeln?

Ein fehlgeschlagener Ping allein beweist nicht, dass das Gateway ausgefallen ist.

---

7. Ist ein anderes Ziel im lokalen Subnetz erreichbar?

Vergleichsziel im gleichen Subnetz testen:

```
ping <lokales-vergleichsziel>
```

Gezielten Dienst prüfen:

```
Test-NetConnection -ComputerName <lokales-vergleichsziel> -Port <port>
```

Entscheidung

- lokales Ziel erreichbar, Gateway nicht → Gateway, ICMP-Filterung oder Gateway-Adresse prüfen.
- weder lokales Ziel noch Gateway erreichbar → Layer 2, VLAN, Subnetzmaske, ARP, Port-Security oder Clientadapter prüfen.
- lokale Ziele funktionieren → Verbindung über das Gateway untersuchen.
- nur ein bestimmtes lokales Ziel scheitert → Zielsystem, Dienst, Firewall oder Berechtigung prüfen.

---

8. Funktioniert die Verbindung zu einer externen IP-Adresse?

Ein freigegebenes bekanntes IP-Ziel verwenden:

```
ping <bekannte-ip-adresse>
```

Pfad untersuchen:

```
tracert <bekannte-ip-adresse>
```

PowerShell-Diagnose:

```
Test-NetConnection -ComputerName <bekannte-ip-adresse> -InformationLevel Detailed
```

Entscheidung

- Gateway erreichbar, externe IP nicht → Routing, Firewall, NAT, VPN oder Internetübergang prüfen.
- externe IP erreichbar → grundlegendes IP-Routing funktioniert; DNS prüfen.
- `tracert` endet am ersten Hop → Gateway oder nachgelagertes Routing untersuchen.
- `tracert` zeigt einzelne Zeitüberschreitungen → nicht automatisch Paketverlust annehmen; Router können ICMP-Antworten begrenzen.
- Vergleichsclient erreicht dasselbe Ziel → clientspezifische Route, Firewall, VPN- oder Proxykonfiguration untersuchen.

Ein erfolgreicher Ping zu einer externen Adresse beweist nicht, dass DNS oder der benötigte Anwendungsdienst funktioniert.

---

9. Funktioniert die Namensauflösung?

Konfigurierte DNS-Server prüfen:

```
ipconfig /all
```

Namensauflösung testen:

```
nslookup <zielname>
```

Mit PowerShell:

```
Resolve-DnsName <zielname>
```

Erreichbarkeit eines DNS-Servers prüfen:

```
Test-NetConnection -ComputerName <dns-server> -Port 53
```

TCP-Port 53 allein genügt nicht für eine vollständige DNS-Prüfung, da DNS abhängig von Anfrage und Umgebung sowohl UDP als auch TCP verwenden kann.

Entscheidungsbaum

```
Ist eine bekannte IP-Adresse erreichbar?
|
+-- Nein -> noch kein reines DNS-Problem;
|           Netzwerkpfad und Routing weiterprüfen
|
+-- Ja
    |
    +-- Kann ein Name aufgelöst werden?
        |
        +-- Ja  -> Zielanwendung oder Zielport prüfen
        |
        +-- Nein
            |
            +-- DNS-Server eingetragen?
            |   |
            |   +-- Nein -> DHCP- oder statische DNS-Konfiguration prüfen
```

```
|
+-- DNS-Server erreichbar?
|   |
|   +-- Nein -> Routing, VLAN, VPN oder Firewall prüfen
|
+-- DNS-Server antwortet, liefert aber keinen passenden Eintrag?
    |
    +-- DNS-Zone, Eintrag, Weiterleitung, Suchsuffix
        und verwendeten Namen prüfen
```

DNS-Cache anzeigen:

```
ipconfig /displaydns
```

Der DNS-Cache sollte vor einer Löschung dokumentiert werden. Eine sofortige Leerung kann diagnostisch wichtige Einträge und Unterschiede beseitigen.

Erst nach der Beweissicherung und wenn dies zur Hypothese passt:

```
ipconfig /flushdns
```

---

10. Funktioniert nur die Anwendung nicht?

Wenn IP-Verbindung und Namensauflösung funktionieren, den tatsächlich benötigten Dienst prüfen.

