19.7 VLAN, Switching, Routing und Firewall Spickzettel

Dieser Spickzettel fasst vier zentrale Netzwerkthemen kompakt zusammen:

- Switching
- VLAN
- Routing
- Firewall

Diese Themen hängen in Prüfungsaufgaben oft zusammen, weil sie bestimmen, wie Geräte im lokalen Netz kommunizieren und wie Verkehr zwischen Netzen erlaubt oder blockiert wird.

Merksatz:

Switches verbinden Geräte im LAN.
VLANs trennen logisch.
Routing verbindet Netze.
Firewalls filtern Verkehr.

Grundübersicht

Begriff	Hauptaufgabe	Typische Schicht
Switch	Frames im lokalen Netz weiterleiten	OSI-Schicht 2
VLAN	logische Trennung innerhalb eines Switch-Netzes	OSI-Schicht 2
Router	IP-Netze miteinander verbinden	OSI-Schicht 3
Firewall	Verkehr erlauben oder blockieren	Schicht 3 bis 7

Merksatz:

VLAN trennt.
Routing verbindet.
Firewall entscheidet,
was erlaubt ist.

Switching kurz erklärt

Ein Switch verbindet Geräte in einem lokalen Netzwerk.

Er arbeitet hauptsächlich auf:

```
OSI-Schicht 2
```

Er leitet Ethernet-Frames anhand von MAC-Adressen weiter.

Merksatz:

```
Switches arbeiten mit MAC-Adressen.
```

MAC-Adresstabelle

Ein Switch lernt, welche MAC-Adresse an welchem Port erreichbar ist.

Beispiel:

MAC-Adresse	Switchport
AA:AA:AA:AA:AA:01	Port 1
AA:AA:AA:AA:AA:02	Port 2
AA:AA:AA:AA:AA:03	Port 3

Der Switch lernt aus der Quell-MAC-Adresse eingehender Frames.

Merksatz:

```
Switch lernt aus Quell-MAC-Adressen.
```

Switching-Ablauf

Wenn ein Frame beim Switch ankommt:

```
1. Switch liest die Quell-MAC-Adresse.

2. Switch speichert:
   Diese MAC-Adresse ist an diesem Port erreichbar.
```

3. Switch liest die Ziel-MAC-Adresse.

4. Wenn Ziel-MAC bekannt ist:
   Frame wird gezielt an den passenden Port gesendet.

5. Wenn Ziel-MAC unbekannt ist:
   Frame wird geflutet.

Merksatz:

Bekannte Ziel-MAC:
gezielte Weiterleitung.

Unbekannte Ziel-MAC:
Flooding.

Flooding

Flooding bedeutet:

Der Switch sendet einen Frame an alle Ports im VLAN,
außer an den Eingangsport.

Flooding passiert bei:

unbekannter Ziel-MAC-Adresse
Broadcast
bestimmten Multicast-Fällen

Merksatz:

Flooding ist nicht immer Fehler,
sondern bei unbekannter Ziel-MAC normal.

Broadcast

Broadcast bedeutet:

```
Nachricht an alle Geräte im lokalen Broadcast-Bereich.
```

Beispiel:

```
ARP Request
```

Broadcast bleibt normalerweise innerhalb:

```
eines VLANs

beziehungsweise

einer Broadcast-Domäne
```

Merksatz:

```
Broadcast erreicht alle Geräte im gleichen VLAN.
```

Broadcast-Domäne

Eine Broadcast-Domäne ist der Bereich, in dem Broadcasts verteilt werden.

Ohne VLAN:

```
oft gesamtes Switch-Netz
```

Mit VLAN:

```
jedes VLAN ist eigene Broadcast-Domäne
```

Merksatz:

```
VLANs trennen Broadcast-Domänen.
```

VLAN kurz erklärt

VLAN steht für:

```
Virtual Local Area Network
```

Ein VLAN trennt ein physisches Netzwerk logisch in mehrere getrennte Netzbereiche.

