2.1 Windows-Netzwerkbefehle

Ziel dieser Seite

Diese Seite enthält die wichtigsten klassischen Windows-Befehle für die praktische Netzwerkdiagnose. Sie behandelt vor allem Werkzeuge, die über die Eingabeaufforderung `cmd.exe` oder aus PowerShell heraus gestartet werden können.

Die objektorientierten PowerShell-Cmdlets wie `Get-NetIPConfiguration`, `Get-NetRoute`, `Resolve-DnsName` und `Test-NetConnection` folgen auf der nächsten Seite.

---

1. Wichtige Hinweise zur Verwendung

Die Kennzeichnungen wie `[RO]`, `[TEST]` und `[CHANGE]` gehören nicht zum Befehl und dürfen nicht mit eingegeben werden.

Die Beispiele verwenden reservierte Dokumentationsadressen und -namen:

Platzhalter	Bedeutung
`192.0.2.25`	Beispielhafte IPv4-Zieladresse
`192.0.2.53`	Beispielhafter DNS-Server
`server.example.test`	Beispielhafter vollständiger DNS-Name
`example.test`	Beispielhafte DNS-Domäne
`<Ziel>`	Durch echten Hostnamen oder echte IP-Adresse ersetzen
`<Adaptername>`	Durch den tatsächlichen Namen des Netzwerkadapters ersetzen
`<PID>`	Durch eine ermittelte Prozess-ID ersetzen
`<Ausgabepfad>`	Durch einen vorhandenen und geeigneten Speicherort ersetzen

Vor einer Veränderung sollten zuerst die `[RO]`-Befehle ausgeführt und deren Ergebnisse gesichert werden.

---

2. Schnellübersicht

Aufgabe	Kennzeichnung	Befehl
Computername anzeigen	`[RO]`	`hostname`
MAC-Adressen anzeigen	`[RO]`	`getmac /v`
Grundlegende IP-Konfiguration	`[RO]`	`ipconfig`

Aufgabe	Kennzeichnung	Befehl
Vollständige IP-Konfiguration	[RO][SENS]	ipconfig /all
DNS-Clientcache anzeigen	[RO][SENS]	ipconfig /displaydns
DNS-Clientcache leeren	[CHANGE]	ipconfig /flushdns
DHCP-Lease freigeben	[CHANGE][DISRUPT]	ipconfig /release
DHCP-Lease erneuern	[TEST][CHANGE]	ipconfig /renew
IPv4-Erreichbarkeit testen	[TEST]	ping /4 <Ziel>
IPv6-Erreichbarkeit testen	[TEST]	ping /6 <Ziel>
Netzwerkpfad anzeigen	[TEST]	tracert /d <Ziel>
Pfad und Paketverlust untersuchen	[TEST]	pathping /n <Ziel>
Routingtabelle anzeigen	[RO]	route print
IPv4-ARP-Cache anzeigen	[RO]	arp -a
DNS-Abfrage ausführen	[TEST]	nslookup <Ziel>
Bestimmten DNS-Server abfragen	[TEST]	nslookup <Ziel> <DNS-Server>
TCP-Verbindungen und Listener anzeigen	[RO][SENS]	netstat -ano
Prozess zu einer PID ermitteln	[RO]	tasklist /FI "PID eq <PID>"
Status der Netzwerkinterfaces	[RO]	netsh interface show interface
IPv4-Nachbartabelle anzeigen	[RO]	netsh interface ipv4 show neighbors
IPv6-Nachbartabelle anzeigen	[RO]	netsh interface ipv6 show neighbors
WLAN-Verbindung anzeigen	[RO][SENS]	netsh wlan show interfaces
Sichtbare WLANs anzeigen	[TEST][SENS]	netsh wlan show networks mode=bssid
WLAN-Bericht erzeugen	[FILE][SENS]	netsh wlan show wlanreport
WinHTTP-Proxy anzeigen	[RO][SENS]	netsh winhttp show proxy
Firewallstatus anzeigen	[RO]	netsh advfirewall show allprofiles state

3. Empfohlene Reihenfolge für eine erste Windows-Netzwerkdiagnose

Schritt	Diagnosefrage	Befehl
1	Auf welchem Computer wird getestet?	hostname
2	Welche Netzwerkadapter sind vorhanden und aktiv?	netsh interface show interface
3	Welche IP-, Gateway-, DHCP- und DNS-Konfiguration liegt vor?	ipconfig /all

Schritt	Diagnosefrage	Befehl
4	Funktioniert der lokale TCP/IP-Stack?	`ping 127.0.0.1`
5	Ist das lokale Standardgateway erreichbar?	`ping <Gateway-IP>`
6	Ist eine entfernte IP-Adresse erreichbar?	`ping /4 <Ziel-IP>`
7	Funktioniert die Namensauflösung?	`nslookup <Zielname>`
8	Sind IP-Adresse und Name unterschiedlich betroffen?	`ping <Ziel-IP>` und `ping <Zielname>`
9	Welchen Weg nimmt der Datenverkehr?	`tracert /d <Ziel>`
10	Gibt es Hinweise auf Verlust oder starke Latenz?	`pathping /n <Ziel>`
11	Welche Route wird wahrscheinlich verwendet?	`route print`
12	Existiert eine lokale Nachbarzuordnung?	`arp -a`
13	Lauscht lokal ein Prozess auf dem erwarteten Port?	`netstat -ano`
14	Welcher Prozess gehört zur gefundenen PID?	`tasklist /FI "PID eq <PID>"`
15	Sind Proxy oder Windows-Firewall relevant?	`netsh winhttp show proxy` und `netsh advfirewall show currentprofile`

Diese Reihenfolge ist ein Ausgangspunkt. Sie wird an das konkrete Fehlerbild angepasst.

---

4. Computername und MAC-Adressen

Computername anzeigen

Kennzeichnung: `[RO]`

```
hostname
```

Der Befehl zeigt den Hostnamenanteil des vollständigen Computernamens an.

Das ist nützlich, um sicherzustellen, dass die Diagnose tatsächlich auf dem vorgesehenen System durchgeführt wird.

Computername über die Umgebungsvariable anzeigen

Kennzeichnung: `[RO]`

```
echo %COMPUTERNAME%
```

`%COMPUTERNAME%` zeigt üblicherweise denselben Computernamen in Großbuchstaben an. In Clusterumgebungen kann sich die Ausgabe von `hostname` jedoch durch die Variable `_CLUSTER_NETWORK_NAME_` unterscheiden.

MAC-Adressen und zugehörige Adapter anzeigen

Kennzeichnung: `[RO]`

```
getmac /v
```

Ausführliche Ausgabe als Liste:

```
getmac /v /fo list
```

Ausgabe als CSV:

```
getmac /v /fo csv
```

Wichtige Felder:

Feld	Bedeutung
Connection Name	Name des Netzwerkadapters
Network Adapter	Beschreibung des Netzwerkgeräts
Physical Address	MAC-Adresse
Transport Name	Windows-interne Transportzuordnung

Wichtig

Bei WLAN können private beziehungsweise zufällige MAC-Adressen verwendet werden. Die aktuell verwendete MAC-Adresse muss deshalb nicht dauerhaft mit der auf dem Gerät aufgedruckten Hardwareadresse übereinstimmen.

---

5. IP-Konfiguration mit ipconfig untersuchen

Grundlegende Konfiguration anzeigen

Kennzeichnung: `[RO]`

```
ipconfig
```

Der Befehl zeigt unter anderem:

- IPv4-Adressen;
- IPv6-Adressen;
- Subnetzmasken;
- Standardgateways;
- Adapter mit getrenntem Medium.