Porttest:

```
Test-NetConnection -ComputerName <zielname> -Port <port>
```

Beispiele:

```
Test-NetConnection -ComputerName <zielname> -Port 443
```

```
Test-NetConnection -ComputerName <zielname> -Port 445
```

```
Test-NetConnection -ComputerName <zielname> -Port 3389
```

Zusätzlich prüfen:

- läuft der Dienst auf dem Zielsystem,
- lauscht er auf dem erwarteten Port,
- blockiert eine lokale oder zentrale Firewall,
- ist ein Proxy erforderlich,
- verwendet die Anwendung einen falschen Proxy,
- beeinflusst ein VPN den Datenverkehr,
- ist das Zertifikat gültig,
- stimmen Systemzeit und Zertifikatszeitraum,
- ist nur ein Benutzerkonto betroffen,
- benötigt die Anwendung zusätzliche Ports oder Dienste,
- funktioniert der Zugriff im Vergleichsclient?

Proxykonfiguration anzeigen:

```
netsh winhttp show proxy
```

Benutzerbezogene Proxy- und Anwendungseinstellungen können davon abweichen. Eine erfolgreiche TCP-Verbindung beweist außerdem nicht, dass TLS, Authentifizierung oder die Anwendung selbst funktionieren.

---

11. Beeinflusst ein VPN oder virtueller Adapter die Verbindung?

Adapter anzeigen:

```
Get-NetAdapter
```

IP-Konfiguration anzeigen:

```
Get-NetIPConfiguration
```

Routingtabelle prüfen:

```
route print
```

DNS-Server je Schnittstelle anzeigen:

```
Get-DnsClientServerAddress
```

Zu prüfen sind:

- aktiver VPN-Tunnel,
- nicht vollständig beendete VPN-Verbindung,
- falsche Standardroute,
- Split-Tunneling-Konfiguration,
- falsche Routenmetrik,
- DNS-Server des VPN,
- virtuelle Hyper-V-, Docker-, WSL- oder Virtualisierungsadapter,
- Security- oder Filtertreiber,
- mehrere gleichzeitig aktive Netzwerkadapter,
- veraltete statische Routen.

Vergleichstest

Wenn betrieblich zulässig, den Zustand dokumentieren und anschließend prüfen, ob das Problem nur mit aktivem VPN auftritt.

- funktioniert die Verbindung ohne VPN → VPN-Routen, DNS, Filter oder Richtlinien untersuchen.
- funktioniert sie ausschließlich mit VPN → lokales Routing, lokales DNS oder Zugriffsvorgaben prüfen.
- betrifft der Fehler nur interne Ziele → interne Routen und interne DNS-Auflösung prüfen.
- betrifft der Fehler nach Trennung weiterhin alle Ziele → verbliebene Routen, Filtertreiber oder Adapterzustände prüfen.

VPN- oder Sicherheitssoftware darf nicht pauschal deinstalliert oder dauerhaft deaktiviert werden.

---

12. Lokale Firewall und Sicherheitssoftware berücksichtigen

Firewallprofile anzeigen:

```
Get-NetFirewallProfile
```

Aktive Verbindungen und lauschende Ports:

```
Get-NetTCPConnection
```

Zu prüfen sind:

- aktuelles Netzwerkprofil,
- ausgehende Blockierregeln,
- Endpoint-Security- oder EDR-Richtlinien,
- Webfilter,

- lokale Paketfilter,
- kürzlich erfolgte Richtlinienänderungen,
- Quarantäne- oder Isolationszustand,
- fehlgeschlagene Gerätekonformität,
- Network Access Control.

Die Firewall oder Sicherheitssoftware darf nicht pauschal deaktiviert werden. Stattdessen sind Protokolle, verworfene Verbindungen, Zieladresse, Zielport, Richtung und Zeitpunkt auszuwerten.

---

13. Vergleichstests durchführen

Geeignete Vergleichstests:

Test	Aussage
anderer Client am selben Anschluss funktioniert	ursprünglichen Client priorisieren
anderer Client am selben Anschluss funktioniert ebenfalls nicht	Anschluss, VLAN oder Netzwerkpfad priorisieren
betroffener Client funktioniert an anderem Anschluss	ursprünglichen Anschluss oder dessen Konfiguration prüfen
betroffener Client funktioniert über WLAN	Ethernetpfad priorisieren
betroffener Client funktioniert über Ethernet	WLANpfad priorisieren
gleiche IP-Konfiguration wie Vergleichsclient, aber keine Verbindung	Adapter, Route, Firewall, VPN oder Adresskonflikt prüfen
nur ein Benutzer betroffen	Benutzerprofil, Proxy, Zertifikat oder Richtlinie prüfen
alle Benutzer am Client betroffen	Computer-, Adapter- oder Systemkonfiguration priorisieren

Beim Anschlusswechsel ist darauf zu achten, dass der Vergleichsport zum selben vorgesehenen Netz und VLAN gehört. Sonst entsteht kein aussagekräftiger Vergleich.

