5.7 Fehlersuche auf Schicht 2

Fehler auf OSI-Schicht 2 betreffen die lokale Datenübertragung im Netzwerk.

Dabei geht es vor allem um:

```
- Ethernet-Frames
- MAC-Adressen
- Switches
- VLANs
- Access-Ports
- Trunk-Ports
- ARP
- Broadcasts
- STP
- Layer-2-Schleifen
```

Schicht 2 liegt zwischen der physischen Verbindung auf Schicht 1 und der IP-Kommunikation auf Schicht 3.

Merksatz:

```
Schicht 2 = lokale Übertragung mit Frames, MAC-Adressen und VLANs.
```

Grundidee der Schicht-2-Fehlersuche

Bei der Fehlersuche auf Schicht 2 prüft man, ob Frames im lokalen Netzwerk korrekt weitergeleitet werden.

Typische Fragen:

```
Wird die MAC-Adresse gelernt?
Ist das richtige VLAN aktiv?
Ist der Switch-Port korrekt konfiguriert?
Ist der Port Access oder Trunk?
Wird das VLAN über den Trunk transportiert?
Gibt es Schleifen?
Gibt es Broadcast-Stürme?
Funktioniert ARP?
```

Blockiert STP einen Port?

Merksatz:

Auf Schicht 2 prüft man lokale Weiterleitung,
MAC-Adressen und VLANs.

Reihenfolge bei der Fehlersuche

Eine sinnvolle Reihenfolge ist:

1. Schicht 1 prüfen:
   Link, Kabel, Port, Signal

2. Schicht 2 prüfen:
   MAC-Adresse, VLAN, Switch-Port, ARP, STP

3. Schicht 3 prüfen:
   IP-Adresse, Subnetzmaske, Gateway, Routing

4. höhere Schichten prüfen:
   DNS, TCP/UDP-Port, Anwendung

Wichtig:

Wenn Schicht 1 nicht funktioniert,
kann Schicht 2 nicht zuverlässig funktionieren.

Merksatz:

Erst Link,
dann MAC/VLAN,
dann IP.

Typische Schicht-2-Fehler

Typische Fehler auf Schicht 2 sind:

```
- falsches VLAN
- Port im falschen Modus
- Access-Port statt Trunk
- Trunk statt Access-Port
- VLAN auf Trunk nicht erlaubt
- falsches Native VLAN
- MAC-Adresse wird nicht gelernt
- MAC-Adresse erscheint auf falschem Port
- MAC Flapping
- Broadcast-Sturm
- Layer-2-Schleife
- STP blockiert unerwartet
- ARP funktioniert nicht
- doppelte MAC-Adresse
- Port Security blockiert Gerät
```

Merksatz:

```
Schicht-2-Fehler betreffen Frames,
MACs,
VLANs
und Switch-Weiterleitung.
```

Fehlerbild: MAC-Adresse wird nicht gelernt

Ein Switch lernt MAC-Adressen über die Quell-MAC-Adresse eingehender Frames.

Wenn eine MAC-Adresse nicht gelernt wird, kann der Switch das Gerät nicht korrekt in seiner MAC-Adresstabelle eintragen.

Mögliche Ursachen:

```
- Gerät sendet keine Frames
- Gerät ist ausgeschaltet
- falscher Switch-Port
- Port deaktiviert
- Link ist nicht aktiv
- falsches VLAN
- Port Security blockiert
```

- Netzwerkkarte deaktiviert
- Kabelproblem auf Schicht 1

Merksatz:

> Keine gelernte MAC-Adresse kann Schicht 1 oder Schicht 2 betreffen.

Fehlerbild: MAC-Adresse auf falschem Port

Ein Switch kann eine MAC-Adresse an einem Port lernen, an dem man sie nicht erwartet.

