5.6 Netzwerkgeräte – Werkzeuge zur Fehleranalyse

Netzwerkgeräte wie Switches, Router, Firewalls, WLAN-Access-Points, Controller, Load Balancer und VPN-Gateways verfügen meist über eigene Diagnosefunktionen. Dazu gehören:

- Kommandozeilenbefehle,
- Weboberflächen,
- Ereignisprotokolle,
- Schnittstellenstatistiken,
- Routing- und Switchingtabellen,
- Paketmitschnitte,
- SNMP-Messwerte,
- Telemetriedaten,
- zentrale Netzwerkmanagementsysteme,
- herstellerspezifische Supportdateien.

> Die genaue Syntax hängt von Hersteller, Produktfamilie, Betriebssystem und Softwareversion ab. Ein Befehl darf deshalb nicht ungeprüft auf ein anderes Gerät übertragen werden.

---

1. Grundregeln für die Untersuchung

Vor jedem Zugriff müssen geklärt werden:

- betroffenes Gerät,
- Hersteller und Modell,
- Betriebssystem und Version,
- Rolle des Geräts,
- Managementadresse,
- vorgesehener Zugriffsweg,
- benötigte Berechtigungen,
- Wartungs- und Änderungsvorgaben,
- vorhandene Redundanz,
- Auswirkungen eines möglichen Ausfalls.

Zuerst nur lesend untersuchen

Geeignet sind zunächst:

- Statusbefehle,

- Protokollabfragen,
- Zählerstände,
- Routingtabellen,
- Nachbartabellen,
- Konfigurationsansichten,
- Paketmitschnitte mit begrenztem Umfang.

Zu vermeiden sind ohne bestätigte Ursache und Freigabe:

- Neustarts,
- Zurücksetzen von Schnittstellen,
- Löschen von Tabellen,
- Leeren von Sitzungen,
- Änderungen an VLANs oder Routen,
- Deaktivieren von Sicherheitsregeln,
- Zurücksetzen von Zählern,
- Firmwareupdates,
- Werkseinstellungen,
- dauerhafte Debug-Ausgaben.

> Eine reine Statusabfrage ist nicht auf jedem Gerät vollständig risikofrei. Umfangreiche Support- oder Diagnosebefehle können CPU, Arbeitsspeicher, Konsole oder Managementverbindung belasten.

---

2. Systematisch von unten nach oben prüfen

Ebene	typische Fragestellung
Stromversorgung	Ist das Gerät eingeschaltet und ausreichend versorgt?
Hardware	Sind Module, Netzteile, Lüfter und Temperatursensoren fehlerfrei?
physische Verbindung	Besteht Link? Stimmen Medium, Kabel, Transceiver und Geschwindigkeit?
Sicherungsschicht	Stimmen VLAN, Trunk, STP, LACP und MAC-Lernen?
Netzwerkschicht	Stimmen IP-Adresse, Präfix, ARP/ND und Routing?
Transport	Ist der benötigte TCP- oder UDP-Port erreichbar?
Sicherheit	Blockieren ACL, Firewall, NAC oder VPN-Richtlinien?
Anwendung	Funktionieren DNS, DHCP, RADIUS, NTP oder andere Dienste?
Management	Erreichen Monitoring, Syslog, SNMP und zentrale Verwaltung das Gerät?

Ein Fehler sollte möglichst auf die kleinste betroffene Ebene eingegrenzt werden.

---

3. Zustand vor Veränderungen sichern

Vor einer Änderung sollten mindestens dokumentiert werden:

- Datum und Uhrzeit,
- Gerätename,
- Seriennummer,
- Modell,
- Softwareversion,
- Laufzeit seit dem letzten Neustart,
- aktuelle Konfiguration,
- gespeicherte Konfiguration,
- Schnittstellenstatus,
- Routingtabelle,
- Nachbartabellen,
- Protokolle,
- CPU- und Speicherauslastung,
- Redundanzstatus,
- betroffene Benutzer oder Standorte,
- zuletzt vorgenommene Änderungen.

Typische Beweissicherung

```
Gerät:
Standort:
Hersteller und Modell:
Betriebssystem und Version:
Managementadresse:
Zeitpunkt:
Symptom:
betroffene Schnittstelle:
betroffenes VLAN beziehungsweise VRF:
Quelladresse:
Zieladresse:
Zielport und Protokoll:
letzte Änderung:
gesicherte Ausgaben:
durchgeführte Tests:
Ergebnis:
```

---

4. Managementzugriff prüfen

Typische Zugriffswege sind:

- lokale Konsole,
- serielle Konsole,
- dedizierter Managementport,
- SSH,
- HTTPS,
- Out-of-Band-Management,
- zentrale Managementplattform,
- API,
- NETCONF oder RESTCONF.

Sicherheitsregeln

- Telnet nur verwenden, wenn es in einer isolierten Altumgebung ausdrücklich vorgeschrieben ist.
- SSH und HTTPS bevorzugen.
- Administrationszugriffe protokollieren.
- Nur persönliche oder nachvollziehbar zugeordnete Konten verwenden.
- Keine Kennwörter in Tickets, Protokollen oder Bildschirmfotos veröffentlichen.
- Managementzugriff möglichst über ein getrenntes Managementnetz führen.
- Änderungen nach dem Vier-Augen- oder Freigabeverfahren des Unternehmens durchführen.

Bei fehlendem Zugriff unterscheiden

Beobachtung	mögliche Ursache
Gerät antwortet nicht auf Ping	ICMP gefiltert, falsche Route, Gerät ausgefallen oder Managementadresse falsch
Ping funktioniert, SSH nicht	Dienst deaktiviert, ACL, falscher Port, Überlastung oder Authentifizierungsproblem
SSH-Verbindung startet, Anmeldung schlägt fehl	lokales Konto, RADIUS, TACACS+, Zertifikat oder Berechtigung
Zugriff nur über Konsole möglich	Managementnetz, Routing, VRF, ACL oder Managementdienst
zentrale Verwaltung zeigt Gerät offline	Managementpfad, Zertifikat, Zeit, DNS, Tunnel oder Controllerverbindung
Zugriff funktioniert nur von einem Netz	Routing, Firewall, Management-ACL oder VRF

---

5. Geräteidentität und Softwarestand

Zu erfassen sind:

- Gerätename,
- Modell,
- Seriennummer,
- Hardwaremodule,
- Betriebssystem,
- Softwareversion,
- Bootimage,
- Lizenzstatus,
- Laufzeit,
- Grund des letzten Neustarts,
- unterstützte und eingesetzte Transceiver.

Cisco IOS beziehungsweise IOS XE

```
show version
```

```
show inventory
```

```
show license summary
```

Juniper Junos

```
show version
```

```
show chassis hardware
```

```
show system uptime
```

Aruba AOS-CX

```
show version
```

```
show system
```

```
show inventory
```

Die verfügbaren Befehle können je nach Plattform und Version abweichen.

---

6. CPU, Arbeitsspeicher und Systemzustand

Hohe Auslastung kann dazu führen, dass:

- Routingprotokolle Nachbarschaften verlieren,
- Managementzugriffe verzögert werden,
- Pakete verworfen werden,
- Protokolle unvollständig erscheinen,
- Kontrollprozesse neu starten,
- Überwachungsabfragen fehlschlagen.