Beispiele:

```
VLAN 10 Verwaltung

VLAN 20 Clients

VLAN 30 Server

VLAN 40 Gäste

VLAN 99 Management
```

Merksatz:

```
VLAN = logische Trennung auf Schicht 2.
```

Warum VLANs verwendet werden

Vorteile:

```
logische Netztrennung
kleinere Broadcast-Domänen
bessere Struktur
Trennung von Abteilungen
Trennung von Gästen und internem Netz
Trennung von Servern und Clients
Managementnetz separat halten
Sicherheitszonen ermöglichen
```

Merksatz:

```
VLANs verbessern Struktur,
Übersicht
und Sicherheit.
```

VLAN ist keine vollständige Firewall

Ein VLAN trennt auf Schicht 2.

Aber:

```
Kommunikation zwischen VLANs ist über Routing möglich.
```

Deshalb braucht man für Sicherheit zusätzlich:

```
Router-Regeln

Firewall-Regeln

ACLs
```

Merksatz:

```
VLAN trennt logisch,
Firewall kontrolliert Verkehr.
```

Access-Port

Ein Access-Port gehört normalerweise zu genau einem VLAN.

Typische Nutzung:

```
Client
Drucker
Telefon
Access Point im einfachen Betrieb
Arbeitsplatzgerät
```

Beispiel:

```
Port 5 ist Access-Port in VLAN 20.
```

Ein angeschlossenes Endgerät muss das VLAN meist nicht kennen.

Merksatz:

```
Access-Port = ein VLAN für Endgeräte.
```

Trunk-Port

Ein Trunk-Port transportiert mehrere VLANs.

Typische Nutzung:

```
Verbindung zwischen Switches

Verbindung zu Router

Verbindung zu Firewall

Verbindung zu Hypervisor

Verbindung zu VLAN-fähigem Access Point
```

Merksatz:

```
Trunk-Port = mehrere VLANs über eine Verbindung.
```

Access-Port und Trunk-Port vergleichen

Porttyp	VLAN-Anzahl	Typische Nutzung
Access-Port	ein VLAN	Endgeräte
Trunk-Port	mehrere VLANs	Switch, Router, Firewall, Hypervisor

Merksatz:

```
Access = ein VLAN.
Trunk = mehrere VLANs.
```

VLAN-Tagging

Bei Trunk-Verbindungen müssen Frames einem VLAN zugeordnet werden.

Dafür wird meistens verwendet:

```
IEEE 802.1Q
```

Dabei bekommt der Frame einen VLAN-Tag.

Merksatz:

```
802.1Q markiert Frames mit VLAN-Information.
```

Untagged und Tagged

Untagged:

```
Frame enthält keinen sichtbaren VLAN-Tag für das Endgerät.
```

Typisch:

```
Access-Port
```

Tagged:

```
Frame enthält VLAN-Information.
```

Typisch:

```
Trunk-Port
```

Merksatz:

```
Access meist untagged.
Trunk meist tagged.
```

Native VLAN

Das Native VLAN ist das VLAN, dessen Frames auf einem Trunk untagged übertragen werden können.

Wichtig:

```
Native VLAN muss auf beiden Seiten passend konfiguriert sein.
```

Risiko:

```
Fehlkonfiguration kann zu unerwarteter Kommunikation führen.
```

Merksatz:

```
Native VLAN auf Trunks bewusst und einheitlich konfigurieren.
```

Management-VLAN

Ein Management-VLAN dient der Verwaltung von Netzwerkgeräten.

Darin liegen zum Beispiel:

```
Switch-Management
Access-Point-Management
Firewall-Management
Monitoring
Administrationszugriffe
```

Merksatz:

```
Managementzugänge nicht ins normale Clientnetz legen.
```

Gast-VLAN

Ein Gast-VLAN trennt Gäste vom internen Netz.

Typische Regeln:

```
Zugriff ins Internet erlaubt

Zugriff auf interne Server blockiert
```

Zugriff auf Managementnetz blockiert

Merksatz:

Gastnetz vom internen Netz trennen.

Voice-VLAN

Ein Voice-VLAN wird für IP-Telefone genutzt.