Mögliche Ursachen:

- Gerät wurde umgesteckt
- Dokumentation ist veraltet
- Patchfeld falsch gepatcht
- Gerät hängt hinter einem anderen Switch
- virtuelle Maschine nutzt diese MAC-Adresse
- falsche Verkabelung
- Layer-2-Schleife

Merksatz:

> Unerwartete MAC-Port-Zuordnung kann auf falsche Patchung oder Topologieprobleme hinweisen.

Fehlerbild: MAC Flapping

MAC Flapping bedeutet:

> dieselbe MAC-Adresse wird ständig an unterschiedlichen Switch-Ports gelernt.

Das ist ein Warnsignal.

Mögliche Ursachen:

- Layer-2-Schleife
- falsch konfigurierte Link Aggregation
- Gerät ist über mehrere Wege angeschlossen

- virtuelle Umgebung sendet über wechselnde Ports
- falsche Switch-Verkabelung
- redundante Links ohne funktionierendes STP

Merksatz:

MAC Flapping kann auf eine Layer-2-Schleife hinweisen.

Fehlerbild: Falsches VLAN

Ein Gerät kann physisch korrekt verbunden sein, sich aber logisch im falschen Netz befinden.

Beispiel:

PC soll in VLAN 10 sein.
Switch-Port ist aber in VLAN 20.

Mögliche Folgen:

- falsche IP-Adresse
- keine IP-Adresse
- falsches Gateway
- Server nicht erreichbar
- Drucker nicht erreichbar
- Internet funktioniert nicht
- Zugriff auf falsche Netzwerkressourcen

Merksatz:

Falsches VLAN kann wie ein IP-Problem aussehen.

Fehlerbild: Client bekommt keine IP-Adresse

Wenn ein Client keine IP-Adresse erhält, denkt man oft zuerst an DHCP.

Die Ursache kann aber auf Schicht 2 liegen.

Mögliche Ursachen:

- Port im falschen VLAN
- VLAN auf Trunk nicht erlaubt
- DHCP-Server nicht im VLAN erreichbar
- DHCP-Relay fehlt
- Access-Port falsch konfiguriert
- Trunk zum Router oder zur Firewall falsch
- STP blockiert den Pfad
- Port Security blockiert Frames

Merksatz:

DHCP-Probleme können durch VLAN-Fehler entstehen.

Fehlerbild: Client bekommt falsche IP-Adresse

Wenn ein Client eine IP-Adresse aus dem falschen Netz bekommt, ist häufig das VLAN falsch.

Beispiel:

Erwartet:
VLAN 10
192.168.10.0/24

Tatsächlich:
VLAN 20
192.168.20.0/24

Mögliche Ursachen:

- Switch-Port im falschen VLAN
- falsche SSID-VLAN-Zuordnung
- Trunk falsch konfiguriert
- falsches Native VLAN
- falscher DHCP-Bereich

Merksatz:

Falsche IP-Adresse kann falsche VLAN-Zuordnung bedeuten.

Fehlerbild: Trunk transportiert VLAN nicht

Ein Trunk-Port soll mehrere VLANs transportieren.

Wenn ein VLAN über den Trunk nicht funktioniert, können Geräte in diesem VLAN nicht kommunizieren.

Mögliche Ursachen:

```
- VLAN ist auf dem Trunk nicht erlaubt
- VLAN existiert auf einem Switch nicht
- Gegenstelle ist kein Trunk
- Native VLAN passt nicht
- Tagging stimmt nicht
- STP blockiert für dieses VLAN
- falsche Port-Konfiguration
```

Merksatz:

```
Trunk-Fehler betreffen oft mehrere Geräte oder ganze VLANs.
```

Fehlerbild: Access-Port statt Trunk

Ein Port ist als Access-Port konfiguriert, obwohl mehrere VLANs darüber laufen sollen.

Typisches Beispiel:

```
Access Point mit mehreren SSIDs
soll VLAN 10, 20 und 30 nutzen.
```

Der Switch-Port ist aber nur Access-Port in VLAN 10.

