3.0 Netzwerkfehler systematisch eingrenzen

Netzwerkstörungen sollten nicht durch zufälliges Ausprobieren einzelner Befehle untersucht werden. Eine zuverlässige Diagnose beginnt beim betroffenen Endgerät und arbeitet sich schrittweise durch die beteiligten Ebenen und Komponenten bis zum Zielsystem vor.

Dieses Kapitel behandelt typische Fehler in lokalen Netzwerken, standortübergreifenden Verbindungen und beim Zugriff auf interne oder externe Dienste.

> **Grundregel:** Zuerst feststellen, auf welcher Ebene die Kommunikation scheitert. Erst danach wird die konkrete Ursache innerhalb dieser Ebene untersucht.

---

1. Welche Ziele verfolgt dieses Kapitel?

Nach diesem Kapitel soll eine Netzwerkstörung strukturiert folgenden Bereichen zugeordnet werden können:

- physische Verbindung,
- Netzwerkschnittstelle und Treiber,
- VLAN und Layer-2-Kommunikation,
- IP-Konfiguration und Subnetz,
- DHCP,
- ARP beziehungsweise IPv6 Neighbor Discovery,
- Routing und Standardgateway,
- DNS und Namensauflösung,
- TCP- und UDP-Ports,
- Firewall und Paketfilter,
- NAT und Portweiterleitung,
- Proxy und Reverse Proxy,
- VPN und Tunnel,
- WLAN,
- Netzwerkperformance,
- Paketverlust und Wiederholungen,
- MTU und Fragmentierung,
- interne oder externe Zielsysteme.

Das Ziel ist nicht nur, die Verbindung wiederherzustellen, sondern die tatsächliche Ursache nachvollziehbar zu bestimmen und zu dokumentieren.

2. Welche Seiten enthält das Kapitel?

Seite	Thema	Zentrale Fragestellung
3.0	Netzwerkfehler systematisch eingrenzen	Wie wird eine Netzwerkstörung grundsätzlich untersucht?
3.1	Störungsumfang und Kommunikationsweg bestimmen	Wer ist betroffen und welchen Weg nimmt die Verbindung?
3.2	Physische Verbindung und Netzwerkschnittstelle	Bestehen Link, Signal und fehlerfreie Schnittstellenkommunikation?
3.3	IP-Konfiguration und Subnetz prüfen	Besitzt das Endgerät eine gültige und passende Konfiguration?
3.4	DHCP-Fehler analysieren	Warum erhält ein Client keine oder eine falsche IP-Konfiguration?
3.5	ARP und IPv6 Neighbor Discovery	Kann die lokale Zieladresse einer MAC-Adresse zugeordnet werden?
3.6	VLAN- und Layer-2-Fehler	Befinden sich Port und Endgerät im richtigen logischen Netz?
3.7	Standardgateway und Routing	Existiert ein gültiger Weg zum Zielnetz?
3.8	DNS-Fehler analysieren	Ist nur die Namensauflösung oder die gesamte Verbindung gestört?
3.9	Ports und Transportprotokolle prüfen	Ist der benötigte TCP- oder UDP-Dienst erreichbar?
3.10	Firewall und Paketfilter untersuchen	Wo und warum wird Kommunikation zugelassen oder verworfen?
3.11	NAT und Portweiterleitungen	Werden Adressen und Ports korrekt übersetzt?
3.12	Proxy und Reverse Proxy	Scheitert die Verbindung am Proxy, Backend oder Client?
3.13	VPN- und Tunnelprobleme	Sind Tunnel, Routen, DNS und MTU korrekt?
3.14	WLAN-Störungen analysieren	Liegt die Ursache bei Signal, Funkkanal, Authentifizierung oder IP-Konfiguration?
3.15	Paketverlust, Latenz und Jitter	Wo entsteht eine instabile oder langsame Verbindung?
3.16	MTU, MSS und Fragmentierungsprobleme	Sind Pakete für einen Teil des Übertragungsweges zu groß?
3.17	Asymmetrisches Routing	Nehmen Hin- und Rückweg unterschiedliche, problematische Wege?

Seite	Thema	Zentrale Fragestellung
3.18	Netzwerkfehler mit Wireshark erkennen	Welche Paketsequenz belegt die technische Störung?
3.19	Typische Netzwerkfehler nach Symptomen	Welche Prüfungen passen zu einem konkreten Fehlerbild?
3.20	Befehlsübersicht für Windows, Linux und macOS	Welcher Befehl prüft welche Netzwerkebene?
3.21	Dokumentations- und Eskalationsvorlage	Wie wird die Analyse vollständig übergeben?

