2.4 macOS-Netzwerkdiagnose

macOS basiert auf Darwin und stellt zahlreiche BSD- und Apple-spezifische Netzwerkwerkzeuge bereit. Einige Befehle ähneln Linux-Kommandos, verwenden aber teilweise andere Optionen und Ausgabeformate.

Wichtige macOS-Werkzeuge sind:

- `networksetup` für Netzwerkdienste und deren Konfiguration
- `scutil` für System Configuration, DNS, Proxys und Netzwerkstatus
- `ifconfig` für Netzwerkschnittstellen
- `route` und `netstat` für Routingtabellen
- `arp` und `ndp` für Nachbartabellen
- `ping` und `traceroute` für Erreichbarkeit und Netzwerkpfade
- `dig`, `host` und `dscacheutil` für DNS
- `wdutil` und Wireless Diagnostics für WLAN
- `networkQuality` für Kapazität und Reaktionsfähigkeit
- `lsof`, `netstat` und `nc` für Ports und Verbindungen
- `log` für das Unified Logging System
- `socketfilterfw` und `pfctl` für die Firewalldiagnose

Kennzeichnungen

Kennzeichnung	Bedeutung
`[RO]`	Nur lesender Befehl; verändert keine Konfiguration
`[TEST]`	Führt einen aktiven Netzwerk- oder Verbindungstest aus
`[PRIV]`	Benötigt Administratorrechte beziehungsweise `sudo`
`[CHANGE]`	Verändert einen Zustand oder eine Konfiguration
`[DISRUPT]`	Kann eine Verbindung oder einen Dienst unterbrechen
`[FILE]`	Schreibt Informationen in eine Datei
`[SENS]`	Ausgabe kann sensible System-, Netzwerk- oder Prozessdaten enthalten

> Vor Änderungen sollten Netzwerkdienst, Schnittstelle, IP-Konfiguration, Route, DNS-Server und aktive VPN- beziehungsweise Proxykonfiguration dokumentiert werden.

---

1. macOS-Version und verfügbare Werkzeuge prüfen

Aufgabe	macOS-Befehl
macOS-Version anzeigen	`[RO] sw_vers`
Produktversion kompakt anzeigen	`[RO] sw_vers -productVersion`
Build-Nummer anzeigen	`[RO] sw_vers -buildVersion`
Kernelversion anzeigen	`[RO] uname -a`
Prozessorarchitektur anzeigen	`[RO] uname -m`
Hardwareübersicht anzeigen	`[RO] system_profiler SPHardwareDataType`
Softwareübersicht anzeigen	`[RO] system_profiler SPSoftwareDataType`
Prüfen, ob ein Befehl vorhanden ist	`[RO] command -v networkQuality`
Mehrere Werkzeuge prüfen	`[RO] command -v networksetup scutil ifconfig route netstat arp ndp ping traceroute dig lsof nc wdutil networkQuality`
Hilfe zu `networksetup` anzeigen	`[RO] networksetup -help`
Lokale Handbuchseite öffnen	`[RO] man networksetup`
Handbuchseite zu `scutil` öffnen	`[RO] man scutil`
Handbuchseite zu `ifconfig` öffnen	`[RO] man ifconfig`

Hinweis zu macOS-Versionen

Nicht jedes Werkzeug steht in jeder macOS-Version zur Verfügung:

- `networkQuality` ist auf aktuellen macOS-Versionen vorhanden.
- `wdutil` ist auf aktuellen macOS-Versionen das Kommandozeilenwerkzeug für WLAN-Diagnosedaten.
- Das frühere private `airport`-Werkzeug ist auf aktuellen macOS-Versionen nicht mehr als zuverlässiger Standard verfügbar.
- Optionen und Ausgaben können sich zwischen macOS-Versionen ändern.

---

2. Netzwerkdienste und Hardwareports zuordnen

Unter macOS muss zwischen einem Netzwerkdienst und der technischen Schnittstelle unterschieden werden.

Beispiele:

Netzwerkdienst	Mögliche Schnittstelle

`Wi-Fi`	`en0` oder eine andere `en`-Schnittstelle
`Ethernet`	`en0` `en1` `en5` oder eine andere Schnittstelle
USB-Ethernet	Abhängig vom angeschlossenen Adapter
Thunderbolt Bridge	Bridge- beziehungsweise Thunderbolt-Schnittstelle
VPN	Häufig `utun0` `utun1` oder eine weitere `utun`-Schnittstelle

Zuordnung prüfen

Aufgabe	macOS-Befehl
Alle Hardwareports auflisten	`[RO] networksetup -listallhardwareports`
Alle Netzwerkdienste auflisten	`[RO] networksetup -listallnetworkservices`
Reihenfolge der Netzwerkdienste anzeigen	`[RO] networksetup -listnetworkserviceorder`
Informationen zum Dienst Wi-Fi anzeigen	`[RO] networksetup -getinfo "Wi-Fi"`
Informationen zum Dienst Ethernet anzeigen	`[RO] networksetup -getinfo "Ethernet"`
Aktive Netzwerksicht anzeigen	`[RO] scutil --nwi`
Netzwerkkonfiguration über System Profiler anzeigen	`[RO][SENS] system_profiler SPNetworkDataType`

Wichtiger Unterschied

- `Wi-Fi` ist normalerweise der Name eines Netzwerkdienstes.
- `en0` ist der Name einer technischen Netzwerkschnittstelle.
- `networksetup` erwartet je nach Option entweder einen Dienstnamen oder einen Gerätenamen.
- Der Gerätename darf nicht anhand eines anderen Macs geraten werden.