Cisco IOS beziehungsweise IOS XE

```
show processes cpu
```

```
show processes memory
```

```
show platform resources
```

Juniper Junos

```
show chassis routing-engine
```

```
show system processes extensive
```

```
show system memory
```

Aruba AOS-CX

```
show system resource-utilization
```

```
top cpu
```

```
top memory
```

Bei Auffälligkeiten prüfen

- Ist die Auslastung dauerhaft oder nur kurzfristig erhöht?
- Welcher Prozess ist betroffen?
- Begann die Auslastung nach einer Änderung?
- Bestehen ungewöhnlich viele Verbindungen oder Routingupdates?
- Läuft eine umfangreiche Protokollierung oder Diagnose?
- Findet ein Angriff oder Netzwerkscan statt?
- Besteht ein Layer-2-Loop?
- Sind Tabellen oder Sitzungsspeicher ausgelastet?
- Werden Pakete in Software statt in Hardware verarbeitet?

> Ein Prozess mit hoher CPU-Auslastung ist nicht automatisch die Ursache. Er kann auf einen Broadcast-Sturm, eine Routinginstabilität oder eine andere Störung reagieren.

---

7. Hardware, Temperatur und Stromversorgung

Zu prüfen sind:

- Netzteile,
- Lüfter,
- Temperatur,
- Spannungswerte,
- Module,
- Linecards,
- Stack-Mitglieder,
- Chassiszustand,
- PoE-Budget,
- Hardwarefehler,
- Redundanz.

Cisco IOS beziehungsweise IOS XE

```
show environment
```

```
show platform
```

```
show power
```

```
show power inline
```

Nicht jeder Befehl ist auf jeder Cisco-Plattform vorhanden.

Juniper Junos

```
show chassis environment
```

```
show chassis alarms
```

```
show system alarms
```

```
show poe controller
```

Aruba AOS-CX

```
show environment
```

```
show system power-supply
```

```
show system fans
```

```
show poe brief
```

Typische Warnsignale

- fehlendes Netzteil,
- ausgefallener Lüfter,
- erhöhte Temperatur,
- überlastetes PoE-Budget,
- nicht erkanntes Modul,
- Hardwarealarm,
- wiederholter Modulneustart,

- unterschiedliche Firmwarestände innerhalb eines Stacks.

---

8. Schnittstellenstatus untersuchen

Für jede betroffene Schnittstelle sind mindestens zu prüfen:

- administrativer Zustand,
- operativer Zustand,
- Geschwindigkeit,
- Duplexmodus,
- MTU,
- Medium,
- VLAN-Zuordnung,
- Beschreibung,
- Ein- und Ausgangsrate,
- Fehlerzähler,
- Drops,
- Linkwechsel,
- Transceiverwerte.

Cisco IOS beziehungsweise IOS XE

Übersicht:

```
show interfaces status
```

IP-bezogene Übersicht:

```
show ip interface brief
```

Details einer Schnittstelle:

```
show interfaces GigabitEthernet1/0/1
```

Beschreibungen:

```
show interfaces description
```

Fehlerübersicht auf unterstützten Switches:

```
show interfaces counters errors
```

Juniper Junos

Übersicht:

```
show interfaces terse
```

Details:

```
show interfaces ge-0/0/1 extensive
```

Beschreibung und Status:

```
show interfaces descriptions
```

Aruba AOS-CX

```
show interface brief
```

```
show interface 1/1/1
```

```
show interface 1/1/1 statistics
```

Status fachlich einordnen

Zustand	mögliche Bedeutung
administrativ deaktiviert	Schnittstelle wurde durch Konfiguration abgeschaltet
physisch down	kein Link, Kabel-, Transceiver-, Gegenstellen- oder Stromproblem
physisch up, Protokoll down	Problem oberhalb der reinen Signalerkennung
häufige Linkwechsel	Kabel, Stecker, Transceiver, Stromversorgung oder Autonegotiation
viele Eingangsfehler	Medium, Signal, Überlastung oder fehlerhafte Hardware
viele Ausgangsdrops	Ausgangswarteschlange überlastet oder Zielverbindung langsamer

Zustand	mögliche Bedeutung
Zähler steigen nicht	möglicherweise falsche Schnittstelle oder kein Verkehr
Link up	bestätigt nur die Verbindung auf der entsprechenden Ebene

---

9. Fehlerzähler bewerten

Typische Zähler sind:

- CRC-Fehler,
- Framefehler,
- Alignment Errors,
- Runts,
- Giants,
- Input Errors,
- Output Errors,
- Discards,
- Queue Drops,
- Collisions,
- Late Collisions,
- Overruns,
- Carrier Transitions,
- Pause Frames.

Mögliche Einordnung

Zähler	mögliche Ursache
CRC-Fehler	Kabel, Steckverbindung, Transceiver, elektromagnetische Störung oder Gegenstelle
Late Collisions	Duplexproblem oder ungeeignete gemeinsame Medienumgebung
Input Drops	Eingangspuffer oder Verarbeitung überlastet
Output Drops	Ausgangsschnittstelle oder Warteschlange überlastet
Giants	zu große Frames, MTU-Abweichung oder fehlerhafte Frames
Runts	beschädigte oder zu kurze Ethernetframes
viele Linkwechsel	instabile physische Verbindung oder Energieversorgung

Für eine korrekte Bewertung

1. aktuellen Zählerstand dokumentieren,
2. Laufzeit des Geräts berücksichtigen,

3. Datenverkehr beobachten,
4. Veränderung des Zählers messen,
5. Gegenstelle prüfen,
6. Kabel beziehungsweise Transceiver kontrolliert gegenprüfen,
7. Fehler nicht allein anhand eines historischen Gesamtwerts bewerten.

> Ein hoher Zählerstand kann über Monate entstanden sein. Entscheidend ist häufig, ob der Wert während des aktuellen Fehlers weiter steigt.

---

10. Geschwindigkeit, Duplex und Autonegotiation

Typische Probleme entstehen durch:

- eine Seite automatisch und die andere fest konfiguriert,
- unterschiedliche feste Geschwindigkeiten,
- ungeeignete Transceiver,
- nicht unterstützte Kabel,
- Energiesparfunktionen,
- fehlerhafte Autonegotiation,
- unterschiedliche FEC-Einstellungen bei schnellen Verbindungen.

Zu vergleichen sind immer beide Seiten der Verbindung.

Prüffragen

- Welche Geschwindigkeit wurde tatsächlich ausgehandelt?
- Welcher Duplexmodus ist aktiv?
- Ist Autonegotiation auf beiden Seiten gleich behandelt?
- Werden Fehlerzähler größer?
- Passt der Transceiver zum Port und zur Gegenstelle?
- Stimmen Wellenlänge, Fasertyp und Reichweite?
- Ist bei höheren Geschwindigkeiten die benötigte Forward Error Correction aktiv?

---

11. Transceiver und Glasfaserdiagnose

Diagnoseinformationen können enthalten:

- Hersteller,
- Teilenummer,
- Seriennummer,
- Wellenlänge,
- Temperatur,
- Spannung,

- Sendeleistung,
- Empfangsleistung,
- Alarmgrenzen.

Cisco – abhängig von Plattform und Software

```
show interfaces transceiver detail
```

Juniper Junos

```
show interfaces diagnostics optics
```

Bestimmte Schnittstelle:

```
show interfaces diagnostics optics ge-0/0/1
```

Aruba AOS-CX

```
show interface transceiver
```

Die genaue Syntax muss in der Dokumentation der verwendeten Plattform geprüft werden.

Wichtige Einordnung

- Zu geringe Empfangsleistung kann auf Dämpfung, Verschmutzung, falsche Faser oder defekte Komponenten hinweisen.
- Zu hohe Empfangsleistung kann einen Empfänger ebenfalls außerhalb des zulässigen Bereichs betreiben.
- Ein angezeigter optischer Wert muss mit den Grenzwerten des konkreten Transceivers verglichen werden.
- Ein Link kann trotz ungünstiger Werte zunächst funktionieren und später instabil werden.
- Glasfaserstecker dürfen nur mit geeigneten Werkzeugen gereinigt und untersucht werden.

