7.4 VLAN- und Switching-Fehleranalyse

Ein Client besitzt eine gültige IP-Konfiguration, kann aber bestimmte Geräte, Server oder Netze nicht erreichen. Andere Clients am gleichen Standort funktionieren möglicherweise problemlos. In solchen Fällen kann die Ursache auf der Sicherungsschicht liegen:

- falsches Access-VLAN,
- VLAN auf einem Switch nicht vorhanden,
- VLAN auf einem Trunk nicht zugelassen,
- Native-VLAN-Mismatch,
- fehlerhafte Portkonfiguration,
- blockierter Port durch Spanning Tree,
- gestörter EtherChannel,
- falsche MAC-Adresszuordnung,
- Port-Security-Verletzung,
- Schleife oder MAC-Flapping,
- physischer Fehler an Port oder Verkabelung.

Die Diagnose muss vom betroffenen Endgerät über jeden beteiligten Switch bis zum Gateway beziehungsweise Zielsystem erfolgen.

> Ein Symptom ist noch keine Ursache. Ein erreichbarer Switch beweist nicht, dass das betroffene VLAN auf dem vollständigen Datenpfad korrekt transportiert wird.

---

1. Typische Fehlerbilder

Beobachtung	Mögliche Ursache
nur ein Client ist betroffen	Access-Port, Kabel, Netzwerkkarte, VLAN-Zuordnung oder Port-Security
alle Clients an einem Switch sind betroffen	Uplink, Trunk, EtherChannel, STP oder Switchausfall
nur ein VLAN ist betroffen	VLAN fehlt, Trunk-Liste, SVI, Gateway oder STP-Instanz
Clients im gleichen VLAN kommunizieren nicht	falsches VLAN, Port-Isolation, Private VLAN, ACL oder lokale Firewall
lokale Geräte sind erreichbar, Gateway nicht	Uplink, Trunk, SVI oder Gateway
Gateway erreichbar, andere VLANs nicht	Routing, ACL oder Firewall statt reines Layer-2-Problem
Fehler tritt nur an einem Standort auf	lokaler Switch, Trunk, Standort-Uplink oder VLAN-Bereitstellung
Fehler tritt nur an einem Port auf	Portkonfiguration, Kabel, Port-Security oder Hardware
Verbindung funktioniert nach Umstecken	unterschiedliche VLAN- oder Portkonfiguration

Beobachtung	Mögliche Ursache
Verbindung fällt wiederholt kurz aus	Link-Flapping, STP-Änderungen, EtherChannel oder Hardware
IP-Telefon funktioniert, angeschlossener PC nicht	Voice-VLAN korrekt, Data-VLAN oder Trunk zum Telefon fehlerhaft
DHCP funktioniert nicht, statische IP teilweise schon	DHCP-Relay, DHCP-Serverpfad oder falsches VLAN
MAC-Adresse erscheint ständig an anderen Ports	Schleife, falsch verbundene Switches oder MAC-Flapping

---

2. Sollzustand vor der Diagnose feststellen

Vor der Fehlersuche muss bekannt sein, wie der Port und der Datenpfad vorgesehen sind.

Zu dokumentieren sind:

- betroffener Client,
- MAC-Adresse des Clients,
- Switchname,
- physischer Switchport,
- vorgesehenes Access-VLAN,
- gegebenenfalls Voice-VLAN,
- IP-Subnetz des VLANs,
- vorgesehene Gateway-Adresse,
- beteiligte Uplinks,
- beteiligte Trunks,
- erlaubte VLANs auf jedem Trunk,
- Native VLAN,
- zuständiges SVI oder Router-Subinterface,
- mögliche EtherChannels,
- verwendete Spanning-Tree-Variante,
- Zeitpunkt und Umfang der Störung.

Beispiel:

```
Client:            client01
MAC-Adresse:       00:11:22:33:44:55
Switch:            access-sw01
Port:              GigabitEthernet1/0/12
Access-VLAN:       20
IP-Netz:           192.0.2.0/24
Gateway:           192.0.2.1
Uplink:            GigabitEthernet1/0/48
Trunk-VLANs:       10,20,30
```

```
Distribution-Switch: dist-sw01
SVI:                 Vlan20
```

Ohne diesen Sollzustand lässt sich eine vorhandene Konfiguration nicht zuverlässig als richtig oder falsch bewerten.

---

3. Umfang der Störung bestimmen

Zuerst prüfen:

- ist nur ein Client betroffen,
- sind mehrere Clients am gleichen Portpfad betroffen,
- betrifft der Fehler alle Ports eines Switches,
- betrifft der Fehler nur ein VLAN,
- betrifft er mehrere VLANs,
- betrifft er nur einen Switch,
- betrifft er mehrere Switches,
- funktioniert die Kommunikation innerhalb des VLANs,
- funktioniert die Kommunikation zum Gateway,
- funktioniert die Kommunikation zwischen VLANs,
- begann die Störung nach einer Änderung?

Vergleichstests

Vergleich	Aussage
anderer Client am gleichen Port	grenzt Client und Port gegeneinander ab
gleicher Client an bekannt funktionierendem Port	prüft Client gegen Switchport
anderer Client im gleichen VLAN	prüft Umfang innerhalb des VLANs
Client in anderem VLAN am gleichen Switch	grenzt VLAN gegen allgemeinen Switchfehler ab
gleiches VLAN an anderem Switch	grenzt lokalen Switch oder Uplink ein
Gateway desselben VLANs	prüft den Layer-2-Pfad bis zum Gateway
Ziel im gleichen Subnetz	prüft lokale Layer-2-Kommunikation
Ziel in anderem Subnetz	bezieht zusätzlich Routing und Firewall ein

Ein Gerät darf nur kontrolliert umgesteckt werden. Vorher müssen ursprünglicher Port, VLAN-Zuordnung und Konfiguration dokumentiert werden.