---

14. Möglichen IP-Adresskonflikt prüfen

Hinweise auf einen Adresskonflikt:

- Windows meldet einen IP-Adresskonflikt,
- Verbindung funktioniert wechselnd,
- ARP-Zuordnung ändert sich,
- ein anderes Gerät antwortet auf die Adresse,
- eine statisch konfigurierte Adresse liegt im DHCP-Bereich,
- nach einem Gerätewechsel tritt der Fehler auf.

Nachbartabelle prüfen:

```
arp -a
```

Eigene MAC-Adresse erfassen:

```
Get-NetAdapter | Format-Table Name, MacAddress, Status
```

Prüfen:

- gehört die zur eigenen IP sichtbare MAC-Adresse tatsächlich zum Client,
- ist die Adresse doppelt vergeben,
- liegt eine statische Adresse im dynamischen DHCP-Bereich,
- existiert eine falsche DHCP-Reservierung,
- wurde ein Gerät geklont,
- verwendet eine virtuelle Maschine dieselbe Adresse?

Die ARP-Tabelle sollte vor dem Löschen dokumentiert werden.

---

15. Ereignisprotokolle prüfen

Relevante Protokolle können sich befinden unter:

```
Ereignisanzeige
└─ Anwendungs- und Dienstprotokolle
   └─ Microsoft
      └─ Windows
         ├─ DHCP-Client
         ├─ DNS-Client
         ├─ NetworkProfile
         ├─ NlaSvc
         ├─ TCPIP
         └─ WLAN-AutoConfig
```

PowerShell-Beispiel für Systemereignisse:

```
Get-WinEvent -LogName System -MaxEvents 200 |
    Where-Object {
        $_.ProviderName -match 'Tcpip|Dhcp|DNS|WLAN|NlaSvc'
    } |
    Select-Object TimeCreated, ProviderName, Id, LevelDisplayName, Message
```

Zu korrelieren sind:

- Beginn der Störung,
- Linkverlust,
- DHCP-Fehler,
- Adresskonflikte,
- DNS-Fehler,
- WLAN-Trennung,
- Treiberneustart,
- VPN-Verbindung,
- Richtlinienänderung,
- Energiesparereignis,
- Systemstart oder Ruhezustand.

Ein einzelnes älteres Ereignis beweist nicht die Ursache der aktuellen Störung. Zeitpunkt, Adapter und Fehlerbild müssen zusammenpassen.

---

16. Treiber und Hardware erst nach der Netzwerkanalyse prüfen

Treiber- oder Hardwareprobleme sind besonders wahrscheinlich, wenn:

- der Adapter nicht erkannt wird,
- der Link ständig auf- und abgebaut wird,
- Ereignisse einen Treiberfehler melden,
- der Fehler nach einem Treiber- oder Betriebssystemupdate begann,
- der Adapter auch in einem anderen Netz nicht funktioniert,
- ein USB-Netzwerkadapter ständig getrennt wird,
- andere Geräte am selben Anschluss funktionieren,
- ein geprüfter Ersatzadapter funktioniert.

Vor Änderungen dokumentieren:

- Adaptermodell,
- Treiberversion,
- Treiberdatum,
- Hardware-ID,
- Ereignisse,
- vorhandene IP-Konfiguration,
- Zeitpunkt der letzten Änderung.

Adapterinformationen:

```
Get-NetAdapter |
    Format-List Name, InterfaceDescription, DriverInformation, Status, LinkSpeed
```

Ein Treiber sollte nicht allein deshalb neu installiert werden, weil keine Netzwerkverbindung besteht. Zuerst muss geklärt werden, ob der Fehler tatsächlich am Clientadapter liegt.

---

17. Paketmitschnitt nur bei weiterhin unklarer Ursache

Ein autorisierter Paketmitschnitt kann prüfen, ob der Client Pakete sendet und Antworten erhält.