3. Welche Kennzeichnungen werden verwendet?

Kennzeichnung	Bedeutung
[RO]	Read-only: liest Informationen aus
[TEST]	führt eine aktive Netzwerkprüfung durch
[PRIV]	benötigt möglicherweise Administrator- oder Root-Rechte
[FILE]	erzeugt oder verändert eine Datei
[SENS]	Ausgabe kann vertrauliche Daten enthalten
[CHANGE]	verändert eine Konfiguration oder einen Systemzustand
[DISRUPT]	kann eine bestehende Verbindung oder einen Dienst unterbrechen

Beispiele

```
[RO] Get-NetIPConfiguration
```

Der Befehl zeigt die vorhandene Windows-Netzwerkkonfiguration an.

```
[TEST] ping -c 4 192.0.2.1
```

Der Befehl sendet aktiv ICMP-Echo-Anfragen.

```
[PRIV][CHANGE][DISRUPT] Restart-NetAdapter -Name 'Ethernet'
```

Dieser Befehl startet den Netzwerkadapter neu und unterbricht dabei bestehende Verbindungen. Er darf nicht als erster Diagnoseschritt verwendet werden.

4. Wie wird der Kommunikationsweg dargestellt?

Vor der technischen Analyse sollte der erwartete Kommunikationsweg gezeichnet werden.

Beispiel: Zugriff auf eine interne Anwendung

```
Client
  → Netzwerkschnittstelle
    → Access Switch
      → VLAN
        → Standardgateway
          → Firewall
            → Reverse Proxy
              → Anwendungsserver
                → Datenbankserver
```

Beispiel: Internetzugriff

```
Client
  → Switch oder Access Point
    → lokales Gateway
      → Firewall
        → NAT
          → Internetprovider
            → externes Zielsystem
```

Beispiel: VPN-Zugriff

```
Client
  → lokales Netzwerk
    → Internet
      → VPN-Gateway
        → VPN-Tunnel
          → interne Firewall
```

→ Zielserver

Jede Verbindung besteht aus mehreren möglichen Fehlerstellen. Der Kommunikationsweg verhindert, dass Komponenten untersucht werden, die an der Verbindung überhaupt nicht beteiligt sind.

5. Wie wird eine Netzwerkstörung sinnvoll eingegrenzt?

Die Untersuchung sollte vom Allgemeinen zum Spezifischen erfolgen.

Schritt	Fragestellung
1	Was funktioniert konkret nicht?
2	Seit wann besteht die Störung?
3	Wer oder was ist betroffen?
4	Was funktioniert weiterhin?
5	Welche Änderung ging der Störung voraus?
6	Welcher Kommunikationsweg wird erwartet?
7	Auf welcher Ebene liegt der erste Fehler?
8	Ist die Störung reproduzierbar?
9	Welche Messung belegt die Vermutung?
10	Welche einzelne Änderung kann die Hypothese prüfen?
11	Wurde die ursprüngliche Funktion wiederhergestellt?
12	Wurden Ursache, Änderung und Ergebnis dokumentiert?

Beispiel

Unzureichende Fehlerbeschreibung:
„Das Netzwerk funktioniert nicht.“

Bessere Fehlerbeschreibung:
„CLIENT-023 kann seit 09:42 Uhr den internen Webserver app.example.intern nicht über TCP 443 erreichen. Andere interne Server sind erreichbar. Weitere Clients im selben VLAN sind nicht betroffen.“

Die zweite Beschreibung grenzt die Störung bereits deutlich ein:

- ein Client betroffen,
- ein bestimmtes Ziel betroffen,
- ein bestimmter Dienst betroffen,
- andere Ziele funktionieren,
- der Fehler besitzt einen bekannten Startzeitpunkt.