Vollständige Konfiguration anzeigen

Kennzeichnung: `[RO][SENS]`

```
ipconfig /all
```

`ipconfig /all` ist einer der wichtigsten ersten Diagnosebefehle auf Windows-Systemen.

Die Ausgabe kann interne Adressen, DNS-Suffixe, DHCP-Server und andere Infrastrukturinformationen enthalten und sollte deshalb als sensibel behandelt werden.

Wichtige Felder in der Ausgabe

Feld	Diagnosebedeutung
Host Name	Name des lokalen Systems
Primary DNS Suffix	Primäres DNS-Suffix des Computers
Node Type	Verwendeter NetBIOS-Namensauflösungstyp
IP Routing Enabled	Gibt an, ob IP-Weiterleitung aktiviert ist
Adapter Description	Treiber- beziehungsweise Adapterbeschreibung
Physical Address	MAC-Adresse des Adapters
DHCP Enabled	Gibt an, ob IPv4 per DHCP konfiguriert wird
Autoconfiguration Enabled	Zeigt, ob automatische Adressierung möglich ist
IPv4 Address	Aktuelle IPv4-Adresse
Subnet Mask	Zugehörige IPv4-Subnetzmaske
Lease Obtained	Beginn des aktuellen DHCP-Leases
Lease Expires	Ablaufzeit des aktuellen DHCP-Leases
Default Gateway	Router für nicht lokal erreichbare Ziele

Feld	Diagnosebedeutung
DHCP Server	DHCP-Server, von dem die Konfiguration stammt
DNS Servers	Eingetragene DNS-Server in ihrer Reihenfolge
Connection-specific DNS Suffix	DNS-Suffix des jeweiligen Adapters
NetBIOS over Tcpip	Status von NetBIOS über TCP/IP
Media State	Verbindungszustand eines Adapters

Typische Auffälligkeiten

Beobachtung	Mögliche Bedeutung	Nächste Prüfung
`Media disconnected`	Adapter besitzt derzeit keine aktive Verbindung	Kabel, WLAN-Verbindung, Adapterstatus und Switchport
IPv4-Adresse aus `169.254.0.0/16`	Windows verwendet wahrscheinlich APIPA, weil keine verwendbare DHCP-Konfiguration vorliegt	DHCP-Server, VLAN, Relay, Firewall und Link prüfen
Kein Standardgateway	Ziele außerhalb des lokalen Subnetzes sind normalerweise nicht über eine Default Route erreichbar	DHCP-Optionen, statische Konfiguration und Routingtabelle
Unerwarteter DNS-Server	DNS-Anfragen können an einen falschen Resolver gehen	DHCP-Option 6, VPN, statische Konfiguration und Richtlinien
Mehrere Standardgateways	Windows kann einen unerwarteten Ausgangspfad wählen	Routingtabelle und Metriken prüfen
Altes Lease	Nicht automatisch fehlerhaft, aber bei Netzänderungen relevant	Lease-Zeiten und DHCP-Server vergleichen
Nur IPv6-Link-Local-Adresse	Keine globale oder standortweite IPv6-Konfiguration erkennbar	Router Advertisements, DHCPv6 und IPv6-Routing
Falsches DNS-Suffix	Kurznamen können falsch oder gar nicht aufgelöst werden	Adapter-, DHCP-, VPN- und Domänenkonfiguration

APIPA richtig bewerten

Eine Adresse aus `169.254.0.0/16` wird von Windows automatisch vergeben, wenn ein DHCP-konfigurierter Adapter keine verwendbare DHCP-Antwort erhält.

Damit ist unter Umständen Kommunikation mit anderen Systemen im selben lokalen Segment möglich, die ebenfalls eine passende Link-Local-Adresse besitzen. Normale geroutete Kommunikation in andere Subnetze ist damit jedoch nicht möglich.

Eine APIPA-Adresse beweist noch nicht, an welcher Stelle DHCP scheitert. Mögliche Ursachen sind unter anderem:

- keine physische Verbindung;
- falsches VLAN;

- DHCP-Server nicht erreichbar;
- DHCP-Scope erschöpft oder deaktiviert;
- DHCP-Relay fehlt;
- Firewall oder DHCP-Snooping blockiert;
- DHCP-Clientdienst gestört.

---

6. DNS-Clientcache mit ipconfig prüfen

DNS-Clientcache anzeigen

Kennzeichnung: `[RO][SENS]`

```
ipconfig /displaydns
```

Der Cache kann enthalten:

- Einträge aus der lokalen hosts-Datei;
- zuvor abgefragte DNS-Einträge;
- positive DNS-Antworten;
- negative Cacheeinträge;
- Record-Typen und TTL-Werte.

Die Ausgabe sollte möglichst vor dem Leeren des Caches gesichert werden.

DNS-Clientcache in eine Datei schreiben

Kennzeichnung: `[RO][FILE][SENS]`

```
ipconfig /displaydns > "<Ausgabepfad>\dns-cache.txt"
```

DNS-Clientcache leeren

Kennzeichnung: `[CHANGE]`

```
ipconfig /flushdns
```

Der Befehl entfernt dynamisch hinzugefügte positive und negative Einträge aus dem DNS-Clientcache.

Nicht sofort ausführen

Das Leeren des Caches kann:

- einen wichtigen Fehlerzustand beseitigen;
- einen veralteten oder negativen Cacheeintrag als Ursache verbergen;
- die anschließende DNS-Anfrage verändern;
- dazu führen, dass ein sporadischer Fehler vorübergehend nicht mehr reproduzierbar ist.

Deshalb zuerst:

```
ipconfig /displaydns
```

Danach bei begründeter Hypothese:

```
ipconfig /flushdns
```

Anschließend denselben Namen erneut testen.

Dynamische DNS-Registrierung anstoßen

Kennzeichnung: `[TEST][CHANGE]`

```
ipconfig /registerdns
```

Der Befehl stößt die manuelle dynamische Registrierung der konfigurierten DNS-Namen und IP-Adressen an.

Er ist für Probleme mit dynamischen DNS-Updates gedacht und nicht als allgemeiner erster Reparaturbefehl.

Nach der Ausführung sollten zusätzlich geprüft werden:

- DNS-Zone;
- Berechtigungen für dynamische Updates;
- DNS-Server-Ereignisse;
- Windows-Ereignisprotokolle;
- tatsächlich angelegte oder aktualisierte Records.

---

7. DHCP-Lease erneuern

Aktuelle DHCP-Konfiguration eines Adapters freigeben

Kennzeichnung: `[CHANGE][DISRUPT]`

```
ipconfig /release "<Adaptername>"
```

Für alle DHCP-konfigurierten IPv4-Adapter:

```
ipconfig /release
```

Dadurch wird die aktuelle DHCP-Konfiguration verworfen. Die Netzwerkverbindung kann unterbrochen werden.

DHCP-Konfiguration erneuern

Kennzeichnung: `[TEST][CHANGE]`

```
ipconfig /renew "<Adaptername>"
```

Für alle DHCP-konfigurierten IPv4-Adapter:

```
ipconfig /renew
```

DHCPv6-Konfiguration freigeben und erneuern

Kennzeichnung: `[CHANGE][DISRUPT]`

```
ipconfig /release6 "<Adaptername>"
```

Kennzeichnung: `[TEST][CHANGE]`

```
ipconfig /renew6 "<Adaptername>"
```

Wichtige Sicherheitsregel

`ipconfig /release` darf nicht unüberlegt in einer entfernten Administrationssitzung ausgeführt werden. Die Verbindung zum System kann dadurch sofort abbrechen.

