6.2 Mehrere Clients oder ganzer Standort ohne Netzwerk

Wenn mehrere Clients, eine Abteilung, ein Stockwerk, ein Gebäude oder ein kompletter Standort gleichzeitig keine Netzwerkverbindung besitzen, ist ein unabhängiger Fehler an jedem einzelnen Endgerät unwahrscheinlich. Der gemeinsame Ausfallbereich rückt in den Mittelpunkt.

Mögliche gemeinsame Komponenten sind:

- Access Switch,
- Switch-Uplink,
- VLAN,
- WLAN-SSID,
- Access Point oder WLAN-Controller,
- Standardgateway,
- DHCP-Dienst,
- DNS-Dienst,
- Firewall,
- Router,
- WAN-Verbindung,
- VPN-Tunnel,
- Internetanschluss,
- Stromversorgung,
- zentrale Authentifizierung,
- Netzwerkzugangskontrolle,
- Providerverbindung,
- gemeinsame Konfigurationsänderung.

Das Ziel der Fehleranalyse besteht darin, den kleinsten gemeinsamen Ausfallbereich zu bestimmen und anschließend die darin enthaltenen Komponenten kontrolliert zu prüfen.

> Je mehr Systeme gleichzeitig betroffen sind, desto wichtiger ist die Frage, welche technische Komponente oder Abhängigkeit sie gemeinsam verwenden.

---

1. Mehrere betroffene Clients verändern die Fehlerhypothese

Bei einem einzelnen betroffenen Client sind lokale Ursachen besonders wahrscheinlich:

- Netzwerkkabel,
- Netzwerkadapter,
- Dockingstation,

- lokale IP-Konfiguration,
- lokaler Treiber,
- lokale Firewall,
- Betriebssystem,
- Benutzerprofil.

Bei mehreren gleichzeitig betroffenen Clients werden gemeinsame Ursachen wahrscheinlicher:

- gemeinsamer Switch,
- gemeinsamer Uplink,
- gemeinsames VLAN,
- gemeinsames Gateway,
- gemeinsamer DHCP-Server,
- gemeinsamer DNS-Server,
- gemeinsamer WLAN-Bereich,
- gemeinsame Firewall,
- gemeinsame Standortanbindung,
- gemeinsame Änderung.

Lokale Clienttests bleiben wichtig. Sie dienen nun jedoch vor allem dazu, den gemeinsamen Fehlerumfang zu bestätigen und Unterschiede zwischen funktionierenden und nicht funktionierenden Bereichen zu erkennen.

---

2. Störungsumfang exakt bestimmen

Die Aussage „Der Standort hat kein Netzwerk“ ist zunächst nur eine ungenaue Symptombeschreibung.

Zu klären sind:

- Wie viele Benutzer melden den Fehler?
- Wie viele Clients wurden tatsächlich geprüft?
- Sind alle Geräte oder nur einzelne Gerätetypen betroffen?
- Betrifft der Fehler Ethernet, WLAN oder beide?
- Sind Drucker, Telefone, Kameras und andere Netzwerkgeräte betroffen?
- Betrifft der Fehler nur einen Raum?
- Betrifft er eine Etage?
- Betrifft er ein Gebäude?
- Betrifft er ein VLAN?
- Betrifft er eine bestimmte SSID?
- Betrifft er einen kompletten Standort?
- Sind weitere Standorte betroffen?
- Funktionieren interne Ziele?
- Funktioniert das Internet?
- Funktioniert die Namensauflösung?
- Sind nur einzelne Anwendungen ausgefallen?

- Können bestehende Verbindungen weiterarbeiten?
- Scheitern nur neue Verbindungen?
- Ist der Ausfall vollständig oder treten Paketverluste und Unterbrechungen auf?

Eine belastbare Aussage lautet beispielsweise:

> Seit etwa 09:17 Uhr können alle bisher geprüften kabelgebundenen Clients der dritten Etage weder das Standardgateway noch interne Dienste erreichen. WLAN-Clients derselben Etage funktionieren. Andere Etagen sind nicht betroffen.

Diese Beschreibung grenzt den Fehler erheblich stärker ein als „Netzwerk ausgefallen“.

---

3. Betroffenheitsmatrix erstellen

Eine einfache Matrix hilft, Gemeinsamkeiten zu erkennen.

Bereich	Ethernet	WLAN	interne Dienste	Internet	DNS
Etage 1	funktioniert	funktioniert	funktioniert	funktioniert	funktioniert
Etage 2	funktioniert	funktioniert	funktioniert	funktioniert	funktioniert
Etage 3	ausgefallen	funktioniert	ausgefallen	ausgefallen	nicht sinnvoll prüfbar
Etage 4	funktioniert	funktioniert	funktioniert	funktioniert	funktioniert

Aus diesem Beispiel ergibt sich:

- kein standortweiter Ausfall,
- kein allgemeiner Internet- oder DNS-Ausfall,
- kein vollständiger Ausfall des zentralen Gateways,
- wahrscheinlicher Fehler im kabelgebundenen Zugangsnetz der dritten Etage,
- möglicher Access-Switch-, Uplink-, VLAN- oder Stromversorgungsfehler.

Eine solche Matrix sollte nicht nur auf Benutzerangaben beruhen. Repräsentative Tests müssen die Angaben bestätigen.

---

4. Zeitpunkt und zeitlichen Verlauf ermitteln

Zu dokumentieren sind:

- erster bekannter Fehlerzeitpunkt,
- letzte bekannte fehlerfreie Nutzung,
- gleichzeitiger oder schrittweiser Ausfall,

- dauerhafter oder sporadischer Fehler,
- Zeitpunkt automatischer Monitoringmeldungen,
- Zeitpunkt letzter Änderungen,
- Zeitpunkt von Strom-, Klima- oder Providerereignissen,
- Wiederkehr in bestimmten Zeitabständen,
- Abhängigkeit von Last oder Benutzeranzahl.

Mögliche zeitliche Muster

Beobachtung	mögliche Einordnung
alle Clients fallen gleichzeitig aus	gemeinsame zentrale Komponente oder Verbindung
Clients fallen nacheinander aus	DHCP-Leases, instabiler Switch, Schleife, Überlastung oder Stromproblem
nur morgens bei Arbeitsbeginn	DHCP-Bereich, Authentifizierung, WLAN-Kapazität oder Lastproblem
kurze Ausfälle in regelmäßigen Abständen	Redundanzumschaltung, instabiler Link, Routingprozess oder geplante Aufgabe
Fehler direkt nach Änderung	Änderung als starke Hypothese untersuchen
Fehler bei hoher Netzlast	Überlastung, Broadcast-Sturm, fehlerhafter Link oder Kapazitätsgrenze
Fehler nach Stromunterbrechung	Gerät, Netzteil, USV, Startreihenfolge oder nicht gespeicherte Konfiguration

Zeitliche Nähe beweist noch keine Ursache. Sie legt jedoch eine gezielte Prüfreihenfolge nahe.

---

5. Letzte Änderungen prüfen

Vor einer Änderung am Netzwerk ist zu prüfen, ob kurz vor Beginn der Störung etwas verändert wurde.

Mögliche Änderungen sind:

- Switch-Konfiguration,
- VLAN-Zuordnung,
- Trunk-Konfiguration,
- Spanning-Tree-Konfiguration,
- Link Aggregation,
- Routing,
- Firewallregeln,
- NAT,
- DHCP-Bereich,
- DHCP-Relay,
- DNS-Konfiguration,
- WLAN-Controller,

- Access-Point-Firmware,
- Netzwerkzugangskontrolle,
- Zertifikate,
- Provideranschluss,
- Verkabelung,
- Patchfeld,
- Stromversorgung,
- Server- oder Netzwerkupdate,
- Wartungsarbeiten,
- Umzug von Geräten,
- Anschluss eines neuen Switches,
- Anschluss eines nicht autorisierten Geräts.

Zu jeder Änderung gehören:

- genauer Zeitpunkt,
- verantwortliche Person oder System,
- betroffene Komponenten,
- erwartete Wirkung,
- dokumentierter Ausgangszustand,
- mögliche Rückfallmaßnahme,
- tatsächliche Protokolleinträge.

> Ein zeitlicher Zusammenhang macht eine Änderung verdächtig, ersetzt aber nicht den technischen Nachweis.

