3.6 VLAN- und Layer-2-Fehler analysieren

Virtual LANs teilen eine physische Switchinfrastruktur in getrennte logische Layer-2-Netze. Geräte in unterschiedlichen VLANs können nicht allein über Switching miteinander kommunizieren. Für die Kommunikation zwischen VLANs ist normalerweise ein Router oder eine Layer-3-Switch-Funktion erforderlich.

VLAN-Fehler können dazu führen, dass ein Endgerät zwar einen aktiven Link besitzt, aber keine passende DHCP-Adresse erhält, sein Gateway nicht erreicht oder im falschen logischen Netz landet.

> **Grundregel:** Linkstatus und VLAN-Zugehörigkeit sind getrennte Eigenschaften. Ein Switchport kann physisch aktiv und gleichzeitig logisch dem falschen VLAN zugeordnet sein.

---

1. Welche Aufgaben erfüllt ein VLAN?

Ein VLAN bildet eine eigene Layer-2-Broadcast-Domain.

```
Physischer Switch
├─ VLAN 10 – Verwaltung
├─ VLAN 20 – Clients
├─ VLAN 30 – VoIP
├─ VLAN 40 – Server
└─ VLAN 50 – Gäste
```

Innerhalb eines VLANs werden unter anderem folgende Nachrichten verteilt:

- Ethernet-Broadcasts,
- ARP-Anfragen,
- bestimmte IPv4-Broadcasts,
- relevante IPv6-Multicasts,
- DHCP-Broadcasts vor einem Relay.

Ein Router trennt normalerweise die Broadcast-Domains und vermittelt bei Bedarf zwischen den VLANs.

Beispiel

```
CLIENT-023 in VLAN 20
192.0.2.23/24

SERVER-01 in VLAN 40
198.51.100.20/24
```

Die Kommunikation benötigt:

```
VLAN 20
  → Gateway für VLAN 20
    → Layer-3-Routing und mögliche Firewallregeln
      → Gateway beziehungsweise Interface für VLAN 40
        → VLAN 40
```

2. Was ist der Unterschied zwischen Access-Port und Trunk?

Porttyp	Typischer Einsatz	Verhalten
Access-Port	normales Endgerät	gehört normalerweise zu einem ungetaggten VLAN
Trunk	Verbindung zwischen Switches, Routern, Servern oder Access Points	transportiert mehrere VLANs
Hybrid-/General-Port	herstellerabhängige Mischform	kombiniert getaggte und ungetaggte VLANs
Routed Port	Layer-3-Verbindung	arbeitet nicht als gewöhnlicher Switchport

Access-Port

```
Client
  │ ungetaggter Ethernetframe
  ▼
Switchport als Access-Port in VLAN 20
```

Der Client muss normalerweise keine VLAN-ID kennen. Der Switch ordnet eingehende ungetaggte Frames dem konfigurierten Access-VLAN zu.

Trunk

```
Switch A
  │ VLAN 10 getaggt
  │ VLAN 20 getaggt
  │ VLAN 40 getaggt
  ▼
Switch B
```

Die VLAN-Zugehörigkeit wird bei IEEE 802.1Q über einen VLAN-Tag im Ethernetframe transportiert.

3. Welche Informationen enthält ein IEEE-802.1Q-Tag?

Ein 802.1Q-Tag enthält unter anderem:

Feld	Bedeutung
PCP	Prioritätsinformation nach IEEE 802.1p
DEI	Drop Eligible Indicator
VLAN ID	VLAN-Kennung

Die VLAN-ID besitzt 12 Bit. Dadurch sind Werte von 0 bis 4095 darstellbar. Die Randwerte sind reserviert beziehungsweise besitzen Sonderbedeutungen; für reguläre VLAN-Zuordnungen werden typischerweise VLAN-IDs 1 bis 4094 verwendet.

Vereinfachter Ethernetframe

```
Ohne VLAN-Tag:

Ziel-MAC
Quell-MAC
EtherType
Nutzdaten
FCS
```

```
Mit 802.1Q-Tag:

Ziel-MAC
Quell-MAC
```

802.1Q-Tag
EtherType
Nutzdaten
FCS

Der zusätzliche Tag vergrößert den Ethernetframe um vier Byte. Geräte und Netzwerkpfade müssen entsprechend kompatibel sein.

4. Welche Symptome sprechen für einen VLAN-Fehler?

- Client erhält keine DHCP-Adresse,
- Client erhält eine Adresse aus dem falschen Subnetz,
- Gateway ist nicht erreichbar,
- nur Geräte an einem Switchport sind betroffen,
- ein Gerät funktioniert an einem anderen Port,
- gleiche SSID führt an verschiedenen Access Points in unterschiedliche Netze,
- Voice-Telefon funktioniert, angeschlossener PC jedoch nicht,
- bestimmte VLANs funktionieren über einen Uplink nicht,
- Server ist lokal erreichbar, aber nicht über andere Switches,
- ungetaggter Verkehr funktioniert, getaggter Verkehr nicht,
- virtuelle Maschine befindet sich im falschen Netz,
- Container- oder Hypervisorbridge transportiert das VLAN nicht,
- VLAN funktioniert nur in eine Richtung,
- nach einer Switchänderung fallen mehrere Geräte eines VLANs aus,
- Spanning Tree blockiert den erwarteten Pfad,
- Port-Security verhindert den Verkehr,
- MAC-Adresse wird an einem unerwarteten Port gelernt,
- Native-VLAN-Konfiguration unterscheidet sich zwischen zwei Seiten.