Folge:

```
Nur ein VLAN funktioniert.
Andere SSIDs bekommen keine passende Verbindung.
```

Merksatz:

Mehrere VLANs brauchen normalerweise einen Trunk.

Fehlerbild: Trunk statt Access-Port

Ein Port ist als Trunk konfiguriert, obwohl ein normales Endgerät angeschlossen ist.

Mögliche Folgen:

- Endgerät versteht VLAN-Tags nicht
- Gerät landet im falschen VLAN
- Sicherheitsrisiko
- unerwartetes Netzwerkverhalten
- DHCP-Probleme

Typische Endgeräte an Access-Ports:

- PC
- Drucker
- Kamera
- einzelnes Telefon
- einfaches Endgerät

Merksatz:

Normale Endgeräte gehören meistens an Access-Ports.

Fehlerbild: Falsches Native VLAN

Bei Trunk-Ports kann ein Native VLAN für untagged Frames verwendet werden.

Wenn das Native VLAN auf beiden Seiten unterschiedlich ist, kann es zu Problemen kommen.

Mögliche Folgen:

- Frames landen im falschen VLAN
- Sicherheitsproblem
- Verbindungsprobleme
- schwer erkennbare Fehlleitung

Merksatz:

```
Native VLAN muss auf beiden Seiten eines Trunks passen.
```

Fehlerbild: ARP funktioniert nicht

ARP wird benötigt, um zu einer IP-Adresse die passende MAC-Adresse im lokalen Netz zu finden.

Wenn ARP nicht funktioniert, kann lokale Kommunikation scheitern.

Mögliche Ursachen:

```
- Zielgerät ist aus
- Zielgerät ist im falschen VLAN
- Absender ist im falschen VLAN
- falsche Subnetzmaske
- falsches Gateway
- ARP wird durch Sicherheitsfunktion blockiert
- IP-Adresskonflikt
- ARP-Spoofing
- Schicht-1-Problem
```

Merksatz:

```
ARP-Probleme zeigen,
dass IP und MAC lokal nicht zusammenfinden.
```

Fehlerbild: ARP-Eintrag ändert sich ständig

Wenn sich die MAC-Adresse zu einer IP-Adresse ständig ändert, ist das auffällig.

Mögliche Ursachen:

```
- IP-Adresskonflikt
- ARP-Spoofing
- Gateway-Failover
- Cluster oder Hochverfügbarkeit
- falsche Konfiguration
- virtuelle Systeme
```

Wichtig:

Nicht jede Änderung ist automatisch ein Angriff.
In Failover- oder Cluster-Umgebungen kann das gewollt sein.

Merksatz:

Wechselnde ARP-Zuordnungen immer prüfen und einordnen.

Fehlerbild: Broadcast-Sturm

Ein Broadcast-Sturm entsteht, wenn sehr viele Broadcast-Frames das Netzwerk belasten.

Mögliche Ursachen:

- Layer-2-Schleife
- fehlerhaftes Gerät
- falsche Switch-Verkabelung
- Broadcast-lastige Anwendung
- Angriff
- STP deaktiviert oder falsch konfiguriert

Typische Symptome:

- Netzwerk extrem langsam
- viele Switch-LEDs blinken stark
- hohe Port-Auslastung
- Geräte verlieren Verbindung
- DHCP oder ARP funktioniert unzuverlässig

Merksatz:

Broadcast-Sturm kann ein Layer-2-Netz lahmlegen.

Fehlerbild: STP blockiert einen Port

Wenn STP einen Port blockiert, ist das nicht automatisch ein Fehler.

STP blockiert Ports, um Schleifen zu verhindern.

Problematisch wird es, wenn:

- der falsche Port blockiert wird
- die Root Bridge ungünstig gewählt ist
- ein wichtiger Pfad unerwartet ausfällt
- STP auf manchen Switches deaktiviert ist
- eine Schleife trotzdem entsteht

Merksatz:

STP-Blocking kann normal sein,
muss aber zur geplanten Topologie passen.