---

6. Priorität und Auswirkung bewerten

Ein Ausfall mehrerer Clients kann ein Major Incident sein, muss es aber nicht automatisch sein.

Zu bewerten sind:

- Anzahl betroffener Benutzer,
- betroffene Geschäftsprozesse,
- betroffene Standorte,
- verfügbare Ausweichmöglichkeiten,
- Sicherheitsauswirkungen,
- Produktionsstillstand,
- Ausfall kritischer Dienste,
- vertragliche Verpflichtungen,
- erwartete Dauer,
- Gefahr einer Ausweitung,
- Abhängigkeit externer Kunden oder Partner.

Beispielhafte Einordnung

Situation	mögliche Auswirkung
ein Besprechungsraum ohne Netzwerk	lokal begrenzt
gesamtes Stockwerk ohne Netzwerk	erhebliche Benutzerbeeinträchtigung
Produktionsnetz ausgefallen	geschäftskritisch
Standort ohne WAN, lokale Systeme funktionieren	standortübergreifende Dienste betroffen
DNS unternehmensweit ausgefallen	sehr großer scheinbarer Netzwerkausfall
redundanter Uplink ausgefallen, Verkehr läuft weiter	noch kein Benutzerausfall, aber Redundanz verloren

Die Priorität richtet sich nach Auswirkung und Dringlichkeit, nicht allein nach der Anzahl eingehender Tickets.

---

7. Kommunikation während einer größeren Störung

Bei einer größeren Störung müssen technische Analyse und Kommunikation parallel organisiert werden.

Sinnvolle Aufgabenverteilung:

- technische Koordination,
- Prüfung des Zugangsnetzes,
- Prüfung zentraler Dienste,
- Prüfung von Firewall, WAN und Provider,
- Dokumentation der Ereignisse,
- Kommunikation mit Benutzern und Verantwortlichen,
- Koordination externer Dienstleister.

Eine Statusmeldung sollte enthalten:

```
Bekannter Umfang:
Kabelgebundene Clients in Gebäude B sind betroffen.
WLAN und andere Gebäude funktionieren.

Beginn:
Etwa 09:17 Uhr.

Aktueller Stand:
Der gemeinsame Uplink des Access-Bereichs wird geprüft.
```

```
Nächste Aktualisierung:
10:00 Uhr oder bei einer wesentlichen Änderung.
```

Nicht bestätigt werden sollten Aussagen wie:

- „Der Provider ist schuld.“
- „Die Firewall ist abgestürzt.“
- „Das Problem ist gleich behoben.“
- „Es gehen keine Daten verloren.“

Solche Aussagen dürfen erst erfolgen, wenn belastbare Nachweise vorliegen.

---

8. Repräsentative Testpunkte auswählen

Nicht jeder einzelne Client muss vollständig untersucht werden. Es werden gezielt Testpunkte ausgewählt.

Geeignete Auswahl:

- ein betroffener Client aus jedem gemeldeten Bereich,
- ein funktionierender Client aus einem benachbarten Bereich,
- ein kabelgebundener und ein drahtloser Client,
- ein Client im gleichen VLAN,
- ein Client in einem anderen VLAN,
- ein infrastrukturelles Gerät im betroffenen Bereich,
- ein Test direkt am Access Switch,
- ein Test hinter dem vermuteten Uplink,
- ein Test am zentralen Standort.

Beispiel

```
Client A: Etage 3, Switch 3A, VLAN 120 → betroffen
Client B: Etage 3, Switch 3B, VLAN 120 → betroffen
Client C: Etage 3, WLAN, VLAN 220 → funktioniert
Client D: Etage 2, VLAN 120 → funktioniert
```

Damit liegt der Verdacht nicht automatisch beim gesamten VLAN 120. Wahrscheinlicher ist zunächst eine Komponente, die nur die kabelgebundene Versorgung der dritten Etage betrifft.

---

9. Gemeinsame Abhängigkeiten abbilden

Für die betroffenen Clients sollte der Kommunikationsweg vereinfacht dargestellt werden.

```
Clients
→ Access Switch
→ Uplink
→ Distribution Switch
→ VLAN-Gateway
→ Firewall oder Router
→ WAN beziehungsweise Internet
→ Zielsystem
```

Für WLAN kann der Weg abweichen:

```
WLAN-Client
→ Access Point
→ Access Switch
→ WLAN-Controller oder lokales Switching
→ VLAN-Gateway
→ Firewall oder Router
→ Zielsystem
```

Für jeden Abschnitt wird geprüft:

- Nutzen alle betroffenen Clients diese Komponente?
- Nutzen funktionierende Clients dieselbe Komponente?
- Ist die Komponente erreichbar?
- Sind Fehler oder Zustandsänderungen protokolliert?
- Besteht eine redundante Verbindung?
- Arbeitet die Redundanz tatsächlich?
- Wurde die Konfiguration verändert?

---

10. Ausfallbereich durch funktionierende Grenzen bestimmen

Nicht nur fehlgeschlagene Tests sind wichtig. Funktionierende Bereiche bilden Grenzen des Fehlers.

Beispiel

```
Clients an Switch A → ausgefallen
Clients an Switch B → funktionieren
beide verwenden dasselbe Gateway
beide verwenden dieselben DNS-Server
beide verwenden dieselbe Firewall
```

Dadurch werden Gateway, DNS und Firewall als alleinige gemeinsame Ursache weniger wahrscheinlich. Der Untersuchungsbereich verschiebt sich zu:

- Switch A,
- dessen Uplink,
- dessen VLAN-Weiterleitung,
- dessen Stromversorgung,
- dessen lokale Verkabelung.

Ein funktionierender Bereich schließt eine Komponente allerdings nur dann sinnvoll aus, wenn tatsächlich dieselbe Instanz, derselbe Pfad und dieselbe Konfiguration verwendet werden.

---

11. Stromversorgung und Umgebungsbedingungen prüfen

Ein Netzwerkausfall kann durch einen Strom- oder Umgebungsfehler verursacht werden.

Zu prüfen sind:

- besitzt der Netzwerkschrank Strom?
- ist die USV aktiv?
- bestehen USV-Alarme?
- sind Sicherungen ausgelöst?
- funktionieren Netzteile und redundante Netzteile?
- sind Power Distribution Units aktiv?
- ist der Switch vollständig gestartet?
- bestehen Temperaturalarme?
- funktioniert die Kühlung?
- wurden Geräte versehentlich ausgeschaltet?
- sind PoE-Verbraucher ausgefallen?
- wurde das Strombudget überschritten?
- gibt es auffälligen Geruch, Hitze oder Geräusche?

Bei ausgefallener PoE-Versorgung können gleichzeitig betroffen sein:

- Access Points,
- IP-Telefone,
- Kameras,
- Zutrittskomponenten,
- Sensoren.

Ein aktiver Switch kann weiterhin ein PoE-Problem besitzen. Deshalb müssen Datenverkehr und Stromversorgung getrennt bewertet werden.

---

12. Physische Infrastruktur prüfen

Bei mehreren betroffenen Clients sind besonders gemeinsame physische Komponenten zu untersuchen:

- Access Switch,
- Switch-Uplink,
- Glasfaserstrecke,
- Kupfer-Uplink,
- Patchkabel,
- Patchfeld,
- Transceiver,
- Medienkonverter,
- Stack-Kabel,
- Modul oder Line Card,
- Gebäudeverkabelung.

Mögliche Hinweise:

- Uplink ohne Link,
- Link wechselt zwischen Up und Down,
- hohe Anzahl CRC-Fehler,
- Eingabefehler,
- Verwerfungen,
- fehlerhafte Transceiverwerte,
- nur eine Richtung funktioniert,
- ungewöhnlich niedrige ausgehandelte Geschwindigkeit,
- Port befindet sich im Fehlerzustand,
- Switch-Mitglied fehlt aus einem Stack,
- Line Card ist ausgefallen.

