

Hier ist deine Master-Referenz für das Troubleshooting:

1. Endgeräte (PCs / Server)

Bevor man auf die Router schaut, muss man sicherstellen, dass das Endgerät richtig konfiguriert ist.

Windows:

- `ipconfig /all` → Zeigt IP, Subnetzmaske, Default Gateway und DNS-Server. (Prüft, ob DHCP funktioniert hat).
- `ping <IP>` → Testet die Erreichbarkeit.
- `tracert <IP>` → Zeigt jeden Router (Hop) auf dem Weg zum Ziel. (Wo bleibt das Paket hängen?)
- `arp -a` → Zeigt den ARP-Cache (welche MAC-Adresse gehört zum Default Gateway?).
- `route print` → Zeigt die lokale Routing-Tabelle des Windows-PCs.
- `nslookup google.com` → Testet, ob der DNS-Server Namen in IPs auflösen kann (Layer 7).

Linux / Mac:

- `ip a` (oder `ifconfig`) → Zeigt IP-Adressen und Interface-Status.
- `ping <IP>` → Testet die Erreichbarkeit.
- `traceroute <IP>` (oder `mtr <IP>`) → Verfolgt den Pfad des Pakets. mtr ist ein großartiges Live-Tool.
- `ip neigh` (oder `arp -n`) → Zeigt die ARP-Tabelle.
- `ip route` → Zeigt das Default Gateway und die Routing-Tabelle.
- `dig google.com` → Detailreiche DNS-Abfrage.

2. Interfaces & Physische Schicht (Layer 1 & 2)

Der erste Blick auf einem Cisco-Router oder -Switch sollte immer den Interfaces gelten.

- `show ip interface brief` → Der wichtigste Befehl! Zeigt, ob Interfaces ein IP haben und ob der Status "Up/Up" ist.
- `show interfaces <Interface>` → (z. B. `show interfaces e0/0`). Zeigt Fehler wie *CRC errors*, *Drops*, Duplex-Mismatches oder falsche MTU-Größen.
- `show interfaces description` → Zeigt deine konfigurierten Beschreibungen (z. B. "##to-Nuernberg##"), extrem hilfreich in großen Netzen.

3. Switching & Layer 2 (L2)

Wenn physisch alles "Up" ist, prüfen wir die Nachbarn und Mac-Adressen.

- `show lldp neighbors` oder `show cdp neighbors` → Zeigt an, welche Cisco/Fremd-Geräte *direkt* per Kabel angeschlossen sind. (Wie wir vorhin beim ISP genutzt haben!). Füge `detail` hinzu, um die IP des Nachbarn zu sehen.
- `show mac address-table` → Zeigt, an welchem Switchport welche MAC-Adresse gelernt wurde.
- `show spanning-tree` → Zeigt, ob ein Port blockiert ist, um einen Loop zu verhindern.
- `show spanning-tree vlan <VLAN-ID>` → Zeigt den Root-Bridge-Status für ein spezifisches VLAN.

4. Routing, DHCP & NAT (Layer 3)

Hier prüfen wir, wie Pakete durch das Netzwerk geleitet werden.

- `show ip route` → Zeigt die komplette Routing-Tabelle. Achte auf O (OSPF), B (BGP), C (Connected) und S* (Default Route).
- `show ip route <IP>` → (z. B. `show ip route 8.8.8.8`). Sagt dir *exakt*, welches Interface der Router für dieses spezifische Ziel benutzen wird.
- `ping <Ziel-IP> source <Quell-Interface/IP>` → Extrem wichtig! Pingt nicht mit der nächstbesten IP, sondern simuliert z. B. den Traffic aus dem LAN. (Beispiel: `ping 8.8.8.8 source 192.168.12.254`).
- `show ip arp` → Zeigt, welche IPs zu welchen MAC-Adressen auf dem Router gehören.
- `show ip dhcp binding` → Zeigt, welchen PCs der DHCP-Server eine IP gegeben hat.
- `show ip nat translations` → Zeigt die aktive NAT-Tabelle. Daran erkennst du, ob interne IPs erfolgreich auf die externe IP übersetzt werden.

5. OSPF Troubleshooting

OSPF-Fehler sind oft Timer, Areas oder fehlende Netzwerke.