> Vor jedem Befehl mit `en0`, `en1` oder einem Dienstnamen muss die tatsächliche Zuordnung mit `networksetup -listallhardwareports` geprüft werden.

---

3. Netzwerkschnittstellen und Linkstatus prüfen

Aufgabe	macOS-Befehl
Alle Schnittstellen anzeigen	`[RO] ifconfig -a`
Einzelne Schnittstelle anzeigen	`[RO] ifconfig en0`

Aufgabe	macOS-Befehl
Aktive Schnittstellen anzeigen	`[RO] ifconfig -u`
Inaktive Schnittstellen anzeigen	`[RO] ifconfig -d`
Schnittstellennamen auflisten	`[RO] ifconfig -l`
Schnittstellenstatistik anzeigen	`[RO] netstat -ibn`
Netzwerkhardware anzeigen	`[RO][SENS] system_profiler SPNetworkDataType`
Ethernet-Hardwareinformationen anzeigen	`[RO] system_profiler SPEthernetDataType`

Wichtige Angaben von `ifconfig`

Angabe	Bedeutung
`UP`	Schnittstelle wurde administrativ aktiviert
`RUNNING`	Schnittstelle ist betriebsbereit
`ACTIVE`	Aktiver physischer beziehungsweise logischer Link
`status: active`	Verbindung wurde erkannt
`status: inactive`	Keine aktive Verbindung erkannt
`ether`	MAC-Adresse
`inet`	IPv4-Adresse
`inet6`	IPv6-Adresse
`netmask`	Netzmaske, häufig hexadezimal dargestellt
`broadcast`	IPv4-Broadcastadresse
`mtu`	Maximum Transmission Unit
`media`	Medium, Geschwindigkeit und Duplexmodus

Typische Fehlerbilder

Beobachtung	Mögliche Bedeutung
`status: inactive`	Kein Link, WLAN getrennt, Kabel- oder Portproblem
Schnittstelle fehlt	Adapter, Treiber, USB-/Thunderbolt-Verbindung oder Hardware prüfen
Keine `inet`-Adresse	Keine verwendbare IPv4-Konfiguration
Nur `169.254.x.x`	Keine reguläre IPv4-Konfiguration beziehungsweise DHCP-Zuweisung
Unerwartete MTU	VPN-, Tunnel- oder Fragmentierungsproblem möglich

Beobachtung	Mögliche Bedeutung
Viele Fehler in `netstat -ibn`	Link-, Adapter-, Treiber- oder Überlastungsproblem möglich

4. IP-Konfiguration und DHCP prüfen

Aufgabe	macOS-Befehl
IPv4-Adresse einer Schnittstelle anzeigen	`[RO] ipconfig getifaddr en0`
Gesamte Schnittstellenkonfiguration anzeigen	`[RO] ifconfig en0`
Informationen des Dienstes Wi-Fi anzeigen	`[RO] networksetup -getinfo "Wi-Fi"`
Informationen des Dienstes Ethernet anzeigen	`[RO] networksetup -getinfo "Ethernet"`
DHCP-Paketinformationen anzeigen	`[RO][PRIV][SENS] sudo ipconfig getpacket en0`
DHCP-Server auslesen	`[RO][PRIV] sudo ipconfig getoption en0 server_identifier`
Subnetzmaske auslesen	`[RO][PRIV] sudo ipconfig getoption en0 subnet_mask`
Router aus DHCP auslesen	`[RO][PRIV] sudo ipconfig getoption en0 router`
DNS-Server aus DHCP auslesen	`[RO][PRIV] sudo ipconfig getoption en0 domain_name_server`
IPv6-Konfiguration anzeigen	`[RO] ifconfig en0 | grep inet6`
Netzwerkstatus zusammengefasst anzeigen	`[RO] scutil --nwi`

Prüfpunkte

- Wurde die erwartete IPv4-Adresse vergeben?
- Stimmt die Subnetzmaske?
- Ist der Router korrekt?
- Ist der erwartete DHCP-Server sichtbar?
- Sind DNS-Server vorhanden?
- Befindet sich die Adresse im Bereich `169.254.0.0/16`?
- Existieren mehrere aktive Schnittstellen mit konkurrierenden Routen?
- Ist ein VPN aktiv, das die Routenauswahl verändert?

> “ `ipconfig getpacket` zeigt die zuletzt erhaltenen DHCP-Informationen. Die Ausgabe kann interne Netzwerkinformationen enthalten.

5. Routingtabelle und verwendeten Netzwerkweg prüfen

Aufgabe	macOS-Befehl
Standardroute anzeigen	`[RO] route -n get default`
Route zu einer IPv4-Adresse anzeigen	`[RO] route -n get 1.1.1.1`
Route zu einem DNS-Namen anzeigen	`[RO][TEST] route -n get example.com`
IPv4-Routingtabelle anzeigen	`[RO] netstat -rn -f inet`
IPv6-Routingtabelle anzeigen	`[RO] netstat -rn -f inet6`
Gesamte Routingtabelle anzeigen	`[RO] netstat -rn`
Netzwerkstatus anzeigen	`[RO] scutil --nwi`
Aktive VPN-/Tunnel-Schnittstellen suchen	`[RO] ifconfig -l | tr ' ' '\n' | grep '^utun'`
Details einer Tunnel-Schnittstelle anzeigen	`[RO] ifconfig utun0`