Typische Zähler

Zähler oder Zustand	mögliche Bedeutung
CRC-Fehler	physische Übertragungsfehler, Kabel, Stecker oder Transceiver
Input Errors	unterschiedliche Empfangsfehler
Output Drops	Warteschlange oder Überlastung
Link Flaps	instabile Verbindung oder Komponente
administratively down	Schnittstelle wurde deaktiviert
err-disabled	Schutzfunktion oder erkannter Fehler
keine optische Empfangsleistung	Glasfaser, Transceiver oder Gegenstelle
viele Interface-Resets	instabiler Port, Treiber oder Hardware

Zähler müssen zusammen mit Laufzeit, Verkehrsmenge und Änderungsrate bewertet werden. Ein historischer Fehlerzähler beweist keinen aktuellen Defekt.

---

13. Access Switch prüfen

Zu einem betroffenen Access Switch sollten mindestens folgende Informationen erhoben werden:

- Erreichbarkeit des Managements,
- Betriebszeit,
- letzter Neustart,
- CPU-Auslastung,
- Speicherauslastung,
- Temperatur,
- Netzteilstatus,
- Stack-Status,
- Uplink-Status,
- Fehlerzähler,
- VLAN-Zustand,
- Spanning-Tree-Zustand,
- MAC-Adresstabelle,
- Port-Sicherheitszustände,
- PoE-Status,
- Systemprotokolle,
- aktuelle Konfiguration,
- letzte Konfigurationsänderung.

Mögliche Befehle hängen von Hersteller und Betriebssystem ab. Bei Cisco-IOS-ähnlichen Systemen können beispielsweise relevant sein:

```
show interfaces status
show interfaces counters errors
show interfaces <schnittstelle>
show logging
show vlan brief
show interfaces trunk
show spanning-tree
show etherchannel summary
show mac address-table
show power inline
show environment
show switch
show version
```

Diese Befehle sind Beispiele. Syntax und Verfügbarkeit müssen anhand der Dokumentation des eingesetzten Geräts geprüft werden.

---

14. Uplink und Trunk untersuchen

Ein Access Switch kann erreichbar sein, während Nutzdaten wegen eines fehlerhaften Uplinks oder Trunks nicht korrekt übertragen werden.

Zu prüfen sind:

- physischer Linkstatus,
- Geschwindigkeit und Duplex,
- erlaubte VLANs,
- native beziehungsweise untagged VLAN-Zuordnung,
- Trunk-Modus,
- VLAN-Pruning,
- Gegenstellenkonfiguration,
- Fehlerzähler,
- Spanning-Tree-Zustand,
- Link Aggregation,
- Port-Sicherheitsmechanismen,
- MTU,
- einseitige Konfigurationsänderung.

Typische Fehler

- benötigtes VLAN nicht auf dem Trunk erlaubt,
- VLAN nur auf einer Seite konfiguriert,
- falsches untagged VLAN,
- Uplink als Access-Port konfiguriert,
- Trunk nach Änderung nicht vollständig übernommen,
- Port durch Spanning Tree blockiert,
- Mitglied einer Link Aggregation fehlerhaft,
- Transceiver oder Faser gestört,
- Uplink physisch aktiv, aber Datenverkehr verworfen.

> Ein aktiver Link bestätigt weder eine korrekte Trunk-Konfiguration noch die Weiterleitung aller benötigten VLANs.

---

15. VLAN-Zuordnung prüfen

Wenn nur bestimmte Benutzergruppen oder Netzsegmente betroffen sind, ist die VLAN-Konfiguration ein zentraler Prüfpunkt.

Zu prüfen sind:

- existiert das VLAN auf allen notwendigen Switches?
- sind Access-Ports dem richtigen VLAN zugeordnet?
- wird das VLAN über alle erforderlichen Trunks transportiert?
- besitzt das VLAN ein aktives Gateway?
- ist DHCP beziehungsweise DHCP-Relay für dieses VLAN erreichbar?
- blockieren Sicherheitsfunktionen den Verkehr?
- stimmen Voice- und Data-VLAN?
- bestehen dynamische VLAN-Zuweisungen?
- verwendet die Netzwerkzugangskontrolle das erwartete VLAN?
- wurde das VLAN umbenannt, gelöscht oder neu nummeriert?

Mögliche Beobachtungen

Beobachtung	mögliche Einordnung
nur ein VLAN betroffen	VLAN-Pfad, Gateway, DHCP oder Richtlinie
mehrere VLANs desselben Switches betroffen	Switch oder gemeinsamer Uplink
VLAN funktioniert auf anderen Switches	lokaler Trunk oder Access Switch
Clients erhalten Adresse aus falschem Netz	falsche VLAN-Zuordnung oder unerwarteter DHCP-Server
statisch konfigurierte Clients funktionieren, DHCP-Clients nicht	DHCP-Pfad oder DHCP-Dienst
Gateway im VLAN nicht per ARP erreichbar	Layer-2-Pfad, Gateway oder VLAN-Zuordnung

---

16. Spanning Tree und Netzwerkschleifen

Spanning Tree verhindert Layer-2-Schleifen in redundanten Ethernet-Netzen. Fehlerhafte Verkabelung oder Konfiguration kann dennoch zu einer Schleife oder instabilen Topologie führen.

Mögliche Symptome:

- sehr hohe Broadcast-Last,
- stark schwankende MAC-Adresstabellen,
- MAC-Adressen erscheinen abwechselnd an verschiedenen Ports,
- hohe CPU-Auslastung auf Switches,
- Paketverluste,
- langsame oder vollständig ausfallende Verbindungen,
- häufige Topology Changes,
- Managementzugriff nur sporadisch möglich,
- mehrere Bereiche gleichzeitig betroffen,
- Ausfall nach Anschluss eines kleinen Switches oder neuen Kabels.

Zu prüfen sind:

- Root Bridge,
- blockierende und weiterleitende Ports,
- letzte Topology Changes,
- Anzahl der Topology Changes,
- unerwartete Root-Bridge-Änderung,
- BPDU Guard,
- Root Guard,
- Loop Guard,
- PortFast beziehungsweise Edge-Port-Konfiguration,
- neu angeschlossene Switches,
- doppelte Verkabelung.

> Bei Verdacht auf eine Schleife dürfen nicht wahllos Verbindungen getrennt werden. Zuerst müssen Topologie, betroffene Ports und aktuelle Zustände soweit möglich dokumentiert werden.

---

17. Link Aggregation und LACP prüfen

Mehrere physische Verbindungen können zu einer logischen Verbindung zusammengefasst sein.

Zu prüfen sind:

- sind alle erwarteten Mitglieder aktiv?
- befinden sich beide Seiten in derselben Aggregation?
- stimmen LACP-Modus und Parameter?
- verwenden alle Mitglieder identische VLAN- und Trunk-Einstellungen?
- bestehen einzelne suspendierte oder nicht gebündelte Ports?
- ist die Hash-Verteilung auffällig?
- funktionieren bestimmte Verbindungen nur über ein einzelnes fehlerhaftes Mitglied?
- ist bei einem Gerätetausch eine alte Konfiguration verblieben?

Mögliche Symptome:

- nur einige Verbindungen funktionieren,
- bestimmte Quell-Ziel-Kombinationen scheitern,
- Paketverluste treten abhängig vom Verkehrsfluss auf,
- Durchsatz ist deutlich reduziert,
- Redundanz ist verloren,
- MAC-Adressen wechseln unerwartet,
- ein Mitglied leitet außerhalb des Bündels weiter.

---

18. Gateway und First-Hop-Redundanz prüfen

Das Gateway eines VLANs kann physisch oder logisch ausgefallen sein.

Zu prüfen sind:

- ist die Gateway-Schnittstelle aktiv?
- ist die virtuelle Gateway-Adresse vorhanden?
- antwortet das Gateway auf ARP beziehungsweise Neighbor Discovery?
- besitzen Clients den richtigen Gateway-Eintrag?
- ist die Gateway-MAC-Adresse plausibel?
- ist die Routingfunktion aktiv?
- besteht die verbundene Route?
- funktionieren andere VLANs auf demselben Gerät?
- bestehen CPU-, Speicher- oder Hardwareprobleme?
- funktioniert ein redundantes Gatewaypaar?
- stimmen aktive und passive Rollen?
- trat ein Rollenwechsel auf?
- besteht ein Split-Brain- oder Dual-Active-Zustand?
- wird der Rückweg korrekt geroutet?

Bei Redundanzprotokollen wie HSRP oder VRRP muss nicht nur der Gerätezustand, sondern auch die tatsächliche Erreichbarkeit der virtuellen Adresse geprüft werden.