- `show ip ospf neighbor` → Zeigt deine Nachbarn. Der Status **muss** auf FULL (oder 2WAY in Broadcast-Netzen) stehen. Alles wie EXSTART, INIT oder DOWN bedeutet Trouble!
- `show ip ospf interface brief` → Genialer Befehl! Zeigt dir auf einen Blick, auf welchen Interfaces OSPF läuft, in welcher **Area** sie sind und ob sie auf **Passive** stehen.
- `show ip route ospf` → Filtert die Routing-Tabelle, sodass du nur die per OSPF gelernten Routen siehst.
- `show ip ospf database` → Für Fortgeschrittene: Zeigt die rohen LSAs (Link-State Advertisements) in der Datenbank.
- `clear ip ospf process` → Startet den OSPF-Prozess hart neu, um Nachbarschaften neu aufzubauen (Achtung: Unterbricht kurz den Traffic).

6. BGP Troubleshooting

BGP verzeiht keine Fehler bei AS-Nummern oder fehlenden Next-Hops.

- `show ip bgp summary` → Der wichtigste BGP-Befehl! Achte ganz rechts auf die Spalte State/PfxRcd. Steht dort eine Zahl (z. B. 0, 3, 10), ist BGP "Up". Steht dort Idle oder Active, ist BGP kaputt.
- `show ip bgp` → Zeigt die BGP-Tabelle. Achte auf das *> (Valid and Best). Fehlt das >, wird die Route nicht ins OSPF weitergegeben. Achte auch auf den "Next Hop" – er muss erreichbar sein!
- `show ip bgp neighbors <IP> advertised-routes` → Zeigt dir genau, welche Netze dein Router *an den Nachbarn schickt*.
- `show ip bgp neighbors <IP> received-routes` → Zeigt, was *der Nachbar dir schickt* (erfordert oft soft-reconfiguration inbound in der Config).
- `clear ip bgp * soft` → Führt einen "Route Refresh" durch, ohne die BGP-Session abubrechen. Das zwingt die Router, sich die Routen neu zu schicken (sehr nützlich nach Config-Änderungen).

Ein goldener Tipp für die Praxis: Troubleshooting verläuft immer am besten nach dem **OSI-Modell von unten nach oben** ("Bottom-Up Approach"):

1. Ist das Kabel drin und der Port up? (L1/L2)
2. Können sich die direkten Nachbarn anpingen? (L3 - IP)
3. Stehen die Nachbarschaften (OSPF/BGP)? (L3/L4 - Routing Protokolle)
4. Kennen sie die Routen von A nach B (und den Rückweg!)? (L3 - Routing Table)

1. Bottom-Up (Layer 1 → Layer 7)

- **Wann nutzt man das?** Wenn das Netzwerk komplett neu aufgebaut wird, bei einem totalen Ausfall (Link Down) oder wenn man absolut keine Anhaltspunkte hat.
- **Die Logik:** Bevor ich mich frage, warum das OSPF-Routing kaputt ist, muss ich wissen, ob überhaupt Strom auf dem Interface ist oder das Kabel steckt.

2. Top-Down (Layer 7 → Layer 1)

- **Wann nutzt man das?** Wenn ein User sagt: *"Ich komme nicht auf die Webseite!"*, aber du siehst, dass sein Teams-Call im Hintergrund fehlerfrei läuft. Das ist ein Indiz dafür, dass L1 bis L3 perfekt funktionieren.
- **Die Logik:** Man fängt ganz oben an (Browser Cache, DNS-Auflösung) und arbeitet sich nach unten durch (Firewall blockiert Port 443?). Oft muss man bei dieser Methode gar nicht erst bis zu den Switches (L2) hinabsteigen.

3. Divide and Conquer (Teile und Herrsche)

- **Wann nutzt man das?** Das ist der absolute Liebling von erfahrenen Admins im Alltag. Man springt direkt in die Mitte des OSI-Modells – meistens auf **Layer 3 (Ping / Traceroute)**.
- **Die Logik:** * Geht der Ping durch? → Fehler liegt weiter *oben* (L4-L7: z.B. Port geblockt, Applikation abgestürzt, DNS kaputt). Schlägt der Ping fehl? → Fehler liegt weiter *unten* (L1-L2: z.B. falsches VLAN, fehlende Route, kaputtes Kabel).