Fehlerbild: Layer-2-Schleife

Eine Layer-2-Schleife kann durch falsche Verkabelung oder falsche Redundanz entstehen.

Typische Hinweise:

- MAC Flapping
- Broadcast-Sturm
- hohe Switch-Auslastung
- Netzwerk wird plötzlich sehr langsam
- viele Frames auf vielen Ports
- STP-Logs zeigen Änderungen
- nach Entfernen eines Kabels wird das Netz stabil

Merksatz:

MAC Flapping und Broadcast-Sturm sind starke Hinweise auf Schleifen.

Fehlerbild: Port Security blockiert Gerät

Port Security kann festlegen, welche oder wie viele MAC-Adressen an einem Port erlaubt sind.

Wenn ein anderes Gerät angeschlossen wird, kann der Switch reagieren.

Mögliche Reaktionen:

- Frames verwerfen
- Warnung erzeugen
- Port deaktivieren
- Ereignis protokollieren

Mögliche Ursachen:

- Gerät wurde getauscht
- anderer PC angeschlossen
- kleiner Switch angeschlossen
- virtuelle Maschinen erzeugen mehrere MAC-Adressen
- falsche Port-Security-Konfiguration

Merksatz:

Port Security schützt,
kann aber bei Gerätewechseln Verbindungen blockieren.

Fehlerbild: Doppelte MAC-Adresse

MAC-Adressen sollten eindeutig sein.

In der Praxis können doppelte MAC-Adressen trotzdem auftreten.

Mögliche Ursachen:

- falsch konfigurierte virtuelle Maschinen
- manuell gesetzte MAC-Adresse
- geklonte Systeme
- fehlerhafte Geräte
- absichtliches MAC-Spoofing

Mögliche Folgen:

- instabile Verbindung
- MAC-Flapping

- falsche Weiterleitung
- schwer nachvollziehbare Netzwerkprobleme

Merksatz:

Doppelte MAC-Adressen stören die Switch-Weiterleitung.

Werkzeuge für Schicht-2-Fehlersuche

Typische Werkzeuge und Informationsquellen:

Werkzeug / Anzeige	Nutzen
MAC-Adresstabelle	zeigt MAC-Adresse zu Switch-Port
Switch-Port-Konfiguration	zeigt Access, Trunk, VLAN
VLAN-Liste	zeigt vorhandene VLANs
Trunk-Status	zeigt erlaubte und aktive VLANs
STP-Status	zeigt Root Bridge und blockierte Ports
Port-Security-Status	zeigt erlaubte oder blockierte MAC-Adressen
ARP-Tabelle	zeigt IP-zu-MAC-Zuordnung
Switch-Logs	zeigen STP, Port-Changes, Security-Events
Packet Capture	zeigt Frames und ARP-Verkehr
Dokumentation	zeigt Soll-Zustand

Merksatz:

Schicht-2-Fehlersuche braucht Switch-Informationen und saubere Dokumentation.

Wichtige Switch-Informationen

Bei Schicht-2-Problemen sind diese Informationen besonders nützlich:

- Port aktiv oder deaktiviert?
- Access-Port oder Trunk-Port?
- welches VLAN?
- welche MAC-Adressen gelernt?
- welche VLANs auf dem Trunk erlaubt?

```
- STP-Status?
- Port Security aktiv?
- Fehlerzähler?
- Broadcast- oder Multicast-Last?
- Logs zu Port-Änderungen?
```

Merksatz:

```
Der Switch zeigt oft,
wo Schicht-2-Probleme entstehen.
```

Schicht-2-Prüfung bei einem Client

Wenn ein Client Probleme hat, prüft man:

```
1. Link vorhanden?
2. richtiger Switch-Port?
3. Port aktiv?
4. richtiges VLAN?
5. MAC-Adresse gelernt?
6. Port Security aktiv?
7. DHCP aus richtigem Netz?
8. ARP zum Gateway vorhanden?
9. Gateway erreichbar?
10. Firewall oder Routing prüfen
```