6. Welche Prüfungsreihenfolge ist in der Praxis sinnvoll?

Reihenfolge	Bereich	Beispielprüfung
1	Fehlerbild und Umfang	ein Benutzer, mehrere Benutzer oder gesamter Standort?
2	lokale Schnittstelle	Adapter aktiv, Link vorhanden, Fehlerzähler?
3	IP-Konfiguration	Adresse, Präfix, Gateway und DNS korrekt?
4	lokale TCP/IP-Funktion	Loopback und eigene Adresse erreichbar?
5	lokales Netz	Gateway und Nachbarn erreichbar?
6	Routing	existiert eine Route zum Ziel?
7	Namensauflösung	wird der richtige Name zur richtigen Adresse aufgelöst?
8	Transportebene	ist der benötigte TCP- oder UDP-Port erreichbar?
9	Sicherheitskomponenten	blockieren Host-Firewall, Netzwerk-Firewall oder ACL?
10	Anwendungsebene	antwortet der eigentliche Dienst korrekt?
11	Performance	treten Latenz, Paketverlust oder Wiederholungen auf?
12	Paketmitschnitt	welche Paketsequenz belegt den Fehler?

Diese Reihenfolge darf an das konkrete Fehlerbild angepasst werden. Wenn beispielsweise bereits eine falsche IP-Adresse sichtbar ist, muss nicht zuerst ein entfernter Anwendungsserver untersucht werden.

7. Wie helfen OSI- und TCP/IP-Modell bei der Fehleranalyse?

OSI-Schicht	Typische Komponenten	Typische Fehler

1 – Bitübertragung	Kabel, Funk, Stecker, Transceiver	kein Link, Signalstörung, beschädigtes Kabel
2 – Sicherung	Ethernet, MAC, Switch, VLAN	falsches VLAN, Portfehler, Layer-2-Schleife
3 – Vermittlung	IPv4, IPv6, Router	falsches Subnetz, fehlende Route, falsches Gateway
4 – Transport	TCP, UDP	Port geschlossen, Verbindungsabbruch, Paketverlust
5 – Sitzung	Sitzungssteuerung	Sitzung läuft ab oder wird nicht aufgebaut
6 – Darstellung	TLS, Kodierung	Zertifikat, Verschlüsselung oder Format inkompatibel
7 – Anwendung	DNS, HTTP, SMB, SSH	Dienstfehler, Authentifizierung oder falsche Konfiguration

Wichtiger Hinweis

Das OSI-Modell ist ein Denk- und Strukturierungsmodell. Reale Protokolle und Anwendungen lassen sich nicht immer vollständig einer einzigen Schicht zuordnen.

Praktische Reihenfolge

```
Link vorhanden?
  ↓
gültige IP-Konfiguration?
  ↓
lokales Gateway erreichbar?
  ↓
Route zum Ziel vorhanden?
  ↓
Name korrekt aufgelöst?
  ↓
Port erreichbar?
  ↓
Anwendungsprotokoll funktioniert?
```

8. Was bedeutet Bottom-up, Top-down und Divide-and-Conquer?

Bottom-up

Die Untersuchung beginnt auf der untersten Ebene:

```
Kabel → Link → VLAN → IP → Route → Port → Anwendung
```

Geeignet bei:

- vollständig fehlender Verbindung,
- unbekannter Fehlerstelle,
- neu aufgebauter Infrastruktur,
- physischen oder lokalen Auffälligkeiten.

Top-down

Die Untersuchung beginnt bei der Anwendung:

```
Anwendung → Port → DNS → Route → IP → Link
```

Geeignet bei:

- klarer Anwendungsfehlermeldung,
- nur einem betroffenen Dienst,
- ansonsten funktionierendem Netzwerk,
- bekanntem HTTP-, TLS- oder Authentifizierungsfehler.

Divide-and-Conquer

Die Untersuchung beginnt an einer sinnvollen mittleren Stelle:

```
Kann der Client das Standardgateway erreichen?
```

- Wenn nein: Fehler wahrscheinlich lokal oder im lokalen Netz.
- Wenn ja: Untersuchung in Richtung Routing, Firewall und Zielsystem fortsetzen.

Diese Methode ist oft besonders effizient, wenn der Kommunikationsweg bekannt ist.

9. Welche Vergleichstests liefern besonders schnell Hinweise?

Vergleich	Aussage
gleicher Client, anderes Ziel	Ist nur ein Ziel betroffen?
anderer Client, gleiches Ziel	Ist nur ein Client betroffen?