---

4. Clientkonfiguration prüfen

Unter Windows:

```
ipconfig /all
```

```
Get-NetAdapter
```

```
Get-NetIPConfiguration
```

```
Get-NetIPAddress
```

```
Get-NetRoute -AddressFamily IPv4
```

Unter Linux:

```
ip link show
```

```
ip address show
```

```
ip route show
```

Unter macOS:

```
ifconfig
```

```
route -n get default
```

Zu prüfen sind:

- ist der richtige Adapter aktiv,
- besitzt der Client eine Adresse aus dem vorgesehenen Subnetz,
- stimmt die Präfixlänge,
- stimmt das Standardgateway,
- stammt die Adresse aus dem erwarteten DHCP-Bereich,
- existieren zusätzliche aktive Adapter,
- verwendet der Client selbst VLAN-Tagging,
- ist eine Bridge oder virtuelle Netzwerkkarte aktiv,
- läuft eine VM oder ein Container mit eigener Netzwerkkonfiguration?

Eine gültig aussehende IP-Adresse beweist nicht, dass der Client am richtigen VLAN angeschlossen ist. In verschiedenen VLANs können ähnliche oder versehentlich überlappende Adressbereiche vorkommen.

---

5. Physische Verbindung und Portstatus prüfen

Am Client prüfen:

```
Get-NetAdapter |
    Format-Table Name, InterfaceDescription, Status, LinkSpeed, MacAddress
```

Auf einem Cisco-IOS-/IOS-XE-Switch beispielsweise:

```
show interfaces status
```

Gezielten Port prüfen:

```
show interfaces GigabitEthernet1/0/12
```

Kurze Fehlerübersicht:

```
show interfaces counters errors
```

Zu prüfen sind:

- Portstatus,
- ausgehandeltes Tempo,
- Duplexmodus,
- Ein- und Ausgangsfehler,
- CRC-Fehler,
- Drops,
- Link-Flapping,
- Zeitpunkt der letzten Statusänderung,
- administrativ deaktivierter Port,
- Fehlerzustand wie `err-disabled`.

Typische Bewertungen

Status oder Zähler	Mögliche Ursache
`notconnect`	kein Link, Kabel, Client oder Gegenstelle

Status oder Zähler	Mögliche Ursache
`disabled`	Port administrativ deaktiviert
`err-disabled`	Schutzfunktion oder erkannter Fehler
viele CRC-Fehler	Kabel, Stecker, Transceiver, Duplex oder physische Störung
viele Input Errors	physischer Fehler, Überlastung oder fehlerhafte Frames
viele Output Drops	Überlastung oder Warteschlange
Geschwindigkeit unerwartet niedrig	Kabel, Aushandlung oder Gegenstelle
Link wechselt ständig	Kabel, Netzwerkkarte, Transceiver, Energieversorgung oder Port

Zähler sollten zuerst dokumentiert und danach über einen festgelegten Zeitraum erneut abgelesen werden. Ein hoher historischer Wert allein beweist keinen aktuell fortbestehenden Fehler.

---

6. Nachbarschaft und tatsächlichen Port ermitteln

Cisco Discovery Protocol:

```
show cdp neighbors
```

Details:

```
show cdp neighbors detail
```

Link Layer Discovery Protocol:

```
show lldp neighbors
```

Details:

```
show lldp neighbors detail
```

Zu prüfen sind:

- welches Gerät tatsächlich angeschlossen ist,
- welcher lokale Port verwendet wird,
- welcher Gegenstellenport gemeldet wird,
- ob statt eines Clients ein weiterer Switch angeschlossen ist,
- ob ein IP-Telefon zwischen Client und Switch liegt,

- ob die dokumentierte Verkabelung mit der erkannten Topologie übereinstimmt.

CDP oder LLDP kann deaktiviert sein. Ein fehlender Nachbar beweist deshalb nicht, dass keine Verbindung besteht.

---

7. VLAN-Zuordnung des Access-Ports prüfen

VLAN-Übersicht:

```
show vlan brief
```

Portbezogene Switchportinformationen:

```
show interfaces GigabitEthernet1/0/12 switchport
```

Relevante Portkonfiguration:

```
show running-config interface GigabitEthernet1/0/12
```

Zu prüfen sind:

- administrativer Portmodus,
- tatsächlich verwendeter Portmodus,
- Access-VLAN,
- Voice-VLAN,
- Native VLAN bei einem Trunk,
- erlaubte VLANs,
- dynamische oder fest konfigurierte Aushandlung,
- zusätzliche Sicherheits- oder Authentifizierungsfunktionen.

Beispiel eines vorgesehenen Access-Ports:

```
interface GigabitEthernet1/0/12
 switchport mode access
 switchport access vlan 20
```

Mögliche Fehler

```
switchport access vlan 10
```

obwohl der Client VLAN 20 verwenden soll.

Oder der Port arbeitet unerwartet als Trunk:

```
switchport mode trunk
```

Eine Konfigurationszeile allein reicht nicht zur Bewertung. Administrative und operative Zustände müssen miteinander verglichen werden.

---

8. Existenz und Status des VLANs prüfen

```
show vlan brief
```

Gezielt:

```
show vlan id 20
```

Zu prüfen sind:

- existiert VLAN 20,
- ist es aktiv,
- besitzt es den erwarteten Namen,
- sind die vorgesehenen Access-Ports zugeordnet,
- existiert das VLAN auf jedem beteiligten Switch,
- wurde es möglicherweise gelöscht oder umnummeriert,
- ist eine VLAN-Verwaltung wie VTP beteiligt?

Wichtig

Ein Access-Port kann auf ein VLAN verweisen, das auf dem Switch nicht ordnungsgemäß vorhanden oder aktiv ist. Ebenso beweist die Existenz des VLANs auf einem Access-Switch nicht, dass es auf allen weiteren Switches des Pfades verfügbar ist.

VLANs dürfen nicht vorschnell neu angelegt werden. Zuerst muss geklärt werden, ob das VLAN absichtlich entfernt wurde oder über ein vorgesehenes Verwaltungsverfahren bereitgestellt werden soll.

---

9. MAC-Adresse des Clients ermitteln

Unter Windows:

```
Get-NetAdapter |
    Format-Table Name, MacAddress, Status
```

Unter Linux:

```
ip link show
```

Unter macOS:

```
ifconfig
```

Die MAC-Adresse muss dem tatsächlich verwendeten physischen Adapter zugeordnet werden. WLAN-, Ethernet-, Docking-, VPN- und virtuelle Adapter besitzen unterschiedliche MAC-Adressen.