Wichtige Angaben von `route -n get`

Angabe	Bedeutung
`destination`	Zieladresse
`gateway`	Nächster Router
`interface`	Verwendete Schnittstelle
`flags`	Eigenschaften der Route
`recvpipe`	Empfangspufferinformationen
`sendpipe`	Sendepufferinformationen

Wichtige Flags der Routingtabelle

Flag	Bedeutung
`U`	Route ist aktiv
`G`	Ziel wird über ein Gateway erreicht
`H`	Hostroute zu einem einzelnen Ziel
`S`	Statische Route
`C`	Geklonte Route
`I`	Schnittstellenroute

Typische Fehlerbilder

- Standardroute fehlt.
- Standardroute verwendet die falsche Schnittstelle.
- VPN- oder `utun`-Schnittstelle übernimmt die Route.
- Ethernet und WLAN sind gleichzeitig aktiv und besitzen konkurrierende Wege.
- Die Reihenfolge der Netzwerkdienste entspricht nicht der erwarteten Priorität.
- Eine spezifischere Route überschreibt den allgemeinen Weg.

---

6. ARP- und IPv6-Nachbartabelle prüfen

Aufgabe	macOS-Befehl
Gesamte IPv4-ARP-Tabelle anzeigen	`[RO] arp -an`
Bestimmte IPv4-Adresse prüfen	`[RO] arp -n 192.0.2.1`
IPv6-Nachbartabelle anzeigen	`[RO] ndp -an`
IPv6-Standardrouter anzeigen	`[RO] ndp -r`
IPv6-Präfixinformationen anzeigen	`[RO] ndp -p`
Schnittstelleninformationen anzeigen	`[RO] ndp -i en0`

Typische Beobachtungen

Beobachtung	Mögliche Bedeutung
`(incomplete)`	MAC-Auflösung wurde nicht abgeschlossen
Kein Gateway-Eintrag	Gateway wurde noch nicht angesprochen oder ist nicht erreichbar
Unerwartete MAC-Adresse	Doppelte IP-Adresse, anderes Gateway oder Sicherheitsproblem möglich
Gleiche IP mit wechselnder MAC-Adresse	Hochverfügbarkeit, doppelte Adresse oder Manipulation prüfen
IPv6-Nachbarstatus nicht erreichbar	Lokalen IPv6-Link und Router Advertisement prüfen

> Ein fehlender ARP-Eintrag beweist nicht automatisch einen Fehler. Ein Eintrag entsteht normalerweise erst, wenn das Ziel angesprochen wurde.

---

7. Erreichbarkeit mit ping prüfen

Aufgabe	macOS-Befehl
Vier Anfragen an das Gateway senden	`[TEST] ping -c 4 192.0.2.1`
Externe IPv4-Adresse testen	`[TEST] ping -c 4 1.1.1.1`
DNS-Namen testen	`[TEST] ping -c 4 example.com`
Bestimmte Quelladresse verwenden	`[TEST] ping -S 192.0.2.10 -c 4 192.0.2.1`
IPv6-Ziel testen	`[TEST] ping6 -c 4 2001:db8::1`
IPv6-Link-Local-Ziel mit Schnittstelle testen	`[TEST] ping6 -c 4 fe80::1%en0`
Paketgröße testen	`[TEST] ping -c 4 -s 1400 192.0.2.1`
Akustisches Signal bei Antwort	`[TEST] ping -a -c 4 192.0.2.1`

Wichtige Ergebnisse

Wert	Bedeutung
`time`	Round Trip Time
`ttl`	Verbleibende IPv4 Time to Live
`icmp_seq`	Nummer der ICMP-Anfrage
`packet loss`	Anteil verlorener Pakete
`min/avg/max/stddev`	Laufzeitstatistik

Interpretation

Ergebnis	Mögliche Bedeutung
Gateway nicht erreichbar	Lokales Netz, WLAN, Kabel, VLAN oder Router prüfen
IP-Adresse erreichbar, DNS-Name nicht	DNS-Problem wahrscheinlich
Externe IP nicht erreichbar, Gateway erreichbar	Routing, Firewall, Provider oder Upstream prüfen
Ping schlägt fehl, TCP-Port funktioniert	ICMP wird möglicherweise blockiert
Hohe Laufzeitschwankungen	WLAN-Störung, Überlastung oder wechselnder Netzwerkweg
Paketverlust	Funkstörung, Linkproblem, Überlastung oder Rate Limiting möglich

---

8. Netzwerkpfad mit traceroute untersuchen

Aufgabe	macOS-Befehl

Netzwerkpfad anzeigen	`[TEST] traceroute example.com`
Keine DNS-Auflösung durchführen	`[TEST] traceroute -n example.com`
Anzahl der Hops begrenzen	`[TEST] traceroute -m 15 example.com`
Wartezeit pro Probe begrenzen	`[TEST] traceroute -w 2 example.com`
IPv6-Netzwerkpfad anzeigen	`[TEST] traceroute6 example.com`
ICMP statt UDP verwenden	`[TEST][PRIV] sudo traceroute -I example.com`

Auswertung

- Ein einzelner Hop ohne Antwort beweist keinen Fehler.
- Router können Diagnosepakete ignorieren und Nutzdaten trotzdem weiterleiten.
- Mehrere unterschiedliche Hops können durch Load Balancing entstehen.
- Entscheidend ist, ob das Ziel erreicht wird.
- Ein Abbruch ab einem bestimmten Hop kann auf Routing, Firewall oder eine Netzstörung hinweisen.
- Unterschiedliche Protokolle können unterschiedliche Pfade beziehungsweise Antworten zeigen.