Eine als aktiv gemeldete Redundanzrolle beweist nicht automatisch, dass:

- die Datenebene funktioniert,
- alle VLANs übertragen werden,
- die Upstream-Verbindung erreichbar ist,
- der Rückweg vorhanden ist.

---

19. DHCP bei mehreren betroffenen Clients prüfen

Wenn viele Clients keine verwendbare IP-Konfiguration erhalten, kann eine gemeinsame DHCP-Störung vorliegen.

Mögliche Symptome:

- Adressen aus `169.254.0.0/16`,
- kein Standardgateway,
- fehlende DNS-Server,
- alte Leases funktionieren noch,
- neue Clients erhalten keine Adresse,
- Clients erhalten Adressen aus dem falschen Netz,
- Fehler beginnt bei hoher Benutzeranzahl,
- nur ein bestimmtes VLAN ist betroffen.

Zu prüfen sind:

- läuft der DHCP-Dienst?
- ist der DHCP-Server erreichbar?
- ist der richtige Bereich aktiv?
- sind freie Adressen vorhanden?
- stimmen Subnetzmaske, Gateway und DNS-Optionen?
- funktioniert DHCP-Relay?
- ist die Relay-Adresse korrekt?
- wird DHCP durch ACLs oder Firewalls blockiert?
- besteht DHCP Snooping?
- sind vertrauenswürdige Ports korrekt festgelegt?
- antwortet ein unerwünschter DHCP-Server?
- funktionieren redundante DHCP-Server?
- stimmt der Failover-Zustand?
- erreichen Discover-Pakete den Server?
- erreicht das Offer den Client?

DHCP-Ablauf

```
Client → DHCP Discover
Server → DHCP Offer
Client → DHCP Request
Server → DHCP Acknowledgement
```

Mögliche Beobachtungen

Beobachtung	mögliche Einordnung
kein Discover sichtbar	Client, Access-Port, VLAN oder Aufzeichnungsstelle
Discover im VLAN, aber nicht am Server	Relay, Routing, ACL oder VLAN-Pfad
Discover erreicht Server, kein Offer	Dienst, Bereich, Richtlinie oder Adressmangel
Offer verlässt Server, erreicht Client nicht	Rückweg, Relay, Snooping oder Layer 2
falscher Server antwortet	Rogue DHCP oder falscher gemeinsamer Layer-2-Bereich
alte Clients funktionieren, neue nicht	erschöpfter Bereich oder gestörter Vergabeprozess

---

20. DNS-Ausfall nicht mit vollständigem Netzwerkausfall verwechseln

Ein zentraler DNS-Ausfall kann bei vielen Benutzern den Eindruck erzeugen, das Netzwerk sei vollständig ausgefallen.

Typische Beobachtungen:

- Ziele sind per IP-Adresse erreichbar,

- Namen können nicht aufgelöst werden,
- bereits bestehende Sitzungen funktionieren teilweise weiter,
- Anwendungen mit zwischengespeicherten Adressen funktionieren,
- Anmeldungen und Active-Directory-Funktionen scheitern,
- interne und externe Namen verhalten sich unterschiedlich.

Zu prüfen sind:

- Erreichbarkeit der DNS-Server per IP,
- DNS-Dienstzustand,
- Abfrage eines bekannten internen Namens,
- Abfrage eines bekannten externen Namens,
- Antwort jedes konfigurierten DNS-Servers,
- Rekursion,
- Weiterleitungen,
- Zonen,
- Replikation,
- DNSSEC, sofern eingesetzt,
- Firewallregeln für UDP und TCP Port 53,
- ausgegebene DHCP-DNS-Optionen,
- Split-DNS,
- Standort- oder VPN-spezifische DNS-Server.

Windows

```
Resolve-DnsName <name>
Resolve-DnsName <name> -Server <dns-server>
Get-DnsClientServerAddress
```

Linux und macOS

```
dig <name>
dig @<dns-server> <name>
```

> Ein DNS-Fehler betrifft die Namensauflösung. Er beweist keinen Ausfall der zugrunde liegenden IP-Verbindung.

---

21. Netzwerkzugangskontrolle und Authentifizierung

In Unternehmensnetzen kann der Netzwerkzugang von einer Authentifizierung oder Autorisierung abhängen.

Mögliche Komponenten:

- IEEE 802.1X,
- RADIUS,
- Network Access Control,
- Zertifikatsdienste,
- Geräteidentifikation,
- dynamische VLAN-Zuweisung,
- Quarantäne-VLAN,
- MAC Authentication Bypass,
- Port-Security.

Mögliche Symptome:

- viele Ports wechseln gleichzeitig in einen nicht autorisierten Zustand,
- Clients erhalten ein Quarantäne-VLAN,
- kabelgebundene und drahtlose Anmeldungen scheitern,
- neue Verbindungen scheitern, bestehende funktionieren,
- Fehler beginnt nach Ablauf eines Zertifikats,
- RADIUS-Server ist nicht erreichbar,
- Uhrzeitabweichungen verhindern die Zertifikatsprüfung,
- eine Richtlinienänderung betrifft ganze Gerätegruppen.

Zu prüfen sind:

- Status des Authentifizierungsdienstes,
- Erreichbarkeit der RADIUS-Server,
- Zertifikatsgültigkeit,
- Systemzeit,
- Richtlinienänderungen,
- Switch- und Controllerprotokolle,
- Ablehnungsgrund,
- zugewiesenes VLAN,
- Failover auf einen zweiten Authentifizierungsserver.

---

22. WLAN als eigene Fehlerdomäne untersuchen

Wenn mehrere WLAN-Clients betroffen sind, müssen Funk-, Zugangs- und zentrale WLAN-Komponenten getrennt geprüft werden.

Zu prüfen sind:

- ist die SSID sichtbar?
- können Clients sich verbinden?
- funktioniert die Authentifizierung?
- erhalten sie eine IP-Adresse?

- betrifft es einen Access Point oder mehrere?
- betrifft es ein Frequenzband?
- betrifft es eine SSID?
- betrifft es einen Standort?
- sind Access Points beim Controller registriert?
- besitzen Access Points Strom und Uplink?
- ist das vorgesehene VLAN verfügbar?
- funktioniert DHCP?
- besteht ausreichende Funkabdeckung?
- gibt es starke Störungen?
- ist die Clientanzahl ungewöhnlich hoch?
- funktionieren Roaming und Controller-Kommunikation?
- wurde Firmware oder Konfiguration geändert?

Abgrenzung

Beobachtung	mögliche Einordnung
SSID nicht sichtbar	Access Point, Funkmodul, Controller oder SSID-Konfiguration
SSID sichtbar, Anmeldung scheitert	Authentifizierung, Zertifikat, RADIUS oder Kennwort
Anmeldung erfolgreich, keine IP-Adresse	VLAN, DHCP oder Tunnel
IP-Adresse vorhanden, Gateway nicht erreichbar	VLAN-Pfad, Gateway oder Client-Isolation
nur ein Access Point betroffen	AP, Uplink, PoE oder lokale Funkumgebung
alle APs eines Standorts betroffen	Controllerpfad, Standort-Uplink, DHCP oder gemeinsame Konfiguration
nur ein Frequenzband betroffen	Funkkonfiguration, Radarereignis oder Hardware

---

23. Firewall, ACL und zentrale Sicherheitskomponenten

Ein gemeinsamer Filterfehler kann viele Clients oder ganze Netze betreffen.

Zu prüfen sind:

- tatsächliche Quellnetze,
- Zielnetze,
- Protokolle und Ports,
- verwendete Sicherheitszone,
- Regelreihenfolge,
- Regeländerungen,
- NAT,
- Sitzungszustände,
- Hochverfügbarkeitsstatus,
- Routing auf der Firewall,

- Schnittstellenstatus,
- Ressourcenverbrauch,
- Lizenz- oder Zertifikatsstatus,
- Protokolle zum Fehlerzeitpunkt,
- IPv4- und IPv6-Regeln,
- Rückweg.

