7.2 Mehrere Clients haben kein Netzwerk

Sind mehrere Clients gleichzeitig betroffen, liegt die Ursache meist nicht an jedem einzelnen Endgerät. Gemeinsam genutzte Komponenten und Dienste müssen deshalb zuerst untersucht werden:

- Switch oder Switch-Uplink,
- Access Point oder WLAN-Controller,
- VLAN,
- DHCP,
- Standardgateway,
- Routing,
- DNS,
- Firewall,
- Standortverbindung,
- zentrale Stromversorgung.

Dieser Entscheidungsbaum dient der schnellen Eingrenzung. Die ausführliche Analyse befindet sich auf der Seite **6.2 Mehrere Clients oder ganzer Standort ohne Netzwerk**.

---

1. Betroffenen Bereich bestimmen

Zuerst feststellen, welche Gemeinsamkeit die betroffenen Clients besitzen.

Betroffene Systeme	Wahrscheinlicher gemeinsamer Bereich
Clients an einer Netzwerkdose	Dose, Kabel, Patchung oder einzelner Switchport
Clients an einem Switch	Switch, Uplink, Stromversorgung oder Switchkonfiguration
Clients in einem VLAN	VLAN, DHCP-Bereich, Gateway, ACL oder Routing
Clients an einem Access Point	Access Point, Uplink, Stromversorgung oder Funkzelle
Clients einer SSID	WLAN-Konfiguration, Authentifizierung, RADIUS oder VLAN-Zuweisung
Clients eines Stockwerks	Etagenverteiler, Access-Switch oder Uplink
Clients eines Gebäudes	Gebäudeverteiler, Firewall, Gateway oder WAN-Verbindung
nur kabelgebundene Clients	Switching, Patchung, VLAN oder Ethernet-Uplink
nur WLAN-Clients	Access Points, Controller, SSID, RADIUS oder Funknetz
alle Clients eines Standorts	Core-Switch, Firewall, Router, WAN, DHCP, DNS oder Stromversorgung
nur interne Dienste betroffen	internes Routing, VPN, Firewall, DNS oder Servernetz
nur Internet betroffen	Internetrouter, Firewall, NAT, Proxy oder Provider

Betroffene Systeme	Wahrscheinlicher gemeinsamer Bereich
nur Namen funktionieren nicht	DNS-Dienst oder DNS-Erreichbarkeit
nur eine Anwendung betroffen	Zielsystem, Dienst, Port, Proxy oder Zertifikat

---

2. Schneller Hauptentscheidungsbaum

```
START: Mehrere Clients haben kein Netzwerk
|
+-- Sind wirklich mehrere Clients betroffen?
|   |
|   +-- Nein -> Entscheidungsbaum 7.1 verwenden
|   |
|   +-- Ja
|
+-- Haben die betroffenen Clients eine erkennbare Gemeinsamkeit?
|   |
|   +-- gleicher Switch
|   |     -> Switchstatus, Ports, Uplink und Stromversorgung prüfen
|   |
|   +-- gleiches VLAN
|   |     -> VLAN, Gateway, DHCP, ACL und Routing prüfen
|   |
|   +-- gleicher Access Point oder gleiche SSID
|   |     -> AP, Controller, Authentifizierung und VLAN-Zuweisung prüfen
|   |
|   +-- gleicher Standort
|         -> Core, Firewall, Router, WAN und zentrale Dienste prüfen
|
+-- Besteht bei den Clients ein physischer Link oder eine WLAN-Verbindung?
|   |
|   +-- Nein -> gemeinsame Netzwerkkomponente, Uplink oder Stromversorgung
|   |           untersuchen
|   |
|   +-- Ja
|
+-- Erhalten die Clients gültige IP-Adressen?
|   |
|   +-- Nein oder 169.254.x.x
```

```
|  |        -> DHCP, Relay, VLAN, Trunk oder DHCP-Bereich prüfen
|  |
|  +-- Ja
|
+-- Ist das lokale Standardgateway erreichbar?
|  |
|  +-- Nein -> VLAN, Switch-Uplink, Gateway, ARP, STP oder Firewall prüfen
|  |
|  +-- Ja
|
+-- Ist eine externe IP-Adresse erreichbar?
|  |
|  +-- Nein -> Routing, Firewall, NAT, WAN oder Provider prüfen
|  |
|  +-- Ja
|
+-- Funktioniert die Namensauflösung?
|  |
|  +-- Nein -> DNS-Server, DNS-Erreichbarkeit und DNS-Dienst prüfen
|  |
|  +-- Ja
|
+-- Ist nur ein bestimmter Dienst nicht erreichbar?
   |
   +-- Ja  -> Zielsystem, Port, Firewall, Proxy oder Anwendung prüfen
   |
   +-- Nein -> genaue Gemeinsamkeit der betroffenen Verbindungen ermitteln
```