Vergleich	Aussage
gleiche Verbindung per IP statt Name	Liegt ein DNS-Problem nahe?
gleicher Dienst über anderen Port	Ist nur ein Port oder Protokoll betroffen?
LAN statt WLAN	Liegt die Ursache möglicherweise im Funknetz?
ohne VPN statt mit VPN	Entsteht das Problem durch Tunnel, Routen oder VPN-DNS?
funktionierendes Referenzsystem	Welche Konfiguration unterscheidet sich?
lokaler Zugriff statt entfernter Zugriff	Funktioniert der Dienst grundsätzlich?
anderer Benutzer am selben Client	Ist das Problem benutzerabhängig?
gleicher Benutzer an anderem Client	Ist das Problem geräteabhängig?

Ein Vergleich ist besonders aussagekräftig, wenn dabei nur ein relevanter Faktor verändert wird.

10. Welche ersten Prüfungen sind betriebssystemübergreifend möglich?

Aufgabe	Windows	Linux	macOS
Hostname	`[RO] hostname`	`[RO] hostname`	`[RO] hostname`
lokale Zeit	`[RO] Get-Date -Format o`	`[RO] date --iso-8601=seconds`	`[RO] date "+%Y-%m-%dT%H:%M:%S%z"`
Adapterübersicht	`[RO] Get-NetAdapter`	`[RO] ip -brief link`	`[RO] ifconfig`
IP-Konfiguration	`[RO] Get-NetIPConfiguration`	`[RO] ip -brief address`	`[RO] ifconfig`
Routingtabelle	`[RO] Get-NetRoute`	`[RO] ip route`	`[RO] netstat -rn`
ARP-/Nachbartabelle	`[RO] Get-NetNeighbor`	`[RO] ip neigh`	`[RO] arp -an`
DNS-Konfiguration	`[RO] Get-DnsClientServerAddress`	`[RO] resolvectl status`	`[RO] scutil --dns`
Name auflösen	`[TEST] Resolve-DnsName example.com`	`[TEST] getent hosts example.com`	`[TEST] dscacheutil -q host -a name example.com`
Gateway testen	`[TEST] Test-Connection GATEWAY -Count 4`	`[TEST] ping -c 4 GATEWAY`	`[TEST] ping -c 4 GATEWAY`
Route verfolgen	`[TEST] tracert ZIEL`	`[TEST] traceroute ZIEL`	`[TEST] traceroute ZIEL`
TCP-Port prüfen	`[TEST] Test-NetConnection ZIEL -Port 443`	`[TEST] nc -vz ZIEL 443`	`[TEST] nc -vz ZIEL 443`
HTTP(S) prüfen	`[TEST] curl -v https://ZIEL/`	`[TEST] curl -v https://ZIEL/`	`[TEST] curl -v https://ZIEL/`
Verbindungen anzeigen	`[RO] Get-NetTCPConnection`	`[RO] ss -tulpen`	`[RO] netstat -anv`

Die Platzhalter `GATEWAY` und `ZIEL` müssen durch vorher eindeutig bestimmte Adressen oder Namen ersetzt werden.

11. Wie werden Testergebnisse richtig bewertet?

Ergebnis	Sichere Aussage	Nicht automatisch bewiesen
Link ist aktiv	physische beziehungsweise logische Linkerkennung besteht	vollständige Netzwerkfunktion
Ping erfolgreich	ICMP-Antwort kam zurück	Anwendungsport funktioniert
Ping fehlgeschlagen	keine ICMP-Antwort erhalten	Zielsystem ist ausgeschaltet
DNS-Auflösung erfolgreich	Name wurde in eine Adresse aufgelöst	Zieladresse ist erreichbar
TCP-Port erreichbar	TCP-Verbindung konnte aufgebaut werden	Anwendung arbeitet fachlich korrekt
HTTP 401	Webdienst antwortet und fordert Authentifizierung	Zugangsdaten sind falsch
HTTP 403	Anfrage wurde verstanden und verweigert	Netzwerk-Firewall blockiert
HTTP 502	Proxy erhielt keine gültige Backendantwort	Proxy selbst ist zwingend defekt
Traceroute endet vor dem Ziel	weitere Antworten fehlen	Fehler liegt sicher am letzten sichtbaren Hop
Keine Pakete im Mitschnitt	am Messpunkt wurde nichts erfasst	Client hat nichts gesendet

Jeder Test beantwortet nur eine begrenzte technische Frage. Die Aussage darf nicht weiter ausgedehnt werden, als das Testergebnis tatsächlich belegt.