Beispiel:

```
00-11-22-33-44-55
```

Auf Cisco-Switches wird sie normalerweise ohne Trennzeichen oder mit Punktgruppen gesucht:

```
0011.2233.4455
```

---

10. MAC-Adress-Tabelle prüfen

Gesamte Tabelle:

```
show mac address-table
```

Bestimmte MAC-Adresse suchen:

```
show mac address-table address 0011.2233.4455
```

MAC-Adressen eines VLANs:

```
show mac address-table vlan 20
```

MAC-Adressen eines Ports:

```
show mac address-table interface GigabitEthernet1/0/12
```

Zu prüfen sind:

- wird die Client-MAC gelernt,
- wird sie im richtigen VLAN gelernt,
- erscheint sie am erwarteten Port,
- erscheint sie auf einem Uplink statt am lokalen Clientport,
- wechselt sie zwischen mehreren Ports,
- fehlt sie vollständig,
- ist der Eintrag dynamisch oder statisch?

Bewertung

Beobachtung	Mögliche Ursache
MAC am richtigen Access-Port und VLAN	lokaler Layer-2-Eingang grundsätzlich erkannt
MAC im falschen VLAN	falsche Access-, Voice- oder Tagging-Konfiguration
MAC auf falschem Port	falsche Dokumentation, Verkabelung oder Schleife
MAC nur am Uplink	Client befindet sich hinter einem anderen Gerät
MAC fehlt	Client sendet nicht, falscher Port, Linkproblem oder Filterung
MAC wechselt zwischen Ports	Schleife, doppelte Verbindung oder MAC-Flapping
sehr viele MAC-Adressen am Clientport	möglicherweise weiterer Switch oder Bridge angeschlossen

Die MAC-Adresse muss auf jedem Switch entlang des Pfades verfolgt werden. Auf einem Access-Switch sollte sie am Clientport erscheinen, auf nachgelagerten Switches am jeweiligen Uplink in Richtung des Clients.

---

11. Layer-2-Pfad anhand der MAC-Adresse verfolgen

Beispiel:

```
Client
  |
  | Gi1/0/12, VLAN 20
  |
Access-Switch
  |
  | Gi1/0/48, Trunk
```

```
  |
Distribution-Switch
  |
  | Port-Channel1, Trunk
  |
Gateway-SVI Vlan20
```

Prüfung auf dem Access-Switch:

```
show mac address-table address 0011.2233.4455
```

Erwartung:

```
VLAN 20 -> GigabitEthernet1/0/12
```

Prüfung auf dem Distribution-Switch:

```
show mac address-table address 0011.2233.4455
```

Erwartung:

```
VLAN 20 -> GigabitEthernet1/0/48
```

oder:

```
VLAN 20 -> Port-channel1
```

Verschwindet die MAC-Adresse an einem Übergang, sind insbesondere zu prüfen:

- VLAN auf dem nächsten Switch vorhanden,
- VLAN am Trunk zugelassen,
- Trunk tatsächlich aktiv,
- STP-Status des VLANs,
- EtherChannel-Zustand,
- Native-VLAN-Konfiguration,
- physische Verbindung.

---

12. Trunkstatus prüfen

Trunkübersicht:

```
show interfaces trunk
```

Gezielten Port prüfen:

```
show interfaces GigabitEthernet1/0/48 switchport
```

Konfiguration anzeigen:

```
show running-config interface GigabitEthernet1/0/48
```

Zu prüfen sind:

- ist der Port operativ ein Trunk,
- wird IEEE 802.1Q verwendet,
- welches Native VLAN ist konfiguriert,
- welche VLANs sind administrativ zugelassen,
- welche VLANs sind aktiv,
- welche VLANs werden tatsächlich weitergeleitet,
- welche VLANs sind durch Spanning Tree nicht blockiert?

Beispiel:

```
interface GigabitEthernet1/0/48
 switchport mode trunk
 switchport trunk native vlan 999
 switchport trunk allowed vlan 10,20,30
```

Wenn VLAN 20 benötigt wird, muss es auf jedem Trunk des vollständigen Pfades zugelassen und aktiv sein.

---

13. Allowed-VLAN-Liste auf jedem Trunk vergleichen

```
show interfaces trunk
```

Beispiel eines Fehlers:

```
Access-Switch:
Allowed VLANs: 10,20,30
```

```
Distribution-Switch:
Allowed VLANs: 10,30
```

VLAN 20 ist nur auf einer Seite zugelassen. Geräte in VLAN 10 und VLAN 30 funktionieren, während VLAN 20 den Trunk nicht vollständig passieren kann.

Typische Ursachen

- VLAN bei einer Änderung aus der Liste entfernt,
- VLAN nur auf einer Trunkseite ergänzt,
- falscher Uplink bearbeitet,
- VLAN-Liste versehentlich vollständig ersetzt,
- EtherChannel-Mitglieder besitzen unterschiedliche Konfigurationen,
- VLAN existiert auf einem Switch nicht.

Eine Allowed-VLAN-Liste darf nicht pauschal auf „alle VLANs“ erweitert werden. Dadurch können Segmentierung, Sicherheit und vorgesehene Netzgrenzen verändert werden.

---

14. Native VLAN prüfen

Auf beiden Seiten des Trunks:

```
show interfaces trunk
```

```
show interfaces <trunk-port> switchport
```

Beispiel eines Mismatch:

```
Switch A: Native VLAN 999
Switch B: Native VLAN 1
```

Mögliche Auswirkungen:

- ungetaggter Verkehr landet auf beiden Seiten in unterschiedlichen VLANs,
- Spanning Tree meldet eine PVID-Inkonsistenz,
- ein Port oder VLAN wird durch Schutzmechanismen blockiert,
- Verwaltungs- oder Steuerverkehr erreicht ein falsches VLAN,

- Sicherheitsrisiken durch unbeabsichtigte VLAN-Zuordnung.

Native VLANs müssen entsprechend der vorgesehenen Architektur auf beiden Seiten übereinstimmen. Ein Mismatch darf nicht dadurch „gelöst“ werden, dass wahllos VLAN 1 verwendet wird.