Typische Filter:

```
arp
```

```
dhcp
```

```
dns
```

```
icmp
```

Kombinierter Wireshark-Anzeigefilter:

```
arp || dhcp || dns || icmp
```

Zu beobachten sind:

- ARP-Anfragen und Antworten,
- DHCP Discover, Offer, Request und Acknowledge,
- DNS-Anfragen und Antworten,
- ICMP-Fehler,
- TCP-Verbindungsaufbau,
- Retransmissions,
- Verbindungszurücksetzungen,
- angesprochene Gateways und DNS-Server.

Paketmitschnitte können interne Adressen, Namen, Benutzerinformationen und andere vertrauliche Daten enthalten. Sie dürfen nur autorisiert, zeitlich begrenzt und geschützt erstellt werden.

---

18. Schneller Hauptentscheidungsbaum

```
START: Ein Client hat kein Netzwerk
|
+-- Sind weitere Clients betroffen?
|   |
|   +-- Ja  -> Bereichs-, Switch-, WLAN-, VLAN-, DHCP- oder Gatewayfehler
|   |          untersuchen; anderen Entscheidungsbaum verwenden
|   |
|   +-- Nein -> am einzelnen Client fortfahren
|
+-- Ist der aktive Netzwerkadapter vorhanden und aktiviert?
|   |
|   +-- Nein -> Adapter, Treiber, Hardware und Gerätestatus prüfen
|   |
|   +-- Ja
|
+-- Besteht Ethernet-Link oder WLAN-Verbindung?
|   |
|   +-- Nein -> Kabel, Dose, Port, SSID, Signal oder Authentifizierung
|   |          prüfen
|   |
|   +-- Ja
|
+-- Besitzt der Client eine gültige IP-Adresse?
|   |
|   +-- Nein oder 169.254.x.x
|   |          -> DHCP, VLAN, Relay, Port oder statische Konfiguration
|   |             prüfen
|   |
|   +-- Ja
|
+-- Ist ein korrektes Standardgateway vorhanden?
|   |
|   +-- Nein -> DHCP-Option oder statische Konfiguration prüfen
|   |
|   +-- Ja
|
+-- Ist das Gateway erreichbar?
|   |
|   +-- Nein -> Subnetzmaske, ARP, VLAN, Switchport, WLAN,
```

```
|   |       NAC oder lokales Netz prüfen
|   |
|   +-- Ja
|
+-- Ist eine freigegebene externe IP-Adresse erreichbar?
|   |
|   +-- Nein -> Routing, Firewall, VPN, NAT oder Internetübergang
|   |       prüfen
|   |
|   +-- Ja
|
+-- Kann der Zielname aufgelöst werden?
|   |
|   +-- Nein -> DNS-Server, DNS-Erreichbarkeit, Suffix und Eintrag
|   |       prüfen
|   |
|   +-- Ja
|
+-- Ist der benötigte Zielport erreichbar?
    |
    +-- Nein -> Zielservice, Firewall, Proxy oder Routing prüfen
    |
    +-- Ja  -> Anwendung, TLS, Authentifizierung oder Berechtigung prüfen
```

---

19. Beispiel für eine schnelle Diagnose

Symptom

Ein Arbeitsplatz-PC meldet „Kein Internet“. Andere Clients im Büro funktionieren.

Prüfung

```
Get-NetAdapter
```

Ergebnis:

```
Name      Status       LinkSpeed
Ethernet  Up           1 Gbps
```

IP-Konfiguration:

```
ipconfig /all
```

Ergebnis:

```
IPv4-Adresse: 169.254.38.17
Subnetzmaske: 255.255.0.0
Standardgateway:
DHCP aktiviert: Ja
```

Bewertung

- Netzwerkadapter ist aktiv.
- Physischer Link besteht.
- Der Client hat jedoch keine verwendbare DHCP-Konfiguration erhalten.
- Es liegt noch kein nachgewiesener Internet- oder DNS-Fehler vor.
- Der DHCP-Pfad muss geprüft werden.

Vergleichstest

Ein anderes Gerät wird kontrolliert am selben Anschluss geprüft und erhält ebenfalls keine DHCP-Adresse.

Nächster Untersuchungsbereich

- Switchport,
- VLAN-Zuordnung,
- Patchung,
- DHCP-Relay,
- DHCP-Erreichbarkeit.

Festgestellte Ursache

Der Switchport wurde versehentlich einem nicht vorgesehenen VLAN zugeordnet.