---

3. Störungsumfang mit Vergleichstests eingrenzen

Geeignete Vergleichsclients auswählen:

- funktionierender Client am selben Switch,
- funktionierender Client in einem anderen VLAN,
- funktionierender Client an einem anderen Access Point,
- funktionierender Client in einem anderen Stockwerk,
- funktionierender Client an einem anderen Standort,
- kabelgebundener Client als Vergleich zu WLAN,
- WLAN-Client als Vergleich zu Ethernet.

Auf jedem Vergleichsclient möglichst dieselben Prüfungen durchführen:

```
ipconfig /all
```

```
ping <gateway-ip>
```

```
ping <freigegebene-externe-ip>
```

```
nslookup <zielname>
```

```
Test-NetConnection -ComputerName <zielname> -Port <port>
```

Bewertung

Ergebnis	Eingrenzung
alle Clients an einem Switch betroffen	Switch oder Uplink priorisieren
mehrere Switches im selben VLAN betroffen	VLAN, Gateway oder zentrale Dienste priorisieren
nur ein VLAN betroffen	VLAN-spezifische Konfiguration prüfen
alle VLANs betroffen	Core, Firewall, Router oder gemeinsame Uplinks prüfen
nur WLAN betroffen	WLAN-Infrastruktur priorisieren
Ethernet und WLAN betroffen	gemeinsame Dienste oder zentrale Infrastruktur prüfen
externe IP funktioniert, Namen nicht	DNS priorisieren
Gateway erreichbar, externe Ziele nicht	Routing, Firewall, NAT oder WAN priorisieren
nur ein Ziel nicht erreichbar	Zielsystem oder Zielpfad priorisieren

Die Tests müssen unter möglichst gleichen Bedingungen erfolgen. Unterschiedliche VLANs, Berechtigungen oder Netzwerkwege können sonst zu falschen Schlussfolgerungen führen.

---

4. Besteht noch eine Verbindung zum Netzwerk?

Auf mehreren betroffenen Clients den Adapterstatus prüfen:

```
Get-NetAdapter
```

Vollständige IP-Konfiguration anzeigen:

```
ipconfig /all
```

Entscheidung

- mehrere Ethernetclients zeigen `Disconnected` → gemeinsamen Switch, Uplink oder Stromausfall prüfen.
- mehrere WLAN-Clients sind getrennt → Access Point, Controller, SSID oder Authentifizierung prüfen.
- Link besteht, aber keine gültige IP-Adresse → DHCP- oder VLAN-Pfad prüfen.
- Link und IP-Konfiguration bestehen → Gateway und Routing prüfen.
- nur einzelne Ports sind ohne Link → Portgruppe, Patchfeld oder Modul untersuchen.
- alle Ports eines Switches sind ohne Link → Switchstatus und Stromversorgung prüfen.

Ein vorhandener Link beweist nur die physische Verbindung zwischen Client und nächster Netzwerkkomponente.

---

5. Switch und Uplink prüfen

Bei einem räumlich begrenzten Ausfall prüfen:

- ist der Switch eingeschaltet,
- sind ungewöhnlich viele Ports ohne Link,
- funktioniert die Stromversorgung,
- meldet die unterbrechungsfreie Stromversorgung einen Fehler,
- ist der Uplink aktiv,
- ist ein redundanter Uplink blockiert oder ausgefallen,
- bestehen ungewöhnlich viele Port-Flaps,
- wurde ein Port durch eine Schutzfunktion deaktiviert,
- bestehen Fehler an einem Interface,
- wurde die VLAN- oder Trunk-Konfiguration geändert,
- gibt es Hinweise auf eine Netzwerkschleife,
- läuft Spanning Tree stabil,
- ist die CPU- oder Speicherauslastung auffällig,
- ist die MAC-Adresstabelle plausibel?