Vorher sichern

```
ipconfig /all
```

Nachher vergleichen

```
ipconfig /all
```

Zu vergleichen sind insbesondere:

- IP-Adresse;
- Subnetzmaske;
- Standardgateway;
- DNS-Server;
- DHCP-Server;
- DNS-Suffix;
- Lease-Beginn;
- Lease-Ablauf.

Auswertung

Ergebnis	Mögliche Schlussfolgerung
Lease wird erfolgreich erneuert	DHCP-Kommunikation funktioniert grundsätzlich
APIPA-Adresse nach dem Versuch	Keine verwendbare DHCP-Antwort erhalten
Alte Adresse bleibt bestehen	Lease möglicherweise noch gültig oder Erneuerung nicht erfolgreich
Neuer falscher Adressbereich	Falsches VLAN, falscher Scope oder nicht autorisierter DHCP-Server möglich
Gateway oder DNS fehlt	DHCP-Antwort beziehungsweise DHCP-Optionen unvollständig oder falsch
Befehl betrifft falschen Adapter	Adaptername, virtuelle Adapter und aktive Verbindung prüfen

---

8. Erreichbarkeit mit ping prüfen

`ping` sendet ICMP-Echoanforderungen und zeigt empfangene Echoantworten sowie die jeweilige Round-Trip-Zeit an.

Ein erfolgreicher Ping beweist nicht, dass ein bestimmter TCP- oder UDP-Dienst funktioniert.

Ein fehlgeschlagener Ping beweist nicht sicher, dass das Ziel ausgeschaltet ist. ICMP kann gefiltert, begrenzt oder deaktiviert sein.

IPv4-Ziel testen

Kennzeichnung: `[TEST]`

```
ping /4 192.0.2.25
```

IPv6-Ziel testen

Kennzeichnung: [TEST]

```
ping /6 server.example.test
```

Namen testen

Kennzeichnung: [TEST]

```
ping server.example.test
```

Die erste Ausgabezeile zeigt normalerweise, in welche IP-Adresse der Name aufgelöst wurde.

Mehrere Anfragen senden

Kennzeichnung: [TEST]

```
ping /n 10 192.0.2.25
```

Windows sendet standardmäßig vier Echoanforderungen. `/n 10` erhöht die Anzahl auf zehn.

Zeitüberschreitung festlegen

Kennzeichnung: [TEST]

```
ping /n 10 /w 1000 192.0.2.25
```

`/w 1000` wartet pro Anfrage maximal 1000 Millisekunden auf eine Antwort.

Dauerhaft testen

Kennzeichnung: [TEST]

```
ping /t 192.0.2.25
```

Steuerung:

Tastenkombination	Wirkung
Strg + Unterbrechen	Zwischenstatistik anzeigen und Test fortsetzen
Strg + C	Test beenden und Abschlussstatistik anzeigen

Ein dauerhafter Ping sollte nicht unbeaufsichtigt laufen.

IPv4 oder IPv6 gezielt erzwingen

```
ping /4 server.example.test
```

```
ping /6 server.example.test
```

Damit lässt sich erkennen, ob nur einer der beiden Protokollpfade betroffen ist.

Paketgröße testen

Kennzeichnung: `[TEST]`

```
ping /4 /f /l 1472 192.0.2.25
```

Bedeutung:

Option	Bedeutung
`/4`	IPv4 verwenden
`/f`	„Do not Fragment“-Bit setzen
`/l 1472`	ICMP-Datenfeld mit 1472 Byte verwenden

1472 Byte plus 20 Byte IPv4-Header und 8 Byte ICMP-Header ergeben 1500 Byte. Das ist ein üblicher Startwert für Ethernet mit einer MTU von 1500, aber nicht für jeden Pfad passend.

Wenn eine Fragmentierungsmeldung erscheint, kann die Nutzlast schrittweise reduziert werden.

Beispiel:

```
ping /4 /f /l 1464 192.0.2.25
```

```
ping /4 /f /l 1400 192.0.2.25
```

Dieser Test kann Hinweise auf Probleme mit folgenden Komponenten geben:

- VPN-Tunnel;
- PPPoE;
- IPsec;
- GRE;

- Providerpfad;
- falsch konfigurierte MTU;
- gestörte Path-MTU-Discovery.

Ping-Ausgaben interpretieren

Ausgabe	Bedeutung
`Reply from ...`	Eine ICMP-Echoantwort wurde empfangen
`Request timed out`	Innerhalb der Wartezeit wurde keine passende Echoantwort empfangen
`Destination host unreachable`	Das meldende System oder ein Router konnte das Ziel nicht erreichen
`General failure`	Lokaler Versand ist fehlgeschlagen; lokale Konfiguration, Route, Interface oder Netzwerkstack prüfen
`Ping request could not find host`	Der angegebene Name konnte nicht aufgelöst werden
Stark wechselnde Laufzeiten	Mögliche Überlastung, WLAN-Störung, Warteschlangen oder wechselnde Pfade
Paketverlust	Mögliche Filterung, Überlastung oder Verbindungsstörung; weitere Messungen erforderlich

Bei `Destination host unreachable` ist entscheidend, welche IP-Adresse die Meldung sendet:

- eigene Adresse: Problem wahrscheinlich lokal oder im lokalen Segment;
- Standardgateway: Gateway besitzt möglicherweise keine passende Route;
- Zwischenrouter: Fehler weiter entfernt im Datenpfad.

TTL nicht als exakte Hopanzahl interpretieren

Der angezeigte TTL-Wert ist der verbleibende TTL-Wert der empfangenen Antwort. Da der ursprüngliche Startwert des Zielsystems normalerweise nicht sicher bekannt ist, kann daraus nicht zuverlässig die genaue Zahl der durchlaufenen Router berechnet werden.

---

9. Systematischer Ping-Test

Die folgende Reihenfolge grenzt den Fehler schrittweise ein.

1. Lokalen IPv4-Loopback testen

```
ping 127.0.0.1
```

Prüft grundlegende lokale IPv4-Verarbeitung. Der Test verlässt den Computer nicht.

2. Lokalen IPv6-Loopback testen

```
ping ::1
```

Prüft grundlegende lokale IPv6-Verarbeitung.

3. Eigene IP-Adresse testen

```
ping <Eigene-IP-Adresse>
```

Prüft die Bindung der Adresse an den lokalen Netzwerkstack. Der Test beweist noch keine funktionierende physische Verbindung.

4. Standardgateway testen

```
ping <Gateway-IP>
```

Prüft die ICMP-Kommunikation zum Gateway, sofern dieses ICMP beantwortet.

5. Entfernte IP-Adresse testen

```
ping <Entfernte-IP-Adresse>
```

Prüft den gerouteten IP-Pfad ohne Abhängigkeit von der DNS-Namensauflösung.

6. Zielname testen

```
ping server.example.test
```

Vergleich:

IP-Test	Namenstest	Wahrscheinlicher Bereich
Erfolgreich	Erfolgreich	Grundlegende IP-Kommunikation und Namensauflösung funktionieren
Erfolgreich	Fehlgeschlagen	Namensauflösung, Suffix, Cache oder hosts-Datei prüfen
Fehlgeschlagen	Name wird aufgelöst	Routing, Firewall, Zielsystem oder Rückweg prüfen
Beide fehlgeschlagen	Keine eindeutige Aussage	Lokale Konfiguration, Gateway, DNS und Pfad getrennt prüfen

---

10. Netzwerkpfad mit tracert untersuchen

`tracert` erhöht schrittweise den TTL-Wert und versucht dadurch, die Router auf dem Weg zum Ziel sichtbar zu machen.