Nachprüfung

- vorgesehene VLAN-Zuordnung wiederhergestellt,
- Client erhält gültige Adresse, Subnetzmaske, Gateway und DNS-Server,
- Gateway erreichbar,
- interne und externe Ziele erreichbar,
- DNS-Auflösung funktioniert,
- benötigte Anwendungen funktionieren,

- zweiter Client am Anschluss ebenfalls erfolgreich,
- Ursache und Änderung dokumentiert.

---

20. Ungeeignete Sofortmaßnahmen

Nicht als erste Maßnahme verwenden:

- Client sofort neu starten,
- Router oder Switch pauschal neu starten,
- Netzwerkadapter mehrfach deaktivieren und aktivieren,
- TCP/IP-Konfiguration ungeprüft zurücksetzen,
- DNS-Cache vor der Dokumentation löschen,
- DHCP-Lease vor der Erfassung freigeben,
- statische IP-Adresse „zum Test“ frei erfinden,
- öffentliche DNS-Server an einem Unternehmensclient eintragen,
- Firewall oder Endpoint-Security vollständig deaktivieren,
- VPN-Software ungeprüft deinstallieren,
- Netzwerkprofil löschen,
- WLAN-Profil sofort entfernen,
- Netzwerktreiber sofort deinstallieren,
- Switchport ungeprüft in ein anderes VLAN verschieben,
- mehrere Änderungen gleichzeitig durchführen,
- einen erfolgreichen Ping mit vollständiger Netzwerkfunktion gleichsetzen.

Solche Maßnahmen verändern den Zustand, beseitigen Beweise oder erzeugen zusätzliche Fehler.

---

21. Vollständige Schnellprüfreihenfolge

1. genaue Fehlermeldung und Uhrzeit erfassen.
2. feststellen, ob nur ein Client betroffen ist.
3. Ethernet, WLAN, VPN und betroffene Ziele unterscheiden.
4. Vergleichsclient prüfen.
5. Adapterstatus erfassen.
6. physischen Link oder WLAN-Verbindung prüfen.
7. `ipconfig /all` dokumentieren.
8. IP-Adresse und Subnetz prüfen.
9. bei `169.254.x.x` den DHCP-Pfad untersuchen.
10. Standardgateway prüfen.
11. Routingtabelle erfassen.
12. eigenes TCP/IP über Loopback testen.
13. lokales Vergleichsziel testen.
14. Gateway testen.
15. externe IP-Verbindung testen.
16. Pfad bei Bedarf mit `tracert` untersuchen.
17. DNS-Server und Namensauflösung prüfen.

18. benötigten Zielport testen.
19. Proxy, VPN und virtuelle Adapter berücksichtigen.
20. Firewall- und Sicherheitsprotokolle prüfen.
21. Ereignisse mit dem Fehlerzeitpunkt korrelieren.
22. genau eine Hypothese formulieren.
23. genau eine kontrollierte Änderung durchführen.
24. dieselben Tests erneut ausführen.
25. interne und externe Ziele prüfen.
26. Namensauflösung prüfen.
27. benötigte Anwendungen testen.
28. Vergleichsclient oder Vergleichsanschluss erneut testen.
29. temporäre Diagnosekonfiguration entfernen.
30. Ursache, Maßnahme und Nachweis dokumentieren.

---

22. Checkliste „Ein Client hat kein Netzwerk“

- [ ] genaue Fehlermeldung wurde dokumentiert.
- [ ] Beginn und Uhrzeit der Störung sind bekannt.
- [ ] es wurde geprüft, ob weitere Clients betroffen sind.
- [ ] Ethernet, WLAN und VPN wurden unterschieden.
- [ ] interne, externe und einzelne Anwendungsziele wurden unterschieden.
- [ ] ein Vergleichsclient wurde geprüft.
- [ ] der aktive Netzwerkadapter ist bekannt.
- [ ] Adapterstatus und Linkgeschwindigkeit wurden dokumentiert.
- [ ] Kabel, Dose oder WLAN-Verbindung wurden geprüft.
- [ ] die vollständige IP-Konfiguration wurde gesichert.
- [ ] IP-Adresse und Subnetzmaske sind plausibel.
- [ ] eine mögliche `169.254.x.x`-Adresse wurde erkannt.
- [ ] DHCP- oder statische Konfiguration wurde eindeutig bestimmt.
- [ ] DHCP-Server und Lease-Daten wurden dokumentiert.
- [ ] Standardgateway ist vorhanden und plausibel.
- [ ] DNS-Server sind vorhanden und vorgesehen.
- [ ] DNS-Suffix wurde berücksichtigt.
- [ ] Loopback-Test wurde durchgeführt.
- [ ] lokales Vergleichsziel wurde geprüft.
- [ ] Standardgateway wurde geprüft.
- [ ] externe IP-Verbindung wurde geprüft.
- [ ] Routingtabelle wurde untersucht.