Die genauen Befehle hängen vom Hersteller und Betriebssystem des Switches ab. Typische Informationen sind:

- Portstatus,
- Uplinkstatus,
- Interfacefehler,
- verworfene Frames,
- VLAN-Zuordnung,
- Trunk-VLANs,
- MAC-Adresstabelle,

- Spanning-Tree-Zustand,
- Port-Security- oder Errdisable-Ereignisse,
- Systemprotokoll,
- letzte Konfigurationsänderung.

Entscheidungsbaum

```
Sind die betroffenen Clients an demselben Switch angeschlossen?
|
+-- Nein
|   -> gemeinsame übergeordnete Komponente suchen
|
+-- Ja
    |
    +-- Ist der Switch erreichbar und betriebsbereit?
        |
        +-- Nein
        |   -> Stromversorgung, Managementzugriff und Hardware prüfen
        |
        +-- Ja
            |
            +-- Ist der Uplink aktiv?
                |
                +-- Nein
                |   -> Kabel, Transceiver, Gegenstelle und Portstatus prüfen
                |
                +-- Ja
                    |
                    +-- Werden die erforderlichen VLANs transportiert?
                        |
                        +-- Nein -> Trunk- und VLAN-Konfiguration prüfen
                        |
                        +-- Ja  -> Gateway, DHCP und Routing prüfen
```

Ein Switch darf nicht als erste Maßnahme neu gestartet werden. Dadurch gehen möglicherweise Protokolle, Tabellen und der ursprüngliche Fehlerzustand verloren.

---

6. Prüfen, ob nur ein VLAN betroffen ist

Hinweise auf einen VLAN-Fehler:

- alle betroffenen Clients befinden sich im selben IP-Subnetz,
- andere VLANs am selben Switch funktionieren,
- Clients erhalten Adressen aus einem falschen Subnetz,
- Clients erhalten überhaupt keine DHCP-Adresse,
- das Gateway dieses VLANs ist nicht erreichbar,
- die Störung begann nach einer Switch- oder Firewalländerung,
- ein neuer Switch oder Access Point wurde eingebunden,
- kabelgebundene und drahtlose Clients desselben VLANs sind betroffen.

Zu prüfen sind:

- Access-VLAN der Clientports,
- VLAN-Zuweisung der SSID,
- erlaubte VLANs auf Trunks,
- native beziehungsweise ungetaggte VLAN-Konfiguration,
- VLAN-Existenz auf beteiligten Switches,
- Spanning-Tree-Zustand des VLANs,
- Gateway-Schnittstelle oder SVI,
- DHCP-Bereich und DHCP-Relay,
- VLAN-spezifische ACLs oder Firewallregeln,
- Routing zwischen den VLANs.

Entscheidung

- nur Clients eines Ports im falschen VLAN → Access-Port-Konfiguration prüfen.
- mehrere Ports eines Switches betroffen → Portprofil oder Switchkonfiguration prüfen.
- VLAN funktioniert auf einem Switch, auf einem anderen nicht → Trunk und VLAN-Weiterleitung prüfen.
- VLAN funktioniert nirgends → Gateway, SVI, DHCP und zentrale Konfiguration prüfen.
- Clients erhalten Adressen eines anderen VLANs → Port-, Trunk-, SSID- oder DHCP-Konfiguration prüfen.

---

7. DHCP-Störung erkennen

Auf mehreren betroffenen Clients prüfen:

```
ipconfig /all
```

Typische Hinweise auf einen gemeinsamen DHCP-Fehler:

- mehrere Clients besitzen Adressen aus `169.254.0.0/16`,
- das Standardgateway fehlt,
- DNS-Server fehlen,
- Clients erhalten Adressen aus einem falschen Subnetz,
- bestehende Clients funktionieren noch, neue Clients jedoch nicht,

- Clients mit gültigem Lease funktionieren bis zur Lease-Erneuerung,
- nur ein bestimmtes Subnetz erhält keine Adressen.