5. Welche Informationen müssen vor einer VLAN-Analyse bekannt sein?

Information	Beispiel
Clienthostname	`CLIENT-023`
Client-MAC-Adresse	`00-11-22-33-44-55`
Switch	`SW-ACCESS-01`
Switchport	Port 17
vorgesehene VLAN-ID	20
Portmodus	Access

Information	Beispiel
erwartetes Subnetz	`192.0.2.0/24`
erwartetes Gateway	`192.0.2.1`
erwarteter DHCP-Server beziehungsweise Relay	dokumentierte Infrastruktur
nächster Uplink	`SW-CORE-01`
Fehlerbeginn	`2026-07-31 09:42 CEST`
letzte Änderung	Portkonfiguration wurde angepasst

Bei einem Trunk zusätzlich:

- erlaubte VLANs,
- ungetaggtes beziehungsweise natives VLAN,
- Tagging auf beiden Seiten,
- LAG- beziehungsweise Port-Channel-Zugehörigkeit,
- Spanning-Tree-Zustand je VLAN,
- Uplinkpfad zum Ziel.

6. Wie wird ein Access-Port systematisch geprüft?

Auf der Switchseite sollten mindestens folgende Eigenschaften geprüft werden:

Eigenschaft	Prüffrage
administrativer Status	Ist der Port aktiviert?
operativer Status	Besteht ein Link?
Portmodus	Ist der Port tatsächlich als Access-Port vorgesehen?
Access-VLAN	Ist das richtige VLAN zugeordnet?
Voice-VLAN	Existiert eine zusätzliche Telefonzuordnung?
MAC-Tabelle	Wird die erwartete MAC-Adresse gelernt?
Port-Security	Ist die Client-MAC zugelassen?
Authentifizierung	Ist 802.1X beziehungsweise MAB erfolgreich?
Spanning Tree	Ist der Port forwarding oder blockiert?
Fehlerzähler	Steigen CRC-, Drop- oder andere Fehler?
Beschreibung	Passt die Dokumentation zum angeschlossenen Gerät?

Erwartetes Muster

Switchport: Port 17

Modus: Access

Access-VLAN: 20

MAC-Adresse: 00:11:22:33:44:55

Spanning Tree: Forwarding

Port-Security: kein Verstoß

Wenn die MAC-Adresse des Clients an diesem Port nicht gelernt wird, müssen Link, Kabel, Clientaktivität, Authentifizierung und Portzustand geprüft werden.

7. Wie wird ein Trunk systematisch geprüft?

Prüfpunkte auf beiden Seiten

Eigenschaft	Seite A	Seite B
Portmodus	Trunk	Trunk
erlaubte VLANs	identische beziehungsweise kompatible Liste	identische beziehungsweise kompatible Liste
natives VLAN	abgestimmt	abgestimmt
Tagging	abgestimmt	abgestimmt
Linkaggregation	gleiche logische Verbindung	gleiche logische Verbindung
Geschwindigkeit und Duplex	kompatibel	kompatibel
Spanning Tree	erwarteter Zustand	erwarteter Zustand

Typischer Fehler

Switch A erlaubt:

VLAN 10, 20, 40

Switch B erlaubt:

VLAN 10, 40

Auswirkung:

VLAN 20 funktioniert nicht über diesen Trunk.

VLAN 10 und VLAN 40 funktionieren weiterhin.

Dadurch kann der Eindruck entstehen, der Uplink sei grundsätzlich in Ordnung, obwohl nur ein bestimmtes VLAN fehlt.

8. Was ist ein Native-VLAN- oder ungetaggtes VLAN?

Auf manchen Trunks wird ein definiertes VLAN ungetaggt übertragen. Die genaue Bezeichnung und das Verhalten sind hersteller- und konfigurationsabhängig.

Fehlkonfiguration

```
Switch A:
ungetaggtes VLAN 10

Switch B:
ungetaggtes VLAN 20
```

Ein ungetaggter Frame wird dann auf beiden Seiten unterschiedlichen VLANs zugeordnet.

Mögliche Auswirkungen:

- Geräte landen im falschen Netz,
- Managementzugriff verhält sich unerwartet,
- DHCP-Antworten stammen aus dem falschen Bereich,
- Verkehr wird zwischen unerwarteten Broadcast-Domains übergeben,
- Sicherheitsgrenzen werden verletzt.

Wichtig

Die Begriffe `native`, `untagged`, `PVID`, `default VLAN` und `access VLAN` werden von Herstellern nicht immer identisch verwendet. Die Dokumentation des konkret eingesetzten Switches muss geprüft werden.

9. Was ist die PVID?

PVID steht für Port VLAN Identifier. Sie bestimmt bei vielen Switchplattformen, welchem VLAN ein ungetaggt eingehender Frame zugeordnet wird.

Vereinfacht:

```
Untagged Frame trifft auf Port mit PVID 20
  → Switch ordnet den Frame VLAN 20 zu
```

Die PVID ist nicht automatisch dasselbe wie die vollständige Liste aus getaggten und ungetaggten VLAN-Mitgliedschaften.

Bei einer Prüfung müssen deshalb getrennt betrachtet werden:

- VLAN-Mitgliedschaft des Ports,
- getaggt oder ungetaggt,
- PVID,
- zulässige VLAN-Liste,
- Verhalten ausgehender Frames.