Merksatz:

```
Beim Client erst Port und VLAN prüfen,
dann IP und Gateway.
```

Schicht-2-Prüfung bei einem Access Point

Bei einem Access Point mit mehreren SSIDs prüft man:

```
- Switch-Port als Trunk konfiguriert?
- richtige VLANs erlaubt?
```

- Native VLAN korrekt?
- SSID-VLAN-Zuordnung korrekt?
- Management-VLAN erreichbar?
- DHCP pro VLAN vorhanden?
- Firewall-Regeln passend?
- Client landet im richtigen VLAN?

Merksatz:

Mehrere SSIDs bedeuten oft mehrere VLANs über einen Trunk.

Schicht-2-Prüfung bei Switch-zu-Switch-Verbindung

Bei einer Verbindung zwischen Switches prüft man:

- Link aktiv?
- Trunk oder Access korrekt?
- gleiche VLANs vorhanden?
- allowed VLANs korrekt?
- Native VLAN korrekt?
- STP-Status korrekt?
- Link Aggregation korrekt?
- MAC-Adressen werden über erwarteten Port gelernt?
- keine Schleife vorhanden?

Merksatz:

Switch-zu-Switch-Verbindungen sind häufig Trunks und müssen sauber passen.

Schicht-2-Prüfung bei Server oder Virtualisierung

Bei Servern und Virtualisierung können mehrere MAC-Adressen über einen Port erscheinen.

Mögliche Gründe:

- virtuelle Maschinen
- Container
- Bridges

- VLAN-Trunks
- Bonding oder Teaming
- Hypervisor-Netzwerke

Wichtig:

Port Security oder falsche VLAN-Konfiguration kann hier Probleme verursachen.

Merksatz:

Virtualisierung kann mehrere MAC-Adressen hinter einem Port erzeugen.

Schicht-2-Fehler und höhere Symptome

Schicht-2-Fehler können wie Schicht-3- oder Anwendungsprobleme aussehen.

sichtbares Problem	mögliche Schicht-2-Ursache
keine IP-Adresse	falsches VLAN, Trunk-Fehler
falsche IP-Adresse	falsches VLAN
Gateway nicht erreichbar	ARP/VLAN-Problem
nur manche Server erreichbar	VLAN- oder Firewall-Zuordnung
WLAN-Gäste im internen Netz	falsche SSID-VLAN-Zuordnung
Netzwerk plötzlich langsam	Broadcast-Sturm oder Schleife
Verbindung instabil	MAC Flapping oder Port Security

Merksatz:

Viele IP-Probleme beginnen mit falscher Schicht-2-Zuordnung.

Schicht 2 oder Schicht 3?

Eine einfache Unterscheidung:

Frage	eher Schicht
Wird die MAC-Adresse gelernt?	2
Ist das richtige VLAN aktiv?	2

Frage	eher Schicht
Ist der Port Access oder Trunk?	2
Funktioniert ARP zum Gateway?	2 / 3
Hat der Client eine passende IP-Adresse?	3
Ist das Gateway korrekt?	3
Gibt es eine Route zum Ziel?	3
Ist ein TCP-Port erreichbar?	4

Merksatz:

```
MAC und VLAN = Schicht 2.
IP und Routing = Schicht 3.
```

Wichtige Befehle und Anzeigen

Je nach System oder Hersteller unterscheiden sich die Befehle.