Schneller DHCP-Entscheidungsbaum

```
Erhalten mehrere Clients keine gültige Adresse?
|
+-- Nein
|   -> Gateway, Routing, DNS oder Anwendung prüfen
|
+-- Ja
    |
    +-- Sind alle DHCP-Subnetze betroffen?
        |
        +-- Ja
        |   -> DHCP-Dienst, Server, Failover und zentrale Erreichbarkeit prüfen
        |
        +-- Nein
            |
            +-- Nur ein DHCP-Bereich betroffen?
                |
                +-- Ja
                |   -> Bereich, freie Leases, Optionen und Ausschlüsse prüfen
                |
                +-- Nein
                    -> VLAN, Trunk und DHCP-Relay prüfen
```

Auf einem autorisierten Windows-DHCP-Server können unter anderem folgende Prüfungen verwendet werden:

```
Get-Service -Name DHCPServer
```

```
Get-DhcpServerv4Scope
```

```
Get-DhcpServerv4ScopeStatistics
```

```
Get-DhcpServerv4Binding
```

```
Get-DhcpServerv4Failover
```

Zu prüfen sind:

- läuft der DHCP-Dienst,
- ist der DHCP-Server autorisiert,
- ist der betreffende Bereich aktiv,
- sind noch freie Adressen vorhanden,
- stimmen Subnetzmaske, Gateway und DNS-Optionen,
- funktioniert ein konfiguriertes DHCP-Failover,
- erreicht die Anfrage den DHCP-Server,
- antwortet der Server,
- funktioniert das DHCP-Relay,
- wird UDP 67 oder 68 blockiert,
- existiert ein nicht autorisierter DHCP-Server?

Ein autorisierter Paketmitschnitt kann zeigen, an welcher Stelle der DORA-Ablauf endet:

1. DHCP Discover,
2. DHCP Offer,
3. DHCP Request,
4. DHCP Acknowledge.

---

8. Bestehende und neue Clients vergleichen

Dieser Vergleich ist bei DHCP-Störungen besonders aussagekräftig.

Beobachtung	Mögliche Erklärung
bestehende Clients funktionieren, neue nicht	DHCP-Bereich ausgeschöpft oder DHCP-Dienst gestört
Clients funktionieren bis zum Ablauf des Leases	Lease-Erneuerung oder DHCP-Erreichbarkeit gestört
Clients mit statischer IP funktionieren	DHCP-Pfad priorisieren
statische und dynamische Clients funktionieren nicht	Gateway, VLAN, Switch oder Routing priorisieren
nur Clients eines Subnetzes betroffen	DHCP-Bereich, Relay oder VLAN prüfen
Clients erhalten unterschiedliche falsche Adressen	fremden DHCP-Server oder falsche VLAN-Zuweisung prüfen

Eine frei gewählte statische IP-Adresse sollte nicht unkontrolliert vergeben werden. Sie kann einen Adresskonflikt verursachen und den ursprünglichen Fehler verdecken.

---

9. Standardgateway prüfen

Auf mehreren Clients das konfigurierte Gateway feststellen:

```
ipconfig
```

Gateway testen:

```
ping <gateway-ip>
```

Routingtabelle anzeigen:

```
route print
```

Alternativ:

```
Get-NetRoute
```

Nachbartabelle prüfen:

```
Get-NetNeighbor
```

Entscheidung

- kein Client erreicht das Gateway → Gateway, VLAN, Switchpfad oder Firewall prüfen.
- nur ein VLAN erreicht sein Gateway nicht → Gateway-Schnittstelle, SVI oder VLAN-Zuordnung prüfen.
- Gateway erscheint nicht in der Nachbartabelle → Layer-2-Pfad und ARP untersuchen.
- Gateway erscheint mit MAC-Adresse, antwortet aber nicht auf Ping → ICMP kann blockiert sein; weitere Dienste testen.
- ein Vergleichs-VLAN erreicht sein Gateway → globale Gateway-Hardware ist nicht automatisch vollständig bestätigt; VLAN-spezifische Konfiguration prüfen.
- mehrere Gateways sind gleichzeitig ausgefallen → redundante Gatewaylösung, Core-Switch oder zentrale Firewall prüfen.

Ein fehlgeschlagener Ping allein beweist keinen Ausfall des Gateways.