Pfad zu einem Ziel anzeigen

Kennzeichnung: `[TEST]`

```
tracert server.example.test
```

Namensauflösung der Zwischenstationen deaktivieren

Kennzeichnung: `[TEST]`

```
tracert /d 192.0.2.25
```

`/d` verhindert Reverse-DNS-Abfragen für Zwischenrouter. Dadurch wird die Ausgabe häufig schneller und DNS-Verzögerungen beeinflussen die Messung weniger.

IPv4 erzwingen

```
tracert /4 server.example.test
```

IPv6 erzwingen

```
tracert /6 server.example.test
```

Maximale Hopanzahl begrenzen

```
tracert /d /h 15 192.0.2.25
```

Wartezeit pro Antwort verringern

```
tracert /d /w 1000 192.0.2.25
```

`/w 1000` wartet bis zu 1000 Millisekunden auf die jeweilige ICMP-Antwort.

Ausgabe interpretieren

Beobachtung	Mögliche Bedeutung
Ziel wird erreicht	Ein ICMP-basierter Pfad konnte bis zum Ziel verfolgt werden
Einzelner Hop zeigt `*`, spätere Hops antworten	Dieser Router antwortet möglicherweise nicht auf TTL-Überschreitungen; Weiterleitung funktioniert trotzdem
Ab einem Hop nur noch `*`	Filterung, fehlende Rückantwort, Pfadunterbrechung oder nicht antwortende Router möglich
Erster Hop unerwartet	Falsches Gateway, VPN, virtueller Adapter oder unerwartete Route möglich
Pfad unterscheidet sich zwischen Tests	Dynamisches Routing, Load Balancing, VPN-Wechsel oder andere Pfadauswahl möglich
Hohe Laufzeit an einem Hop, spätere Hops wieder normal	Der Router priorisiert seine eigenen ICMP-Antworten möglicherweise niedrig; kein sicherer Beweis für Weiterleitungsverzögerung
Hohe Laufzeit beginnt an einem Hop und bleibt danach erhöht	Möglicher Engpass oder langsamer Abschnitt ab diesem Bereich

Wichtig

Drei Sternchen bedeuten nur, dass für diese Versuche keine erwartete ICMP-Antwort empfangen wurde. Sie beweisen nicht automatisch einen Paketverlust für normalen Anwendungsverkehr.

---

11. Paketverlust und Latenz mit pathping untersuchen

`pathping` kombiniert eine Pfadermittlung mit wiederholten ICMP-Messungen zu den Zwischenstationen.

Standardtest

Kennzeichnung: `[TEST]`

```
pathping 192.0.2.25
```

Ohne Namensauflösung

Kennzeichnung: `[TEST]`

```
pathping /n 192.0.2.25
```

Anzahl der Abfragen begrenzen

```
pathping /n /q 20 192.0.2.25
```

Zeitabstand zwischen aufeinanderfolgenden Pings festlegen

```
pathping /n /q 20 /p 500 192.0.2.25
```

Option	Bedeutung
`/n`	Keine Namensauflösung der Zwischenrouter
`/q 20`	20 Echoanforderungen pro Router
`/p 500`	500 Millisekunden zwischen aufeinanderfolgenden Pings
`/w 1000`	Bis zu 1000 Millisekunden auf eine Antwort warten
`/4`	Nur IPv4 verwenden
`/6`	Nur IPv6 verwenden

Wartezeit beachten

`pathping` benötigt deutlich länger als `tracert`, weil nach der Pfaderkennung über einen Zeitraum Messwerte gesammelt werden.

Verlust richtig interpretieren

Wenn ein Zwischenrouter bei an ihn gerichteten ICMP-Paketen Verlust zeigt, aber alle folgenden Hops und das Ziel keinen entsprechenden Verlust zeigen, ist die Weiterleitung wahrscheinlich nicht im gleichen Maß betroffen.

Mögliche Erklärung:

- ICMP-Antworten des Routers werden begrenzt;
- der Router priorisiert Transitverkehr höher als eigene Diagnoseantworten;
- die Control Plane ist ausgelastet, während die Weiterleitung weiterhin funktioniert.

Wird ein Verlust ab einem bestimmten Link angezeigt und setzt sich bis zum Ziel fort, ist dieser Abschnitt wesentlich verdächtiger.

Pathping ist kein Beweis für Anwendungsleistung

Der Befehl prüft ICMP. Eine TCP-, UDP-, TLS- oder Anwendungsstörung muss mit dem tatsächlichen Protokoll weiter untersucht werden.

---

12. Routingtabelle mit route anzeigen

Gesamte Routingtabelle anzeigen

Kennzeichnung: `[RO][SENS]`

```
route print
```

Die Ausgabe enthält:

- Interface List;
- IPv4-Routingtabelle;
- IPv6-Routingtabelle;
- aktive Routen;
- persistente Routen;
- Netzwerkziele;
- Netzmasken beziehungsweise Präfixe;
- Gateways;
- Interfaceadressen;
- Metriken.

Routen für einen bestimmten Bereich filtern

Kennzeichnung: `[RO]`

```
route print 192.0.2.*
```

Wichtige Bestandteile

Spalte	Bedeutung
Network Destination	Zielnetz oder Zielhost
Netmask	Netzmaske der Route
Gateway	Nächster Router beziehungsweise Next Hop
Interface	Lokale Ausgangsadresse
Metric	Kostenwert der Route
On-link	Ziel ist über das angegebene Interface direkt erreichbar

Default Route erkennen

```
Network Destination: 0.0.0.0
Netmask:             0.0.0.0
```

Diese Route wird verwendet, wenn keine spezifischere passende IPv4-Route vorhanden ist.

Routenauswahl vereinfacht

Windows berücksichtigt grundsätzlich:

1. passende Zielpräfixe;
2. die spezifischste passende Route;
3. bei gleich spezifischen Routen die Metriken;
4. die zugehörige Interfacemetrik und Routenkonfiguration.

Eine Route zu `192.0.2.0/24` ist beispielsweise spezifischer als die Default Route `0.0.0.0/0`.

Typische Auffälligkeiten

Beobachtung	Mögliche Ursache
Keine Default Route	Kein Gateway konfiguriert oder DHCP-Konfiguration unvollständig
Mehrere Default Routes	Mehrere Adapter, VPN, virtuelle Netzwerke oder fehlerhafte Konfiguration
Unerwartet niedrige Metrik	Datenverkehr verwendet möglicherweise den falschen Adapter
Zielroute zeigt auf VPN	Split-Tunnel- oder VPN-Routing relevant
Spezifische Route zeigt auf falsches Gateway	Statische Route oder Software hat die Pfadauswahl verändert
Route ist `On-link`, Ziel liegt aber nicht im lokalen Segment	Falsche Subnetzmaske oder Präfixlänge möglich
Persistente Route unerwartet vorhanden	Frühere manuelle Konfiguration oder Softwareinstallation prüfen

Verändernde route-Befehle

Folgende Befehle verändern die Routingtabelle und sind keine reinen Diagnosebefehle:

```
route add
route change
route delete
route /f
```

`route /f` entfernt einen großen Teil der Routingeinträge und kann Netzwerk- sowie Remotesitzungen unterbrechen. Der Befehl darf nicht als allgemeiner Reparaturversuch verwendet werden.

---

13. ARP-Cache und IPv4-Nachbartabelle prüfen

ARP ordnet IPv4-Adressen im lokalen Segment den zugehörigen MAC-Adressen zu.