---

12. VLAN-Zuordnung prüfen

Typische Ursachen sind:

- falsches Access-VLAN,
- fehlendes VLAN,
- VLAN nicht auf dem Trunk erlaubt,
- unterschiedliche native VLANs,

- falsche Voice-VLAN-Konfiguration,
- VLAN auf einem Zwischen-Switch nicht vorhanden,
- falsche Portrolle.

Cisco IOS beziehungsweise IOS XE

```
show vlan brief
```

```
show interfaces trunk
```

```
show interfaces GigabitEthernet1/0/1 switchport
```

Juniper Junos – abhängig vom Switching-Modell

```
show vlans
```

```
show ethernet-switching interfaces
```

Aruba AOS-CX

```
show vlan
```

```
show vlan port 1/1/1
```

```
show interface 1/1/1
```

Prüfreihenfolge

1. Endgeräteport identifizieren.
2. Portmodus bestimmen.
3. Access- oder untagged VLAN prüfen.
4. Trunk beziehungsweise tagged VLANs prüfen.
5. Zwischenverbindungen untersuchen.
6. VLAN auf jedem beteiligten Gerät prüfen.
7. Layer-3-Gateway des VLANs kontrollieren.
8. DHCP, ARP und Sicherheitsrichtlinien prüfen.

---

13. MAC-Adresstabelle untersuchen

Die MAC-Adresstabelle zeigt, an welcher Schnittstelle ein Switch eine MAC-Adresse gelernt hat.

Cisco IOS beziehungsweise IOS XE

```
show mac address-table
```

Bestimmte Adresse:

```
show mac address-table address aaaa.bbbb.cccc
```

Bestimmte Schnittstelle:

```
show mac address-table interface GigabitEthernet1/0/1
```

Juniper Junos

```
show ethernet-switching table
```

Aruba AOS-CX

```
show mac-address-table
```

Mögliche Beobachtungen

Beobachtung	Einordnung
MAC-Adresse fehlt	kein Verkehr, falsches VLAN, Port down oder Gerät nicht verbunden
MAC-Adresse am erwarteten Port	Layer-2-Lernen funktioniert zumindest in dieser Richtung
MAC-Adresse an unerwartetem Port	Verkabelung, Schleife, virtuelle Umgebung oder Topologie prüfen
MAC-Adresse wechselt zwischen Ports	Schleife, redundante Fehlkonfiguration oder tatsächlich bewegtes Gerät
sehr viele MAC-Adressen an einem Endgeräteport	unerwarteter Switch, Hypervisor, Access Point oder Sicherheitsproblem
Tabelle nahezu ausgelastet	ungewöhnlich viele Geräte, Angriff oder Dimensionierungsproblem

> Eine gelernte MAC-Adresse bestätigt nicht, dass IP-Konfiguration, Routing, DNS oder die Anwendung funktionieren.

---

14. Spanning Tree untersuchen

Spanning Tree verhindert Layer-2-Schleifen in redundanten Ethernetnetzen.

Zu prüfen sind:

- Root Bridge,
- Root Port,
- Portrollen,
- Portzustände,
- Topology Changes,
- blockierte beziehungsweise verworfene Ports,
- verwendete STP-Variante,
- unerwartete Root-Wahl,
- Schutzmechanismen.

Cisco IOS beziehungsweise IOS XE

```
show spanning-tree
```

Bestimmtes VLAN:

```
show spanning-tree vlan 10
```

Details:

```
show spanning-tree detail
```

Juniper Junos

```
show spanning-tree bridge
```

```
show spanning-tree interface
```

Aruba AOS-CX

```
show spanning-tree
```

```
show spanning-tree detail
```

Hinweise auf eine Layer-2-Schleife

- sehr hohe Broadcast- oder Multicastlast,
- stark erhöhte CPU-Auslastung,
- MAC-Adressen wechseln zwischen Ports,
- Managementzugriff ist instabil,
- viele Topology Changes,
- Paketverlust im gesamten VLAN,
- mehrere Ports zeigen außergewöhnlich hohe Datenraten.

> Ein durch STP blockierter Port ist nicht automatisch fehlerhaft. Das Blockieren kann die beabsichtigte schleifenfreie Topologie herstellen.

---

15. Link Aggregation und LACP

Bei gebündelten Verbindungen müssen geprüft werden:

- Mitgliedsschnittstellen,
- physischer Linkstatus,
- LACP-Zustand,
- aktive und passive Seite,
- Aggregationskennung,
- Geschwindigkeit,
- VLAN-Konfiguration,
- Hashverfahren,
- Mindestanzahl benötigter Mitglieder,
- Konfiguration der Gegenstelle.

Cisco IOS beziehungsweise IOS XE

```
show etherchannel summary
```

```
show lacp neighbor
```

```
show interfaces port-channel 1
```

Juniper Junos

```
show interfaces ae0 extensive
```

```
show lacp interfaces
```

Aruba AOS-CX

```
show lacp interfaces
```

```
show interface lag 1
```

Typische Fehler

- Port ist nicht im Bündel aktiv,
- unterschiedliche LACP-Modi,
- ungleiche Geschwindigkeiten,
- verschiedene VLAN-Listen,
- Verbindung zu unterschiedlichen logischen Gegenstellen ohne passende Multi-Chassis-Technik,
- fehlerhaftes Mitglied beeinträchtigt einen Teil des Datenverkehrs,
- Hashverteilung belastet einzelne Mitglieder stärker.

---

16. LLDP und CDP zur Topologieprüfung

Nachbarerkennungsprotokolle helfen dabei, die tatsächlich angeschlossene Gegenstelle zu bestimmen.

Cisco Discovery Protocol

```
show cdp neighbors
```

Details:

```
show cdp neighbors detail
```

Link Layer Discovery Protocol auf Cisco

```
show lldp neighbors
```

```
show lldp neighbors detail
```

Juniper Junos

```
show lldp neighbors
```

```
show lldp neighbors detail
```

Aruba AOS-CX

```
show lldp neighbor-info
```

Zu beachten

- CDP ist proprietär und nicht auf allen Herstellern verfügbar.
- LLDP ist herstellerübergreifend, kann aber deaktiviert sein.
- Fehlende Nachbarinformationen beweisen nicht, dass keine physische Verbindung besteht.
- Nachbardaten können Gerätenamen, Managementadressen und Topologieinformationen enthalten und müssen geschützt werden.

---

17. ARP und IPv6 Neighbor Discovery

ARP ordnet IPv4-Adressen MAC-Adressen zu. IPv6 verwendet Neighbor Discovery.

Cisco IOS beziehungsweise IOS XE

```
show ip arp
```

```
show ipv6 neighbors
```

Juniper Junos

```
show arp
```

```
show ipv6 neighbors
```

Aruba AOS-CX

```
show arp
```

```
show ipv6 neighbors
```

Typische Beobachtungen

Beobachtung	mögliche Ursache
kein Eintrag	Ziel nicht lokal, keine Antwort, falsches VLAN oder falsches Präfix
Eintrag unvollständig	ARP- beziehungsweise Neighbor-Anfrage bleibt unbeantwortet
wechselnde MAC-Adresse	doppelte IP-Adresse, Cluster, Proxy ARP oder Fehlkonfiguration
MAC-Adresse stimmt nicht mit erwartetem Gerät überein	doppelte Adresse, falsche Dokumentation oder Manipulation
Eintrag vorhanden, Kommunikation scheitert	Problem kann oberhalb der Nachbarauflösung liegen

Das manuelle Löschen von ARP- oder Neighbor-Einträgen verändert den Zustand und sollte erst nach Dokumentation und mit konkreter Hypothese erfolgen.