Vorteile:

Sprachverkehr getrennt vom normalen Clientverkehr
QoS leichter möglich
bessere Übersicht
getrennte Sicherheitsregeln möglich

Merksatz:

Voice-VLAN trennt Telefonie vom normalen Datenverkehr.

Inter-VLAN-Routing

VLANs sind getrennte Layer-2-Netze.

Damit Geräte aus verschiedenen VLANs miteinander kommunizieren können, braucht man Routing.

Das nennt man:

Inter-VLAN-Routing

Möglich über:

Router

Layer-3-Switch

Firewall

Merksatz:

VLANs trennen.
Inter-VLAN-Routing verbindet sie wieder gezielt.

Router-on-a-Stick

Router-on-a-Stick bedeutet:

Ein Router verbindet mehrere VLANs über eine Trunk-Verbindung.

Der Router hat logische Subinterfaces, zum Beispiel:

VLAN 10

VLAN 20

VLAN 30

Merksatz:

Router-on-a-Stick routet mehrere VLANs über einen Trunk.

Layer-3-Switch

Ein Layer-3-Switch kann:

switchen auf Schicht 2

und

routen auf Schicht 3

Typische Nutzung:

schnelles Routing zwischen VLANs im internen Netz

Merksatz:

Layer-3-Switch verbindet Switching und Routing.

Routing kurz erklärt

Routing bedeutet:

Pakete zwischen verschiedenen IP-Netzen weiterleiten.

Ein Router entscheidet anhand der Routing-Tabelle, wohin ein IP-Paket gesendet wird.

Merksatz:

Routing verbindet IP-Netze.

Routing-Tabelle

Eine Routing-Tabelle enthält typischerweise:

Zielnetz

Präfix

Next Hop

Interface

Metrik

Beispiel:

Zielnetz	Next Hop	Bedeutung
192.168.10.0/24	direkt verbunden	lokales Netz
192.168.20.0/24	192.168.10.1	über Router erreichbar

Zielnetz	Next Hop	Bedeutung
0.0.0.0/0	192.168.10.254	Standardroute

Merksatz:

```
Routing-Tabelle bestimmt den nächsten Weg.
```

Standardroute

Die Standardroute ist die Route für alle Ziele, für die keine spezifischere Route vorhanden ist.

IPv4-Schreibweise:

```
0.0.0.0/0
```

Typisch:

```
Weg zum Internetrouter
```

Merksatz:

```
Standardroute = Route für unbekannte Ziele.
```

Spezifischste Route gewinnt

Wenn mehrere Routen passen, wird die Route mit dem längsten passenden Präfix verwendet.

Beispiel:

```
192.168.10.0/24
```

ist spezifischer als:

```
192.168.0.0/16
```

Merksatz:

```
Längster passender Präfix gewinnt.
```

Gateway

Das Standardgateway ist der Router, über den ein Client andere Netze erreicht.

Wichtig:

```
Das Gateway muss im lokalen Subnetz des Clients erreichbar sein.
```

Merksatz:

```
Gateway = Ausgang aus dem eigenen Netz.
```

Firewall kurz erklärt

Eine Firewall filtert Netzwerkverkehr.

Sie entscheidet anhand von Regeln:

```
erlauben

oder

blockieren
```

Typische Kriterien:

```
Quelle
Ziel
Port
Protokoll
Richtung
Benutzer
Anwendung
Zustand
Zeit
Zone
```

Merksatz:

> Firewall = kontrollierter Verkehr zwischen Bereichen.

Firewall-Regel

Eine gute Firewall-Regel enthält:

> Quelle
>
> Ziel
>
> Dienst oder Port
>
> Protokoll
>
> Richtung
>
> Aktion
>
> Zweck
>
> Verantwortlichen
>
> Datum

Beispiel:

Quelle	Ziel	Protokoll	Port	Aktion	Zweck
Client-VLAN	Webserver-DMZ	TCP	443	erlauben	HTTPS-Zugriff
Gast-VLAN	internes Servernetz	any	any	blockieren	internes Netz schützen
Admin-VLAN	Switch-Management	TCP	22	erlauben	SSH-Administration

Merksatz:

> Jede Firewall-Regel braucht einen Zweck.