12. Welche Störungsumfänge werden unterschieden?

Umfang	Mögliche Untersuchungsrichtung
ein Benutzer	Benutzerprofil, Berechtigung oder individuelle Konfiguration
ein Endgerät	Adapter, Treiber, IP-Konfiguration oder lokale Firewall
ein Switchport	Kabel, Port, VLAN oder Port-Security
ein VLAN	Gateway, DHCP, ACL oder VLAN-Konfiguration
ein Standort	WAN, Standortfirewall, DNS oder Internetanschluss
ein Dienst	Serverprozess, Port, Firewall oder Backend

Umfang	Mögliche Untersuchungsrichtung
mehrere Dienste auf einem Server	Server, Betriebssystem oder gemeinsame Ressource
alle internen Ziele	lokales Routing, Gateway oder Firewall
nur externe Ziele	NAT, Proxy, Internetzugang oder Provider
alle Systeme	zentrale Infrastruktur, Stromversorgung oder großflächige Störung

Hilfreiche Eingrenzungsfragen

Funktioniert derselbe Zugriff von einem anderen Client?

Kann der betroffene Client ein anderes Ziel erreichen?

Funktioniert der Zugriff über die IP-Adresse?

Ist nur ein Port oder sind alle Dienste des Zielsystems betroffen?

Tritt der Fehler per LAN und WLAN auf?

Tritt der Fehler nur bei aktivem VPN auf?

13. Welche Änderungen sind besonders häufig mit Netzwerkstörungen verbunden?

- Änderung einer IP-Adresse oder eines Subnetzes,
- neuer DHCP-Bereich,
- geänderte DNS-Server,
- neue Firewall- oder ACL-Regel,
- VLAN-Änderung am Switchport,
- Firmware- oder Treiberupdate,
- neues Zertifikat,
- Proxyänderung,
- VPN-Client-Update,
- Änderung an NAT oder Portweiterleitung,
- Routingänderung,
- Wechsel des Internetproviders,

- neue Sicherheitssoftware,
- Änderung an Load Balancer oder Reverse Proxy,
- Server- oder Containerupdate,
- Änderung von MTU oder Tunnelkonfiguration,
- Ablauf eines Zertifikats oder Kennworts,
- Wartungsarbeiten am Switch, Router oder Access Point.

Die zeitliche Nähe einer Änderung ist ein wichtiger Hinweis, aber noch kein Beweis für die Ursache.

14. Welche Maßnahmen sollten nicht vorschnell durchgeführt werden?

Maßnahme	Risiko
Netzwerkadapter neu starten	bestehende Verbindungen werden unterbrochen
DHCP-Lease freigeben	Remotezugriff kann verloren gehen
IP-Adresse ändern	Adresskonflikt oder vollständiger Verbindungsverlust
Routingtabelle verändern	falsche oder asymmetrische Wege
DNS-Cache löschen	Beweise und Vergleichszustand verändern sich
Firewall deaktivieren	erhebliche Sicherheitslücke
Switchport neu konfigurieren	mehrere Systeme können betroffen sein
VLAN ändern	Endgerät verliert möglicherweise jede Erreichbarkeit
Router oder Firewall neu starten	großflächiger Ausfall
VPN neu installieren	Konfiguration und Protokolle können verloren gehen
Zertifikatsprüfung abschalten	Sicherheitsmechanismus wird umgangen
MTU blind reduzieren	Symptom wird möglicherweise nur verdeckt
Paketfilterregeln löschen	Sicherheits- und Betriebsrisiko

Vor einer Änderung sollten der Ausgangszustand, die Hypothese, die erwartete Wirkung und der Rückweg dokumentiert werden.

15. Wie wird eine Netzwerkhypothese korrekt formuliert?

Ungeeignete Vermutung

> „Bestimmt ist die Firewall schuld.“

Prüfbare Hypothese

Der Client erreicht das Zielsystem auf ICMP-Ebene, aber der TCP-Verbindungsaufbau zu Port 443 erhält keine Antwort. Andere Clients im selben VLAN können den Port erreichen. Deshalb wird eine clientbezogene Filterung oder ein Rückwegproblem vermutet.

Dazugehörige Prüfungen

1. Quell-IP des betroffenen Clients bestätigen.
2. TCP-Porttest mit Zeitstempel durchführen.
3. Host-Firewall und Sicherheitssoftware prüfen.
4. Firewall-Logs nach Quell- und Zieladresse durchsuchen.
5. Paketmitschnitt am Client und gegebenenfalls am Ziel vergleichen.
6. Funktionierenden Referenzclient gegenüberstellen.