---

18. IP-Adressen und Routingtabelle

Zu prüfen sind:

- IP-Adresse,
- Präfixlänge,
- direkt verbundene Netze,
- Standardroute,
- spezifische Routen,
- nächste Hops,
- Routingprotokoll,
- administrative Distanz beziehungsweise Präferenz,
- Metrik,
- VRF oder Routinginstanz,

- Rückweg.

Cisco IOS beziehungsweise IOS XE

```
show ip interface brief
```

```
show ip route
```

Bestimmtes Ziel:

```
show ip route 192.0.2.10
```

IPv6:

```
show ipv6 route
```

VRF-Übersicht:

```
show vrf
```

Juniper Junos

```
show interfaces terse
```

```
show route
```

Bestimmtes Ziel:

```
show route 192.0.2.10
```

Routinginstanzen:

```
show route instance
```

Aruba AOS-CX

```
show ip interface brief
```

```
show ip route
```

```
show vrf
```

Routingprüfung

1. Quellnetz bestimmen.
2. Zieladresse exakt bestimmen.
3. verwendete VRF beziehungsweise Routinginstanz feststellen.
4. Route zum Ziel prüfen.
5. nächsten Hop prüfen.
6. Erreichbarkeit des nächsten Hops prüfen.
7. Rückroute untersuchen.
8. Policy-Based Routing berücksichtigen.
9. NAT, Firewall und VPN berücksichtigen.
10. bei dynamischem Routing den Protokollzustand prüfen.

> Eine vorhandene Hinroute bestätigt keine funktionierende Rückroute. Asymmetrische Wege können insbesondere bei Firewalls und zustandsbehafteten Systemen Probleme verursachen.

---

19. Ping richtig verwenden

Ping verwendet ICMP Echo Request und Echo Reply.

Damit können unter anderem untersucht werden:

- grundsätzliche IP-Erreichbarkeit,
- Paketverlust,
- Laufzeit,
- Erreichbarkeit aus einer bestimmten Quelle,
- MTU-Probleme mit geeigneten Optionen.

Cisco IOS beziehungsweise IOS XE

```
ping 192.0.2.10
```

Erweiterter Dialog:

```
ping
```

Juniper Junos

```
ping 192.0.2.10
```

Bestimmte Quelladresse:

```
ping 192.0.2.10 source 192.0.2.1
```

Aruba AOS-CX

```
ping 192.0.2.10
```

Die Optionen für Quelladresse, VRF, Paketgröße und Anzahl sind versionsabhängig.

Sinnvolle Zielreihenfolge

1. eigene Schnittstellenadresse,
2. direkt verbundener nächster Hop,
3. Gateway,
4. entferntes IP-Ziel,
5. Ziel über Namen.

Grenzen

- ICMP kann gefiltert werden.
- Eine Firewall kann Ping anders behandeln als Anwendungsverkehr.
- Ein erfolgreicher Ping prüft keinen TCP-Port.
- Ein erfolgreicher Ping bestätigt keine Anmeldung oder Anwendung.
- Ein Ping ohne festgelegte Quelladresse kann einen anderen Pfad verwenden als der betroffene Datenverkehr.

---

20. Traceroute richtig verwenden

Traceroute hilft dabei, den Pfad beziehungsweise die antwortenden Zwischenstationen zu untersuchen.

Cisco IOS beziehungsweise IOS XE

```
traceroute 192.0.2.10
```

Juniper Junos

```
traceroute 192.0.2.10
```

Aruba AOS-CX

```
traceroute 192.0.2.10
```

Einordnung

- Sternchen bedeuten nicht automatisch, dass der gesamte folgende Pfad unterbrochen ist.
- Router können Ablaufmeldungen filtern oder begrenzen.
- Lastverteilung kann verschiedene Pfade zeigen.
- Hin- und Rückweg können unterschiedlich sein.
- Tunnel und MPLS können physische Zwischenwege verbergen.
- Ein Abbruch an einem Hop beweist nicht, dass genau dieses Gerät die Ursache ist.

---

21. Dynamische Routingprotokolle

Bei OSPF, BGP und anderen Protokollen sind drei Ebenen getrennt zu prüfen:

1. besteht die Nachbarschaft?
2. werden erwartete Routen ausgetauscht?
3. wird die gewünschte Route tatsächlich für die Weiterleitung verwendet?

Cisco – OSPF

```
show ip ospf neighbor
```

```
show ip ospf interface
```

```
show ip route ospf
```

Cisco – BGP

```
show ip bgp summary
```

```
show ip bgp
```

```
show ip route bgp
```

Juniper – OSPF

```
show ospf neighbor
```

```
show ospf interface
```

```
show route protocol ospf
```

Juniper – BGP

```
show bgp summary
```

```
show route protocol bgp
```

Aruba AOS-CX – je nach Plattform und Funktionsumfang

```
show ip ospf neighbors
```

```
show bgp all summary
```

Typische Ursachen

- Schnittstelle down,
- falsche IP-Adresse oder Präfixlänge,
- unterschiedliche Area,
- Authentifizierungsfehler,
- unterschiedliche Timer,
- MTU-Abweichung,
- fehlende Route zur Nachbaradresse,
- falsche Autonomous-System-Nummer,
- Filterrichtlinie,
- maximale Präfixanzahl,

- fehlende Freigabe durch ACL oder Firewall,
- instabile Verbindung,
- unterschiedliche VRF.

> Eine bestehende Routingnachbarschaft bestätigt nicht, dass alle benötigten Präfixe korrekt angenommen, ausgewählt und weitergeleitet werden.

---

22. ACL- und Firewallregeln prüfen

Bei Zugriffslisten und Firewalls müssen geprüft werden:

- Quelle,
- Ziel,
- Protokoll,
- Quellport,
- Zielport,
- Eingangszone,
- Ausgangszone,
- Richtung,
- Regelreihenfolge,
- Zähler,
- NAT,
- Sitzungstabelle,
- Benutzer- oder Anwendungsidentität,
- Zeitplan,
- Protokollierung.

Cisco IOS beziehungsweise IOS XE

```
show access-lists
```

```
show ip access-lists
```

Zuordnung zu Schnittstellen:

```
show ip interface
```

Juniper SRX

```
show security policies
```

```
show security policies hit-count
```

```
show security flow session
```

```
show security nat source rule all
```

Wichtige Einordnung

- Ein Regelzähler kann historischen Verkehr enthalten.
- Ein Zähler von null kann bedeuten, dass der Datenverkehr eine frühere Regel trifft.
- Zustandsbehaftete Firewalls benötigen häufig einen passenden Rückweg.
- NAT kann dazu führen, dass Protokolle eine andere Adresse zeigen.
- Eine erlaubende Regel bestätigt nicht, dass Routing, NAT oder Zielservice funktionieren.
- Ein Paket kann vor oder nach einer untersuchten Regel verworfen werden.

---

23. DHCP untersuchen

Zu prüfen sind:

- erhält der Client überhaupt eine DHCP-Antwort?
- befindet sich Client und Server im selben Netz?
- ist DHCP-Relay erforderlich?
- stimmt die Relay-Zieladresse?
- ist der Adressbereich erschöpft?
- besteht eine Sicherheitsfunktion wie DHCP Snooping?
- stimmen Gateway, DNS und Lease-Zeit?
- erreicht die Antwort den Client zurück?