Mögliche Symptome

Beobachtung	mögliche Einordnung
interne Kommunikation funktioniert, Internet nicht	Firewall, NAT, WAN oder Provider
nur ein VLAN erreicht das Internet nicht	Zone, Regel, NAT oder Route
neue Verbindungen scheitern, bestehende funktionieren	Sitzungsgrenze, Zustandsübergang oder Regeländerung
nur HTTPS scheitert	Filter, Proxy, TLS-Inspektion oder Zertifikat
aktive Firewall meldet fehlerfreien Zustand, Verkehr fällt aus	Datenebene, Route, Schnittstelle oder Clusterzustand
nach Failover tritt Fehler auf	unsynchronisierte Zustände, Route, NAT oder Konfiguration

Eine Firewall sollte während einer größeren Störung nicht pauschal deaktiviert werden. Regeln und Protokolle müssen gezielt untersucht werden.

---

24. Routing und Rückweg prüfen

Wenn mehrere Netze betroffen sind, ist die Routingstruktur zu untersuchen.

Zu prüfen sind:

- verbundene Netze,
- statische Routen,
- dynamische Routingnachbarschaften,
- Standardroute,
- spezifische Zielrouten,
- Routenauswahl,
- Metrik beziehungsweise administrative Distanz,
- Policy-based Routing,
- VRF,
- Route Redistribution,
- zusammengefasste Routen,
- Rückroute,
- asymmetrisches Routing,
- kürzlich zurückgezogene Präfixe.

Mögliche Beobachtungen

- Gateway ist erreichbar, entfernte Netze nicht.
- Einige Zielnetze funktionieren, andere nicht.
- Verkehr verlässt den Standort, Antworten kommen nicht zurück.
- Nach einem Failover wird ein falscher Pfad gewählt.
- Eine spezifische Route fehlt, während die Standardroute besteht.
- Ein Standortpräfix wird nicht mehr angekündigt.
- Dieselben Adressbereiche werden an mehreren Stellen verwendet.

> Ein erfolgreicher Hinweg reicht nicht aus. Ende-zu-Ende-Kommunikation benötigt grundsätzlich auch einen funktionsfähigen Rückweg.

---

25. WAN- und Standortverbindung prüfen

Wenn lokale Kommunikation funktioniert, aber zentrale Systeme oder andere Standorte nicht erreichbar sind, liegt der Untersuchungsbereich häufig bei der Standortanbindung.

Mögliche Verbindungen:

- MPLS,
- SD-WAN,
- Site-to-Site-VPN,
- Standleitung,
- Metro Ethernet,
- Internet-VPN,
- Mobilfunk-Fallback,
- direkte Cloud-Verbindung.

Zu prüfen sind:

- physischer WAN-Link,
- Providerübergabe,
- WAN-IP-Konfiguration,
- Tunnelzustand,
- Routingnachbarschaften,
- Latenz,
- Paketverlust,
- Jitter,
- MTU,
- Verschlüsselungsstatus,
- Zertifikate,
- aktive und passive Leitungen,
- automatische Umschaltung,

- tatsächlicher Datenpfad,
- Providerstörungsmeldungen.

Abgrenzung

```
lokales Gateway erreichbar
→ lokaler Server erreichbar
→ zentraler Server nicht erreichbar
→ Internet erreichbar
```

Dies spricht eher für:

- ausgefallenen Standorttunnel,
- fehlende Route,
- zentrale Firewallregel,
- Rückwegproblem,
- Ausfall des zentralen Ziels.

Es spricht nicht für einen vollständigen lokalen Netzwerkausfall.

---

26. Internet- oder Providerstörung prüfen

Ein Provider sollte erst dann als Ursache benannt werden, wenn der lokale Verantwortungsbereich ausreichend geprüft wurde.

Vor einer Eskalation sollten dokumentiert sein:

- Kundennummer oder Anschlusskennung,
- betroffener Standort,
- Beginn der Störung,
- Art des Anschlusses,
- Status des Providerübergabegeräts,
- physischer Link,
- WAN-Adresse,
- Erreichbarkeit des nächsten Provider-Hops, sofern testbar,
- Paketverlust und Laufzeit,
- Verhalten einer Ersatzverbindung,
- lokale Router- und Firewallzustände,
- bereits durchgeführte Tests,
- relevante Protokolle.

Ein fehlgeschlagener Ping auf einen Providerrouter beweist keinen Ausfall, da ICMP gefiltert sein kann.

Eine erfolgreiche Mobilfunk- oder Ersatzverbindung zeigt, dass die Anwendung und das Ziel grundsätzlich funktionieren können. Sie beweist aber nicht allein, an welcher Stelle der ursprüngliche Anschluss fehlerhaft ist.

---

27. Redundanz und Failover nicht voraussetzen

Vorhandene Redundanz bedeutet nicht automatisch, dass ein Ausfall ohne Unterbrechung abgefangen wird.

Zu prüfen sind:

- ist die Ersatzkomponente tatsächlich betriebsbereit?
- wird ihr Zustand überwacht?
- sind Konfigurationen synchron?
- existieren gültige Routen?
- funktioniert die Umschaltung?
- wird die Datenebene geprüft oder nur der Linkstatus?
- bestehen gültige Lizenzen und Zertifikate?
- reicht die Kapazität der Ersatzverbindung?
- wurde das Failover regelmäßig getestet?
- funktioniert auch die Rückschaltung?

Mögliche Fehlerbilder

- primäre Verbindung ausgefallen, sekundäre Verbindung übernimmt nicht,
- sekundäre Verbindung wird aktiv, besitzt aber keine Route,
- Firewallcluster wechselt die Rolle, Upstream-Switch verwendet weiterhin den alten Pfad,
- Mobilfunk-Fallback ist aktiv, aber dessen Datenvolumen oder Richtlinie verhindert den Verkehr,
- beide redundanten Geräte hängen an derselben ausgefallenen Stromversorgung,
- beide Leitungen verwenden denselben physischen Gebäudeeintritt.

> Redundanz schützt nur vor Fehlern, die im Entwurf berücksichtigt wurden und deren Umschaltung technisch funktioniert.

---

28. Broadcast-Sturm und Überlastung

Ein größeres Netz kann durch ungewöhnlich hohe Last stark beeinträchtigt werden.

Mögliche Ursachen:

- Layer-2-Schleife,
- fehlerhaftes Gerät,

- Broadcast-Sturm,
- Multicast-Flut,
- übermäßige unbekannte Unicasts,
- Schadsoftware,
- fehlerhafte Netzwerkkarte,
- Backup- oder Replikationsverkehr,
- Denial-of-Service,
- überlasteter Uplink,
- ausgeschöpfte Firewall-Sitzungstabelle.

Mögliche Hinweise:

- hohe Switch-CPU,
- stark erhöhte Broadcast-Zähler,
- Managementzugriff instabil,
- hohe Portauslastung,
- Output Drops,
- Paketverlust über viele Clients,
- zunehmende Latenz,
- MAC-Adresstabelle verändert sich fortlaufend,
- Problem verschwindet nach Isolation eines bestimmten Bereichs.

Die verursachende Quelle sollte anhand von:

- Interface-Zählern,
- Flussdaten,
- Switch-Protokollen,
- MAC-Adresstabellen,
- Port Mirroring,
- Paketaufzeichnung,
- Monitoringverlauf

eingegrenzt werden.

---

29. Monitoringdaten auswerten

Monitoring kann zeigen, ob der Fehler lokal, zentral oder schrittweise entstanden ist.

Relevante Messwerte:

- Geräteerreichbarkeit,
- Interface-Status,
- Link Flaps,
- Bandbreite,
- Paketverlust,
- Latenz,

- CPU,
- Speicher,
- Temperatur,
- Netzteilstatus,
- PoE-Verbrauch,
- Routingnachbarschaften,
- VPN-Tunnel,
- DHCP-Auslastung,
- DNS-Antwortzeiten,
- Firewall-Sitzungen,
- Anzahl verbundener WLAN-Clients,
- Access-Point-Zustände.

Beispielhafte Ereignisfolge

```
09:16:58 Uplink Gi1/0/48 meldet Down
09:16:59 Access Switch wird vom Monitoring nicht mehr erreicht
09:17:03 42 Clients werden als nicht erreichbar gemeldet
09:17:05 Access Points verlieren Controllerverbindung
09:17:21 Uplink meldet kurzzeitig Up
09:17:24 Uplink meldet erneut Down
```

Diese Reihenfolge spricht stärker für einen instabilen gemeinsamen Uplink als für unabhängige Fehler an 42 Clients.