---

15. Access-Port und Trunk nicht verwechseln

Access-Port

- transportiert normalerweise den Datenverkehr genau eines Data-VLANs,
- Endgerät sendet üblicherweise ungetaggte Ethernet-Frames,
- Switch ordnet eingehende Frames dem Access-VLAN zu.

Trunk-Port

- transportiert mehrere VLANs,
- VLAN-Zuordnung erfolgt normalerweise über IEEE 802.1Q-Tags,
- Native-VLAN-Verkehr kann abhängig von der Konfiguration ungetaggt sein.

Typische Fehlkonfigurationen

Seite A	Seite B	Mögliche Folge
Access VLAN 20	Access VLAN 20	korrekt für eine einfache Verbindung im selben VLAN
Trunk	Trunk	korrekt, wenn VLANs und Native VLAN übereinstimmen
Access	Trunk	VLAN-Mismatch und unerwartete Zuordnung
Access VLAN 10	Access VLAN 20	ungetaggter Verkehr wird verschiedenen VLANs zugeordnet
Trunk mit VLAN 20	Trunk ohne VLAN 20	VLAN 20 kann den Pfad nicht vollständig nutzen
Trunk Native 999	Trunk Native 1	Native-VLAN-Mismatch

---

16. Clientseitiges VLAN-Tagging berücksichtigen

Ein normaler Arbeitsplatzclient sendet an einem Access-Port gewöhnlich keine VLAN-Tags. VLAN-Tagging am Client kann jedoch vorkommen bei:

- Servern mit mehreren VLANs,
- Hypervisoren,
- virtuellen Switches,
- Containernetzwerken,

- Firewalls,
- Access Points,
- IP-Telefonen,
- Netzwerktestgeräten,
- speziellen Netzwerkkartentreibern.

Zu prüfen sind:

- ist am Client eine VLAN-ID konfiguriert,
- erwartet der Switch einen Access-Port oder Trunk,
- stimmt die VLAN-ID des Clients mit der Switchkonfiguration überein,
- entfernt der Netzwerkkartentreiber VLAN-Tags,
- existiert ein Hypervisor-vSwitch mit eigener VLAN-Zuordnung,
- wird das Tag bereits an einer anderen Ebene hinzugefügt?

Beispiel eines Fehlers:

```
Server-NIC taggt VLAN 20
Switchport ist Access-Port in VLAN 20
```

Abhängig von Gerät und Konfiguration kann der getaggte Frame verworfen oder unerwartet verarbeitet werden.

---

17. Voice-VLAN und IP-Telefone prüfen

Beispiel:

```
interface GigabitEthernet1/0/12
 switchport mode access
 switchport access vlan 20
 switchport voice vlan 30
```

Dabei kann gelten:

```
PC-Daten:       VLAN 20
Telefonverkehr: VLAN 30
```

Zu prüfen sind:

- funktioniert nur Telefonie oder nur der PC,
- ist das Data-VLAN korrekt,
- ist das Voice-VLAN korrekt,

- erkennt das Telefon die VLAN-Information,
- ist der PC-Port des Telefons aktiv,
- wird das Telefon per LLDP-MED oder CDP konfiguriert,
- sind beide VLANs auf dem Uplink zugelassen,
- existieren DHCP und Gateway in beiden VLANs?

Dass das Telefon funktioniert, beweist nicht, dass auch das Data-VLAN korrekt eingerichtet ist.

---

18. ARP beziehungsweise Neighbor Cache prüfen

Unter Windows:

```
Get-NetNeighbor
```

```
arp -a
```

Unter Linux:

```
ip neighbor show
```

Unter macOS:

```
arp -a
```

Zu prüfen sind:

- besitzt der Client einen Eintrag für das Gateway,
- ist der Eintrag erreichbar oder unvollständig,
- stimmt die MAC-Adresse des Gateways,
- ändert sich die Gateway-MAC unerwartet,
- antworten Geräte im gleichen Subnetz auf ARP?

Bewertung

Beobachtung	Mögliche Eingrenzung
Gateway-Eintrag ist erreichbar	Layer-2-Kommunikation zum Gateway grundsätzlich möglich
Gateway bleibt `Incomplete`	ARP-Anfrage oder Antwort erreicht das Ziel nicht
falsche Gateway-MAC	falsches Gerät, doppelte IP, Fehlkonfiguration oder Angriff
lokales Ziel im gleichen VLAN nicht auflösbar	Layer-2-Pfad, Zielgerät oder lokale Firewall prüfen

Beobachtung	Mögliche Eingrenzung
Gateway erreichbar, anderes Subnetz nicht	Routing, ACL oder Firewall untersuchen

ARP darf erst nach Dokumentation kontrolliert geleert werden. Ein Cache-Reset beseitigt sonst möglicherweise relevante Hinweise.

---

19. Gateway-SVI prüfen

Auf einem Layer-3-Switch beispielsweise:

```
show ip interface brief
```

Gezielt:

```
show interfaces Vlan20
```

Konfiguration:

```
show running-config interface Vlan20
```

ARP-Tabelle:

```
show ip arp
```

Zu prüfen sind:

- existiert das SVI,
- besitzt es die vorgesehene IP-Adresse,
- ist es administrativ aktiv,
- ist der Protokollstatus aktiv,
- ist das zugehörige VLAN vorhanden und aktiv,
- existiert mindestens ein erforderlicher aktiver Layer-2-Pfad,
- wird die Client-MAC beziehungsweise IP gelernt,
- ist ein Redundanzprotokoll beteiligt?

Typisches Fehlerbild

```
Vlan20 is administratively up, line protocol is down
```

Mögliche Ursache:

- VLAN 20 existiert nicht aktiv,
- kein zugehöriger Layer-2-Port ist aktiv,
- VLAN wird nicht über einen funktionierenden Trunk transportiert,
- plattformspezifische Voraussetzungen sind nicht erfüllt.

Ein erreichbares SVI in einem anderen VLAN beweist nicht, dass das SVI des betroffenen VLANs funktioniert.

---

20. Kommunikation innerhalb und außerhalb des VLANs trennen

Vom Client aus nacheinander prüfen:

1. eigene IP-Konfiguration,
2. Ziel im gleichen VLAN,
3. Standardgateway,
4. Ziel in einem anderen internen VLAN,
5. externes Ziel.