10. Wie wird die lokale VLAN-Konfiguration unter Windows geprüft?

Normale Endgeräte an Access-Ports besitzen häufig keine lokale VLAN-Konfiguration. Die VLAN-Zuordnung erfolgt dann ausschließlich am Switch.

Adapter und erweiterte Eigenschaften anzeigen

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

```
[RO] Get-NetAdapterAdvancedProperty -Name 'Ethernet'
```

Nach VLAN-bezogenen Eigenschaften suchen:

```
[RO] Get-NetAdapterAdvancedProperty -Name 'Ethernet' |
    Where-Object {
        $_.DisplayName -Match 'VLAN|Priority' -or
        $_.RegistryKeyword -Match 'VLAN|Priority'
    } |
    Format-Table DisplayName,
```

```
    DisplayValue,
    RegistryKeyword,
    RegistryValue
```

Wichtige Einschränkung

Bezeichnungen und Verfügbarkeit hängen vom Netzwerktreiber ab. Ein fehlendes VLAN-Feld bedeutet nicht automatisch, dass keine VLAN-Nutzung möglich ist.

Hyper-V-Adapter anzeigen

Falls Hyper-V installiert und der Administrator dafür zuständig ist:

```
[RO][PRIV] Get-VMNetworkAdapterVlan -ManagementOS
```

VLAN-Konfiguration virtueller Maschinen:

```
[RO][PRIV] Get-VM |
    Get-VMNetworkAdapter |
    Get-VMNetworkAdapterVlan
```

Die Hyper-V-Cmdlets sind nur verfügbar, wenn die entsprechenden Hyper-V-Komponenten installiert sind.

11. Wie wird die VLAN-Konfiguration unter Linux geprüft?

Detaillierte Linkinformationen

```
[RO] ip -d link show
```

Bestimmte Schnittstelle

```
[RO] ip -d link show dev eth0.20
```

Beispiel einer VLAN-Schnittstelle:

```
eth0.20@eth0
    vlan protocol 802.1Q id 20
```

Bestandteil	Bedeutung
`eth0.20`	Name der logischen VLAN-Schnittstelle
`@eth0`	zugrunde liegende Schnittstelle
`802.1Q`	VLAN-Tagging-Protokoll
`id 20`	VLAN-ID 20

VLAN-Schnittstellen übersichtlich suchen

```
[RO] ip -d -o link show |
    grep -i 'vlan'
```

Linux-Bridge-VLANs

Falls Linux Bridging mit VLAN-Filtering verwendet wird:

```
[RO][PRIV] sudo bridge vlan show
```

Detaillierte Bridge-Links:

```
[RO][PRIV] sudo bridge -d link show
```

Forwarding-Datenbank beziehungsweise MAC-Tabelle:

```
[RO][PRIV] sudo bridge fdb show
```

NetworkManager-Verbindungen

```
[RO] nmcli connection show
```

Nur VLAN-Verbindungen:

```
[RO] nmcli -f NAME,TYPE,DEVICE connection show |
    grep -i vlan
```

Vollständiges Profil:

```
[RO][SENS] nmcli connection show "VLAN-VERBINDUNGSNAME"
```

12. Wie wird die VLAN-Konfiguration unter macOS geprüft?

Alle Schnittstellen

```
[RO] ifconfig
```

VLAN-Schnittstellen suchen

```
[RO] ifconfig -a |
    grep -E '^[[:alnum:]].*:|vlan:'
```

Eine VLAN-Schnittstelle kann abhängig von Konfiguration und macOS-Version beispielsweise als `vlan0` erscheinen.

Netzwerkdienste

```
[RO] networksetup -listallnetworkservices
```

Hardwareports

```
[RO] networksetup -listallhardwareports
```

Die grafische VLAN-Verwaltung und ihre Verfügbarkeit hängen von macOS-Version, Adapter und Treiber ab. Nicht jeder USB- oder Thunderbolt-Ethernetadapter unterstützt VLAN-Konfigurationen in gleicher Weise.

Ein Mac an einem gewöhnlichen Access-Port benötigt normalerweise keine lokale VLAN-ID.

13. Wie wird geprüft, ob der Client im erwarteten VLAN gelandet ist?

Der Client sieht die VLAN-ID an einem gewöhnlichen Access-Port normalerweise nicht direkt. Deshalb werden mehrere Informationen kombiniert.

Prüfung	Erwartetes Ergebnis
Switchportkonfiguration	vorgesehenes Access-VLAN
erhaltene DHCP-Adresse	Subnetz des vorgesehenen VLANs
Standardgateway	Gateway des vorgesehenen VLANs
DNS-Server	passende Infrastruktur
sichtbare Nachbarn	Geräte des erwarteten Netzes
Switch-MAC-Tabelle	Client-MAC am erwarteten Port und VLAN
Vergleichsclient	passende Konfiguration am gleichen Standort

Beispiel

Vorgesehen:

```
VLAN 20
Subnetz 192.0.2.0/24
Gateway 192.0.2.1
```

Tatsächlich:

```
Clientadresse 198.51.100.45/24
Gateway 198.51.100.1
```

Dies ist ein starker Hinweis auf:

- falsches Access-VLAN,
- falsche SSID-zu-VLAN-Zuordnung,
- fehlerhafte dynamische VLAN-Zuweisung,
- nicht vorgesehenen DHCP-Server,
- falsches Netzwerkprofil.