Monitoring kann jedoch Lücken besitzen:

- Messintervall zu groß,
- Überwachung nur per ICMP,
- Monitoringpfad selbst betroffen,
- Gerät antwortet auf Management, leitet aber keine Nutzdaten,
- Messung erfolgt von nur einem Standort.

---

30. Protokolle zeitlich korrelieren

Bei einem größeren Ausfall sollten Protokolle verschiedener Systeme anhand derselben Zeitachse verglichen werden.

Relevante Quellen:

- Access Switch,
- Distribution- und Core-Switch,
- Router,
- Firewall,

- WLAN-Controller,
- Access Points,
- DHCP-Server,
- DNS-Server,
- RADIUS-Server,
- VPN-Gateway,
- Providergerät,
- USV,
- Virtualisierungsplattform,
- Monitoring,
- ausgewählte Clients.

Voraussetzung für eine sinnvolle Korrelation ist eine möglichst genaue Zeitsynchronisation.

Beispiel

```
09:17:02 Distribution Switch: LACP-Mitglied verloren
09:17:03 Access Switch: Uplink-Protokoll wechselt Zustand
09:17:04 Spanning Tree: Topologieänderung
09:17:07 Monitoring: Access Switch nicht erreichbar
09:17:10 DHCP: Anfragen aus VLAN 120 bleiben aus
```

Diese Kombination ist aussagekräftiger als ein einzelner Clientfehler.

---

31. Paketaufzeichnung an geeigneten Punkten

Eine Paketaufzeichnung kann zeigen, bis zu welcher Stelle Verkehr gelangt.

Mögliche Aufzeichnungspunkte:

- betroffener Client,
- funktionierender Vergleichsclient,
- Access-Port,
- Switch-Uplink,
- VLAN-Gateway,
- DHCP-Server,
- DNS-Server,
- Firewall,
- Zielserver,
- WAN-Schnittstelle.

Mögliche Fragestellungen:

- sendet der Client ARP-Anfragen?

- erreicht ARP das Gateway?
- antwortet das Gateway?
- verlassen DHCP-Discover-Pakete das VLAN?
- erreicht das DHCP-Offer den Uplink?
- werden DNS-Anfragen gesendet?
- antwortet der DNS-Server?
- erreicht ein TCP-SYN die Firewall?
- verlässt es die WAN-Schnittstelle?
- kommt eine Antwort zurück?
- treten Wiederholungen auf?
- werden ICMP-Fehlermeldungen zurückgesendet?

Beispielhafte Wireshark-Filter

```
arp
dhcp
dns
icmp
icmpv6
stp
eth.addr == <mac-adresse>
ip.addr == <ip-adresse>
tcp.port == 443
```

Eine Aufzeichnung an nur einem Punkt zeigt nicht automatisch, an welchem Abschnitt eines längeren Pfades ein Paket verloren geht. Bei komplexen Fehlern können zeitlich abgestimmte Aufzeichnungen an mehreren Stellen erforderlich sein.

Paketaufzeichnungen dürfen nur mit Berechtigung erstellt und müssen geschützt gespeichert werden.

---

32. Änderungen kontrolliert zurücknehmen

Wenn eine konkrete Änderung als Ursache bestätigt oder sehr stark eingegrenzt wurde, kann eine Rücknahme sinnvoll sein.

Vor dem Rollback sind zu klären:

- ist der vorherige Zustand dokumentiert?
- ist die alte Konfiguration weiterhin gültig?
- wurden seitdem weitere abhängige Änderungen durchgeführt?
- bestehen Sicherheitsrisiken durch die Rücknahme?
- ist ein Wartungs- oder Freigabeprozess erforderlich?

- kann die Rücknahme weitere Bereiche beeinträchtigen?
- existiert eine aktuelle Sicherung?
- wie wird der Erfolg geprüft?
- wie wird bei Misserfolg weiter vorgegangen?

Ein Rollback ist keine beliebige Rückkehr zu einer alten Konfiguration. Es ist eine geplante Änderung mit eigener Risiko- und Nachprüfung.

---

33. Ungeeignete Sofortmaßnahmen

Bei einem größeren Ausfall können unkoordinierte Eingriffe den Fehler ausweiten oder wichtige Spuren vernichten.

Problematisch sind insbesondere:

- alle Switches neu starten,
- Firewall neu starten,
- Router neu starten,
- mehrere Uplinks gleichzeitig trennen,
- Spanning Tree deaktivieren,
- alle Ports administrativ aktivieren,
- VLANs neu anlegen, ohne den Ausgangszustand zu sichern,
- Firewall vollständig deaktivieren,
- DHCP-Bereiche ungeprüft vergrößern,
- Switch-Konfiguration durch eine alte Sicherung überschreiben,
- Firmware während der Störung aktualisieren,
- Provider ohne lokale Prüfung als Ursache festlegen,
- mehrere Teams unabhängig Änderungen durchführen lassen,
- Geräte austauschen, bevor Verkabelung und Konfiguration dokumentiert wurden.

Solche Maßnahmen können im Einzelfall notwendig sein. Sie benötigen jedoch:

- technische Begründung,
- Freigabe,
- Koordination,
- dokumentierten Ausgangszustand,
- Rückfallmöglichkeit,
- vollständige Nachprüfung.

---

34. Praxisfall A: Gesamte Etage ohne kabelgebundenes Netzwerk

Symptom

- alle geprüften Ethernet-Clients der dritten Etage sind betroffen,
- WLAN funktioniert,

- andere Etagen funktionieren,
- Clients erhalten keine DHCP-Adresse,
- Access Switch ist über eine separate Managementverbindung erreichbar.

Prüfung

1. betroffene Access-Ports und VLANs dokumentieren.
2. Uplinkstatus des Etagen-Switches prüfen.
3. Trunk-Konfiguration beider Seiten vergleichen.
4. erlaubte VLANs kontrollieren.
5. Spanning-Tree-Zustand prüfen.
6. Fehlerzähler des Uplinks auswerten.
7. MAC-Adresstabelle kontrollieren.
8. DHCP-Verkehr am Client-VLAN untersuchen.
9. letzte Konfigurationsänderungen prüfen.
10. nach einer freigegebenen Korrektur alle betroffenen VLANs testen.

Mögliche Ursache

Bei einer Änderung wurde das Client-VLAN aus der Liste der auf dem Uplink erlaubten VLANs entfernt. Das Management-VLAN blieb verfügbar, weshalb der Switch weiterhin administrierbar war.

Nachprüfung

- Clients erhalten Adressen aus dem richtigen Bereich,
- Gateway ist erreichbar,
- interne DNS-Auflösung funktioniert,
- zentrale Anwendungen sind erreichbar,
- Internetzugriff funktioniert,
- weitere VLANs des Switches funktionieren,
- Trunk-Konfiguration beider Seiten ist dokumentiert.

---

35. Praxisfall B: Ganzer Standort erreicht zentrale Systeme nicht

Symptom

- lokale Drucker und lokale Server funktionieren,
- das lokale Gateway ist erreichbar,
- zentrale Anwendungen sind nicht erreichbar,
- andere Standorte funktionieren,
- öffentlicher Internetzugriff funktioniert.

Prüfung

1. lokale Kommunikation bestätigen.

2. zentrale Ziele per IP testen.
3. Standorttunnel prüfen.
4. Routingtabelle kontrollieren.
5. Ankündigung des Standortpräfixes prüfen.
6. Rückroute am zentralen Standort untersuchen.
7. Firewallprotokolle auswerten.
8. Tunnel- und Routingereignisse zeitlich vergleichen.
9. redundante Verbindung prüfen.
10. ursprünglichen Anwendungszugriff nach der Korrektur wiederholen.

Mögliche Ursache

Nach einer Änderung wurde das lokale Standortpräfix nicht mehr über den VPN-Tunnel angekündigt. Der Hinweg zu zentralen Systemen war teilweise vorhanden, die Antworten besaßen jedoch keine passende Rückroute.

Nachprüfung

- zentrale IP-Ziele erreichbar,
- zentrale DNS-Namen auflösbar,
- benötigte Anwendungsports erreichbar,
- Hin- und Rückroute vorhanden,
- erneuter Tunnelaufbau erfolgreich,
- Internetverkehr weiterhin funktionsfähig.