Eine Hypothese muss durch Beobachtungen begründet und durch einen konkreten Test widerlegbar sein.

16. Welche Mindestinformationen gehören in ein Netzwerkticket?

Ticketnummer:
Meldende Person:
Betroffener Benutzer:
Betroffenes Endgerät:
Standort:
Verbindungsart: LAN / WLAN / VPN / Mobilfunk
Fehlerbeginn:
Zeitzone:
Letzter funktionierender Zeitpunkt:
Fehler reproduzierbar: Ja / Nein
Exakte Fehlermeldung:

Quellhostname:
Quell-IP:
Quell-MAC:
Quell-VLAN:
Quellgateway:

Verwendete DNS-Server:

Zielhostname:
Ziel-IP:
Zielport:
Transportprotokoll:
Anwendungsprotokoll:

Betroffene Benutzer oder Geräte:
Funktionierende Vergleichssysteme:
Weiterhin funktionierende Verbindungen:
Kürzliche Änderungen:

Erwarteter Kommunikationsweg:
1.
2.
3.
4.

Bisherige Prüfungen:
-
-
-

Bisherige Änderungen:
-
-
-

Arbeitshypothese:
Nächster Prüfschritt:
Rückweg bei Änderung:

17. Wann muss eine Netzwerkstörung eskaliert werden?

Eine Eskalation ist sinnvoll oder erforderlich, wenn:

- mehrere Benutzer oder Standorte betroffen sind,

- ein geschäftskritischer Dienst ausgefallen ist,
- ein Sicherheitsvorfall vermutet wird,
- unautorisierte Netzwerkänderungen erkennbar sind,
- Administratorrechte oder Zuständigkeiten fehlen,
- eine Änderung an produktiver Kerninfrastruktur erforderlich wird,
- Provider- oder Herstellerunterstützung benötigt wird,
- redundante Systeme ebenfalls ausfallen,
- die vereinbarte Bearbeitungszeit überschritten wird,
- Paketmitschnitte sensible Daten enthalten,
- Datenverlust oder Manipulation möglich ist.

Eine gute Eskalation enthält:

- klare Fehlerbeschreibung,
- Auswirkung und Priorität,
- betroffene Systeme,
- Beginn und Zeitzone,
- erwarteten Kommunikationsweg,
- bereits durchgeführte Prüfungen,
- Messergebnisse und Logauszüge,
- ausgeschlossene Ursachen,
- aktuelle Hypothese,
- konkrete Frage an die nächste Stelle,
- sichere Kontakt- und Übergabemöglichkeit.

18. Merkschema für die erste Eingrenzung

1. Wer ist betroffen?
2. Was genau funktioniert nicht?
3. Was funktioniert weiterhin?
4. Seit wann besteht der Fehler?
5. Was wurde vorher geändert?
6. Welcher Kommunikationsweg wird erwartet?
7. Besteht ein Link?
8. Ist die IP-Konfiguration gültig?
9. Ist das Gateway erreichbar?
10. Existiert eine Route?
11. Funktioniert die Namensauflösung?
12. Ist der Zielport erreichbar?
13. Antwortet die Anwendung?

14. Wo befindet sich der erste belegte Fehler?
15. Welche Messung bestätigt die Ursache?

Kurzform

```
Umfang → Link → IP → Gateway → Route → DNS → Port → Anwendung
```

19. Offizielle Quellen und weiterführende Dokumentation

Microsoft

- Grundlagen von TCP/IP
- Get-NetAdapter
- Get-NetIPConfiguration
- Get-NetRoute
- Get-NetNeighbor
- Test-NetConnection
- Resolve-DnsName

Linux

- ip-address – Linux Manual Page
- ip-link – Linux Manual Page
- ip-route – Linux Manual Page
- ip-neighbour – Linux Manual Page
- ss – Linux Manual Page

Apple

- Lokale Befehlsreferenzen: `man ifconfig`, `man route`, `man netstat`, `man arp`, `man ping` und `man traceroute`
- Apple Platform Deployment – Network Services

Wireshark und tcpdump

- Wireshark User’s Guide
- Wireshark Display Filter Reference

- tcpdump Manual Page
- pcap-filter Manual Page

> Die genaue Befehlssyntax und die verfügbaren Optionen können von Betriebssystem- und Werkzeugversion abhängen. Vor Änderungen an produktiven Systemen muss zusätzlich die lokale Dokumentation geprüft werden.