14. Wie wird die MAC-Adresstabelle zur VLAN-Diagnose verwendet?

Ein Switch lernt Quell-MAC-Adressen eingehender Frames und ordnet sie normalerweise einem Port und VLAN zu.

Zu prüfende Zuordnung

```
MAC-Adresse: 00:11:22:33:44:55
VLAN: 20
Port: 17
```

Mögliche Auffälligkeiten

Beobachtung	Mögliche Ursache
MAC nicht gelernt	kein Verkehr, Linkproblem, Authentifizierung oder Port blockiert
MAC im falschen VLAN	Port- oder Taggingfehler
MAC am falschen Port	Dokumentationsfehler, Umstecken oder Layer-2-Schleife
MAC wechselt schnell zwischen Ports	Schleife, redundanter Pfad oder Fehlverkabelung
viele MACs an Clientport	Switch, Bridge, Hypervisor oder unerlaubtes Gerät angeschlossen
nur Telefon-MAC sichtbar	PC-Port des Telefons oder Daten-VLAN prüfen
MAC erscheint hinter Uplink	Client befindet sich an nachgelagertem Switch

Die konkreten Befehle zur MAC-Tabelle sind herstellerabhängig. Suchkriterium sollte die zuvor eindeutig ermittelte Client-MAC-Adresse sein.

15. Wie werden Voice-VLAN und angeschlossener PC berücksichtigt?

Ein IP-Telefon kann zwei logische Verbindungen bereitstellen:

```
Switchport
  → Voice-VLAN für Telefon
  → Data-VLAN für PC hinter dem Telefon
```

Mögliche Fehlerbilder:

- Telefon funktioniert, PC erhält keine Adresse,
- PC funktioniert, Telefon registriert sich nicht,
- beide Geräte erhalten Adressen aus demselben falschen VLAN,

- Telefon kündigt dem PC falsche Parameter an,
- Voice-VLAN wird nicht über den Trunk transportiert,
- Datenport des Telefons ist deaktiviert,
- 802.1X- oder MAB-Reihenfolge ist fehlerhaft.

Zu prüfen sind:

- Access-/Data-VLAN,
- Voice-VLAN,
- Erkennungsmechanismus des Telefons,
- MAC-Adressen beider Geräte,
- Authentifizierungsstatus,
- DHCP-Bereiche beider VLANs,
- Uplink- und Trunkfreigabe.

16. Wie beeinflussen 802.1X und dynamische VLAN-Zuweisung die Diagnose?

Bei portbasierter Netzwerkzugangskontrolle kann ein Gerät abhängig von seiner Authentifizierung einem VLAN zugewiesen werden.

Vereinfachter Ablauf:

```
Client
  → Switch oder Access Point
    → Authentifizierungsdienst
      → Zugelassenes VLAN
```

Mögliche Ergebnisse:

- vorgesehenes Produktions-VLAN,
- Gast-VLAN,
- Quarantäne-VLAN,
- Authentifizierungsfehler,
- eingeschränkter Netzwerkzugriff,
- MAC-basierte Ersatzauthentifizierung.

Typische Symptome

- korrekte Zugangsdaten, aber falsches VLAN,
- Gerät erhält eine Quarantäneadresse,
- Verbindung funktioniert erst nach erneuter Anmeldung,
- Zertifikat oder Gerätekonto wird abgelehnt,

- Telefon und PC werden unterschiedlich behandelt,
- Switchport ist aktiv, aber normaler Datenverkehr wird blockiert.

Zu erfassen

- Authentifizierungsmethode,
- Benutzer- oder Geräteidentität,
- Ergebnis,
- zugewiesenes VLAN,
- Zeitstempel,
- Switchport,
- Richtlinie,
- Authentifizierungsserver.

Das manuelle Setzen eines festen VLANs kann die eigentliche Authentifizierungsstörung verdecken und Sicherheitsrichtlinien umgehen.

17. Wie beeinflusst Spanning Tree die Layer-2-Kommunikation?

Spanning Tree verhindert Layer-2-Schleifen, indem redundante Pfade kontrolliert blockiert werden.

Mögliche Portzustände beziehungsweise Rollen unterscheiden sich je nach verwendeter STP-Variante und Hersteller. Für die Diagnose ist entscheidend, ob der erwartete Port Nutzdaten weiterleitet.

Mögliche Symptome

- VLAN ist über einen bestimmten Uplink nicht erreichbar,
- Verbindung funktioniert nach Verzögerung,
- MAC-Adressen wechseln zwischen Ports,
- Broadcastlast steigt stark,
- Switch-CPU steigt,
- Ports werden wiederholt blockiert und freigegeben,
- Topology Changes treten häufig auf,
- nur einzelne VLANs sind betroffen.

Wichtige Prüfung

```
Ist der Port für das betroffene VLAN im Zustand Forwarding?
```

Ein physisch aktiver Port kann durch Spanning Tree logisch blockiert sein.

Warnung

[CHANGE][DISRUPT] Spanning Tree darf nicht als schnelle Fehlerbehebung deaktiviert werden. Dadurch können Layer-2-Schleifen und großflächige Netzwerkausfälle entstehen.

18. Was ist eine Layer-2-Schleife und wie wird sie erkannt?

Ethernetframes besitzen auf Layer 2 kein mit IP-TTL direkt vergleichbares allgemeines Feld, das eine Schleife zuverlässig beendet. Eine Schleife kann deshalb zu einem Broadcast Storm führen.