Cisco IOS beziehungsweise IOS XE

DHCP-Relay auf einer Schnittstelle erkennen:

```
show running-config interface Vlan10
```

DHCP Snooping:

```
show ip dhcp snooping
```

DHCP-Bindings bei lokalem DHCP-Server:

```
show ip dhcp binding
```

Juniper Junos

Die Befehle hängen davon ab, ob das Gerät als DHCP-Server, Relay oder Sicherheitsgerät arbeitet. Beispiele:

```
show dhcp server binding
```

```
show dhcp relay binding
```

Diese Befehle sind nicht auf jeder Junos-Plattform in derselben Form verfügbar.

Typische Fehlerkette

```
Client Discover
→ Switch und VLAN
→ DHCP Relay
→ Routing beziehungsweise Firewall
→ DHCP Server
→ Offer und Acknowledgement
→ Rückweg zum Client
```

---

24. DNS, NTP, RADIUS und TACACS+

Netzwerkgeräte sind häufig von Infrastrukturdiensten abhängig.

DNS-Probleme können verursachen

- fehlgeschlagene Hostnamensauflösung,
- nicht erreichbare Controller,
- fehlgeschlagene Zertifikatsprüfung,
- Probleme mit Cloudmanagement,
- verzögerte Kommandoeingaben bei ungeeigneter Namensauflösung.

NTP-Probleme können verursachen

- falsche Protokollzeitpunkte,
- Zertifikatsfehler,

- Authentifizierungsprobleme,
- unbrauchbare Ereigniskorrelation,
- Probleme mit zeitabhängigen Sicherheitsmechanismen.

RADIUS- oder TACACS+-Probleme können verursachen

- fehlgeschlagene Administratoranmeldung,
- fehlende Autorisierung einzelner Befehle,
- fehlgeschlagene Netzwerkzugangskontrolle,
- Abhängigkeit von einem nicht erreichbaren Server.

Cisco IOS beziehungsweise IOS XE

```
show clock
```

```
show ntp associations
```

```
show ntp status
```

```
show aaa servers
```

Die verfügbaren AAA-Befehle unterscheiden sich nach Plattform und Version.

Juniper Junos

```
show system uptime
```

```
show ntp associations
```

```
show system users
```

Prüfen

- stimmt die Uhrzeit?
- stimmt die Zeitzone?
- ist der Zeitserver erreichbar?
- wird die erwartete Quelladresse verwendet?
- erreicht der Dienst die richtige VRF?
- blockiert eine ACL den Verkehr?

- ist ein lokales Notfallkonto gemäß Unternehmensvorgabe vorhanden?

---

25. Protokolle auswerten

Netzwerkgeräte können Protokolle speichern oder an einen zentralen Syslog-Server senden.

Zu erfassen sind:

- genauer Zeitpunkt,
- Zeitzone,
- Meldungsquelle,
- Schweregrad,
- Prozess oder Subsystem,
- betroffene Schnittstelle,
- Meldung vor und nach dem Ereignis,
- wiederkehrende Muster,
- Zusammenhang mit Konfigurationsänderungen.

Cisco IOS beziehungsweise IOS XE

```
show logging
```

Juniper Junos

```
show log messages
```

Letzte Einträge:

```
show log messages | last 50
```

Aruba AOS-CX

```
show logging
```

Typische Meldungen

- Link up oder down,
- STP-Änderung,
- Routingnachbarschaft verloren,
- Authentifizierungsfehler,
- Hardwarealarm,

- Temperaturwarnung,
- Konfigurationsänderung,
- Prozessneustart,
- Ressourcengrenze,
- Firewallblockierung,
- VPN-Neuverhandlung.

> Eine einzelne Fehlermeldung beweist nicht automatisch die Ursache. Sie muss zeitlich und technisch mit dem beobachteten Symptom verbunden werden.

---

26. Syslog-Schweregrade

Die verbreitete Syslog-Einteilung umfasst:

Wert	Bezeichnung	Bedeutung
0	Emergency	System nicht verwendbar
1	Alert	sofortige Maßnahme erforderlich
2	Critical	kritischer Zustand
3	Error	Fehlerzustand
4	Warning	Warnung
5	Notice	bedeutender normaler Zustand
6	Informational	Informationsmeldung
7	Debug	ausführliche Diagnosemeldung

Die tatsächliche Nutzung der Stufen hängt vom Hersteller und der jeweiligen Komponente ab.

Zu beachten

- Zu niedrige Schwelle kann wichtige Meldungen auslassen.
- Zu ausführliche Protokollierung kann sehr große Datenmengen erzeugen.
- Debug-Protokolle können sensible Informationen enthalten.
- Zentrale Protokolle benötigen korrekte Zeitstempel.
- UDP-Syslog bestätigt keine zuverlässige Zustellung.
- Transport, Verschlüsselung und Aufbewahrung müssen den Sicherheitsvorgaben entsprechen.

---

27. SNMP und Telemetrie

SNMP und Streaming-Telemetrie können langfristige Messwerte liefern.

Typische Werte sind:

- Schnittstellenstatus,
- Datenraten,
- Fehlerzähler,
- Paketverluste,
- CPU-Auslastung,
- Speichernutzung,
- Temperatur,
- Netzteilzustand,
- Routingnachbarschaften,
- Verfügbarkeit.

SNMP-Versionen

Version	Einordnung
SNMPv1	veraltet, keine moderne Absicherung
SNMPv2c	Community-basierte Absicherung, keine angemessene Vertraulichkeit
SNMPv3	unterstützt Benutzer-, Authentifizierungs- und Verschlüsselungsmechanismen

SNMPv3 sollte bevorzugt werden, sofern die Umgebung es unterstützt.

Diagnostischer Nutzen

- Beginn einer Störung zeitlich bestimmen,
- kurzfristige und langfristige Werte vergleichen,
- Lastspitzen erkennen,
- wachsende Fehlerzähler sehen,
- wiederkehrende Ausfälle untersuchen,
- Geräte miteinander vergleichen.

Grenzen

- Abfrageintervalle können kurze Ereignisse übersehen.
- Ein Mittelwert kann Spitzen verbergen.
- Zähler können nach Neustarts zurückgesetzt werden.
- 32-Bit-Zähler können bei schnellen Verbindungen überlaufen.
- fehlerhafte Zeitsynchronisation erschwert die Korrelation.
- Monitoringausfall bedeutet nicht automatisch Geräteausfall.

---

28. Paketmitschnitt auf Netzwerkgeräten

Viele Router, Firewalls und Switches unterstützen lokale oder gespiegelte Paketmitschnitte.

Mögliche Verfahren:

- integrierter Paketmitschnitt,
- Port Mirroring,
- SPAN,
- Remote SPAN,
- ERSPAN,
- Firewall Packet Capture,
- Controller-basierter Mitschnitt,
- externer Netzwerk-TAP.

Vorher festlegen

- betroffene Schnittstelle,
- Richtung,
- VLAN,
- Quelladresse,
- Zieladresse,
- Protokoll,
- Zielport,
- maximale Paketanzahl,
- maximale Dateigröße,
- Dauer,
- Speicherort,
- Datenschutz,
- Löschzeitpunkt.