Windows:

```
Test-NetConnection -ComputerName <ziel-im-gleichen-vlan>
```

```
Test-NetConnection -ComputerName <gateway-ip>
```

```
Test-NetConnection -ComputerName <ziel-in-anderem-vlan> -Port <port>
```

Bewertung

Gleiches VLAN	Gateway	Anderes VLAN	Eingrenzung
fehlerhaft	fehlerhaft	fehlerhaft	Access-VLAN, Layer-2-Pfad oder Client prüfen
erfolgreich	fehlerhaft	fehlerhaft	Gateway-SVI, Trunk oder Gateway prüfen
erfolgreich	erfolgreich	fehlerhaft	Routing, ACL oder Firewall prüfen
erfolgreich	erfolgreich	erfolgreich	konkrete Anwendung oder Zielport prüfen

Ping kann durch eine Firewall blockiert werden. Für die Prüfung eines Dienstes ist zusätzlich der tatsächlich benötigte TCP- oder UDP-Port zu berücksichtigen.

---

21. Spanning-Tree-Zustand prüfen

Übersicht:

```
show spanning-tree
```

Bestimmtes VLAN:

```
show spanning-tree vlan 20
```

Bestimmten Port:

```
show spanning-tree interface GigabitEthernet1/0/48 detail
```

Zu prüfen sind:

- Root Bridge,
- Root Port,
- Designated Ports,
- blockierende beziehungsweise verwerfende Ports,
- Kosten und Prioritäten,
- Topology Changes,
- letzte Statusänderungen,
- inkonsistente Ports,
- unterschiedliche STP-Modi,
- unerwartete Root Bridge.

Ein durch Spanning Tree blockierter redundanter Port ist nicht automatisch fehlerhaft. Die Blockierung kann notwendig sein, um eine Layer-2-Schleife zu verhindern.

Problematisch ist beispielsweise:

- der einzige vorgesehene Pfad wird blockiert,
- Root Bridge befindet sich unerwartet an einem Access-Switch,
- Ports wechseln wiederholt ihren Zustand,
- VLANs verwenden unbeabsichtigt unterschiedliche Pfade,
- PVID- oder Type-Inconsistency wird gemeldet.

---

22. Spanning-Tree-Änderungen und Schleifen untersuchen

```
show spanning-tree detail
```

Zusätzlich Systemprotokoll prüfen:

```
show logging
```

Hinweise auf mögliche Schleifen:

- sehr viele Topology Changes,
- MAC-Adresse wechselt zwischen Ports,
- Broadcast- oder Multicast-Auslastung steigt stark,
- Switchmanagement reagiert langsam,
- mehrere Ports zeigen ungewöhnlich hohe Auslastung,
- Netzwerk fällt periodisch aus,
- STP-Root oder Root Port wechselt wiederholt.

Die physische Schleife darf nicht durch dauerhaftes Deaktivieren von Spanning Tree „behoben“ werden. Dadurch kann die Störung massiv verschärft werden.

---

23. MAC-Flapping prüfen

Protokolle untersuchen:

```
show logging
```

MAC-Adresse gezielt suchen:

```
show mac address-table address <mac-adresse>
```

Wiederholt prüfen, ob der Port wechselt.

Beispiel:

```
VLAN 20, MAC 0011.2233.4455:
Gi1/0/47 -> Gi1/0/48 -> Gi1/0/47
```

Mögliche Ursachen:

- Layer-2-Schleife,
- zwei aktive Verbindungen desselben Endgeräts ohne korrektes Teaming,
- falsch aufgebauter EtherChannel,
- nicht verwalteter Switch,
- Bridge auf einem Client,

- Hypervisor- oder Clusterkonfiguration,
- absichtlich bewegte virtuelle MAC-Adresse,
- Redundanzprotokoll.

Ein MAC-Wechsel ist nicht immer ein Fehler. Bei Clustern oder Redundanzmechanismen kann eine virtuelle MAC kontrolliert den Port wechseln. Häufigkeit, Zeitpunkt und vorgesehene Architektur müssen berücksichtigt werden.

---

24. EtherChannel beziehungsweise Port-Channel prüfen

Übersicht:

```
show etherchannel summary
```

Port-Channel prüfen:

```
show interfaces Port-channel1
```

Trunkstatus:

```
show interfaces trunk
```

Konfiguration der Mitglieder vergleichen:

```
show running-config interface GigabitEthernet1/0/47
```

```
show running-config interface GigabitEthernet1/0/48
```

Zu prüfen sind:

- gehören alle vorgesehenen Ports zum Channel,
- sind die Ports tatsächlich gebündelt,
- verwenden beide Seiten dasselbe Verfahren,
- stimmen Access- oder Trunkmodus überein,
- stimmen Native VLAN und Allowed-VLAN-Liste überein,
- stimmen Geschwindigkeit und Duplex,
- ist der Port-Channel durch STP freigegeben,
- sind einzelne Mitglieder suspendiert oder eigenständig aktiv?

Typische Fehler

- ein Link ist nicht im Bundle,
- LACP ist nur auf einer Seite passend konfiguriert,
- Mitglieder besitzen unterschiedliche VLAN-Listen,
- physische Ports werden einzeln statt über den Port-Channel konfiguriert,
- ein paralleler Link bildet unbeabsichtigt eine Schleife.

---

25. Port-Security prüfen

Auf Cisco-Switches beispielsweise:

```
show port-security
```

Gezielter Port:

```
show port-security interface GigabitEthernet1/0/12
```

Portstatus:

```
show interfaces status err-disabled
```

Zu prüfen sind:

- ist Port-Security aktiviert,
- wie viele MAC-Adressen sind erlaubt,
- welche MAC-Adressen wurden gelernt,
- liegt eine Verletzung vor,
- welche Reaktion wurde ausgelöst,
- wurde der Port deaktiviert,
- wurde ein anderes Endgerät oder Dock angeschlossen?

Typisches Fehlerbild

Ein Arbeitsplatz wird von einem PC auf eine Dockingstation umgestellt. Dadurch erscheint eine neue MAC-Adresse. Wenn nur eine bestimmte MAC zugelassen ist, kann der Port den Verkehr verwerfen oder in einen Fehlerzustand wechseln.