Mögliche Symptome

- Netzwerk wird plötzlich extrem langsam,
- sehr hohe Broadcast- und Multicastrate,
- Switch-CPU ist stark ausgelastet,
- MAC-Adressen springen zwischen Ports,
- mehrere Switchports blinken dauerhaft stark,
- DHCP und ARP funktionieren unzuverlässig,
- Managementzugriff auf Switches bricht ab,
- Spanning-Tree-Topology-Changes treten wiederholt auf.

Sicheres Vorgehen

1. Netzwerkverantwortliche und Incident-Prozess aktivieren.
2. betroffene Switches und VLANs bestimmen,
3. STP-Ereignisse und MAC-Flapping prüfen,
4. letzte Verkabelungs- und Portänderungen kontrollieren,
5. Schleifenpfad anhand der Topologie eingrenzen,
6. nur koordiniert einen eindeutig bestimmten Port isolieren,
7. Stabilisierung und Ursache dokumentieren.

Ein wahlloses Entfernen von Uplinks kann Redundanz und weitere Standorte beeinträchtigen.

19. Wie wirken Port-Security und MAC-Limits?

Port-Security kann die Anzahl oder Identität zugelassener MAC-Adressen begrenzen.

Mögliche Reaktionen bei einem Verstoß:

- Frames verwerfen,
- unbekannte MAC-Adressen blockieren,
- Ereignis protokollieren,
- Port in einen Fehler- oder Shutdownzustand versetzen,
- Alarm an das Monitoring senden.

Typische Ursachen eines Verstoßes

- Endgerät wurde ersetzt,
- Dockingstation verwendet andere MAC-Adresse,
- IP-Telefon und PC erzeugen zwei MAC-Adressen,
- Hypervisor oder Bridge sendet mehrere MAC-Adressen,
- kleiner Switch wurde unerlaubt angeschlossen,
- zufällige beziehungsweise private MAC-Adresse wird verwendet,
- konfigurierte Sticky-MAC ist veraltet.

Zu prüfen

- erlaubte Anzahl MAC-Adressen,
- aktuell gelernte MAC-Adressen,
- fest konfigurierte oder dynamisch gelernte Einträge,
- Verstoßzähler,
- Reaktionsmodus,
- Portstatus,
- Endgerätetyp.

Port-Security darf nicht einfach deaktiviert werden, ohne Sicherheitszweck und Richtlinie zu prüfen.

20. Wie werden private oder zufällige MAC-Adressen berücksichtigt?

Moderne Betriebssysteme können bei WLAN-Verbindungen private beziehungsweise zufällige MAC-Adressen verwenden. Abhängig von Plattform und Konfiguration kann dies auch die Wiedererkennung eines Geräts beeinflussen.

Mögliche Auswirkungen:

- DHCP-Reservierung greift nicht,
- MAC-basierte Authentifizierung schlägt fehl,
- Gerät erscheint als neuer Client,
- Port- oder WLAN-Richtlinie greift nicht,
- Inventarisierung stimmt nicht,
- mehrere Leases werden erzeugt.

Prüfung

Die aktuell verwendete MAC-Adresse muss mit folgenden Stellen verglichen werden:

- Betriebssystem,
- Switch oder Access Point,
- DHCP-Lease,
- Netzwerkzugangskontrolle,
- Inventarsystem.

Eine private MAC-Adresse ist nicht automatisch eine Fehlfunktion. Ihre Verwendung kann beabsichtigter Datenschutzstandard oder durch eine Richtlinie gesteuert sein.

21. Wie werden VLAN-Tags mit Wireshark geprüft?

Wireshark-Display-Filter für VLAN-Tags

```
vlan
```

Bestimmte VLAN-ID:

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

Mehrere VLAN-IDs:

```
vlan.id == 20 || vlan.id == 40
```

Nur DHCP in VLAN 20:

```
vlan.id == 20 && (udp.port == 67 || udp.port == 68)
```

Capture-Filter

```
vlan
```

Bestimmtes VLAN:

```
vlan 20
```

Bestimmtes VLAN und Host:

```
vlan 20 and host 192.0.2.23
```

Zeitlich begrenzte Aufnahme

```
[TEST][PRIV][FILE][SENS] dumpcap \
  -i INTERFACE \
  -f "vlan 20" \
  -a duration:30 \
  -w vlan20.pcapng
```

TShark-Auswertung

```
[RO][SENS] tshark \
  -r vlan20.pcapng \
  -Y "vlan" \
  -T fields \
  -e frame.time \
  -e eth.src \
  -e eth.dst \
  -e vlan.id \
  -e vlan.priority
```

Lokal verfügbare VLAN-Felder:

```
[RO] tshark -G fields |
    grep -E $'\tvlan\.'
```

22. Warum ist ein VLAN-Tag im Clientmitschnitt möglicherweise nicht sichtbar?

Mögliche Gründe:

1. Der Client befindet sich an einem Access-Port und empfängt ungetaggte Frames.

2. Der Netzwerkadapter entfernt VLAN-Tags in Hardware.
3. Der Treiber übergibt Tags nicht an das Capture-Werkzeug.
4. Offloading beeinflusst die lokale Darstellung.
5. Es wurde auf der falschen Schnittstelle mitgeschnitten.
6. Der Tag befindet sich nur auf einem anderen Abschnitt des Netzwerkweges.
7. Eine virtuelle Bridge oder ein Hypervisor verarbeitet den Tag vor der Aufzeichnung.

```
Kein sichtbarer VLAN-Tag im lokalen Mitschnitt
≠ kein VLAN im Netzwerk
```

Für die Prüfung eines Trunks ist ein geeigneter Messpunkt am Trunk beziehungsweise ein korrekt konfigurierter Mirror-Port erforderlich. Eine solche Aufzeichnung muss autorisiert und datenschutzgerecht durchgeführt werden.