---

10. Routing, Firewall und Internetübergang prüfen

Wenn das Gateway erreichbar ist, eine freigegebene externe IP-Adresse testen:

```
ping <freigegebene-externe-ip>
```

Pfad anzeigen:

```
tracert <freigegebene-externe-ip>
```

PowerShell-Test:

```
Test-NetConnection -ComputerName <freigegebene-externe-ip> -InformationLevel Detailed
```

Entscheidungsbaum

```
Ist das lokale Gateway erreichbar?
|
+-- Nein
|   -> lokales VLAN, Switching und Gateway prüfen
|
+-- Ja
    |
    +-- Ist eine externe IP-Adresse erreichbar?
        |
        +-- Ja
        |   -> DNS und Zielanwendung prüfen
        |
        +-- Nein
            |
            +-- Sind interne geroutete Netze erreichbar?
                |
                +-- Ja
                |   -> Firewall, NAT, WAN oder Provider prüfen
                |
                +-- Nein
                    -> internes Routing, Core oder Firewall prüfen
```

Zu prüfen sind:

- Standardroute,
- dynamische oder statische Routen,
- Firewallzustand,

- NAT-Regeln,
- WAN-Schnittstelle,
- Providerverbindung,
- VPN- oder Standorttunnel,
- Hochverfügbarkeitsstatus,
- Routingnachbarschaften,
- kürzlich geänderte ACLs oder Firewallregeln.

---

11. DNS als gemeinsame Ursache erkennen

Wenn IP-Adressen erreichbar sind, Namen jedoch auf mehreren Clients nicht funktionieren:

```
nslookup <zielname>
```

```
Resolve-DnsName <zielname>
```

Konfigurierte DNS-Server anzeigen:

```
Get-DnsClientServerAddress
```

DNS-Port prüfen:

```
Test-NetConnection -ComputerName <dns-server> -Port 53
```

Ein erfolgreicher TCP-Test auf Port 53 ist kein vollständiger DNS-Funktionstest, da DNS abhängig von Anfrage und Umgebung UDP oder TCP verwenden kann.

Entscheidung

- alle Clients verwenden denselben nicht erreichbaren DNS-Server → DNS-Server oder Netzwerkpfad prüfen.
- nur ein VLAN erreicht den DNS-Server nicht → Routing, ACL oder Firewall prüfen.
- DNS-Server antwortet, löst aber interne Namen nicht auf → Zone, Einträge oder Replikation prüfen.
- interne Namen funktionieren, externe nicht → Weiterleitung oder externe DNS-Erreichbarkeit prüfen.
- externe Namen funktionieren, interne nicht → interne DNS-Zone, Suchsuffix oder verwendeten DNS-Server prüfen.
- Clients verwenden falsche DNS-Server → DHCP-Optionen oder statische Konfiguration prüfen.

DNS-Caches sollten nicht gleichzeitig auf allen Clients gelöscht werden. Zuerst muss geprüft werden, ob tatsächlich ein veralteter Cache-Eintrag vorliegt.

---

12. WLAN-Ausfall mehrerer Clients

Sind mehrere WLAN-Clients betroffen, zunächst unterscheiden:

```
Sind alle WLAN-Clients betroffen?
|
+-- Nein
|   |
|   +-- nur ein Access Point
|   |     -> AP, Uplink, Stromversorgung und Funkzelle prüfen
|   |
|   +-- nur eine SSID
|         -> SSID, Authentifizierung, RADIUS und VLAN prüfen
|
+-- Ja
    |
    +-- Ethernet funktioniert?
        |
        +-- Ja
        |   -> WLAN-Controller, zentrale AP-Verwaltung,
        |      RADIUS oder WLAN-Infrastruktur prüfen
        |
        +-- Nein
            -> gemeinsame Switching-, Routing- oder Dienstestörung prüfen
```

Zusätzlich prüfen:

- sind die Access Points erreichbar,
- erhalten sie Strom über PoE,
- ist der PoE-Budget-Grenzwert des Switches erreicht,
- besteht die Verbindung zum WLAN-Controller,
- wird die SSID ausgestrahlt,
- funktioniert RADIUS oder 802.1X,
- sind Zertifikate gültig,
- stimmt die Systemzeit,
- werden Clients dem vorgesehenen VLAN zugeordnet,
- funktioniert DHCP in diesem VLAN,
- besteht eine ungewöhnlich hohe Funkbelastung,

- trat der Fehler nach einer Konfigurationsänderung auf?