Port-Security darf nicht pauschal deaktiviert werden. Zuerst sind vorgesehene Sicherheitsrichtlinie, erlaubte Geräte und tatsächlich erkannte MAC-Adressen zu prüfen.

---

26. Weitere Schutzfunktionen berücksichtigen

Abhängig von der Umgebung können unter anderem beteiligt sein:

- 802.1X,
- MAC Authentication Bypass,
- Dynamic VLAN Assignment,
- DHCP Snooping,
- Dynamic ARP Inspection,
- IP Source Guard,
- BPDU Guard,
- Root Guard,
- Loop Guard,
- Storm Control,
- Private VLANs,
- Port-Isolation,
- Access Control Lists,
- Network Access Control.

Mögliche Prüfungen auf Cisco-Geräten:

```
show authentication sessions
```

```
show dot1x all
```

```
show ip dhcp snooping
```

```
show ip arp inspection
```

```
show interfaces status err-disabled
```

```
show logging
```

Die tatsächlich verfügbaren Befehle hängen von Plattform und Softwareversion ab.

Typische Fehlerbilder

Beobachtung	Mögliche Funktion
Port erhält nach Anmeldung anderes VLAN	802.1X oder dynamische VLAN-Zuweisung
DHCP-Antworten werden verworfen	DHCP Snooping
ARP-Pakete werden verworfen	Dynamic ARP Inspection

Beobachtung	Mögliche Funktion
Port nach Anschluss eines Switches deaktiviert	BPDU Guard
Datenverkehr oberhalb eines Grenzwerts verworfen	Storm Control
Clients im gleichen VLAN sehen sich nicht	Port-Isolation oder Private VLAN
nur autorisierte MAC funktioniert	Port-Security oder NAC

---

27. `err-disabled`-Ursache untersuchen

```
show interfaces status err-disabled
```

```
show errdisable recovery
```

```
show logging
```

Je nach Plattform können Ursachen sein:

- BPDU Guard,
- Port-Security,
- Link-Flapping,
- EtherChannel-Fehlkonfiguration,
- UDLD,
- Loopback-Erkennung,
- DHCP-Ratenbegrenzung,
- Sicherheitsverletzung.

Der Port darf nicht einfach wieder aktiviert werden, ohne die Ursache zu beseitigen. Andernfalls tritt der Fehler erneut auf oder eine Schleife wird wieder in Betrieb genommen.

Kontrollierte Wiederaktivierung erst nach Ursachenklärung:

```
interface <port>
 shutdown
 no shutdown
```

Dieser Eingriff verändert den Zustand und unterbricht die Verbindung. Er darf nur autorisiert und nach Sicherung der Diagnoseinformationen erfolgen.

---

28. Paketmitschnitt für VLAN-Tags verwenden

Ein Paketmitschnitt kann zeigen:

- ob Frames VLAN-Tags besitzen,
- welche VLAN-ID verwendet wird,
- ob ARP-Anfragen gesendet werden,
- ob ARP-Antworten zurückkommen,
- ob DHCP Discover und Offer sichtbar sind,
- ob nur eine Richtung des Verkehrs vorhanden ist,
- ob LLDP- oder STP-Informationen auftreten.

Wireshark-Anzeigefilter für VLAN-Verkehr:

```
vlan
```

Bestimmte VLAN-ID:

```
vlan.id == 20
```

ARP:

```
arp
```

DHCP:

```
dhcp
```

LLDP:

```
lldp
```

STP:

```
stp
```

Wichtig

Ein Endgerät an einem normalen Access-Port sieht üblicherweise keine IEEE-802.1Q-Tags für sein Access-VLAN. Der Switch fügt die VLAN-Zuordnung intern hinzu beziehungsweise entfernt das Tag am Access-Port.

Für eine aussagekräftige Analyse auf einem Switch kann ein kontrolliert konfigurierter Mirror- oder SPAN-Port erforderlich sein. Mitschnitte dürfen nur autorisiert erfolgen und können vertrauliche Daten, Adressen, Namen und Anmeldeinformationen enthalten.

Netzwerkkarten und Treiber können VLAN-Tags vor der Übergabe an die Aufzeichnungssoftware verarbeiten. Das Fehlen eines sichtbaren Tags beweist daher nicht in jedem Mitschnitt, dass auf dem beobachteten Netzwerkpfad kein Tag verwendet wurde.

---

29. Beispiel für eine systematische Diagnose

Symptom

Ein Client erhält keine Verbindung zu internen Diensten. Andere Clients am gleichen Switch funktionieren.

Sollzustand

```
Clientport:    GigabitEthernet1/0/12
Access-VLAN:   20
Gateway:       192.0.2.1
Uplink:        GigabitEthernet1/0/48
```

Clientprüfung

```
ipconfig /all
```

Ergebnis:

```
IPv4-Adresse: 192.0.2.45
Gateway:      192.0.2.1
```

Portprüfung

```
show interfaces GigabitEthernet1/0/12 switchport
```

Ergebnis:

```
Operational Mode: static access
Access Mode VLAN: 20
```

MAC-Prüfung

```
show mac address-table address 0011.2233.4455
```

Ergebnis:

```
VLAN 20    0011.2233.4455    DYNAMIC    Gi1/0/12
```

Der Client wird am richtigen lokalen Port und im richtigen VLAN gelernt.

Trunkprüfung

```
show interfaces trunk
```

Ergebnis am Access-Switch:

```
Port Gi1/0/48
Allowed VLANs: 10,20,30
```

Ergebnis am Distribution-Switch:

```
Port Gi1/0/48
Allowed VLANs: 10,30
```

Festgestellte Ursache

VLAN 20 war auf der Distribution-Seite des Trunks nicht zugelassen. Dadurch wurde die Client-MAC am Access-Switch gelernt, der Datenverkehr erreichte jedoch nicht das Gateway.

Kontrollierte Maßnahme

Nach Prüfung des Sollzustands und Sicherung der Konfiguration wurde VLAN 20 auf der fehlenden Trunkseite ergänzt.