---

9. DNS-Konfiguration und Namensauflösung prüfen

`scutil --dns` zeigt die tatsächlich vom macOS-System verwendete Resolverkonfiguration. Die Ausgabe kann mehrere Resolver für verschiedene Domänen und Schnittstellen enthalten.

Aufgabe	macOS-Befehl
Gesamte Resolverkonfiguration anzeigen	`[RO][SENS] scutil --dns`
DNS-Server des Dienstes Wi-Fi anzeigen	`[RO] networksetup -getdnsservers "Wi-Fi"`
DNS-Server des Dienstes Ethernet anzeigen	`[RO] networksetup -getdnsservers "Ethernet"`
Suchdomänen anzeigen	`[RO] networksetup -getsearchdomains "Wi-Fi"`
Namen über den Systemcache abfragen	`[TEST] dscacheutil -q host -a name example.com`
Standard-DNS-Abfrage durchführen	`[TEST] dig example.com`
IPv4-Adresse abfragen	`[TEST] dig A example.com`
IPv6-Adresse abfragen	`[TEST] dig AAAA example.com`
Mailserver abfragen	`[TEST] dig MX example.com`
Kurzausgabe erzeugen	`[TEST] dig +short example.com`
Bestimmten Resolver verwenden	`[TEST] dig @192.0.2.53 example.com`

Aufgabe	macOS-Befehl
Vollständigen Delegationsweg prüfen	`[TEST] dig +trace example.com`
Reverse-DNS-Abfrage durchführen	`[TEST] dig -x 192.0.2.10`
Alternative Abfrage durchführen	`[TEST] host example.com`
Lokale Hosts-Datei anzeigen	`[RO] cat /etc/hosts`

Warum kann macOS mehrere Resolver anzeigen?

macOS kann Resolver abhängig von folgenden Faktoren auswählen:

- Netzwerkdienst
- VPN-Verbindung
- Suchdomäne
- Split-DNS-Konfiguration
- verwaltetes Konfigurationsprofil
- iCloud Private Relay
- Network Extension
- lokale Hosts-Datei
- Anwendungsinterner DNS-Resolver

Typische Fehlerbilder

Beobachtung	Mögliche Ursache
`dig` funktioniert, Anwendung jedoch nicht	Anwendung, Cache, Proxy oder eigener Resolver
Öffentlicher Name funktioniert, interner nicht	Split-DNS, VPN oder interner Resolver prüfen
Falscher DNS-Server in `scutil --dns`	Netzwerkdienst, VPN oder Profil prüfen
Mehrere Resolver mit unterschiedlicher Reihenfolge	Domänenspezifische Resolver oder VPN-Konfiguration
IP-Adresse erreichbar, Name nicht	DNS-Problem wahrscheinlich
Unterschiedliche Antworten verschiedener DNS-Server	Split-DNS, Cache oder unterschiedliche Zonen

> Für die tatsächliche Resolverauswahl von macOS ist `scutil --dns` normalerweise aussagekräftiger als eine isolierte Betrachtung einzelner Konfigurationsfelder.

---

10. Proxy-, VPN- und Network-Extension-Einflüsse prüfen

Aufgabe	macOS-Befehl
Systemweite Proxykonfiguration anzeigen	`[RO][SENS] scutil --proxy`
HTTP-Proxy für Wi-Fi anzeigen	`[RO] networksetup -getwebproxy "Wi-Fi"`
HTTPS-Proxy für Wi-Fi anzeigen	`[RO] networksetup -getsecurewebproxy "Wi-Fi"`
Automatische Proxykonfiguration anzeigen	`[RO] networksetup -getautoproxyurl "Wi-Fi"`
Proxy-Bypass-Domänen anzeigen	`[RO][SENS] networksetup -getproxybypassdomains "Wi-Fi"`
Aktive Netzwerksicht anzeigen	`[RO] scutil --nwi`
Tunnel-Schnittstellen anzeigen	`[RO] ifconfig -l | tr ' ' '\n' | grep '^utun'`
Systemerweiterungen anzeigen	`[RO][SENS] systemextensionsctl list`
Netzwerkdienste nach Reihenfolge anzeigen	`[RO] networksetup -listnetworkserviceorder`

Mögliche Einflussfaktoren

- Unternehmens-VPN
- Content-Filter
- Endpoint-Security-Software
- DNS-Filter
- Webproxy
- PAC-Datei
- iCloud Private Relay
- lokale Firewall
- Network Extension
- Sicherheitssoftware eines Drittanbieters

Typisches Fehlerbild

Beobachtung	Mögliche Ursache
Ping funktioniert, Webseiten nicht	Proxy, DNS, TLS, Browser oder Filtersoftware
Nur einzelne Anwendungen betroffen	Anwendungsproxy oder anwendungsspezifische Network Extension
Verbindung funktioniert ohne VPN	VPN-Routing, DNS oder Richtlinie prüfen
Interne Namen funktionieren nur mit VPN	Split-DNS oder interne DNS-Zone
Falsche Route über `utun`	VPN- oder Filtersoftware beeinflusst Routing

---

11. WLAN-Verbindung und Funkqualität prüfen

Zuordnung und Status

Aufgabe	macOS-Befehl
Wi-Fi-Hardwareport bestimmen	`[RO] networksetup -listallhardwareports`
Wi-Fi-Energiezustand anzeigen	`[RO] networksetup -getairportpower en0`
Verbundenes WLAN anzeigen	`[RO] networksetup -getairportnetwork en0`
WLAN-Informationen anzeigen	`[RO][PRIV][SENS] sudo wdutil info`
Ausführliche WLAN-Hardwareinformationen	`[RO][SENS] system_profiler SPAirPortDataType`
WLAN-Schnittstelle anzeigen	`[RO] ifconfig en0`

> Vor der Verwendung von `en0` muss die tatsächliche Wi-Fi-Schnittstelle mit `networksetup -listallhardwareports` bestimmt werden.