Wenn Clients mit dem WLAN verbunden sind, aber keine IP-Adresse erhalten, liegt nicht automatisch ein Funkproblem vor. Dann sind insbesondere VLAN und DHCP zu prüfen.

---

13. Redundanz- und Hochverfügbarkeitsfehler berücksichtigen

Eine vorhandene Redundanz garantiert nicht, dass die Umschaltung funktioniert hat.

Zu prüfen sind:

- Status beider Firewalls oder Router,
- aktive und passive Rolle,
- Zustand des Synchronisationslinks,
- gemeinsames virtuelles Gateway,
- Status redundanter Switch-Uplinks,
- Link Aggregation oder EtherChannel,
- Spanning-Tree-Zustand,
- DHCP-Failover,
- DNS-Redundanz,
- redundante WAN-Verbindungen,
- Standort-VPN-Tunnel,
- Zeitpunkt eines Failovers.

Mögliche Fehlerbilder:

- beide Systeme glauben, aktiv zu sein,
- kein System übernimmt die aktive Rolle,
- Zustände wurden nicht synchronisiert,
- virtuelle IP-Adresse ist nicht erreichbar,
- ein Teil der VLANs wurde nicht übernommen,
- Routing oder NAT fehlt nach der Umschaltung,
- ein redundanter Link ist physisch aktiv, transportiert aber nicht alle VLANs.

---

14. Änderungen und Zeitpunkte korrelieren

Vor Maßnahmen prüfen:

- wann begann die Störung,
- wurden Switch-, Firewall- oder Routerregeln geändert,
- wurde ein VLAN hinzugefügt oder entfernt,
- gab es ein Firmware- oder Betriebssystemupdate,
- wurde ein Access Point oder Switch ausgetauscht,
- wurde die Patchung verändert,
- gab es einen Stromausfall,

- wurde ein Zertifikat erneuert,
- wurde eine DHCP- oder DNS-Konfiguration geändert,
- fand ein Failover statt,
- meldet der Provider eine Störung?

Die zeitliche Nähe einer Änderung ist ein Hinweis, aber noch kein Beweis. Die vermutete Ursache muss durch passende Messwerte, Protokolle oder einen kontrollierten Rückbau bestätigt werden.

---

15. Beispiel für eine schnelle Diagnose

Symptom

Alle Clients eines Stockwerks melden seit 10:15 Uhr keine Netzwerkverbindung. Andere Stockwerke funktionieren.

Erste Eingrenzung

- Ethernet und WLAN des Stockwerks sind betroffen.
- Alle betroffenen Access Points und Netzwerkdosen führen über denselben Etagen-Switch.
- Clients anderer Etagen erreichen interne Systeme und das Internet.

Clientprüfung

```
ipconfig /all
```

Ergebnis auf mehreren Clients:

```
IPv4-Adresse: 169.254.x.x
Standardgateway:
DHCP aktiviert: Ja
```

Bewertung

- die Störung betrifft nicht nur einen Client,
- mehrere Clients erhalten keine DHCP-Konfiguration,
- Ethernet und WLAN besitzen dieselbe gemeinsame Infrastruktur,
- der Etagen-Switch oder dessen Uplink ist zu priorisieren.

Infrastrukturprüfung

- Etagen-Switch ist eingeschaltet,
- Clientports besitzen Link,
- Uplink-Port ist jedoch ohne Verbindung,
- Gegenstelle zeigt ebenfalls keinen Link.

Festgestellte Ursache

Ein defekter Transceiver hat den Uplink des Etagen-Switches unterbrochen.

Kontrollierte Maßnahme

Der defekte Transceiver wurde nach Freigabe durch ein geprüftes Ersatzgerät ersetzt.

Nachprüfung

- Uplink ist stabil aktiv,
- erforderliche VLANs werden transportiert,
- Clients erhalten gültige DHCP-Adressen,
- Gateways sind erreichbar,
- interne Systeme sind erreichbar,
- externe IP-Verbindung funktioniert,
- DNS-Auflösung funktioniert,
- Ethernet- und WLAN-Clients wurden getestet,
- Schnittstellenfehler und Protokolle wurden erneut geprüft,
- Ursache und Austausch wurden dokumentiert.