Typische Informationen, die man sucht:

```
MAC-Adresstabelle anzeigen
VLAN-Zuordnung anzeigen
Port-Konfiguration anzeigen
Trunk-Status anzeigen
STP-Status anzeigen
ARP-Tabelle anzeigen
Port-Security-Status anzeigen
Logs anzeigen
```

Wichtig:

```
Nicht der konkrete Befehl ist immer prüfungsentscheidend,
sondern welche Information du damit prüfen willst.
```

Merksatz:

```
Bei Fehlersuche zählt:
Welche Information brauche ich?
```

Beispiel: Falsches VLAN

Fehlerbild:

```
Ein PC bekommt eine IP-Adresse aus dem Gastnetz,
obwohl er im Mitarbeiter-Netz sein soll.
```

Wahrscheinliche Schicht-2-Ursache:

```
Der Switch-Port ist im falschen VLAN.
```

Prüfung:

```
Port-Konfiguration prüfen.
VLAN-Zuordnung prüfen.
Dokumentation prüfen.
DHCP-Bereich vergleichen.
```

Lösung:

```
Port dem richtigen VLAN zuordnen.
```

Merksatz:

```
IP-Bereich verrät oft,
in welchem VLAN ein Client wirklich gelandet ist.
```

Beispiel: Access Point Gast-WLAN funktioniert nicht

Fehlerbild:

```
Mitarbeiter-WLAN funktioniert.
Gast-WLAN funktioniert nicht.
```

Mögliche Ursache:

VLAN für Gastnetz wird nicht über den Trunk transportiert.

Prüfung:

SSID-VLAN-Zuordnung prüfen.
Switch-Port zum Access Point prüfen.
Trunk-Konfiguration prüfen.
Allowed VLANs prüfen.
DHCP im Gast-VLAN prüfen.
Firewall-Regeln prüfen.

Merksatz:

Wenn nur eine SSID nicht funktioniert,
oft VLAN-Zuordnung oder Trunk prüfen.

Beispiel: Netzwerk plötzlich extrem langsam

Fehlerbild:

Das ganze lokale Netz ist plötzlich sehr langsam.

Mögliche Schicht-2-Ursachen:

- Broadcast-Sturm
- Layer-2-Schleife
- MAC Flapping
- defektes Gerät sendet massenhaft Frames
- STP falsch konfiguriert
- unmanaged Switch verursacht Schleife

Prüfung:

Switch-Auslastung prüfen.
Port-Statistiken prüfen.
MAC-Flapping-Meldungen prüfen.
STP-Status prüfen.

auffällige Ports isolieren.

Merksatz:

Plötzliche starke LAN-Probleme können Layer-2-Schleifen sein.

Was Schicht-2-Fehlersuche nicht löst

Nicht jedes Problem liegt auf Schicht 2.

Wenn MAC, VLAN, ARP und Switching korrekt sind, prüft man weiter:

- IP-Adresse
- Subnetzmaske
- Gateway
- Routing
- Firewall
- DNS
- TCP-/UDP-Port
- Anwendung
- Benutzerrechte

Merksatz:

Schicht 2 ist wichtig,
aber nicht jede Störung ist ein VLAN- oder Switch-Problem.

Typische IHK-Fragen

In AP1 und AP2 kann zum Beispiel gefragt werden:

- Welche Fehler gehören typischerweise zu Schicht 2?
- Warum kann ein falsches VLAN wie ein IP-Problem aussehen?
- Wie prüft man, ob ein Switch eine MAC-Adresse gelernt hat?
- Was bedeutet MAC Flapping?
- Was kann ein Broadcast-Sturm verursachen?
- Warum ist ein Trunk-Port wichtig?
- Was passiert, wenn ein VLAN auf einem Trunk nicht erlaubt ist?

- Warum kann Port Security ein Gerät blockieren?
- Was prüft man bei ARP-Problemen?
- Warum sollte man bei Netzwerkfehlern erst Schicht 1 und dann Schicht 2 prüfen?

Typische Prüfungsfallen

Falsches VLAN kann DHCP-Probleme verursachen.

Falsches VLAN kann wie falsche IP-Konfiguration wirken.