ARP-Cache aller Interfaces anzeigen

Kennzeichnung: `[RO][SENS]`

```
arp -a
```

Ein bestimmtes Ziel anzeigen

```
arp -a 192.0.2.25
```

Tabelle eines bestimmten Interfaces anzeigen

```
arp -a -N <Lokale-Interface-IP>
```

Ausgabe interpretieren

Typ	Bedeutung
dynamic	Zuordnung wurde dynamisch per ARP gelernt
static	Zuordnung wurde statisch eingetragen oder vom System vorgegeben
Kein Eintrag	Ziel wurde noch nicht lokal aufgelöst, liegt nicht im lokalen Segment oder ARP-Auflösung ist fehlgeschlagen

Gezielte Prüfung

Zuerst das lokale Ziel ansprechen:

```
ping 192.0.2.25
```

Danach ARP-Tabelle prüfen:

```
arp -a 192.0.2.25
```

Wenn das Ziel im selben IPv4-Subnetz liegt, aber trotz eines Kommunikationsversuchs keine passende MAC-Adresse gelernt wird, sollten unter anderem geprüft werden:

- VLAN-Zuordnung;
- Switchport;

- Kabel oder WLAN;
- falsche Subnetzmaske;
- Zielsystem ausgeschaltet;
- ARP-Filterung;
- Duplicate Address;
- Security-Funktionen wie Dynamic ARP Inspection;
- virtuelle Switches und Bridges.

ARP-Eintrag löschen

Kennzeichnung: `[PRIV][CHANGE]`

```
arp -d 192.0.2.25
```

Der Eintrag sollte erst gelöscht werden, nachdem sein vorheriger Zustand dokumentiert wurde.

Das Löschen erzwingt bei der nächsten Kommunikation eine neue ARP-Auflösung. Es beweist jedoch nicht, warum ein vorheriger Eintrag falsch oder veraltet war.

IPv6 beachten

`arp` gilt für IPv4. IPv6 verwendet Neighbor Discovery.

IPv6-Nachbarn anzeigen:

```
netsh interface ipv6 show neighbors
```

---

14. DNS mit nslookup prüfen

`nslookup` kann DNS-Server direkt abfragen und unterstützt einen nicht interaktiven sowie einen interaktiven Modus.

Einzelnen Namen mit dem Standard-DNS-Server abfragen

Kennzeichnung: `[TEST][SENS]`

```
nslookup server.example.test
```

Bestimmten DNS-Server abfragen

```
nslookup server.example.test 192.0.2.53
```

So können Antworten unterschiedlicher DNS-Server miteinander verglichen werden.

IPv4-A-Record abfragen

```
nslookup -type=A server.example.test 192.0.2.53
```

IPv6-AAAA-Record abfragen

```
nslookup -type=AAAA server.example.test 192.0.2.53
```

Mailserver abfragen

```
nslookup -type=MX example.test 192.0.2.53
```

Nameserver einer Zone abfragen

```
nslookup -type=NS example.test 192.0.2.53
```

TXT-Record abfragen

```
nslookup -type=TXT example.test 192.0.2.53
```

SRV-Record abfragen

```
nslookup -type=SRV _ldap._tcp.dc._msdcs.example.test 192.0.2.53
```

Reverse Lookup ausführen

```
nslookup 192.0.2.25 192.0.2.53
```

Dabei wird nach einem PTR-Record gesucht.

Interaktiven Modus starten

```
nslookup
```

Beispiel innerhalb des interaktiven Modus:

```
server 192.0.2.53
set type=AAAA
server.example.test
exit
```

Ausgabe interpretieren

Ausgabe	Bedeutung
`Server`	Verwendeter DNS-Server
`Address`	Adresse des verwendeten DNS-Servers
`Name`	Zurückgegebener kanonischer Name
`Addresses`	Zurückgegebene IP-Adressen
`Aliases`	Gefundene Aliasnamen
`Non-authoritative answer`	Antwort stammt nicht direkt vom autoritativen Server
`NXDOMAIN` beziehungsweise „Non-existent domain“	Angefragter Name existiert laut Antwort nicht
`Request timed out`	DNS-Server antwortete innerhalb des Timeouts nicht
`Server failed`	DNS-Server meldet einen Verarbeitungsfehler
`Refused`	DNS-Server lehnt die Anfrage ab

Wichtige Einschränkung

Eine erfolgreiche `nslookup`-Abfrage beweist nicht, dass eine Anwendung denselben Namen auf dieselbe Weise auflöst.

Zusätzlich relevant sein können:

- Windows-DNS-Clientcache;
- hosts-Datei;
- DNS-Suffixsuchliste;
- VPN-Namensauflösung;
- Split-DNS;
- DoH in einem Browser;
- Proxyauflösung;
- anwendungseigener DNS-Cache;
- NetBIOS oder LLMNR.

Die Anwendung sollte deshalb anschließend ebenfalls direkt getestet werden.

---

15. NetBIOS-Namensauflösung mit nbtstat prüfen

`nbtstat` ist hauptsächlich für ältere beziehungsweise weiterhin verwendete NetBIOS-over-TCP/IP-Umgebungen relevant.

Lokale NetBIOS-Namenstabelle anzeigen

Kennzeichnung: `[RO][SENS]`

```
nbtstat /n
```

NetBIOS-Namenscache anzeigen

```
nbtstat /c
```

Remote-Tabelle über den NetBIOS-Namen abfragen

Kennzeichnung: `[TEST][SENS]`

```
nbtstat /a <Remote-NetBIOS-Name>
```

Remote-Tabelle über die IPv4-Adresse abfragen

```
nbtstat /A 192.0.2.25
```

Groß- und Kleinschreibung der Optionen ist hier wichtig:

Option	Abfrage
`/a`	Remotecomputer über NetBIOS-Namen
`/A`	Remotecomputer über IPv4-Adresse

`nbtstat` sollte nur verwendet werden, wenn NetBIOS, WINS, ältere SMB-Namensauflösung oder eine entsprechende Legacy-Anwendung tatsächlich relevant ist.

---

16. Verbindungen, Listener und Ports mit netstat prüfen

Aktive TCP-Verbindungen anzeigen

Kennzeichnung: `[RO][SENS]`

```
netstat
```

Alle Verbindungen und Listener numerisch anzeigen

```
netstat -an
```

Verbindungen, Listener und Prozess-IDs anzeigen

```
netstat -ano
```

Bedeutung:

Option	Funktion
`-a`	Alle aktiven TCP-Verbindungen sowie TCP- und UDP-Listener anzeigen
`-n`	Adressen und Ports numerisch anzeigen
`-o`	Zugehörige Prozess-ID anzeigen
`-b`	Beteiligte ausführbare Datei anzeigen
`-e`	Ethernet-Statistiken anzeigen
`-r`	Routingtabelle anzeigen
`-s`	Protokollstatistiken anzeigen
`-p`	Ausgabe auf ein Protokoll begrenzen

Ausführbare Programme anzeigen

Kennzeichnung: `[RO][PRIV][SENS]`

```
netstat -abno
```

`-b` kann langsam sein und benötigt ausreichende Rechte.

Nach einem Port filtern

Kennzeichnung: `[RO][SENS]`

```
netstat -ano | findstr ":443"
```

Achtung

Die Suche findet `:443` sowohl bei lokalen als auch bei entfernten Adressen. Das Ergebnis muss anhand der Spalte `Local Address` beziehungsweise `Foreign Address` bewertet werden.

Nur Listener suchen

```
netstat -ano | findstr "LISTENING"
```

Auf einem deutschsprachigen Windows kann die Zustandsbezeichnung lokalisiert ausgegeben werden. Für zuverlässig automatisierbare Abfragen sind die PowerShell-Cmdlets der nächsten Seite besser geeignet.