---

16. Ungeeignete Sofortmaßnahmen

Nicht als erste Maßnahme verwenden:

- alle betroffenen Clients neu starten,
- Switch oder Router ohne Diagnose neu starten,
- Firewall ungeprüft deaktivieren,
- VLAN-Zuordnungen versuchsweise ändern,
- Switchports wahllos deaktivieren und aktivieren,
- DHCP-Leases auf allen Clients freigeben,
- allen Clients statische Adressen geben,
- öffentliche DNS-Server eintragen,
- Spanning Tree deaktivieren,
- redundante Links ungeprüft umstecken,
- Firewallregeln vollständig zurücksetzen,
- mehrere Infrastrukturänderungen gleichzeitig durchführen,
- funktionierende Konfigurationen überschreiben,
- Werkseinstellungen laden.

Solche Maßnahmen können den Fehler vergrößern, Diagnoseinformationen vernichten oder weitere Netzwerkbereiche beeinträchtigen.

---

17. Vollständige Schnellprüfreihenfolge

1. genaue Fehlermeldung und Beginn erfassen.
2. Anzahl und Standort der betroffenen Clients bestimmen.
3. funktionierende Vergleichsclients suchen.
4. gemeinsame Switches, VLANs, Access Points oder Dienste ermitteln.
5. Ethernet und WLAN getrennt vergleichen.
6. Adapter- und Linkstatus mehrerer Clients prüfen.
7. IP-Konfiguration mehrerer Clients vergleichen.
8. auf `169.254.x.x`, falsche Subnetze oder fehlende Gateways achten.
9. DHCP-Dienst, Bereich und Relay prüfen.
10. Gateway jedes betroffenen VLANs testen.
11. lokales Vergleichsziel testen.
12. externe IP-Adresse testen.
13. DNS-Auflösung getrennt prüfen.
14. benötigten Zielport prüfen.
15. Switchstatus und Uplinks untersuchen.
16. VLAN- und Trunk-Konfiguration prüfen.
17. Spanning Tree und Portschutz berücksichtigen.
18. Firewall, NAT und Routing prüfen.
19. WAN- und Standortverbindungen prüfen.
20. Redundanz- und Failoverstatus prüfen.
21. Ereignisse mit dem Fehlerbeginn korrelieren.
22. letzte Änderungen ermitteln.
23. eine gemeinsame Ursache als Hypothese formulieren.
24. genau eine kontrollierte Maßnahme durchführen.
25. dieselben Tests nach der Änderung wiederholen.
26. alle zuvor betroffenen Bereiche testen.
27. Überwachung und Protokolle kontrollieren.
28. temporäre Diagnoseänderungen entfernen.
29. Ursache, Maßnahme und Nachweis dokumentieren.

---

18. Checkliste „Mehrere Clients haben kein Netzwerk“

- [ ] Beginn und genaue Auswirkung der Störung sind dokumentiert.
- [ ] die betroffenen Clients und Standorte sind bekannt.
- [ ] funktionierende Vergleichsclients wurden geprüft.
- [ ] gemeinsame Switches, VLANs oder Access Points wurden ermittelt.
- [ ] Ethernet und WLAN wurden getrennt betrachtet.
- [ ] interne und externe Ziele wurden unterschieden.
- [ ] Linkstatus mehrerer Clients wurde geprüft.
- [ ] IP-Konfigurationen wurden miteinander verglichen.
- [ ] DHCP-Ausfall oder falscher DHCP-Bereich wurde berücksichtigt.
- [ ] freie DHCP-Leases wurden geprüft.