23. Wie werden virtuelle Maschinen und Hypervisor-VLANs berücksichtigt?

Mögliche Modelle:

VLAN-Zuordnung am virtuellen Switch

```
VM sendet ungetaggt
  → virtueller Switch ordnet VLAN 40 zu
    → physischer Uplink überträgt VLAN 40 getaggt
```

VLAN-Zuordnung in der VM

```
VM erzeugt 802.1Q-Tag
  → virtueller Switch reicht Tag durch
    → physischer Trunk transportiert VLAN
```

Mögliche Fehler

- falsche VLAN-ID am virtuellen Adapter,
- physischer Uplink erlaubt VLAN nicht,
- virtueller Switch entfernt oder erwartet Tags,
- VM und Hypervisor taggen gleichzeitig,
- Portgruppe gehört zum falschen VLAN,
- Teaming- oder Bond-Uplink ist inkonsistent,
- Migration verschiebt VM auf Host ohne passende Trunkfreigabe.

Zu prüfen sind:

- virtuelle Netzwerkkarte,
- Portgruppe beziehungsweise virtueller Switchport,
- virtueller Switch,
- physischer Uplink,
- Switch-Trunk,
- erlaubte VLANs auf allen beteiligten Pfaden.

24. Wie werden Linux-Bridge und Container-VLANs berücksichtigt?

Vereinfachter Pfad:

```
Container oder VM
  → virtuelle Schnittstelle
    → Linux-Bridge
      → VLAN-Filterung
        → physische Schnittstelle
          → Switch-Trunk
```

Bridge-Übersicht

```
[RO][PRIV] sudo bridge link show
```

VLAN-Zuordnungen

```
[RO][PRIV] sudo bridge vlan show
```

MAC-Tabelle der Bridge

```
[RO][PRIV] sudo bridge fdb show
```

Detaillierte Links

```
[RO] ip -d link show
```

Mögliche Fehler:

- VLAN-Filtering ist anders konfiguriert als erwartet,
- VLAN fehlt am Bridgeport,
- PVID ist falsch,
- VLAN ist ungetaggt statt getaggt,
- physischer Uplink transportiert das VLAN nicht,
- Container-MAC wird nicht korrekt gelernt,
- Firewall- beziehungsweise Bridge-Filter verwirft Frames.

Docker-Standardbridges verwenden nicht automatisch dieselbe VLAN-Struktur wie ein physischer Switch. Das konkrete Container- und Hostnetz muss separat dokumentiert werden.

25. Wie werden VLANs über mehrere Switches verfolgt?

Beispielpfad

```
CLIENT-023
  → SW-ACCESS-01 Port 17
    → VLAN 20
      → Uplink 1
        → SW-DISTRIBUTION-01
          → Port-Channel 10
            → SW-CORE-01
              → Gateway VLAN 20
```

Für jeden Abschnitt wird geprüft:

Abschnitt	Prüfung
Clientport	Access-VLAN und Client-MAC
erster Switch	MAC wird im richtigen VLAN gelernt
Uplink	VLAN 20 ist erlaubt
nächster Switch	VLAN existiert und ist aktiv
Linkaggregation	alle Mitglieder sind konsistent
Spanning Tree	erwarteter Pfad ist forwarding
Gateway	VLAN-Interface ist aktiv
Rückweg	führt zurück in dasselbe Client-VLAN

Methode

Die Client-MAC-Adresse wird vom Access-Port in Richtung Core verfolgt. Die Gateway-MAC-Adresse wird in Gegenrichtung geprüft.

26. Was ist bei Link Aggregation und Port-Channels zu beachten?

Mehrere physische Links können zu einer logischen Verbindung gebündelt werden.

Mögliche Fehler:

- ein Mitglied besitzt andere VLAN-Einstellungen,
- nur einige Mitglieder transportieren das betroffene VLAN,
- LACP-Zustand ist fehlerhaft,
- ein Link ist physisch aktiv, aber nicht im Bundle,
- Lastverteilung führt nur bestimmte Verbindungen über den fehlerhaften Link,
- native beziehungsweise ungetaggte VLANs unterscheiden sich,
- Spanning Tree sieht eine unerwartete Topologie.

Typisches Symptom

> Einige Verbindungen funktionieren, andere nicht.
>
> Der Fehler hängt von Quell- und Zieladresse oder Sitzung ab.

Dies kann auftreten, wenn die Hash-basierte Lastverteilung bestimmte Datenströme über ein fehlerhaftes Mitglied leitet.

Auf allen Mitgliedern müssen relevante Konfigurationen konsistent sein. Änderungen dürfen nur über die vorgesehene logische Port-Channel-Konfiguration erfolgen.