Wichtige Einschränkungen

- Ein Mitschnitt auf einem überlasteten Gerät kann unvollständig sein.
- Hardwareweiterleitung kann dazu führen, dass nicht jeder Verkehr an der CPU sichtbar ist.
- Ein SPAN-Ziel kann bei Überlastung Pakete verlieren.
- Der Mitschnittpunkt bestimmt, ob VLAN-Tags, NAT-Adressen oder entschlüsselter Verkehr sichtbar sind.
- Eine Firewall kann Pakete an einer Schnittstelle empfangen und später durch eine Regel verwerfen.
- Verschlüsselter Datenverkehr zeigt ohne zulässige Entschlüsselung keine Anwendungsinhalte.

Paketmitschnitte können enthalten:

- IP-Adressen,
- MAC-Adressen,
- Hostnamen,
- DNS-Abfragen,
- Anmeldedaten bei unverschlüsselten Protokollen,

- Sitzungskennungen,
- personenbezogene Daten,
- vertrauliche Anwendungsinhalte.

---

29. Debug-Befehle

Debug-Befehle erzeugen detaillierte Laufzeitinformationen.

Sie können:

- sehr viele Meldungen erzeugen,
- CPU und Speicher belasten,
- die Konsole überfluten,
- Sitzungen unterbrechen,
- sensible Inhalte protokollieren,
- bei produktiven Geräten einen Ausfall verschärfen.

Vor einem Debug

1. konkrete Hypothese formulieren,
2. Herstellerdokumentation prüfen,
3. Auswirkungen für die Plattform prüfen,
4. Wartungsfreigabe einholen,
5. Filter festlegen,
6. Zeitdauer begrenzen,
7. Beendigung des Debugs vorbereiten,
8. alternative Beobachtungsmöglichkeit prüfen.

Cisco IOS beziehungsweise IOS XE

Aktive Debugs anzeigen:

```
show debugging
```

Debug-Ausgaben vollständig beenden:

```
undebug all
```

Der Befehl `debug all` darf auf produktiven Geräten nicht als allgemeine Diagnosemaßnahme verwendet werden.

> Ein Debug sollte nur gezielt, zeitlich begrenzt und unter Beobachtung durchgeführt werden.

---

30. Konfiguration vergleichen

Zu unterscheiden sind:

- aktuell laufende Konfiguration,
- für den nächsten Start gespeicherte Konfiguration,
- zentral verwaltete Konfiguration,
- automatisch erzeugte Konfiguration,
- Konfigurationsvorlage,
- tatsächlicher operativer Zustand.

Cisco IOS beziehungsweise IOS XE

```
show running-config
```

```
show startup-config
```

Letzte Konfigurationsänderung:

```
show archive log config all
```

Der Archivierungsbefehl liefert nur dann passende Daten, wenn die entsprechende Funktion unterstützt und eingerichtet ist.

Juniper Junos

```
show configuration
```

Vergleich mit vorheriger Konfiguration:

```
show system commit
```

```
show system rollback compare 1
```

Aruba AOS-CX

```
show running-config
```

```
show startup-config
```

Beim Vergleich beachten

- automatisch erzeugte Zeilen,
- unterschiedliche Reihenfolge ohne Funktionsänderung,
- verschlüsselte oder maskierte Geheimnisse,
- dynamisch gelernte Zustände,
- Änderungen durch Controller oder Automatisierung,
- nicht gespeicherte Änderungen,
- gerätespezifische Standardwerte.

> Eine Konfiguration darf nicht ungeprüft vollständig in ein Ticket oder öffentliches Dokument kopiert werden. Sie kann Kennwörter, Schlüssel, Community-Strings, Adressen und interne Topologieinformationen enthalten.

---

31. Hochverfügbarkeit und Stacks

Bei redundanten Geräten sind zusätzlich zu prüfen:

- aktives und passives Mitglied,
- Synchronisationsstatus,
- letzte Rollenänderung,
- Split-Brain-Schutz,
- Heartbeat- oder Keepalive-Verbindung,
- Versionsgleichheit,
- Konfigurationsgleichheit,
- Sitzungssynchronisation,
- Uplinkzustand beider Geräte,
- Stack-Ring,
- Stack-Mitglieder,
- Redundanz der Stromversorgung.

Mögliche Fehlerbilder

Beobachtung	mögliche Ursache
beide Geräte halten sich für aktiv	Split Brain oder unterbrochene Kontrollverbindung
passives Gerät nicht bereit	Versions-, Konfigurations- oder Hardwareproblem

Beobachtung	mögliche Ursache
Failover funktioniert, Sitzungen brechen ab	fehlende oder unvollständige Sitzungssynchronisation
nur Ports eines Stack-Mitglieds betroffen	Mitglied, Stack-Verbindung oder Stromversorgung
wiederholte Rollenwechsel	instabile Verbindung, Ressourcenproblem oder fehlerhafte Zustandsprüfung
Redundanz angezeigt, aber gemeinsamer Uplink fehlt	logische Redundanz ohne vollständige Pfadredundanz

Ein manuell ausgelöstes Failover ist eine produktive Änderung und benötigt eine Risikoprüfung.

---

32. WLAN-Access-Points und Controller

Bei WLAN-Problemen müssen Funk-, Netzwerk- und Authentifizierungsebene getrennt werden.

Zu prüfen sind:

- wird der Access Point mit Strom versorgt?
- erhält er eine IP-Adresse?
- erreicht er Controller oder Cloudplattform?
- wird die erwartete Konfiguration übernommen?
- sendet die gewünschte SSID?
- stimmen VLAN und Trunk?
- funktioniert Authentifizierung?
- erhält der Client eine IP-Adresse?
- bestehen Störungen oder hohe Kanalauslastung?
- wechselt der Client zwischen Access Points?
- funktionieren DNS und Gateway?

Typische WLAN-Werte

- RSSI,
- SNR,
- Kanal,
- Kanalbreite,
- Frequenzband,
- Sendeleistung,
- Retries,
- Kanalnutzung,
- Clientanzahl,
- Datenrate,
- Roamingereignisse,
- Authentifizierungsstatus.

Fehlinterpretationen vermeiden

Beobachtung	Einordnung
starke Signalstärke	bestätigt nicht automatisch gute Signalqualität oder geringen Störpegel
Client ist verbunden	bestätigt nicht automatisch DHCP, Routing oder Internetzugriff
SSID ist sichtbar	bestätigt nicht automatisch erfolgreiche Authentifizierung
Access Point ist online	bestätigt nicht automatisch störungsfreien Funkbetrieb
hohe theoretische Datenrate	entspricht nicht automatisch dem tatsächlichen Durchsatz
viele Access Points	können bei ungeeigneter Planung zusätzliche Störungen verursachen

---

33. VPN untersuchen

Bei einem VPN müssen getrennt geprüft werden:

1. physische und IP-Erreichbarkeit,
2. Namensauflösung,
3. IKE- beziehungsweise Kontrollverbindung,
4. Authentifizierung,
5. Tunnelaufbau,
6. Verschlüsselungsparameter,
7. Routen,
8. Sicherheitsrichtlinien,
9. NAT-Ausnahmen,
10. Datenzähler,
11. Rückweg,
12. MTU und Fragmentierung.

Typische Fehler

- falsche Peer-Adresse,
- Zertifikat abgelaufen,
- falsche Systemzeit,
- unterschiedliche Verschlüsselungsverfahren,
- unterschiedliche Netzdefinitionen,
- fehlende Route,
- NAT vor dem Tunnel,
- Firewall blockiert IKE oder ESP,
- Tunnel steht, aber keine Sicherheitsrichtlinie erlaubt den Verkehr,
- überlappende Adressbereiche,
- asymmetrischer Rückweg,
- MTU-Problem.

> Ein angezeigter VPN-Status „up“ bestätigt nicht automatisch, dass Nutzdaten in beide Richtungen übertragen werden.