Wichtige WLAN-Werte

Wert	Bedeutung
`SSID`	Name des WLANs
`BSSID`	MAC-Adresse des Access Points
`RSSI`	Empfangssignalstärke
`Noise`	Grundrauschen
`Channel`	Verwendeter Funkkanal
`Tx Rate`	Aktuelle Übertragungsrate
`PHY Mode`	Verwendeter WLAN-Standard
`Security`	Sicherheitsverfahren
`MCS`	Modulation and Coding Scheme
`NSS`	Anzahl räumlicher Datenströme

Signalbewertung als grobe Orientierung

RSSI	Grobe Einordnung
etwa `-30 dBm`	Sehr stark
etwa `-50 dBm`	Gut
etwa `-67 dBm`	Für viele Anwendungen noch brauchbar
etwa `-70 dBm`	Schwach
unter `-80 dBm`	Häufig instabil

> RSSI-Werte allein beweisen keinen Fehler. Kanalbelegung, Störungen, Rauschen, Wiederholungen, Access-Point-Auslastung und Roaming müssen ebenfalls berücksichtigt werden.

Grafische Wireless Diagnostics öffnen

1. Wahltaste beziehungsweise `Option` gedrückt halten.
2. In der Menüleiste auf das Wi-Fi-Symbol klicken.
3. **Wireless Diagnostics öffnen** auswählen.
4. Anweisungen des Assistenten befolgen.

Wireless Diagnostics verändert laut Apple nicht die Netzwerksettings. Nach einer Analyse kann eine Diagnosedatei unter `/var/tmp` erzeugt werden. Der Dateiname beginnt mit `WirelessDiagnostics` und endet mit `.tar.gz`.

---

12. Netzwerkqualität und Reaktionsfähigkeit messen

`networkQuality` misst nicht nur die verfügbare Kapazität, sondern auch die Reaktionsfähigkeit der Verbindung unter Last.

Aufgabe	macOS-Befehl
Standardmessung durchführen	`[TEST] networkQuality`
Ausführliche Messung durchführen	`[TEST] networkQuality -v`
Upload und Download nacheinander messen	`[TEST] networkQuality -s`
Bestimmte Schnittstelle verwenden	`[TEST] networkQuality -I en0`
Hilfe anzeigen	`[RO] networkQuality -h`
Lokale Handbuchseite öffnen	`[RO] man networkQuality`

Typische Ergebnisfelder

Ergebnis	Bedeutung
`Downlink capacity`	Gemessene Downloadkapazität
`Uplink capacity`	Gemessene Uploadkapazität
`Responsiveness`	Reaktionsfähigkeit unter Last
`Idle Latency`	Latenz ohne zusätzliche Last
`RPM`	Round-trips per Minute

Hinweise

- Die Messung erzeugt aktiven Netzwerkverkehr.
- Andere Benutzer und Anwendungen können das Ergebnis beeinflussen.
- WLAN- und Ethernet-Ergebnisse sollten getrennt betrachtet werden.
- Ein einzelner Test ist keine belastbare Langzeitmessung.
- Für Vergleiche sollten mehrere Messungen unter ähnlichen Bedingungen durchgeführt werden.
- VPN, Proxy, Filtersoftware und Private Relay können das Ergebnis beeinflussen.

---

13. Offene Ports, Verbindungen und Prozesse prüfen

Aufgabe	macOS-Befehl
Lauschende TCP-Ports anzeigen	`[RO][PRIV] sudo lsof -nP -iTCP -sTCP:LISTEN`
Alle Netzwerkverbindungen anzeigen	`[RO][PRIV] sudo lsof -nP -i`
TCP-Port 443 untersuchen	`[RO][PRIV] sudo lsof -nP -iTCP:443`
UDP-Port 53 untersuchen	`[RO][PRIV] sudo lsof -nP -iUDP:53`
TCP-Sockets anzeigen	`[RO] netstat -anv -p tcp`
UDP-Sockets anzeigen	`[RO] netstat -anv -p udp`
Netzwerkstatistik anzeigen	`[RO] netstat -s`
Schnittstellenstatistik anzeigen	`[RO] netstat -ibn`
Prozessdetails anzeigen	`[RO] ps -p 1234 -o pid,ppid,user,command`

Interpretation

Beobachtung	Mögliche Bedeutung
Erwarteter Port fehlt	Dienst läuft nicht oder lauscht auf einem anderen Port
Dienst lauscht auf `127.0.0.1`	Nur lokal erreichbar
Dienst lauscht auf `0.0.0.0`	Lauscht grundsätzlich auf allen IPv4-Schnittstellen
Dienst lauscht auf `::`	Lauscht auf IPv6; IPv4-Verhalten ist zusätzlich zu prüfen
Unerwarteter Prozess lauscht	Dienstzuordnung und Sicherheitslage prüfen
Viele Verbindungen im Verbindungsaufbau	Ziel, Route, Dienst oder Firewall antwortet möglicherweise nicht