Ein Access-Port transportiert normalerweise ein VLAN.

Ein Trunk-Port transportiert mehrere VLANs.

VLAN auf Trunk nicht erlaubt = VLAN funktioniert über diese Verbindung nicht.

MAC-Adresse nicht gelernt kann auch Schicht 1 bedeuten.

MAC Flapping kann auf Schleifen hinweisen.

Broadcast-Sturm kann ein ganzes LAN stören.

STP-Blocking ist nicht automatisch ein Fehler.

Port Security kann legitime Geräte nach einem Wechsel blockieren.

ARP-Probleme können VLAN-, IP- oder Sicherheitsursachen haben.

Wichtige Begriffe kurz erklärt

Begriff	Kurze Erklärung
Schicht-2-Fehler	Fehler bei lokaler Frame-Weiterleitung
MAC-Adresstabelle	Zuordnung von MAC-Adresse zu Switch-Port
MAC Flapping	MAC-Adresse erscheint wechselnd an verschiedenen Ports
VLAN-Fehler	falsche logische Netzzuordnung
Access-Port	Port für ein VLAN
Trunk-Port	Port für mehrere VLANs

Begriff	Kurze Erklärung
Allowed VLANs	VLANs, die über einen Trunk erlaubt sind
Native VLAN	untagged VLAN auf einem Trunk
ARP-Problem	IP-MAC-Auflösung funktioniert nicht korrekt
Broadcast-Sturm	übermäßige Broadcast-Last
Layer-2-Schleife	Kreis im Switch-Netz
STP-Blocking	Port wird zur Schleifenvermeidung blockiert
Port Security	Begrenzung erlaubter MAC-Adressen
doppelte MAC-Adresse	gleiche MAC-Adresse mehrfach im Netz
Packet Capture	Mitschnitt von Netzwerkverkehr
Switch-Logs	Ereignisprotokolle des Switches

IHK-sichere Kurzformulierung

Fehlersuche auf OSI-Schicht 2 bedeutet, die lokale Weiterleitung von Ethernet-Frames zu prüfen. Dabei betrachtet man MAC-Adressen, MAC-Adresstabellen, Switch-Ports, VLANs, Access- und Trunk-Ports, ARP, STP und Broadcast-Domänen. Typische Schicht-2-Fehler sind falsche VLAN-Zuordnungen, nicht erlaubte VLANs auf Trunks, MAC Flapping, Broadcast-Stürme, Layer-2-Schleifen, ARP-Probleme oder blockierte Ports durch Port Security oder STP. Viele dieser Fehler wirken wie IP- oder DHCP-Probleme, obwohl die Ursache auf der lokalen Sicherungsschicht liegt.

Merksätze

Schicht-2-Fehlersuche = MAC, VLAN, Switch und ARP prüfen.

Erst Schicht 1,
dann Schicht 2.

MAC-Adresse gelernt?
VLAN richtig?
Port korrekt?

Falsches VLAN kann wie ein IP-Problem aussehen.

Keine IP-Adresse kann ein VLAN-Problem sein.

Falsche IP-Adresse kann falsches VLAN bedeuten.

Access-Port = ein VLAN.

Trunk-Port = mehrere VLANs.

VLAN auf Trunk nicht erlaubt = VLAN kommt nicht durch.

Native VLAN muss passen.

ARP zeigt,
ob IP und MAC lokal zusammenfinden.

MAC Flapping kann auf Schleifen hinweisen.

Broadcast-Sturm kann ein LAN lahmlegen.

STP blockiert Ports zur Schleifenvermeidung.

STP-Blocking ist nicht automatisch falsch.

Port Security kann Geräte blockieren.

Viele DHCP-Probleme beginnen auf Schicht 2.

MAC und VLAN = Schicht 2.

IP und Routing = Schicht 3.

Erst Link,
dann MAC/VLAN,
dann IP.