Default Deny

Default Deny bedeutet:

```
Standardmäßig ist alles verboten.
```

Nur ausdrücklich erlaubter Verkehr wird zugelassen.

Vorteil:

```
kleinere Angriffsfläche
bessere Kontrolle
weniger unbeabsichtigte Freigaben
```

Merksatz:

```
Erst blockieren,
dann gezielt erlauben.
```

Any-to-Any

Any-to-Any bedeutet:

```
jede Quelle

zu

jedem Ziel
```

Problem:

```
sehr breite Freigabe
schlechte Nachvollziehbarkeit
große Angriffsfläche
Sicherheitszonen werden umgangen
```

Merksatz:

```
Any-to-Any ist in der Regel kritisch.
```

Stateful Firewall

Eine Stateful Firewall merkt sich den Zustand einer Verbindung.

Beispiel:

```
Client startet HTTPS-Verbindung nach außen.

Antwortpakete werden automatisch zugelassen,
weil sie zur bestehenden Verbindung gehören.
```

Merksatz:

```
Stateful Firewall kennt Verbindungszustände.
```

Stateless Firewall

Eine Stateless Firewall betrachtet Pakete einzeln, ohne Verbindungszustand zu merken.

Sie prüft nur einzelne Paketinformationen, zum Beispiel:

```
Quelle

Ziel

Port

Protokoll
```

Merksatz:

```
Stateless Firewall kennt keinen Verbindungszustand.
```

Firewall-Zonen

Firewall-Zonen teilen Netzbereiche nach Schutzbedarf.

Beispiele:

```
Internet

DMZ

internes Netz

Servernetz

Clientnetz

Gastnetz

Managementnetz
```

Merksatz:

```
Zonen helfen,
Sicherheitsregeln strukturiert aufzubauen.
```

DMZ

DMZ steht für:

```
Demilitarized Zone
```

Eine DMZ ist ein getrenntes Netz für öffentlich erreichbare Dienste.

Beispiele:

```
Webserver

Reverse Proxy

Mail-Gateway

VPN-Gateway
```

Ziel:

```
interne Netze schützen,
wenn ein öffentlich erreichbarer Dienst kompromittiert wird.
```

Merksatz:

```
DMZ trennt öffentliche Dienste vom internen Netz.
```

ACL

ACL steht für:

```
Access Control List
```

Eine ACL ist eine Liste von Regeln, die Zugriff erlauben oder verweigern.

Einsatz:

```
Router
Switches
Firewalls
Betriebssysteme
Anwendungen
```

Merksatz:

```
ACL = Regelbasierte Zugriffskontrolle.
```

VLAN und Firewall zusammendenken

VLANs trennen Netzbereiche.

Firewalls regeln, welcher Verkehr zwischen diesen Bereichen erlaubt ist.

Beispiel:

Quelle	Ziel	Erlaubt?	Grund

Client-VLAN	Internet	ja	normaler Zugriff
Gast-VLAN	internes Servernetz	nein	Schutz interner Daten
Admin-VLAN	Management-VLAN	ja	Administration
Server-VLAN	Datenbank-VLAN	nur benötigter Port	Least Privilege

Merksatz:

VLAN ohne Regeln ist nur Trennung.
Firewall macht daraus kontrollierte Sicherheit.

Typisches Fehlerbild: falsches VLAN

Symptome:

Client bekommt keine passende IP-Adresse.
Client erreicht lokale Systeme nicht.
DHCP funktioniert nicht.
Gerät ist im falschen Netz.
nur ein Switchport betroffen.

Prüfen:

Access-Port-VLAN
Trunk erlaubt VLAN?
VLAN existiert?
DHCP-Scope passt?
Switchport aktiv?
Dokumentation korrekt?

Merksatz:

Falsches VLAN führt oft zu falscher oder fehlender IP-Konfiguration.