Prozess zu einer PID suchen

```
tasklist /FI "PID eq 1234"
```

Wenn mehrere Windows-Dienste von einem gemeinsamen `svchost.exe`-Prozess gehostet werden:

```
tasklist /SVC /FI "PID eq 1234"
```

Protokollstatistiken anzeigen

```
netstat -s
```

Ethernet- und Protokollstatistiken anzeigen

```
netstat -e -s
```

Routingtabelle über netstat anzeigen

```
netstat -r
```

Das entspricht funktional weitgehend:

```
route print
```

Ausgabe regelmäßig aktualisieren

```
netstat -ano 5
```

Die Ausgabe wird alle fünf Sekunden aktualisiert. Mit `Strg` + `C` wird die Wiederholung beendet.

---

17. TCP-Zustände interpretieren

Zustand	Bedeutung	Diagnosehinweis
`LISTENING`	Lokaler Prozess wartet auf Verbindungen	Erwarteter Dienst besitzt grundsätzlich einen Listener
`SYN_SENT`	Verbindungsanfrage wurde gesendet, passende Antwort steht aus	Ziel, Firewall, Route oder Rückweg prüfen
`SYN_RECEIVED`	Anfrage wurde empfangen und beantwortet, Abschluss des Handshakes steht aus	Clientantwort oder Rückweg prüfen
`ESTABLISHED`	TCP-Verbindung ist aufgebaut	TCP funktioniert; Anwendung kann trotzdem fehlerhaft sein
`FIN_WAIT_1`	Lokale Seite hat das Beenden eingeleitet	Kurzzeitig normal
`FIN_WAIT_2`	Bestätigung liegt vor, Beendigung der Gegenseite steht aus	Viele dauerhafte Einträge können auf Anwendungsprobleme hindeuten
`CLOSE_WAIT`	Gegenseite hat beendet; lokale Anwendung muss noch schließen	Viele dauerhafte Einträge deuten häufig auf eine nicht sauber schließende Anwendung
`LAST_ACK`	Lokale Seite wartet auf letzte Bestätigung	Kurzzeitig normal
`TIME_WAIT`	Verbindung wartet vor vollständiger Freigabe	Viele Einträge können bei hoher Verbindungsrate normal sein
`CLOSED`	Keine aktive TCP-Verbindung	Normaler Endzustand

Ein einzelner Zustand ist selten ausreichend. Entscheidend sind:

- Anzahl;
- Dauer;
- betroffene lokale und entfernte Endpunkte;
- zugehöriger Prozess;
- Entwicklung während der Störung;
- Vergleich mit einem funktionierenden System.

---

18. Netzwerkinterfaces mit netsh prüfen

Status aller Netzwerkinterfaces anzeigen

Kennzeichnung: `[RO]`

```
netsh interface show interface
```

Typische Felder:

Feld	Bedeutung
Admin State	Administrativ aktiviert oder deaktiviert
State	Aktueller Verbindungszustand
Type	Art des Interfaces
Interface Name	Windows-Name des Interfaces

IPv4-Interfaces anzeigen

```
netsh interface ipv4 show interfaces
```

IPv6-Interfaces anzeigen

```
netsh interface ipv6 show interfaces
```

IPv4-Konfiguration anzeigen

```
netsh interface ipv4 show config
```

IPv4-Adressen anzeigen

```
netsh interface ipv4 show addresses
```

IPv4-Routen anzeigen

```
netsh interface ipv4 show route
```

IPv4-Nachbarn anzeigen

```
netsh interface ipv4 show neighbors
```

IPv6-Adressen anzeigen

```
netsh interface ipv6 show addresses
```

IPv6-Routen anzeigen

```
netsh interface ipv6 show route
```

IPv6-Nachbarn anzeigen

```
netsh interface ipv6 show neighbors
```

Subinterfaces und MTU anzeigen

```
netsh interface ipv4 show subinterfaces
```

Diese Ausgabe ist unter anderem für folgende Probleme hilfreich:

- falsche MTU;
- VPN- oder Tunnelinterface;
- mehrere aktive Adapter;
- unerwartete Interface-Metrik;
- falsche Nachbarzuordnung;
- IPv4 funktioniert, IPv6 nicht;
- Datenverkehr verwendet ein virtuelles Interface.

---

19. WLAN mit netsh untersuchen

Aktuelle WLAN-Verbindung anzeigen

Kennzeichnung: `[RO][SENS]`

```
netsh wlan show interfaces
```

Mögliche Angaben:

- Name des WLAN-Interfaces;
- Beschreibung und Treiber;
- Status;
- SSID;
- BSSID;
- verwendeter Funkstandard;
- Authentifizierung;
- Verschlüsselung;
- Kanal;
- Empfangs- und Senderate;
- Signalstärke;

- Profilname.

WLAN-Treiber und Fähigkeiten anzeigen

```
netsh wlan show drivers
```

Damit lassen sich unter anderem prüfen:

- unterstützte Funktypen;
- unterstützte Authentifizierungsverfahren;
- unterstützte Verschlüsselungsverfahren;
- Treiberversion;
- Hersteller;
- Datum des Treibers;
- unterstützte WLAN-Funktionen.

Sichtbare WLANs anzeigen

Kennzeichnung: `[TEST][SENS]`

```
netsh wlan show networks
```

Sichtbare WLANs einschließlich BSSIDs anzeigen

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

Damit können unter anderem verglichen werden:

- SSID;
- BSSID des Access Points;
- Signalstärke;
- Kanal;
- Authentifizierung;
- Verschlüsselung;
- mehrere Access Points derselben SSID.

Gespeicherte WLAN-Profile anzeigen

Kennzeichnung: `[RO][SENS]`

```
netsh wlan show profiles
```

Bestimmtes WLAN-Profil anzeigen

```
netsh wlan show profile name="<Profilname>"
```

Die Liste gespeicherter SSIDs kann sensible Informationen über Standorte oder interne Netzwerknamen enthalten.

WLAN-Bericht erzeugen

Kennzeichnung: `[FILE][SENS]`

```
netsh wlan show wlanreport
```

Windows erzeugt einen HTML-Bericht und zeigt den Speicherort in der Ausgabe an.

Der Bericht kann Informationen enthalten über:

- WLAN-Sitzungen;
- Verbindungsabbrüche;
- Verbindungsdauer;
- Fehlergründe;
- Netzwerkadapter;
- Treiber;
- gespeicherte oder verwendete Netzwerke;
- Systemereignisse.

Der Bericht ist als sensible Diagnosedatei zu behandeln.

Typische WLAN-Auffälligkeiten

Beobachtung	Mögliche Ursache
Interface State ist `disconnected`	Keine WLAN-Verbindung aktiv
Unerwartete SSID	Client ist mit dem falschen Netz verbunden
Unerwartete BSSID	Verbindung mit anderem Access Point als erwartet
Niedrige Signalstärke	Entfernung, Dämpfung, Antenne oder ungünstiger Standort
Niedrige Datenrate	Schlechte Funkbedingungen, alter Standard oder Störung
Stark schwankendes Signal	Bewegung, Interferenz, Roaming oder Treiberproblem
Überfüllter Kanal	Co-Channel-Interference möglich
Profil vorhanden, Verbindung scheitert	Authentifizierung, Zertifikat, Schlüssel oder Richtlinie prüfen

Beobachtung	Mögliche Ursache
WLAN verbunden, aber APIPA	WLAN-Assoziierung funktioniert, DHCP jedoch möglicherweise nicht

---

20. Proxykonfiguration prüfen

WinHTTP-Proxy anzeigen

Kennzeichnung: `[RO][SENS]`

```
netsh winhttp show proxy
```

Der Befehl zeigt die Proxykonfiguration für Anwendungen und Dienste an, die WinHTTP verwenden.

Mögliche Ausgaben:

- direkter Zugriff ohne Proxy;
- Proxyserver;
- Proxyport;
- Bypass-Liste.