---

14. TCP- und UDP-Ports aktiv testen

Aufgabe	macOS-Befehl
HTTPS-Port testen	`[TEST] nc -vz -w 3 example.com 443`
SSH-Port testen	`[TEST] nc -vz -w 3 192.0.2.10 22`
SMB-Port testen	`[TEST] nc -vz -w 3 192.0.2.10 445`
Mehrere Ports testen	`[TEST] nc -vz -w 3 192.0.2.10 22 80 443`
UDP-Port testen	`[TEST] nc -vzu -w 3 192.0.2.53 53`

Mögliche Ergebnisse

Ergebnis	Bedeutung
`succeeded`	TCP-Verbindung konnte aufgebaut werden
`Connection refused`	Ziel erreichbar, aber Port geschlossen oder aktiv abgelehnt
Timeout	Keine rechtzeitige Antwort; Firewall, Route oder Ziel prüfen
`No route to host`	Kein verwendbarer Netzwerkweg oder entsprechende Rückmeldung
Namensauflösungsfehler	DNS-Konfiguration prüfen

> Bei UDP kann ein fehlendes Ergebnis nicht zuverlässig beweisen, dass ein Port offen oder geschlossen ist.

---

15. macOS-Firewall und Packet Filter prüfen

macOS besitzt verschiedene Sicherheitskomponenten:

- Application Firewall
- Packet Filter `pf`
- Network Extensions
- Content Filter und Endpoint-Security-Produkte

Application Firewall

Aufgabe	macOS-Befehl

Globalen Firewallstatus anzeigen	`[RO] /usr/libexec/ApplicationFirewall/socketfilterfw --getglobalstate`
Stealth-Modus anzeigen	`[RO] /usr/libexec/ApplicationFirewall/socketfilterfw --getstealthmode`
Block-all-Modus anzeigen	`[RO] /usr/libexec/ApplicationFirewall/socketfilterfw --getblockall`
Registrierte Anwendungen anzeigen	`[RO][PRIV][SENS] sudo /usr/libexec/ApplicationFirewall/socketfilterfw --listapps`

Packet Filter

Aufgabe	macOS-Befehl
PF-Status anzeigen	`[RO][PRIV] sudo pfctl -s info`
Geladene Regeln anzeigen	`[RO][PRIV][SENS] sudo pfctl -sr`
NAT-Regeln anzeigen	`[RO][PRIV][SENS] sudo pfctl -sn`
Status und Statistiken anzeigen	`[RO][PRIV] sudo pfctl -s all`
PF-Tabellen anzeigen	`[RO][PRIV][SENS] sudo pfctl -s Tables`

Prüfreihenfolge

1. Prüfen, ob der Dienst lokal auf dem erwarteten Port lauscht.
2. Bind-Adresse des Dienstes prüfen.
3. Application-Firewallstatus prüfen.
4. PF-Status und Regeln prüfen.
5. Network Extensions und Sicherheitssoftware berücksichtigen.
6. Port von einem autorisierten zweiten System testen.

> Die Firewall nicht pauschal deaktivieren. Dadurch wird die Sicherheitslage verändert und das ursprüngliche Fehlerbild verfälscht.

---

16. Netzwerkprotokolle mit log untersuchen

macOS verwendet das Unified Logging System.

Aufgabe	macOS-Befehl
Meldungen der letzten 30 Minuten anzeigen	`[RO][PRIV][SENS] sudo log show --last 30m --style compact`
Meldungen von mDNSResponder anzeigen	`[RO][PRIV][SENS] sudo log show --last 30m --predicate 'process == "mDNSResponder"' --style compact`

Aufgabe	macOS-Befehl
Meldungen von configd anzeigen	`[RO][PRIV][SENS] sudo log show --last 30m --predicate 'process == "configd"' --style compact`
WLAN-Prozesse suchen	`[RO][PRIV][SENS] sudo log show --last 30m --predicate 'process CONTAINS[c] "airport" OR process CONTAINS[c] "WiFi"' --style compact`
DNS-Meldungen live verfolgen	`[RO][PRIV][SENS] sudo log stream --predicate 'process == "mDNSResponder"' --style compact`
Allgemeine Netzwerkbegriffe suchen	`` `[RO][PRIV][SENS] sudo log show --last 30m --style compact | grep -Ei 'network`

Prüfpunkte

- Exakter Zeitstempel der Störung
- Betroffene Schnittstelle
- DHCP-Ereignisse
- DNS-Fehler
- Verbindungsabbrüche
- WLAN-Roaming
- Authentifizierungsfehler
- VPN- oder Network-Extension-Ereignisse
- Interface-Wechsel
- Schlaf- und Aufwachereignisse

> Das macOS-Protokoll kann private und sensible Inhalte maskieren. Mit Administratorrechten können dennoch schützenswerte System- und Netzwerkdaten sichtbar werden.