---

36. Praxisfall C: Neue Clients erhalten kein Netzwerk

Symptom

- bereits aktive Clients funktionieren,
- neu gestartete oder neu angeschlossene Clients erhalten keine Adresse,
- mehrere Bereiche desselben VLANs sind betroffen,
- statisch konfigurierte Infrastrukturgeräte bleiben erreichbar.

Prüfung

1. Adressbereich und freie Leases kontrollieren.
2. DHCP-Dienstzustand prüfen.
3. DHCP-Failoverstatus prüfen.
4. Discover-, Offer-, Request- und ACK-Ablauf aufzeichnen.
5. DHCP-Relay prüfen.
6. DHCP-Snooping-Zustand kontrollieren.
7. Lease-Dauer und Anzahl aktiver Geräte auswerten.
8. unerwünschte DHCP-Server ausschließen.
9. freigegebene Korrektur durchführen.
10. mehrere neue Adressvergaben testen.

Mögliche Ursache

Der DHCP-Bereich besitzt keine freien Adressen mehr. Bestehende Clients können ihre noch gültigen Adressen weiterverwenden, während neue Clients keine Lease erhalten.

Nachprüfung

- neue Clients erhalten gültige Adressen,
- Gateway- und DNS-Optionen stimmen,
- Lease-Erneuerung funktioniert,
- Failoverzustand ist fehlerfrei,
- Adressauslastung wird überwacht,
- Ursache der unerwartet hohen Belegung ist dokumentiert.

---

37. Praxisfall D: Viele Benutzer melden „kein Internet“

Symptom

- Gateway ist erreichbar,
- öffentliche IP-Ziele sind erreichbar,
- Websites können über Namen nicht geöffnet werden,
- interne Anwendungen mit bereits bekannten Adressen funktionieren teilweise.

Prüfung

1. IP-Verbindung getrennt von DNS testen.
2. jeden konfigurierten DNS-Server einzeln abfragen.
3. DNS-Dienstzustand prüfen.
4. Firewallregeln für DNS kontrollieren.
5. Weiterleitungen und Rekursion prüfen.
6. DHCP-DNS-Optionen auswerten.
7. Serverprotokolle zum Fehlerzeitpunkt prüfen.
8. internen und externen Namen testen.
9. DNS-Korrektur durchführen.
10. ursprüngliche Anwendungen erneut prüfen.

Mögliche Ursache

Der primäre und sekundäre DNS-Dienst waren auf derselben ausgefallenen Virtualisierungsplattform betrieben. Die Clients besaßen weiterhin eine funktionierende IP-Verbindung, konnten jedoch keine Namen auflösen.

Nachprüfung

- interne Namen werden korrekt aufgelöst,
- externe Namen werden korrekt aufgelöst,

- jeder vorgesehene DNS-Server antwortet,
- Webanwendungen funktionieren,
- Active-Directory-abhängige Dienste funktionieren,
- tatsächliche Unabhängigkeit der DNS-Redundanz wird bewertet.

---

38. Praxisfall E: Standort fällt trotz redundanter WAN-Leitung aus

Symptom

- primäre Leitung ist ausgefallen,
- sekundäre Leitung wird als aktiv angezeigt,
- zentrale Anwendungen und Internet sind trotzdem nicht erreichbar,
- lokale Kommunikation funktioniert.

Prüfung

1. physischen Zustand beider Leitungen prüfen.
2. aktive Standardroute kontrollieren.
3. Tunnelzustand der Ersatzleitung prüfen.
4. NAT und Firewallregeln prüfen.
5. Routingankündigungen kontrollieren.
6. DNS-Erreichbarkeit über den Ersatzpfad testen.
7. MTU und Paketgröße berücksichtigen.
8. Providerübergaben beider Leitungen vergleichen.
9. Datenverkehr auf der Ersatzschnittstelle aufzeichnen.
10. vollständigen Failover- und Rückschalttest planen.

Mögliche Ursache

Die Ersatzleitung war physisch aktiv, besaß jedoch wegen einer fehlenden Standardroute keinen verwendbaren Datenpfad.

Nachprüfung

- Internet und zentrale Dienste über Ersatzleitung erreichbar,
- Tunnel aktiv,
- DNS erreichbar,
- benötigte NAT- und Firewallregeln wirksam,
- automatisches Failover reproduzierbar,
- Rückschaltung kontrolliert,
- Monitoring erkennt nicht nur den Link-, sondern auch den Dienstzustand.

---

39. Häufige Fehlinterpretationen

Aussage	fachliche Einordnung

„Viele Benutzer sind betroffen, also ist der Provider ausgefallen.“	Auch Switch, VLAN, Gateway, DHCP, DNS, Firewall oder Standortanbindung können gemeinsam verantwortlich sein.
„Der Switch ist erreichbar, also funktioniert er.“	Management- und Nutzdatenpfad können getrennt sein.
„Alle Ports zeigen Link, also ist das Netzwerk in Ordnung.“	VLAN, Trunk, Gateway, DHCP und Routing können trotzdem fehlerhaft sein.
„WLAN funktioniert, also kann der Switch nicht betroffen sein.“	WLAN kann einen anderen Access Switch, ein anderes VLAN oder einen anderen Datenpfad verwenden.
„Nur ein VLAN ist ausgefallen, also ist das Gateway defekt.“	Auch Trunk, Relay, ACL oder VLAN-Zuordnung können betroffen sein.
„Alte Clients funktionieren, also funktioniert DHCP.“	Alte Clients können noch gültige Leases verwenden.
„Die redundante Leitung ist aktiv, also funktioniert das Failover.“	Linkstatus bestätigt keinen vollständigen Datenpfad.
„Die Firewall zeigt Grün, also blockiert sie nichts.“	Regeln, NAT, Routing oder Datenebene können trotzdem fehlerhaft sein.
„Nach einem Neustart funktioniert alles, also ist die Ursache behoben.“	Der Neustart kann Zustand und Spuren verändert haben, ohne die Ursache zu erklären.
„Eine hohe CPU-Auslastung beweist einen Angriff.“	Schleifen, Fehler, Monitoring, legitime Last und Kontrollprotokolle sind ebenfalls möglich.
„Der letzte sichtbare Traceroute-Hop ist defekt.“	Router können Antworten filtern und Verkehr trotzdem weiterleiten.
„Zwei Netzteile bedeuten vollständige Redundanz.“	Beide können an derselben Stromquelle oder USV angeschlossen sein.

---

40. Vollständige Prüfreihenfolge

1. konkrete Symptome und betroffene Anwendungen erfassen.
2. Anzahl und Verteilung der betroffenen Clients bestimmen.
3. Ethernet, WLAN, Telefonie und andere Gerätetypen unterscheiden.
4. funktionierende Vergleichsbereiche bestimmen.
5. Beginn, Verlauf und letzte bekannte Funktion dokumentieren.
6. letzte Änderungen und Wartungsarbeiten prüfen.
7. geschäftliche Auswirkung und Priorität bewerten.
8. Zuständigkeiten und Kommunikation koordinieren.
9. repräsentative betroffene und funktionierende Testpunkte auswählen.
10. gemeinsame technische Abhängigkeiten abbilden.
11. Stromversorgung, USV und Umgebung prüfen.
12. Access Switch und physische Uplinks untersuchen.
13. Fehlerzähler und Link Flaps auswerten.
14. Trunk- und VLAN-Konfiguration prüfen.
15. Spanning Tree und mögliche Schleifen untersuchen.
16. Link Aggregation und LACP prüfen.
17. Gateway und First-Hop-Redundanz kontrollieren.

18. DHCP-Dienst, Bereiche und Relay untersuchen.
19. DNS getrennt von der IP-Verbindung prüfen.
20. Netzwerkzugangskontrolle und Authentifizierung berücksichtigen.
21. bei WLAN-Störungen Access Points und Controller prüfen.
22. Firewall, ACL, NAT und Sicherheitszonen untersuchen.
23. Routing einschließlich Rückweg prüfen.
24. WAN, VPN und Providerübergabe kontrollieren.
25. tatsächliche Funktion redundanter Pfade prüfen.
26. Monitoringdaten und Protokolle zeitlich korrelieren.
27. bei Bedarf autorisierte Paketaufzeichnungen erstellen.
28. eine konkrete Hypothese formulieren.
29. Änderung oder Rollback freigeben lassen.
30. immer nur eine kontrollierbare Änderung durchführen.
31. ursprüngliches Symptom erneut testen.
32. weitere VLANs, Standorte und Dienste auf Nebenwirkungen prüfen.
33. Redundanz und erneuten Verbindungsaufbau testen.
34. Ursache, Maßnahme, Ergebnis und verbleibendes Risiko dokumentieren.
35. notwendige Präventionsmaßnahmen festlegen.