27. Wie wird zwischen VLAN-, DHCP- und Routingproblem unterschieden?

Beobachtung	Wahrscheinlichere Richtung
keine DHCP-Adresse, ARP ebenfalls ohne Antwort	VLAN oder Layer 2 möglich
DHCP-Adresse aus falschem Subnetz	falsches VLAN oder Rogue-DHCP möglich
korrekte Adresse, Gateway-MAC nicht auflösbar	VLAN, Gatewayinterface oder Layer 2
Gateway erreichbar, anderes VLAN nicht	Routing oder Firewall
Geräte im selben VLAN kommunizieren	lokales Layer 2 grundsätzlich aktiv
nur ein Trunkabschnitt betroffen	erlaubte VLANs oder Tagging
nur neue Clients betroffen	DHCP oder Zugangskontrolle

Beobachtung	Wahrscheinlichere Richtung
nur ein Port betroffen	Access-VLAN, Port-Security oder Verkabelung
alle Ports eines VLANs betroffen	VLAN, Gateway, STP oder Uplink
VLAN lokal verfügbar, über Uplink nicht	Trunk oder Spanning Tree
Ziel wird im falschen Subnetz gesucht	Clientpräfix oder DHCP-Option

Ein Fehler kann mehrere Ebenen gleichzeitig betreffen. Beispielsweise kann ein falsches Access-VLAN zu einer falschen DHCP-Konfiguration führen.

28. Welche eingreifenden Änderungen dürfen nicht vorschnell erfolgen?

Änderung	Risiko
Access-VLAN ändern	Client verliert Verbindung oder landet im falschen Sicherheitsbereich
Trunk-VLAN hinzufügen	unerwartete Netze werden erweitert
Trunk-VLAN entfernen	gesamtes VLAN fällt über den Uplink aus
natives VLAN ändern	ungetaggter Verkehr wird falsch zugeordnet
Port auf Trunk umstellen	Endgerät kann Tags erhalten oder Sicherheitsgrenze verändert sich
Port-Security deaktivieren	Zugriffsschutz wird aufgehoben
802.1X umgehen	Sicherheitsrichtlinie wird umgangen
Spanning Tree deaktivieren	Layer-2-Schleife und Broadcast Storm möglich
Port-Channel verändern	mehrere Verbindungen können ausfallen
VLAN auf Hypervisor ändern	VM- oder Managementzugriff kann ausfallen
VLAN-Interface löschen	IP-Kommunikation dieses Netzes fällt aus

Vor jeder Änderung müssen dokumentiert werden:

- Ausgangskonfiguration,
- betroffener Port,
- abhängige Geräte,
- vorgesehener Sollzustand,
- erwartete Wirkung,
- Rückweg,
- Wartungs- und Kommunikationsplan.

29. Welche typischen Fehlinterpretationen müssen vermieden werden?

Beobachtung	Falscher Schluss	Richtige Einordnung
Link ist aktiv	VLAN ist korrekt	Link und VLAN sind getrennte Zustände
Client sieht keinen VLAN-Tag	kein VLAN vorhanden	Access-Port liefert gewöhnlich ungetaggte Frames
DHCP funktioniert	VLAN ist korrekt	DHCP kann aus falschem VLAN stammen
Ping im VLAN funktioniert	Trunk ist vollständig korrekt	andere VLANs können fehlen
VLAN 20 funktioniert lokal	VLAN 20 funktioniert überall	Uplinkpfad separat prüfen
MAC fehlt in Tabelle	Gerät ist ausgeschaltet	Authentifizierung, Port oder fehlende Aktivität möglich
MAC wechselt den Port	Angriff	Schleife, Redundanz oder legitime Migration möglich
STP blockiert Port	STP ist defekt	Blockierung kann notwendiger Schleifenschutz sein
mehrere MACs am Port	unerlaubter Switch	Telefon, Hypervisor oder Bridge möglich
gleiche VLAN-ID	gleiches Layer-2-Netz	getrennte Switchdomänen können dieselbe ID verwenden
Portwechsel behebt Fehler	Switchport ist defekt	anderer Port kann anderes VLAN oder Policy besitzen
VLAN hinzufügen behebt Fehler	Änderung war korrekt	Sicherheits- und Architekturprüfung bleibt erforderlich

30. Wie sieht der systematische Prüfablauf aus?

Schritt	Prüfung
1	Client, MAC-Adresse, Switch und Port bestimmen
2	vorgesehenes VLAN und Subnetz aus Dokumentation ermitteln
3	aktuelle Clientadresse mit dem vorgesehenen VLAN vergleichen
4	Portmodus, Access-VLAN, PVID und Voice-VLAN prüfen
5	Authentifizierungs- und Port-Security-Status prüfen
6	Client-MAC in der Switchtabelle suchen

Schritt	Prüfung
7	Gateway-MAC und lokale Kommunikation prüfen
8	betroffenen VLAN-Pfad über alle Uplinks verfolgen
9	erlaubte und getaggte VLANs auf beiden Seiten vergleichen
10	Spanning-Tree-Zustand je betroffenem VLAN prüfen
11	Linkaggregation und Mitgliedsports vergleichen
12	virtuelle Switches und Bridges einbeziehen
13	bei Bedarf autorisierten Mitschnitt am geeigneten Messpunkt erstellen
14	Hypothese mit einer einzelnen kontrollierten Änderung testen
15	DHCP, Gateway und Zielverbindung erneut prüfen
16	ursprüngliche Konfiguration beziehungsweise Rückweg dokumentieren