---

17. Diagnoseinformationen sichern und vergleichen

Aufgabe	macOS-Befehl
Schnittstellen sichern	`[RO][FILE][SENS] ifconfig -a > interfaces.txt`
Routingtabelle sichern	`[RO][FILE][SENS] netstat -rn > routes.txt`
Standardroute sichern	`[RO][FILE][SENS] route -n get default > default-route.txt`
DNS-Konfiguration sichern	`[RO][FILE][SENS] scutil --dns > dns-status.txt`
Proxykonfiguration sichern	`[RO][FILE][SENS] scutil --proxy > proxy-status.txt`
Netzwerkdienste sichern	`[RO][FILE][SENS] networksetup -listnetworkserviceorder > network-services.txt`

Aufgabe	macOS-Befehl
Netzwerkübersicht sichern	[RO][FILE][SENS] system_profiler SPNetworkDataType > network-profiler.txt
Offene Ports sichern	[RO][PRIV][FILE][SENS] sudo lsof -nP -i > network-connections.txt
WLAN-Diagnose sichern	[RO][PRIV][FILE][SENS] sudo wdutil info > wifi-status.txt

Zwei Zustände vergleichen

```
ifconfig -a > interfaces-vorher.txt
netstat -rn > routes-vorher.txt
scutil --dns > dns-vorher.txt

# Messung oder freigegebene Änderung durchführen

ifconfig -a > interfaces-nachher.txt
netstat -rn > routes-nachher.txt
scutil --dns > dns-nachher.txt

diff -u interfaces-vorher.txt interfaces-nachher.txt
diff -u routes-vorher.txt routes-nachher.txt
diff -u dns-vorher.txt dns-nachher.txt
```

Datenschutz

Diagnoseausgaben können enthalten:

- interne und externe IP-Adressen
- MAC-Adressen
- DNS-Suchdomänen
- WLAN-Namen und BSSIDs
- VPN- und Proxyinformationen
- Prozessnamen
- Benutzerinformationen
- installierte Network Extensions
- interne Netzwerkstrukturen

Vor einer Weitergabe müssen sensible Angaben redigiert werden.

---

18. Eingreifende Befehle und Rückfallmöglichkeiten

Die folgenden Befehle verändern einen Zustand und können eine Remoteverbindung sofort unterbrechen.

Maßnahme	macOS-Befehl	Auswirkung
DNS-Cache leeren	`[CHANGE][PRIV] sudo dscacheutil -flushcache; sudo killall -HUP mDNSResponder`	Lokale DNS-Cacheeinträge werden verworfen
Wi-Fi ausschalten	`[CHANGE][PRIV][DISRUPT] sudo networksetup -setairportpower en0 off`	WLAN-Verbindung wird getrennt
Wi-Fi einschalten	`[CHANGE][PRIV] sudo networksetup -setairportpower en0 on`	WLAN wird wieder aktiviert
Schnittstelle deaktivieren	`[CHANGE][PRIV][DISRUPT] sudo ifconfig en0 down`	Alle Verbindungen über die Schnittstelle werden getrennt
Schnittstelle aktivieren	`[CHANGE][PRIV] sudo ifconfig en0 up`	Schnittstelle wird wieder aktiviert
Netzwerkdienst auf DHCP setzen	`[CHANGE][PRIV][DISRUPT] sudo networksetup -setdhcp "Wi-Fi"`	Vorhandene manuelle IPv4-Konfiguration wird ersetzt

> `en0` und `Wi-Fi` sind Beispiele. Vorher müssen die tatsächliche Schnittstelle und der tatsächliche Netzwerkdienst bestimmt werden.

Vor einem Eingriff prüfen

- Erfolgt der Zugriff lokal oder per Remotezugriff?
- Wird die aktive Managementverbindung unterbrochen?
- Ist die aktuelle manuelle IP-Konfiguration dokumentiert?
- Sind DNS-, Proxy- und VPN-Einstellungen gesichert?
- Ist ein lokaler Zugriff auf den Mac möglich?
- Wird der Mac durch MDM oder ein Konfigurationsprofil verwaltet?
- Existiert eine geeignete Rückfallmöglichkeit?

Rollback-Beispiele

Änderung	Rückfall
Wi-Fi ausgeschaltet	Wi-Fi mit `networksetup -setairportpower ... on` wieder einschalten
Schnittstelle deaktiviert	Schnittstelle mit `ifconfig ... up` wieder aktivieren
DHCP statt statischer IP gesetzt	Dokumentierte IP-, Masken-, Router- und DNS-Werte wiederherstellen
Netzwerkumgebung gewechselt	Vorherige Netzwerkumgebung wieder auswählen
Proxy verändert	Dokumentierte Proxywerte wiederherstellen

Verifikation nach einer Änderung

```
networksetup -getinfo "Wi-Fi"
ifconfig en0
route -n get default
scutil --dns
ping -c 4 192.0.2.1
ping -c 4 1.1.1.1
dig example.com
nc -vz -w 3 example.com 443
```

---

19. Praktische macOS-Diagnosereihenfolge

Schritt 1 – macOS-Version erfassen

```
sw_vers
```

Schritt 2 – Netzwerkdienst und Schnittstelle zuordnen

```
networksetup -listallhardwareports
networksetup -listnetworkserviceorder
```

Schritt 3 – Schnittstellenstatus prüfen

```
ifconfig -a
netstat -ibn
```

Schritt 4 – IP-Konfiguration prüfen

```
networksetup -getinfo "Wi-Fi"
ipconfig getifaddr en0
```

Schritt 5 – Standardroute prüfen

```
route -n get default
route -n get 1.1.1.1
```

Schritt 6 – Nachbartabelle prüfen

```
arp -an
ndp -an
```

Schritt 7 – Standardgateway testen

```
ping -c 4 192.0.2.1
```

Schritt 8 – Externe IP-Adresse testen

```
ping -c 4 1.1.1.1
```

Schritt 9 – DNS-Konfiguration prüfen

```
scutil --dns
networksetup -getdnsservers "Wi-Fi"
```

Schritt 10 – DNS-Auflösung testen

```
dscacheutil -q host -a name example.com
dig example.com
```