---

34. NAT untersuchen

Bei NAT sind zu erfassen:

- ursprüngliche Quelladresse,
- ursprüngliche Zieladresse,
- übersetzte Quelladresse,
- übersetzte Zieladresse,
- Quellport,
- Zielport,
- zugehörige Regel,
- Richtung,
- Zone,
- Sitzung,
- Rückweg.

Typische Probleme

- falsche Regelreihenfolge,
- fehlende NAT-Ausnahme für VPN,
- Adresspool erschöpft,
- Portübersetzung erschöpft,
- unerwartetes doppeltes NAT,
- Rückroute zur übersetzten Adresse fehlt,
- Anwendung überträgt eingebettete Adressen,
- Protokolle zeigen nur eine Seite der Übersetzung.

Eine erfolgreiche NAT-Übersetzung bestätigt noch nicht, dass der Zielservice antwortet.

---

35. Support- und Diagnosepakete

Viele Hersteller bieten einen Sammelbefehl oder eine Supportdatei an.

Beispiele:

Cisco – plattformabhängig

```
show tech-support
```

Juniper Junos

```
request support information
```

Aruba AOS-CX

```
show tech
```

Diese Ausgaben können sehr umfangreich sein und das Gerät belasten.

Sie können enthalten:

- vollständige oder teilweise Konfiguration,
- IP-Adressen,
- Seriennummern,
- Benutzernamen,
- Routinginformationen,
- Nachbarn,
- Protokolle,
- Zertifikatsinformationen,
- Sitzungstabellen,
- interne Topologie,
- Sicherheitsrichtlinien.

Vor der Erstellung

- Speicherplatz prüfen,
- Belastung abschätzen,
- Freigabe einholen,
- sicheren Speicherort bestimmen,
- Übertragungsweg festlegen,
- Empfängerkreis begrenzen,
- Aufbewahrungsdauer definieren,
- vertrauliche Inhalte prüfen.

---

36. Typische Prüfreihenfolge bei einem ausgefallenen Switchport

1. betroffenes Endgerät und Port bestimmen,
2. Linkstatus prüfen,
3. Portbeschreibung kontrollieren,
4. Fehlerzähler dokumentieren,
5. Geschwindigkeit und Duplex prüfen,
6. VLAN-Zuordnung prüfen,
7. MAC-Adresstabelle prüfen,
8. STP-Zustand prüfen,

9. Port-Security oder NAC prüfen,
10. PoE-Zustand prüfen,
11. Nachbarinformationen prüfen,
12. Gegenstelle untersuchen,
13. Kabel oder Transceiver kontrolliert gegenprüfen,
14. nach jeder Maßnahme erneut testen.

Beispiel Cisco IOS beziehungsweise IOS XE

```
show interfaces status
```

```
show interfaces GigabitEthernet1/0/1
```

```
show interfaces GigabitEthernet1/0/1 switchport
```

```
show mac address-table interface GigabitEthernet1/0/1
```

```
show spanning-tree interface GigabitEthernet1/0/1 detail
```

```
show power inline GigabitEthernet1/0/1
```

---

37. Praxisbeispiel: Client erreicht das Gateway nicht

Symptom

Ein Client besitzt eine IP-Adresse, kann aber sein Standardgateway nicht erreichen.

Prüfung

1. IP-Adresse und Präfix des Clients kontrollieren.
2. Standardgateway kontrollieren.
3. physische Verbindung prüfen.
4. Access-VLAN des Ports prüfen.
5. VLAN auf den Trunks verfolgen.
6. MAC-Adresse des Clients suchen.
7. ARP-Eintrag auf Client und Gateway prüfen.
8. Gateway-Schnittstelle beziehungsweise SVI prüfen.
9. STP-Zustand prüfen.
10. Port-Security, NAC und ACL prüfen.

11. Paketmitschnitt nur bei verbleibender Unklarheit verwenden.

Mögliche Ursachen

- falsche Clientadresse,
- falsches Präfix,
- falsches Gateway,
- falsches Access-VLAN,
- VLAN fehlt auf einem Trunk,
- Gateway-Schnittstelle down,
- doppelte IP-Adresse,
- ARP-Problem,
- Port-Security,
- NAC-Quarantäne,
- Layer-2-Schleife,
- fehlerhafte physische Verbindung.

---

38. Praxisbeispiel: VLAN funktioniert an einem Switch, am nächsten nicht

Prüfung

1. VLAN auf beiden Switches anzeigen.
2. Access-Port des Clients prüfen.
3. Uplink und Trunk bestimmen.
4. erlaubte VLANs auf beiden Seiten vergleichen.
5. native beziehungsweise untagged VLANs vergleichen.
6. STP-Zustand für das VLAN prüfen.
7. MAC-Adresse entlang des Pfads verfolgen.
8. LACP-Zustand bei gebündeltem Uplink prüfen.
9. Zwischen-Switches einbeziehen.
10. erst danach Konfiguration ändern.

Mögliche Ursachen

- VLAN auf einem Gerät nicht angelegt,
- VLAN nicht auf dem Trunk erlaubt,
- unterschiedliche Portmodi,
- falsches untagged beziehungsweise native VLAN,
- STP blockiert den erwarteten Pfad,
- fehlerhaftes LACP-Mitglied,
- falsche physische Verbindung,
- VLAN-Zuordnung durch Controller oder Vorlage überschrieben.

---

39. Praxisbeispiel: Standortverbindung ist langsam

Zuerst messen

- betroffene Standorte,
- betroffene Anwendungen,
- Beginn und Dauer,
- Paketverlust,
- Laufzeit,
- Durchsatz,
- Schnittstellenauslastung,
- Fehlerzähler,
- Drops,
- QoS-Warteschlangen,
- VPN-Zähler,
- CPU-Auslastung,
- MTU.

Mögliche Ursachen

- ausgelastete WAN-Verbindung,
- Output Drops,
- physische Fehler,
- Duplexproblem,
- ungeeignete QoS-Regel,
- Backup- oder Synchronisationsverkehr,
- Paketverlust im Providerpfad,
- VPN-Neuverschlüsselung,
- MTU- oder Fragmentierungsproblem,
- Anwendung oder Server statt Netzwerk,
- asymmetrischer Pfad.

> Ein hoher Ping-Wert allein beweist keine geringe verfügbare Bandbreite. Laufzeit, Paketverlust, Jitter und Durchsatz sind unterschiedliche Messgrößen.

---

40. Praxisbeispiel: Gerät ist im Monitoring offline

Prüfreihenfolge

1. ist nur das Monitoring oder auch die Nutzfunktion betroffen?
2. ist die Managementadresse erreichbar?
3. stimmt die Route zum Managementnetz?
4. funktioniert der verwendete SNMP-, HTTPS- oder Telemetrieport?
5. stimmt die Management-VRF?
6. sind ACL und Firewallregeln unverändert?

7. sind Zugangsdaten oder Zertifikate abgelaufen?
8. stimmt die Gerätezeit?
9. ist der Monitoringdienst selbst funktionsfähig?
10. antwortet das Gerät über einen anderen Managementweg?