Wichtige Einschränkung

Die WinHTTP-Konfiguration ist nicht automatisch identisch mit:

- Browser-Proxyeinstellungen;
- benutzerspezifischen Systemeinstellungen;
- PAC-Dateien;
- Proxykonfiguration einer Anwendung;
- Umgebungsvariablen;
- VPN- oder Security-Agent-Konfigurationen.

Ein funktionierender Browser beweist daher nicht, dass ein Windows-Dienst mit WinHTTP ebenfalls den richtigen Proxy verwendet.

Nicht ungeprüft ausführen

Folgende Befehle verändern die Proxykonfiguration:

```
netsh winhttp set proxy
netsh winhttp reset proxy
netsh winhttp import proxy
```

Sie benötigen eine begründete Änderung, eine dokumentierte Ausgangskonfiguration und einen Rückfallplan.

---

21. Windows-Firewallstatus prüfen

Status aller Firewallprofile anzeigen

Kennzeichnung: `[RO]`

```
netsh advfirewall show allprofiles state
```

Aktuelles Firewallprofil anzeigen

```
netsh advfirewall show currentprofile
```

Firewallrichtlinie des aktuellen Profils anzeigen

```
netsh advfirewall show currentprofile firewallpolicy
```

Protokollierung des aktuellen Profils anzeigen

```
netsh advfirewall show currentprofile logging
```

Zu prüfen sind:

- aktives Profil;
- Firewallstatus;
- Standardaktion für eingehende Verbindungen;
- Standardaktion für ausgehende Verbindungen;
- Protokollierung verworfener Verbindungen;
- Speicherort des Firewalllogs;
- Gruppenrichtlinien oder zentrale Verwaltung.

Firewall nicht pauschal deaktivieren

Das vollständige Ausschalten der Firewall ist kein geeigneter erster Diagnosetest.

Besser:

1. betroffenes Profil feststellen;
2. Richtung bestimmen;
3. Protokoll und Port bestimmen;

4. lokale und entfernte Adresse bestimmen;
5. passende Regeln und Logs prüfen;
6. nur bei Freigabe eine eng begrenzte temporäre Testregel verwenden;
7. Testregel anschließend wieder entfernen.

---

22. Diagnoseausgaben sichern

IP-Konfiguration exportieren

Kennzeichnung: `[RO][FILE][SENS]`

```
ipconfig /all > "<Ausgabepfad>\ipconfig-all.txt"
```

Routingtabelle exportieren

```
route print > "<Ausgabepfad>\route-print.txt"
```

ARP-Tabelle exportieren

```
arp -a > "<Ausgabepfad>\arp-cache.txt"
```

Verbindungen und Listener exportieren

```
netstat -ano > "<Ausgabepfad>\netstat-ano.txt"
```

Pfadtest exportieren

Kennzeichnung: `[TEST][FILE][SENS]`

```
tracert /d 192.0.2.25 > "<Ausgabepfad>\tracert.txt"
```

Standardausgabe und Fehlermeldungen gemeinsam sichern

```
pathping /n 192.0.2.25 > "<Ausgabepfad>\pathping.txt" 2>&1
```

An eine vorhandene Datei anhängen

```
ipconfig /all >> "<Ausgabepfad>\netzdiagnose.txt"
```

Bedeutung:

Operator	Wirkung
`>`	Datei neu erstellen beziehungsweise vorhandenen Inhalt überschreiben
`>>`	Ausgabe an vorhandene Datei anhängen
`2>&1`	Fehlermeldungen zusammen mit der Standardausgabe umleiten

Vor dem Überschreiben einer vorhandenen Diagnosedatei muss geprüft werden, ob sie noch benötigt wird.

---

23. Kompakter Erfassungsblock

Die folgenden Befehle verändern keine Netzwerkkonfiguration. Die Ausgabe kann jedoch sensible Informationen enthalten.

```
hostname
getmac /v
ipconfig /all
route print
arp -a
netstat -ano
netsh interface show interface
netsh interface ipv4 show neighbors
netsh interface ipv6 show neighbors
netsh winhttp show proxy
netsh advfirewall show allprofiles state
```

Bei WLAN-Systemen zusätzlich:

```
netsh wlan show interfaces
netsh wlan show drivers
netsh wlan show profiles
```

Diese Sammlung ist nur eine Bestandsaufnahme. Sie ersetzt keine gezielte Bewertung der Ergebnisse.

---

24. Diagnosepfade für häufige Fehlerbilder

Fehlerbild: Keine Netzwerkverbindung

```
netsh interface show interface
ipconfig /all
route print
arp -a
```

Prüfen:

- Adapter administrativ aktiviert?
- Medium verbunden?
- gültige IP-Adresse?
- Standardgateway vorhanden?
- DNS-Server vorhanden?
- APIPA-Adresse?
- passende Route vorhanden?

Fehlerbild: IP-Adresse vorhanden, aber kein Internet

```
ipconfig /all
ping <Gateway-IP>
ping /4 <Bekannte-Ziel-IP>
nslookup <Bekannter-Zielname>
tracert /d <Bekannte-Ziel-IP>
netsh winhttp show proxy
netsh advfirewall show currentprofile
```

Auswertung:

Ergebnis	Verdächtiger Bereich
Gateway nicht erreichbar	lokales Netz, VLAN, WLAN, Kabel oder Gateway
Gateway erreichbar, externe IP nicht	Routing, Firewall, NAT oder Provider
Externe IP erreichbar, Name nicht	DNS
Name und IP erreichbar, Anwendung nicht	Port, TLS, Proxy oder Anwendung
Nur Dienst verwendet keinen Internetzugriff	WinHTTP-Proxy, Dienstkonto oder Firewall

---

Fehlerbild: DNS funktioniert nicht

```
ipconfig /all
ipconfig /displaydns
nslookup server.example.test
nslookup server.example.test 192.0.2.53
ping /4 server.example.test
ping /6 server.example.test
```

Prüfen:

- korrekte DNS-Server?
- antworten alle eingetragenen DNS-Server?
- unterschiedliche Antworten je DNS-Server?
- A- und AAAA-Record korrekt?
- negativer Cacheeintrag?
- falsches DNS-Suffix?
- Split-DNS oder VPN relevant?
- hosts-Datei oder Anwendungscache relevant?

Fehlerbild: Ein lokaler Dienst ist nicht erreichbar

```
netstat -ano | findstr ":443"
tasklist /FI "PID eq <PID>"
netsh advfirewall show currentprofile
```

Prüfen:

- existiert ein `LISTENING`-Eintrag?
- lauscht der Dienst auf der erwarteten Adresse?
- lauscht er nur auf `127.0.0.1` oder `::1`?
- stimmt der Port?
- stimmt die PID mit dem erwarteten Prozess überein?
- ist die Firewallregel für das aktive Profil gültig?

Der Test eines entfernten TCP-Ports folgt auf der nächsten Seite mit `Test-NetConnection`.

Fehlerbild: Verbindung ist langsam oder instabil

```
ping /n 50 <Gateway-IP>
ping /n 50 <Ziel-IP>
tracert /d <Ziel-IP>
```

```
pathping /n <Ziel-IP>
netstat -e -s
```

Bei WLAN zusätzlich:

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

Prüfen:

- Verlust bereits zum Gateway?
- nur entferntes Ziel betroffen?
- steigende Latenz ab bestimmtem Abschnitt?
- schwankendes WLAN-Signal?
- Kanal oder BSSID wechseln?
- Fehlerzähler steigen während der Störung?
- ist nur ICMP oder auch die Anwendung betroffen?