Schritt 11 – Proxy und VPN prüfen

```
scutil --proxy
scutil --nwi
ifconfig -l | tr ' ' '\n' | grep '^utun'
```

Schritt 12 – Zielport testen

```
nc -vz -w 3 example.com 443
```

Schritt 13 – Lokale Ports prüfen

```
sudo lsof -nP -iTCP -sTCP:LISTEN
```

Schritt 14 – Netzwerkpfad prüfen

```
traceroute -n example.com
```

Schritt 15 – Netzwerkqualität messen

```
networkQuality -v
```

Schritt 16 – Firewall und Protokolle prüfen

```
/usr/libexec/ApplicationFirewall/socketfilterfw --getglobalstate
sudo pfctl -s info
sudo log show --last 30m --style compact
```

Diagnoselogik

Ergebnis	Nächster Schwerpunkt
Schnittstelle fehlt	Adapter, USB-/Thunderbolt-Verbindung oder Hardware prüfen
Schnittstelle inaktiv	WLAN, Kabel, Netzwerkdienst oder Port prüfen
Keine passende IP-Adresse	DHCP oder manuelle Konfiguration prüfen
Keine Standardroute	Router, Dienstreihenfolge, VPN oder Konfiguration prüfen
Gateway nicht erreichbar	Lokales Netz, WLAN, VLAN, Switch oder Router prüfen
Externe IP erreichbar, DNS-Name nicht	Resolver, DNS-Server und Split-DNS prüfen
Ziel-IP erreichbar, Zielport nicht	Dienst, Bind-Adresse und Firewall prüfen
Nur Anwendungen betroffen	Proxy, TLS, Private Relay oder Network Extension prüfen
Falsche Route über `utun`	VPN- beziehungsweise Filtersoftware prüfen
Schlechte WLAN-Werte	Signal, Kanal, Rauschen, Roaming und Access Point prüfen

---

Kurzreferenz

Diagnoseziel	macOS-Befehl
macOS-Version	`[RO] sw_vers`
Hardwareports	`[RO] networksetup -listallhardwareports`
Netzwerkdienste	`[RO] networksetup -listallnetworkservices`
Dienstreihenfolge	`[RO] networksetup -listnetworkserviceorder`
Netzwerkschnittstellen	`[RO] ifconfig -a`
Schnittstellenstatistik	`[RO] netstat -ibn`
IPv4-Adresse	`[RO] ipconfig getifaddr en0`
Dienstinformationen	`[RO] networksetup -getinfo "Wi-Fi"`
Standardroute	`[RO] route -n get default`
Route zu einem Ziel	`[RO] route -n get 1.1.1.1`
IPv4-Routingtabelle	`[RO] netstat -rn -f inet`
ARP-Tabelle	`[RO] arp -an`
IPv6-Nachbarn	`[RO] ndp -an`
Gateway testen	`[TEST] ping -c 4 192.0.2.1`
Netzwerkpfad	`[TEST] traceroute -n example.com`
DNS-Konfiguration	`[RO] scutil --dns`
DNS-Abfrage	`[TEST] dig example.com`
Systemresolver testen	`[TEST] dscacheutil -q host -a name example.com`
Proxykonfiguration	`[RO] scutil --proxy`
Netzwerkstatus	`[RO] scutil --nwi`
WLAN-Informationen	`[RO][PRIV] sudo wdutil info`
Netzwerkqualität	`[TEST] networkQuality -v`
Lauschende Ports	`[RO][PRIV] sudo lsof -nP -iTCP -sTCP:LISTEN`
TCP-Port testen	`[TEST] nc -vz -w 3 example.com 443`
Application Firewall	`[RO] /usr/libexec/ApplicationFirewall/socketfilterfw --getglobalstate`
Packet Filter	`[RO][PRIV] sudo pfctl -s info`
Systemprotokoll	`[RO][PRIV] sudo log show --last 30m --style compact`

Veraltete beziehungsweise nicht mehr zuverlässige Werkzeuge

Werkzeug	Bewertung

Privates `airport`-Kommandozeilenwerkzeug	Auf aktuellen macOS-Versionen nicht als zuverlässiger Standard verwenden
`ifconfig`	Unter macOS weiterhin Bestandteil des Systems und für Diagnose geeignet
`netstat`	Unter macOS weiterhin für Routing-, Socket- und Schnittstellendiagnose verwendbar
`wdutil`	Auf aktuellen macOS-Versionen für WLAN-Diagnose bevorzugen
Wireless Diagnostics	Von Apple bereitgestelltes grafisches Diagnosewerkzeug

---

Merksatz

> Die macOS-Netzwerkdiagnose folgt der Kette: Netzwerkdienst → Schnittstelle → Link → IP-Adresse → Nachbartabelle → Route → Gateway → DNS → Proxy/VPN → Zielport → lokaler Dienst → Firewall → Protokolle.

Quellen

- Apple Support – Internetverbindungsprobleme auf dem Mac lösen
- Apple Support – Netzwerkstatus auf dem Mac prüfen
- Apple Support – Wireless Diagnostics verwenden
- Apple Support – Wi-Fi-Statusmenü verwenden
- Apple Support – Wi-Fi-Einstellungen auf dem Mac
- Apple Support – Informationen zu networksetup
- Apple Support – Terminal-Benutzerhandbuch
- Lokale Apple-Manpages: `man networksetup`, `man scutil`, `man ifconfig`, `man route`, `man netstat`, `man arp`, `man ndp`, `man ping`, `man traceroute`, `man networkQuality`, `man pfctl`