Nachprüfung

Auf beiden Switches:

```
show interfaces trunk
```

Ergebnis:

```
Allowed VLANs: 10,20,30
```

MAC-Adresse auf dem Distribution-Switch:

```
show mac address-table address 0011.2233.4455
```

Ergebnis:

```
VLAN 20    0011.2233.4455    DYNAMIC    Gi1/0/48
```

Clienttest:

```
Test-NetConnection -ComputerName 192.0.2.1
```

Der Client erreicht anschließend das Gateway und die vorgesehenen Dienste.

---

30. Beispiel „Port sieht korrekt aus, Client ist trotzdem im falschen VLAN“

Symptom

Der Client ist an Port `GigabitEthernet1/0/12` dokumentiert. Die Prüfung dieses Ports zeigt das richtige VLAN. Der Client erhält trotzdem eine Adresse aus einem anderen Subnetz.

Prüfung der MAC-Adresse

```
show mac address-table address 0011.2233.4455
```

Ergebnis:

```
VLAN 30    0011.2233.4455    DYNAMIC    Gi1/0/18
```

Festgestellte Ursache

Der Client war physisch an Port `GigabitEthernet1/0/18` angeschlossen. Die Dokumentation war veraltet. Port 18 gehörte zu VLAN 30.

Lehre

Nicht nur den dokumentierten Port prüfen. Der tatsächliche Port muss anhand von MAC-Adresse, LLDP/CDP, Verkabelung oder Portstatus bestätigt werden.

---

31. Ungeeignete Sofortmaßnahmen

Nicht als erste Maßnahme verwenden:

- Switch ohne Diagnose neu starten,
- Portkonfiguration vollständig löschen,
- VLAN vorschnell neu anlegen,
- alle VLANs auf jedem Trunk erlauben,
- Native VLAN wahllos auf VLAN 1 setzen,
- Spanning Tree deaktivieren,
- blockierte STP-Ports ungeprüft freigeben,
- EtherChannel auflösen,
- Port-Security pauschal deaktivieren,
- 802.1X oder NAC umgehen,
- BPDU Guard deaktivieren,
- DHCP Snooping oder ARP Inspection deaktivieren,
- MAC-Tabelle vor der Dokumentation vollständig löschen,
- alle Schnittstellen gleichzeitig zurücksetzen,
- redundante Links abziehen, ohne die Topologie zu prüfen,
- Firewall oder ACL als vermeintlichen VLAN-Test deaktivieren,
- mehrere Konfigurationsänderungen gleichzeitig durchführen,
- ausschließlich mit `ping` testen,
- einen erreichbaren Switch mit einem funktionierenden VLAN-Pfad gleichsetzen.

Solche Maßnahmen können Diagnoseinformationen beseitigen, Sicherheitsgrenzen verändern oder eine Layer-2-Schleife verursachen.

---

32. Vollständige Schnellprüfreihenfolge

1. genaue Störung, Zeitpunkt und Auswirkung dokumentieren.
2. feststellen, ob ein oder mehrere Clients betroffen sind.
3. vorgesehenes VLAN, Subnetz und Gateway ermitteln.
4. tatsächliche Client-MAC-Adresse feststellen.
5. tatsächlichen Switch und Port ermitteln.
6. physischen Linkstatus prüfen.
7. Fehlerzähler dokumentieren.
8. Portmodus prüfen.
9. Access- und Voice-VLAN prüfen.
10. Existenz und Status des VLANs prüfen.
11. Client-MAC in der MAC-Tabelle suchen.
12. MAC-Adresse über alle beteiligten Switches verfolgen.
13. jeden Uplink und Trunk ermitteln.

14. operativen Trunkstatus prüfen.
15. Allowed-VLAN-Listen auf beiden Seiten vergleichen.
16. Native VLAN auf beiden Seiten vergleichen.
17. VLAN-Existenz auf jedem Switch prüfen.
18. Spanning-Tree-Zustand für das betroffene VLAN prüfen.
19. blockierte oder inkonsistente Ports untersuchen.
20. Topology Changes und MAC-Flapping prüfen.
21. EtherChannel und seine Mitglieder prüfen.
22. Port-Security und `err-disabled` prüfen.
23. 802.1X, NAC und dynamische VLAN-Zuweisung berücksichtigen.
24. DHCP Snooping, ARP Inspection und IP Source Guard prüfen.
25. Gateway-SVI und dessen Status prüfen.
26. ARP- beziehungsweise Neighbor-Einträge untersuchen.
27. Kommunikation im gleichen VLAN testen.
28. Gateway separat testen.
29. Inter-VLAN-Kommunikation separat testen.
30. bei Bedarf autorisierten Paketmitschnitt durchführen.
31. genau eine Hypothese formulieren.
32. genau eine kontrollierte Maßnahme durchführen.
33. Port-, VLAN-, Trunk-, STP- und MAC-Zustand erneut prüfen.
34. Clientverbindung und benötigten Dienst erneut testen.
35. Ursache, Änderung und Nachweis dokumentieren.

---

33. Checkliste VLAN und Switching

- [ ] genaue Fehlermeldung wurde dokumentiert.
- [ ] Zeitpunkt der Störung ist bekannt.
- [ ] Umfang der Störung wurde bestimmt.
- [ ] vorgesehenes Client-VLAN ist bekannt.
- [ ] vorgesehenes IP-Subnetz ist bekannt.
- [ ] vorgesehenes Gateway ist bekannt.
- [ ] tatsächliche Client-MAC-Adresse wurde ermittelt.
- [ ] tatsächlicher Switch wurde ermittelt.
- [ ] tatsächlicher Switchport wurde ermittelt.
- [ ] physischer Linkstatus wurde geprüft.
- [ ] Geschwindigkeit und Duplex wurden geprüft.
- [ ] Fehlerzähler wurden dokumentiert.
- [ ] Link-Flapping wurde berücksichtigt.
- [ ] administrativer Portmodus wurde geprüft.
- [ ] operativer Portmodus wurde geprüft.