- [ ] ARP- beziehungsweise Nachbartabelle wurde berücksichtigt.
- [ ] Namensauflösung wurde getrennt von IP-Erreichbarkeit geprüft.
- [ ] benötigter Zielport wurde getestet.
- [ ] Proxykonfiguration wurde bei Bedarf geprüft.
- [ ] VPN und virtuelle Adapter wurden berücksichtigt.
- [ ] lokale Firewall und Sicherheitssoftware wurden nicht pauschal deaktiviert.
- [ ] ein IP-Adresskonflikt wurde berücksichtigt.
- [ ] Ereignisprotokolle wurden mit dem Fehlerzeitpunkt korreliert.
- [ ] Treiberänderungen wurden erst nach der Netzwerkanalyse erwogen.
- [ ] vor aktiven Änderungen wurden Diagnoseinformationen gesichert.
- [ ] nur eine kontrollierbare Änderung wurde durchgeführt.
- [ ] die gleichen Tests wurden nach der Änderung wiederholt.
- [ ] interne und externe Ziele funktionieren.
- [ ] DNS-Auflösung funktioniert.
- [ ] benötigte Anwendungen funktionieren.
- [ ] Ursache, Änderung und Nachweis wurden dokumentiert.

---

23. Schnellreferenz

Ergebnis	Nächster Schritt
Adapter fehlt	Hardware, Treiber oder Geräteerkennung prüfen
Adapter deaktiviert	Ursache der Deaktivierung klären
Ethernet `Disconnected`	Kabel, Dose, Patchung und Switchport prüfen
WLAN nicht verbunden	SSID, Signal, Profil und Authentifizierung prüfen
Adresse `169.254.x.x`	DHCP-Pfad und VLAN untersuchen
falsches Subnetz	VLAN, DHCP-Bereich oder statische Adresse prüfen
kein Gateway	DHCP-Option oder statische Konfiguration prüfen
Gateway nicht erreichbar	Layer 2, ARP, VLAN, Subnetzmaske oder NAC prüfen
Gateway erreichbar, externe IP nicht	Routing, Firewall, VPN oder Internetübergang prüfen
externe IP erreichbar, Name nicht	DNS prüfen
Name auflösbar, Port nicht erreichbar	Dienst, Firewall oder Zielsystem prüfen
Port erreichbar, Anwendung scheitert	TLS, Authentifizierung, Proxy oder Anwendung prüfen
nur mit VPN gestört	VPN-Routen, DNS und Filter prüfen
nur ein Benutzer betroffen	Benutzerprofil, Proxy, Zertifikat oder Richtlinie prüfen

Ergebnis	Nächster Schritt
anderer Client am Port ebenfalls gestört	Port, VLAN oder Netzwerkpfad prüfen
Client funktioniert an anderem Port	ursprünglichen Anschluss prüfen
Problem nach Neustart verschwunden	Ursache weiterhin nicht bewiesen; Ereignisse auswerten
Verbindung nach mehreren Änderungen funktioniert	keine eindeutige Ursachenbestätigung möglich

---

Merksatz

> Beginne nicht mit dem Internet, sondern am betroffenen Client: Adapter, Link, IP-Adresse, Gateway, externe IP, DNS und Zielport. Jeder erfolgreiche Test bestätigt nur die bis dahin geprüfte Ebene – nicht die gesamte Netzwerkverbindung.

Quellen und weiterführende Dokumentation

- Microsoft Learn – ipconfig
- Microsoft Learn – ping
- Microsoft Learn – tracert
- Microsoft Learn – pathping
- Microsoft Learn – arp
- Microsoft Learn – route
- Microsoft Learn – nslookup
- Microsoft Learn – Get-NetAdapter
- Microsoft Learn – Get-NetIPConfiguration
- Microsoft Learn – Get-NetRoute
- Microsoft Learn – Get-NetNeighbor
- Microsoft Learn – Test-NetConnection
- Microsoft Learn – Resolve-DnsName
- Microsoft Learn – Get-DnsClientServerAddress
- Microsoft Learn – netsh wlan
- Microsoft Learn – DHCP troubleshooting guidance
- Microsoft Learn – DHCP overview
- Microsoft Learn – Get-WinEvent