Merksatz

Client-MAC → Access-Port → VLAN → Uplink → Trunk
→ Spanning Tree → Gateway

31. Kompakte Befehlsübersicht

Aufgabe	Windows	Linux	macOS
Adapter anzeigen	`[RO] Get-NetAdapter`	`[RO] ip -brief link`	`[RO] ifconfig`
VLAN-Eigenschaften der NIC	`[RO] Get-NetAdapterAdvancedProperty -Name 'Ethernet'`	`[RO] ip -d link show`	`[RO] ifconfig -a`
VLAN-Schnittstellen suchen	treiberabhängig	`[RO] ip -d -o link show | grep -i vlan`	`` `[RO] ifconfig -a | grep -E '^[[:alnum:]].*:`
Hyper-V-VLANs	`[RO][PRIV] Get-VMNetworkAdapterVlan -ManagementOS`	nicht zutreffend	nicht zutreffend
VM-VLANs	`[RO][PRIV] Get-VM | Get-VMNetworkAdapter | Get-VMNetworkAdapterVlan`	hypervisorabhängig	hypervisorabhängig
Linux-Bridge-VLANs	nicht zutreffend	`[RO][PRIV] sudo bridge vlan show`	nicht standardmäßig gleichwertig

Aufgabe	Windows	Linux	macOS
Linux-Bridge-MAC-Tabelle	nicht zutreffend	`[RO][PRIV] sudo bridge fdb show`	nicht standardmäßig gleichwertig
VLAN-Tags anzeigen	`[RO][SENS] tshark -r DATEI -Y "vlan"`	gleicher Befehl	gleicher Befehl
VLAN 20 mitschneiden	`[TEST][PRIV][FILE][SENS] dumpcap -i INTERFACE -f "vlan 20" -a duration:30 -w vlan20.pcapng`	gleicher Befehl	gleicher Befehl
DHCP in VLAN 20 anzeigen	`[RO][SENS] tshark -r DATEI -Y "vlan.id == 20 && (udp.port == 67 || udp.port == 68)"`	gleicher Befehl	gleicher Befehl

Switchbefehle sind hersteller- und betriebssystemspezifisch. Für produktive Switches müssen ausschließlich die offiziellen Befehle der tatsächlich eingesetzten Plattform verwendet werden.

32. Dokumentationsvorlage

Ticketnummer:
Prüfzeitpunkt:
Zeitzone:
Standort:
Betroffener Client:
Client-MAC:
Client-IP:
Erwartetes Subnetz:
Erwartetes Gateway:
Erwartete VLAN-ID:

ACCESS-PORT

Switch:
Switchmodell:
Switch-Betriebssystem:
Switchport:
Portbeschreibung:
Administrativer Status:
Operativer Status:
Portmodus:
Access-/Data-VLAN:

Voice-VLAN:

PVID:

Getaggte VLANs:

Ungetaggte VLANs:

802.1X-Status:

Dynamisch zugewiesenes VLAN:

Port-Security-Status:

Erlaubte MAC-Anzahl:

Gelernte MAC-Adressen:

Verstoßzähler:

STP-Zustand:

Fehlerzähler:

UPLINKPFAD

Switch 1:

Ausgangsport:

Erlaubte VLANs:

Natives/ungetaggtes VLAN:

Port-Channel:

STP-Zustand:

Switch 2:

Eingangsport:

Erlaubte VLANs:

Natives/ungetaggtes VLAN:

Port-Channel:

STP-Zustand:

Weitere Switches:

-

GATEWAY

Gatewaygerät:

VLAN-Interface:

Interfacezustand:

Gateway-IP:

Gateway-MAC:

Routing aktiv:

Firewall beteiligt:

CLIENTPRÜFUNG

Erhaltene IPv4-Adresse:

Präfix:

DHCP-Server:

Standardgateway:

DNS-Server:

Gateway-MAC aufgelöst:

Gateway erreichbar:

Referenzclient:

Relevante Abweichungen:

VIRTUELLE INFRASTRUKTUR

Hypervisor:

Virtueller Switch:

Portgruppe:

VM-VLAN:

Physischer Uplink:

Bridge-VLAN:

PVID:

Getaggt/ungetaggt:

PAKETMITSCHNITT

Messpunkt:

Sichtbare VLAN-ID:

Erwartete VLAN-ID:

DHCP sichtbar:

ARP sichtbar:

Unbeabsichtigter Fremdverkehr:

Capture-Datei:

Hash:

Arbeitshypothese:

Begründung:

Gesicherte Ausgangskonfiguration:

Geplante Änderung:

Freigabe:

Rückweg:

Tatsächliches Ergebnis:

Abschlussprüfung:

Ermittelte Ursache:

33. Offizielle Quellen und weiterführende Dokumentation

Microsoft

- Get-NetAdapterAdvancedProperty
- Get-VMNetworkAdapterVlan
- Hyper-V Virtual Switch
- Hyper-V-Netzwerkvirtualisierung

Linux

- ip-link – Linux Manual Page
- bridge – Linux Manual Page
- Linux Bridge VLAN Filtering
- NetworkManager nm-settings

Apple

- Lokale Befehlsreferenzen: `man ifconfig` und `man networksetup`
- Netzwerkstatus auf dem Mac prüfen

Wireshark

- IEEE 802.1Q VLAN Display Filter Reference
- Wireshark Capture Filters
- dumpcap Manual Page
- tshark Manual Page

Standards

- IEEE 802.1Q – Bridges and Bridged Networks

> VLAN-Begriffe und Konfigurationsmodelle unterscheiden sich zwischen Switchherstellern. Insbesondere die Bedeutung von Access, Trunk, Tagged, Untagged, Native VLAN und PVID muss anhand der offiziellen Dokumentation des konkret eingesetzten Geräts geprüft werden.