- [ ] Access-VLAN wurde geprüft.
- [ ] Voice-VLAN wurde bei Bedarf geprüft.
- [ ] clientseitiges VLAN-Tagging wurde berücksichtigt.
- [ ] VLAN existiert auf dem Access-Switch.
- [ ] VLAN ist aktiv.
- [ ] Client-MAC wird gelernt.
- [ ] MAC erscheint im richtigen VLAN.
- [ ] MAC erscheint am erwarteten Port.
- [ ] MAC wurde über den vollständigen Switchpfad verfolgt.
- [ ] alle beteiligten Uplinks wurden ermittelt.
- [ ] Trunkstatus wurde auf beiden Seiten geprüft.
- [ ] Allowed-VLAN-Listen wurden verglichen.
- [ ] Native VLAN wurde auf beiden Seiten geprüft.
- [ ] VLAN existiert auf jedem beteiligten Switch.
- [ ] Spanning Tree wurde für das betroffene VLAN geprüft.
- [ ] Root Bridge und Root Port wurden geprüft.
- [ ] blockierte Ports wurden bewertet.
- [ ] STP-Inkonsistenzen wurden berücksichtigt.
- [ ] Topology Changes wurden geprüft.
- [ ] MAC-Flapping wurde berücksichtigt.
- [ ] EtherChannel wurde geprüft.
- [ ] Konfiguration der Channel-Mitglieder wurde verglichen.
- [ ] Port-Security wurde geprüft.
- [ ] `err-disabled` wurde geprüft.
- [ ] 802.1X und NAC wurden berücksichtigt.
- [ ] DHCP Snooping wurde berücksichtigt.
- [ ] Dynamic ARP Inspection wurde berücksichtigt.
- [ ] Gateway-SVI wurde geprüft.
- [ ] ARP- beziehungsweise Neighbor Cache wurde geprüft.
- [ ] Ziel im gleichen VLAN wurde getestet.
- [ ] Gateway wurde getestet.
- [ ] Ziel in einem anderen VLAN wurde getestet.
- [ ] Layer-2- und Layer-3-Fehler wurden getrennt.
- [ ] vor Änderungen wurde der Ausgangszustand gesichert.

- [ ] nur eine kontrollierte Änderung wurde durchgeführt.
- [ ] ursprüngliche Prüfungen wurden anschließend wiederholt.
- [ ] temporäre Diagnoseänderungen wurden entfernt.
- [ ] Ursache, Maßnahme und Nachweis wurden dokumentiert.

---

34. Schnellreferenz

Ergebnis	Nächster Schritt
Port ist `notconnect`	Kabel, Client, Transceiver und Gegenstelle prüfen
Port ist `err-disabled`	genaue Schutz- oder Fehlerursache ermitteln
viele neue CRC-Fehler	physischen Pfad und Aushandlung prüfen
Client erhält falsches Subnetz	Access-VLAN, dynamische VLAN-Zuweisung und DHCP prüfen
MAC fehlt vollständig	tatsächlichen Port, Clientübertragung und Link prüfen
MAC erscheint im falschen VLAN	Access-, Voice- oder Client-Tagging prüfen
MAC erscheint am falschen Port	Verkabelung, Dokumentation oder Schleife prüfen
MAC wechselt zwischen Ports	Schleife, Teaming, Cluster oder EtherChannel prüfen
VLAN fehlt auf einem Switch	vorgesehene VLAN-Bereitstellung prüfen
VLAN fehlt in Allowed-Liste	Trunkkonfiguration auf beiden Seiten vergleichen
Native VLAN unterscheidet sich	Mismatch kontrolliert korrigieren
Trunk nur auf einer Seite aktiv	Portmodus und Aushandlung prüfen
nur ein VLAN über Trunk gestört	VLAN-Existenz, Allowed-Liste und STP prüfen
alle VLANs über Uplink gestört	Link, Trunk, EtherChannel und Hardware prüfen
STP blockiert redundanten Port	prüfen, ob Blockierung vorgesehen ist
STP meldet PVID-Inkonsistenz	Native VLAN und Portmodi vergleichen
viele Topology Changes	Schleife, instabilen Link oder Root-Wechsel suchen
gleicher VLAN-Verkehr funktioniert	Layer-2-Pfad grundsätzlich vorhanden
Gateway nicht per ARP erreichbar	VLAN-Pfad, Trunk und SVI prüfen
Gateway erreichbar, andere VLANs nicht	Routing, ACL oder Firewall prüfen
Telefon funktioniert, PC nicht	Data-VLAN und PC-Port des Telefons prüfen
PC funktioniert, Telefon nicht	Voice-VLAN, LLDP/CDP und Voice-DHCP prüfen
nur ein EtherChannel-Mitglied aktiv	LACP und Mitgliedskonfiguration vergleichen
Paketmitschnitt zeigt falsche VLAN-ID	Taggingquelle und Portmodus prüfen
Paketmitschnitt zeigt am Access-Port kein Tag	kann bei einem Access-Port normal sein

Merksatz

> Bei VLAN- und Switching-Fehlern wird der Datenpfad nicht erraten, sondern anhand von Portstatus, VLAN-Zuordnung, MAC-Adresse, Trunk, Spanning Tree und Gateway Schritt für Schritt verfolgt. Ein VLAN funktioniert erst dann, wenn es auf jedem beteiligten Switch vorhanden, auf jedem Trunk zugelassen und über einen freigegebenen Layer-2-Pfad bis zum vorgesehenen Gateway transportiert wird.

Quellen und weiterführende Dokumentation

- Cisco – Configure VLANs on Catalyst Switches
- Cisco – Configuring VLAN Trunks
- Cisco – Configure and Troubleshoot Inter-VLAN Routing
- Cisco – Troubleshoot LAN Switching Environments
- Cisco – Troubleshoot Spanning Tree Issues
- Cisco – Troubleshoot Spanning Tree PVID and Type Inconsistencies
- Cisco – Troubleshoot MAC Flaps and Loops
- Cisco – Understand Rapid Spanning Tree Protocol
- Cisco – IOS LAN Switching Command Reference
- Microsoft Learn – Get-NetAdapter
- Microsoft Learn – Get-NetIPConfiguration
- Microsoft Learn – Get-NetIPAddress
- Microsoft Learn – Get-NetNeighbor
- Microsoft Learn – Test-NetConnection
- Wireshark – IEEE 802.1Q VLAN Display Filter Reference
- Wireshark – VLAN Capture Setup
- Wireshark – PCAP Filter Reference