---

41. Dokumentationsbeispiel

```
Ticket: INC-20614
Beginn: 01.08.2026, etwa 09:17 Uhr
Standort: Gebäude B
Umfang: kabelgebundene Clients der dritten Etage
Nicht betroffen: WLAN, andere Etagen, zentrale Server

Symptom:
Betroffene Clients erhalten keine DHCP-Adresse und können das
Standardgateway nicht erreichen.

Ausgangszustand:
- Access Switch erreichbar
- Clientports physisch aktiv
- WLAN derselben Etage funktioniert
- andere Etagen im gleichen Client-VLAN funktionieren
- Uplink des Access Switches aktiv
- Client-VLAN nicht in der Liste der erlaubten Uplink-VLANs
- Management-VLAN weiterhin erlaubt

Hypothese:
```

Das Client-VLAN wird am Uplink des Etagen-Switches nicht mehr transportiert.

Prüfung:
- Trunk-Konfiguration beider Uplink-Seiten verglichen
- Konfigurationsänderung um 09:14 Uhr festgestellt
- Client-VLAN fehlte nur auf der Seite des Access Switches
- DHCP-Discover war am Clientport, aber nicht am Distribution Switch sichtbar

Ursache:
Unvollständige Liste erlaubter VLANs nach einer Uplink-Änderung.

Maßnahme:
Client-VLAN nach Freigabe wieder auf dem Uplink zugelassen.

Nachprüfung:
- mehrere Clients erhalten gültige DHCP-Adressen
- Standardgateway erreichbar
- interne DNS-Auflösung erfolgreich
- zentrale Anwendungen erreichbar
- Internetzugriff funktioniert
- WLAN weiterhin funktionsfähig
- weitere VLANs des Access Switches geprüft
- Konfiguration gespeichert und dokumentiert

Prävention:
- Konfigurationsprüfung für Trunk-Änderungen ergänzen
- VLAN-Erreichbarkeit in das Monitoring aufnehmen
- Peer-Review für Änderungen an produktiven Uplinks einführen

---

42. Checkliste für mehrere Clients oder einen Standort ohne Netzwerk

- [ ] genaue Anzahl und Verteilung der betroffenen Clients wurden bestimmt.
- [ ] Benutzerangaben wurden durch repräsentative Tests bestätigt.
- [ ] Ethernet und WLAN wurden getrennt geprüft.
- [ ] funktionierende Vergleichsbereiche wurden dokumentiert.
- [ ] interne Dienste, Internet und DNS wurden getrennt bewertet.
- [ ] Beginn und zeitlicher Verlauf wurden erfasst.

- [ ] letzte Änderungen wurden geprüft.
- [ ] geschäftliche Auswirkung und Priorität wurden bewertet.
- [ ] technische und kommunikative Zuständigkeiten wurden festgelegt.
- [ ] gemeinsame Komponenten der betroffenen Clients wurden bestimmt.
- [ ] Stromversorgung und USV wurden geprüft.
- [ ] Access Switches wurden auf Zustand und Erreichbarkeit geprüft.
- [ ] Uplink-Status und Fehlerzähler wurden kontrolliert.
- [ ] Trunk-Konfiguration wurde auf beiden Seiten verglichen.
- [ ] benötigte VLANs wurden über den vollständigen Pfad geprüft.
- [ ] Spanning-Tree-Zustand und Topology Changes wurden untersucht.
- [ ] Link Aggregation und LACP wurden berücksichtigt.
- [ ] Gateway und Gateway-Redundanz wurden geprüft.
- [ ] DHCP-Dienst, Bereich und Relay wurden untersucht.
- [ ] DNS wurde getrennt von der IP-Verbindung getestet.
- [ ] Netzwerkzugangskontrolle und RADIUS wurden berücksichtigt.
- [ ] WLAN-Controller und Access Points wurden bei Bedarf geprüft.
- [ ] Firewallregeln, NAT und ACLs wurden kontrolliert.
- [ ] Hin- und Rückrouting wurden geprüft.
- [ ] WAN- und VPN-Zustand wurden untersucht.
- [ ] Provider wurde erst nach lokaler Eingrenzung einbezogen.
- [ ] redundante Pfade wurden tatsächlich getestet.
- [ ] Monitoringdaten wurden ausgewertet.
- [ ] Protokolle verschiedener Komponenten wurden zeitlich korreliert.
- [ ] Paketaufzeichnungen erfolgten nur mit Berechtigung.
- [ ] eine konkrete technische Hypothese wurde formuliert.
- [ ] Ausgangskonfiguration wurde vor Änderungen gesichert.
- [ ] Änderung oder Rollback wurde freigegeben.
- [ ] es wurde nur eine kontrollierbare Änderung gleichzeitig durchgeführt.
- [ ] ursprüngliches Symptom wurde erneut getestet.
- [ ] weitere Dienste und Bereiche wurden auf Nebenwirkungen geprüft.
- [ ] Ursache, Maßnahme und Nachweis wurden dokumentiert.
- [ ] Präventionsmaßnahmen wurden festgelegt.

---

43. Schnellreferenz

Fehlerumfang	wahrscheinlicher gemeinsamer Untersuchungsbereich
einzelne Clients an einem Switch	Access-Ports, VLAN, Switch oder Uplink
komplette Etage	Etagen-Switch, Uplink, Strom oder VLAN-Pfad
ein VLAN an mehreren Switches	Gateway, DHCP, VLAN-Trunks, ACL oder Routing
nur neue Clients	DHCP, Authentifizierung oder Adressbereich
nur WLAN-Clients	Access Points, Controller, SSID, RADIUS, VLAN oder DHCP
Ethernet und WLAN eines Standorts	Gateway, Firewall, WAN, zentrale Dienste oder Strom
lokale Systeme funktionieren, zentrale nicht	WAN, VPN, Routing, Firewall oder Rückweg
IP-Ziele funktionieren, Namen nicht	DNS
interne Ziele funktionieren, Internet nicht	Firewall, NAT, WAN oder Provider
alle Standorte betroffen	zentrale Firewall, DNS, Rechenzentrum, Cloud oder zentraler Routingbereich
sporadische Ausfälle vieler Clients	Schleife, instabiler Uplink, Überlastung oder Redundanzproblem
bestehende Sitzungen funktionieren, neue nicht	DHCP, DNS, Authentifizierung, Firewallzustand oder Kapazitätsgrenze

---

Merksatz

> Bei mehreren gleichzeitig betroffenen Clients wird nicht jedes Endgerät einzeln als unabhängiger Fehlerfall behandelt. Entscheidend ist der kleinste gemeinsame Ausfallbereich. Funktionierende Vergleichsbereiche, gemeinsame Abhängigkeiten, Zeitstempel und gezielte Tests führen von der allgemeinen Meldung „Standort ohne Netzwerk“ zu einer überprüfbaren Ursache.

Quellen und weiterführende Dokumentation

- Microsoft Learn – DHCP troubleshooting guidance for Windows Server
- Microsoft Learn – Guidance for troubleshooting DNS
- Microsoft Learn – Troubleshooting DNS servers
- Cisco – Troubleshoot DHCP in Enterprise Networks
- Cisco – Troubleshoot DHCP in a Layer 2 Only VLAN – Wired
- Cisco – High Availability Campus Recovery Analysis
- Red Hat – Network troubleshooting and performance tuning
- Red Hat – Introduction to NetworkManager debugging

- Red Hat – Mirroring a network interface
- Wireshark – Benutzerhandbuch
- Wireshark – Display Filter Reference
- RFC 2131 – Dynamic Host Configuration Protocol
- RFC 826 – Address Resolution Protocol
- RFC 1034 – Domain Names: Concepts and Facilities
- RFC 1035 – Domain Names: Implementation and Specification
- RFC 5798 – Virtual Router Redundancy Protocol Version 3
- IEEE 802.1 Working Group