- [ ] DHCP-Relay wurde bei Bedarf geprüft.
- [ ] Standardgateways wurden getestet.
- [ ] lokale Vergleichsziele wurden getestet.
- [ ] externe IP-Ziele wurden getestet.
- [ ] DNS wurde getrennt von der IP-Erreichbarkeit geprüft.
- [ ] betroffene Zielports wurden geprüft.
- [ ] Switchstatus und Stromversorgung wurden kontrolliert.
- [ ] Switch-Uplinks wurden geprüft.
- [ ] Interfacefehler und Port-Flaps wurden berücksichtigt.
- [ ] VLAN- und Trunk-Konfigurationen wurden geprüft.
- [ ] Spanning-Tree-Zustand wurde berücksichtigt.
- [ ] Port-Security oder Errdisable wurde geprüft.
- [ ] Firewallregeln und ACLs wurden berücksichtigt.
- [ ] Routing und Standardroute wurden geprüft.
- [ ] NAT und Internetübergang wurden geprüft.
- [ ] WAN- oder Standortverbindungen wurden geprüft.
- [ ] WLAN-Controller, RADIUS und PoE wurden bei Bedarf geprüft.
- [ ] Hochverfügbarkeits- und Failoverstatus wurde kontrolliert.
- [ ] letzte Änderungen wurden mit dem Fehlerbeginn verglichen.
- [ ] vor Eingriffen wurden Protokolle und Zustände gesichert.
- [ ] nur eine kontrollierte Änderung wurde durchgeführt.
- [ ] dieselben Tests wurden anschließend wiederholt.
- [ ] alle betroffenen Clientgruppen funktionieren wieder.
- [ ] die Infrastrukturüberwachung zeigt einen stabilen Zustand.
- [ ] Ursache, Maßnahme und Nachweis wurden dokumentiert.

---

19. Schnellreferenz

Ergebnis	Nächster Schritt
nur ein Client betroffen	Entscheidungsbaum 7.1 verwenden
alle Clients eines Switches betroffen	Switch, Stromversorgung und Uplink prüfen
nur ein VLAN betroffen	VLAN, Gateway, DHCP, ACL und Trunk prüfen
nur ein Access Point betroffen	AP, PoE, Uplink und Funkzelle prüfen
nur eine SSID betroffen	SSID, RADIUS, Zertifikate und VLAN-Zuweisung prüfen

Ergebnis	Nächster Schritt
alle WLAN-Clients betroffen	Controller, RADIUS oder zentrale WLAN-Infrastruktur prüfen
Ethernet und WLAN betroffen	gemeinsame Switching-, Routing- oder Dienstekomponente prüfen
mehrere Clients mit `169.254.x.x`	DHCP-Pfad prüfen
bestehende Clients funktionieren, neue nicht	DHCP-Bereich oder DHCP-Dienst prüfen
falsches Subnetz wird vergeben	VLAN, DHCP-Relay oder fremden DHCP-Server prüfen
Gateway eines VLANs nicht erreichbar	SVI, VLAN, Trunk oder Firewall prüfen
Gateway erreichbar, externe IP nicht	Routing, NAT, Firewall oder WAN prüfen
externe IP erreichbar, Name nicht	DNS prüfen
nur ein Dienst betroffen	Zielsystem, Port, Firewall oder Proxy prüfen
gesamter Standort betroffen	Core, Firewall, Router, WAN oder Stromversorgung prüfen
Ausfall nach Änderung	Änderung mit Protokollen und Vergleichstest überprüfen
Fehler nach Neustart verschwunden	Ursache nicht bewiesen; Protokolle weiter auswerten

---

Merksatz

> Je mehr Clients gleichzeitig betroffen sind, desto wichtiger ist ihre gemeinsame Abhängigkeit. Suche zuerst nach dem gemeinsamen Switch, VLAN, Access Point, Gateway oder zentralen Dienst – nicht nach identischen Einzeldefekten an allen Endgeräten.

Quellen und weiterführende Dokumentation

- Microsoft Learn – DHCP troubleshooting guidance
- Microsoft Learn – Troubleshoot problems on the DHCP server
- Microsoft Learn – Troubleshoot problems on the DHCP client
- Microsoft Learn – Get-DhcpServerv4Scope
- Microsoft Learn – Get-DhcpServerv4ScopeStatistics
- Microsoft Learn – Get-DhcpServerv4Binding
- Microsoft Learn – Get-DhcpServerv4Failover
- Microsoft Learn – ipconfig
- Microsoft Learn – ping
- Microsoft Learn – tracert

- Microsoft Learn – Get-NetAdapter
- Microsoft Learn – Get-NetRoute
- Microsoft Learn – Get-NetNeighbor
- Microsoft Learn – Test-NetConnection
- Microsoft Learn – Resolve-DnsName
- Cisco – Troubleshoot STP problems and related design considerations
- Cisco – Spanning Tree Protocol documentation