Fehlerbild: Nur IPv4 oder nur IPv6 funktioniert

```
ipconfig /all
ping /4 server.example.test
ping /6 server.example.test
tracert /4 server.example.test
tracert /6 server.example.test
route print
netsh interface ipv4 show route
netsh interface ipv6 show route
netsh interface ipv6 show neighbors
```

Prüfen:

- A- und AAAA-Record vorhanden?
- IPv6-Adresse außer Link-Local vorhanden?
- IPv6-Default-Route vorhanden?
- Router Advertisements funktionieren?
- VPN oder Firewall behandelt IPv4 und IPv6 unterschiedlich?
- Anwendung bevorzugt einen nicht funktionierenden IPv6-Pfad?

---

25. Typische Fehlinterpretationen

Fehlinterpretation	Richtige Bewertung
Ping funktioniert, also funktioniert das Netzwerk vollständig	Ping prüft nur eine bestimmte ICMP-Kommunikation
Ping funktioniert nicht, also ist das Ziel ausgeschaltet	ICMP kann gefiltert oder begrenzt sein
Sternchen bei tracert bedeuten Paketverlust	Der Router hat möglicherweise nur keine ICMP-Antwort gesendet
Verlust an einem pathping-Zwischenhop beweist einen defekten Router	Entscheidend ist, ob sich der Verlust bis zum Ziel fortsetzt
`nslookup` funktioniert, also funktioniert DNS für jede Anwendung	Anwendungen können andere Resolverpfade, Caches oder Proxys verwenden
Eine ARP-Tabelle zeigt alle erreichbaren Systeme	Sie enthält nur bereits gelernte oder statische lokale IPv4-Nachbarn
`ESTABLISHED` bedeutet, dass die Anwendung funktioniert	Es beweist nur eine aufgebaute TCP-Verbindung
Viele `TIME_WAIT`-Einträge sind automatisch ein Fehler	Sie können bei hoher normaler Verbindungsrate entstehen
`169.254.x.x` bedeutet defekte Netzwerkkarte	Es weist normalerweise auf automatische Adressierung ohne verwendbare DHCP-Konfiguration hin
Mehrere Gateways sind automatisch redundant	Sie können zu unerwarteter Routenauswahl führen
Firewall ausschalten ist der schnellste Test	Das erzeugt ein Sicherheitsrisiko und liefert oft keine saubere Ursachenanalyse
DNS-Cache sofort leeren hilft immer	Dabei kann der ursprüngliche Fehlerzustand verloren gehen

---

26. Befehle mit besonderer Vorsicht

Befehl	Kennzeichnung	Risiko
`ipconfig /release`	`[CHANGE][DISRUPT]`	Entfernt die aktuelle DHCP-Konfiguration
`ipconfig /renew`	`[TEST][CHANGE]`	Verändert die aktuelle DHCP-Konfiguration
`ipconfig /flushdns`	`[CHANGE]`	Entfernt den DNS-Clientcache und mögliche Beweise
`ipconfig /registerdns`	`[TEST][CHANGE]`	Stößt dynamische DNS-Registrierungen an
`arp -d <IP>`	`[PRIV][CHANGE]`	Entfernt eine Nachbarzuordnung
`route add`	`[PRIV][CHANGE]`	Fügt eine Route hinzu
`route change`	`[PRIV][CHANGE]`	Verändert eine Route
`route delete`	`[PRIV][CHANGE][DISRUPT]`	Entfernt eine Route

Befehl	Kennzeichnung	Risiko
`route /f`	`[PRIV][CHANGE][DISRUPT]`	Entfernt einen großen Teil der Routingtabelle
`netsh interface set ...`	`[PRIV][CHANGE][DISRUPT]`	Verändert Interfacekonfiguration
`netsh winhttp reset proxy`	`[PRIV][CHANGE]`	Entfernt die WinHTTP-Proxykonfiguration
`netsh advfirewall set ...`	`[PRIV][CHANGE][DISRUPT]`	Verändert Firewallrichtlinien
`netsh wlan disconnect`	`[CHANGE][DISRUPT]`	Trennt eine WLAN-Verbindung
`netsh wlan delete profile`	`[PRIV][CHANGE]`	Löscht ein gespeichertes WLAN-Profil

Vor diesen Befehlen müssen Ausgangszustand, Auswirkung und Rückfallplan dokumentiert werden.

---

27. Grenzen der klassischen Windows-Befehle

Die klassischen Befehle sind schnell verfügbar und eignen sich gut für eine erste Diagnose. Sie haben jedoch einige Einschränkungen:

- Ausgaben sind teilweise sprachabhängig;
- Textausgaben sind für Automatisierung schlechter geeignet;
- komplexe Filterungen sind umständlich;
- IPv4- und IPv6-Informationen sind teilweise getrennt;
- strukturierte Weiterverarbeitung ist begrenzt;
- ein beliebiger entfernter TCP-Port lässt sich mit den klassischen Grundbefehlen nicht so bequem testen;
- mehrere Adapter und Routen sind in Textausgaben schwerer vergleichbar.

Für strukturierte und gezielte Windows-Diagnosen folgt deshalb:

> **2.2 PowerShell-Netzwerkdiagnose**

Quellen und weiterführende Dokumentation

- Microsoft Learn – `hostname`: https://learn.microsoft.com/en-us/windows-server/administration/windows-commands/hostname
- Microsoft Learn – `getmac`: https://learn.microsoft.com/en-us/windows-server/administration/windows-commands/getmac
- Microsoft Learn – `ipconfig`: https://learn.microsoft.com/en-us/windows-server/administration/windows-

commands/ipconfig

- Microsoft Learn – Automatic Private IP Addressing: https://learn.microsoft.com/en-us/windows-server/troubleshoot/how-to-use-automatic-tcpip-addressing-without-a-dh
- Microsoft Learn – `ping`: https://learn.microsoft.com/en-us/windows-server/administration/windows-commands/ping
- Microsoft Learn – `tracert`: https://learn.microsoft.com/en-us/windows-server/administration/windows-commands/tracert
- Microsoft Learn – `pathping`: https://learn.microsoft.com/en-us/windows-server/administration/windows-commands/pathping
- Microsoft Learn – `route`: https://learn.microsoft.com/en-us/windows-server/administration/windows-commands/route_ws2008
- Microsoft Learn – `arp`: https://learn.microsoft.com/en-us/windows-server/administration/windows-commands/arp
- Microsoft Learn – `nslookup`: https://learn.microsoft.com/en-us/windows-server/administration/windows-commands/nslookup
- Microsoft Learn – `nbtstat`: https://learn.microsoft.com/en-us/windows-server/administration/windows-commands/nbtstat
- Microsoft Learn – `netstat`: https://learn.microsoft.com/en-us/windows-server/administration/windows-commands/netstat
- Microsoft Learn – TCP-Zustände: https://learn.microsoft.com/en-us/windows/win32/api/mstcpip/ne-mstcpip-tcpstate
- Microsoft Learn – `tasklist`: https://learn.microsoft.com/en-us/windows-server/administration/windows-commands/tasklist
- Microsoft Learn – `findstr`: https://learn.microsoft.com/en-us/windows-server/administration/windows-commands/findstr
- Microsoft Learn – Network Shell `netsh`: https://learn.microsoft.com/en-us/windows-server/administration/windows-commands/netsh

- Microsoft Learn – `netsh interface`: https://learn.microsoft.com/en-us/windows-server/administration/windows-commands/netsh-interface
- Microsoft Learn – `netsh wlan`: https://learn.microsoft.com/en-us/windows-server/administration/windows-commands/netsh-wlan
- Microsoft Learn – `netsh winhttp`: https://learn.microsoft.com/en-us/windows-server/administration/windows-commands/netsh-winhttp
- Microsoft Learn – `netsh advfirewall`: https://learn.microsoft.com/en-us/windows-server/administration/windows-commands/netsh-advfirewall

---