Mögliche Einordnung

Ergebnis	mögliche Ursache
Nutzdaten funktionieren, Monitoring nicht	Managementpfad, SNMP, Zertifikat oder Monitoringserver
Ping funktioniert, SNMP nicht	SNMP-Konfiguration, ACL, Zugangsdaten oder Dienst
mehrere Geräte gleichzeitig offline	Monitoringserver, gemeinsamer Managementpfad oder zentrale Firewall
nur ein Standort offline	WAN-, VPN- oder Standortproblem
Gerät nur über Konsole erreichbar	Managementnetz, Routing, ACL oder Überlastung

---

41. Häufige Fehlinterpretationen

Aussage	fachliche Einordnung
„Der Port ist up, also ist die Verbindung in Ordnung.“	Linkstatus bestätigt nicht VLAN, Routing, Fehlerfreiheit oder Anwendung.
„Ping funktioniert, daher ist der Dienst erreichbar.“	Ping prüft keinen Anwendungsport und keine Anmeldung.
„Die Route ist vorhanden, also muss der Verkehr funktionieren.“	Rückroute, Firewall, NAT und operative Weiterleitung müssen ebenfalls stimmen.
„Der Traceroute endet an einem Router, also ist dieser defekt.“	Zwischenstationen können Antworten filtern oder begrenzen.
„STP blockiert einen Port, deshalb liegt ein Fehler vor.“	Das Blockieren kann die beabsichtigte Schleifenvermeidung sein.
„Der Fehlerzähler ist hoch, daher besteht der Fehler noch.“	Entscheidend ist, ob der Zähler während der Störung weiter steigt.
„Die MAC-Adresse wurde gelernt, also funktioniert der Client.“	Nur das Layer-2-Lernen wurde nachgewiesen.
„Das VPN ist up, also fließen Daten.“	Routen, Richtlinien, NAT und Rückweg können weiterhin fehlerhaft sein.
„Das Gerät ist im Monitoring offline, also ist es ausgefallen.“	Nur der Management- oder Monitoringpfad kann gestört sein.
„Ein Neustart behebt das Problem.“	Er kann nur flüchtigen Zustand entfernen und Beweise vernichten.
„`show tech` ist nur eine harmlose Abfrage.“	Umfangreiche Ausgaben können Ressourcen beanspruchen und vertrauliche Daten enthalten.

Aussage	fachliche Einordnung
„Debug zeigt viele Fehler, also ist die Ursache gefunden.“	Debug-Meldungen müssen mit Zeitpunkt, Datenpfad und Symptom abgeglichen werden.

42. Checkliste Netzwerkgeräte-Fehleranalyse

- [ ] betroffenes Gerät und dessen Rolle sind bekannt.
- [ ] Hersteller, Modell und Softwareversion wurden erfasst.
- [ ] Zeitpunkt und letzte Änderungen wurden dokumentiert.
- [ ] laufende und gespeicherte Konfiguration wurden unterschieden.
- [ ] Managementzugriff wurde ohne unsichere Protokolle geprüft.
- [ ] CPU, Arbeitsspeicher und Hardwarezustand wurden kontrolliert.
- [ ] Schnittstellenstatus und Fehlerzähler wurden dokumentiert.
- [ ] Geschwindigkeit, Duplex und Medium wurden auf beiden Seiten geprüft.
- [ ] VLANs und Trunks wurden entlang des gesamten Pfads untersucht.
- [ ] MAC-, ARP- und IPv6-Nachbartabellen wurden geprüft.
- [ ] STP und LACP wurden berücksichtigt.
- [ ] Hin- und Rückroute wurden geprüft.
- [ ] richtige VRF beziehungsweise Routinginstanz wurde verwendet.
- [ ] Ping wurde bei Bedarf mit passender Quelladresse durchgeführt.
- [ ] Traceroute-Ergebnisse wurden nicht vorschnell interpretiert.
- [ ] ACL, Firewall, NAT und Sitzungstabellen wurden berücksichtigt.
- [ ] DNS, DHCP, NTP und Authentifizierungsdienste wurden getrennt geprüft.
- [ ] Protokolle wurden zeitlich mit dem Symptom abgeglichen.
- [ ] Zeitzone und Zeitsynchronisation wurden berücksichtigt.
- [ ] Monitoringwerte wurden mit aktuellen Gerätedaten verglichen.
- [ ] Debugging wurde nur gezielt und zeitlich begrenzt verwendet.
- [ ] Paketmitschnitte wurden begrenzt und geschützt.
- [ ] Supportdateien wurden auf vertrauliche Inhalte geprüft.
- [ ] Änderungen wurden einzeln und möglichst reversibel durchgeführt.
- [ ] Funktion und Nebenwirkungen wurden nach jeder Änderung geprüft.
- [ ] Ursache, Maßnahme und Ergebnis wurden dokumentiert.

43. Schnellreferenz

Aufgabe	Cisco IOS/IOS XE	Juniper Junos	Aruba AOS-CX
Version	`show version`	`show version`	`show version`
Hardware	`show inventory`	`show chassis hardware`	`show inventory`
Systemzustand	`show platform resources`	`show chassis routing-engine`	`show system resource-utilization`
Schnittstellenübersicht	`show ip interface brief`	`show interfaces terse`	`show ip interface brief`
Schnittstellendetails	`show interfaces ...`	`show interfaces ... extensive`	`show interface ...`
VLANs	`show vlan brief`	`show vlans`	`show vlan`
Trunks	`show interfaces trunk`	`show ethernet-switching interfaces`	Port- und VLAN-Status prüfen
MAC-Tabelle	`show mac address-table`	`show ethernet-switching table`	`show mac-address-table`
Spanning Tree	`show spanning-tree`	`show spanning-tree bridge`	`show spanning-tree`
LACP	`show lacp neighbor`	`show lacp interfaces`	`show lacp interfaces`
LLDP	`show lldp neighbors`	`show lldp neighbors`	`show lldp neighbor-info`
ARP	`show ip arp`	`show arp`	`show arp`
Routingtabelle	`show ip route`	`show route`	`show ip route`
OSPF-Nachbarn	`show ip ospf neighbor`	`show ospf neighbor`	`show ip ospf neighbors`
BGP-Übersicht	`show ip bgp summary`	`show bgp summary`	`show bgp all summary`
Protokolle	`show logging`	`show log messages`	`show logging`
NTP	`show ntp associations`	`show ntp associations`	versionsabhängig
Ping	`ping Ziel`	`ping Ziel`	`ping Ziel`
Traceroute	`traceroute Ziel`	`traceroute Ziel`	`traceroute Ziel`
Supportausgabe	`show tech-support`	`request support information`	`show tech`

> Diese Tabelle ist eine Orientierung. Vor der Verwendung muss die Befehlsreferenz der konkreten Plattform und Softwareversion geprüft werden.

Merksatz

> Netzwerkgeräte werden nicht durch wahllose Neustarts, Tabellenlöschungen oder dauerhafte Debug-Ausgaben untersucht. Zuerst werden Hardware, Schnittstellen, VLANs, Nachbartabellen, Routing, Sicherheitsregeln, Protokolle und Abhängigkeiten getrennt geprüft. Danach wird eine konkrete Hypothese mit

> einer kleinen, kontrollierten und möglichst reversiblen Maßnahme getestet.

Quellen und weiterführende Dokumentation

- Cisco – Ping- und Traceroute-Befehle verstehen
- Cisco – Extended Ping und Extended Traceroute
- Cisco – Switch-Port- und Schnittstellenprobleme untersuchen
- Cisco – Troubleshooting Tools
- Juniper – `show interfaces terse`
- Juniper – Netzwerkprobleme untersuchen
- Juniper – Junos OS CLI User Guide
- HPE Aruba Networking – AOS-CX 10.15 CLI Guide für 6300/6400
- HPE Aruba Networking – AOS-CX `show tech`
- IETF RFC 5424 – The Syslog Protocol
- IETF RFC 3411 – SNMP Management Frameworks
- IETF RFC 3414 – SNMPv3 User-based Security Model
- IETF RFC 5905 – Network Time Protocol Version 4