Typisches Fehlerbild: Trunk falsch konfiguriert

Symptome:

mehrere VLANs funktionieren nicht
ein bestimmtes VLAN fehlt auf zweitem Switch
Access Points liefern falsche Netze
Hypervisor-VLANs nicht erreichbar

Prüfen:

Trunk-Port aktiv?
VLANs erlaubt?
Tagging korrekt?
Native VLAN gleich?
Gegenstelle passend konfiguriert?

Merksatz:

Trunk-Probleme betreffen oft mehrere VLANs.

Typisches Fehlerbild: Routing fehlt

Symptome:

Geräte im gleichen VLAN erreichen sich.
Geräte in anderen VLANs nicht.
Gateway erreichbar,
aber Zielnetz nicht.

Prüfen:

Routing-Tabelle
Gateway
Layer-3-Switch oder Router
Inter-VLAN-Routing
Firewall-Regeln
Rückroute

Merksatz:

Gleiches VLAN geht,
anderes Netz nicht:
Routing und Firewall prüfen.

Typisches Fehlerbild: Firewall blockiert

Symptome:

Zielhost erreichbar,
aber bestimmter Dienst nicht.
Porttest schlägt fehl.
Firewall-Log zeigt Drop oder Deny.
nach Regeländerung funktioniert Dienst nicht mehr.

Prüfen:

Quelle
Ziel
Port
Protokoll
Richtung
Zone
NAT
Regelreihenfolge
Logs

Merksatz:

Host erreichbar,
Dienst nicht:
Port,
Dienst
und Firewall prüfen.

Typisches Fehlerbild: Rückroute fehlt

Bei Kommunikation zwischen Netzen muss nicht nur der Hinweg funktionieren, sondern auch der Rückweg.

Symptom:

Anfrage geht raus,
Antwort kommt nicht zurück.

Ursachen:

Rückroute fehlt
falsches Gateway
asymmetrisches Routing
Firewall blockiert Rückverkehr
NAT falsch

Merksatz:

Netzwerkkommunikation braucht Hinweg und Rückweg.

STP kurz erklärt

STP steht für:

Spanning Tree Protocol

Aufgabe:

Schleifen auf Schicht 2 verhindern.

Warum wichtig?

Layer-2-Schleifen können Broadcast-Stürme verursachen.

Merksatz:

STP verhindert Switch-Schleifen.

Broadcast-Sturm

Ein Broadcast-Sturm entsteht, wenn Broadcasts durch Schleifen immer wieder weitergeleitet werden.

Folgen:

```
Netz wird langsam
Switches stark belastet
Clients verlieren Verbindung
Dienste brechen ab
```

Merksatz:

```
Layer-2-Schleifen können das Netz lahmlegen.
```

Port Security

Port Security begrenzt, welche oder wie viele MAC-Adressen an einem Switchport erlaubt sind.

Ziel:

```
unautorisierte Geräte erschweren
einfache Angriffe reduzieren
Portmissbrauch begrenzen
```

Merksatz:

```
Port Security kontrolliert MAC-Adressen am Switchport.
```

802.1X

802.1X ist portbasierte Netzwerkzugangskontrolle.

Prinzip:

```
Gerät oder Benutzer muss sich authentifizieren,
bevor Netzwerkzugriff erlaubt wird.
```

Typisch mit:

RADIUS

Zertifikat

Benutzerkonto

Merksatz:

802.1X prüft Zugriff vor Netzzugang.

Switching, Routing und Firewall unterscheiden

Begriff	Aufgabe	Typische Entscheidung
Switching	Frames im LAN weiterleiten	Welche MAC an welchem Port?
Routing	Pakete zwischen Netzen weiterleiten	Welcher nächste Hop?
Firewall	Verkehr filtern	Erlauben oder blockieren?

Merksatz:

Switch leitet lokal.
Router leitet zwischen Netzen.
Firewall entscheidet über Erlaubnis.

Typische Prüfungsfallen

VLAN und Subnetz gleichsetzen.

Access-Port und Trunk-Port verwechseln.

VLAN ohne Routing als netzübergreifende Verbindung verstehen.

Firewall und Router gleichsetzen.

Routing vergessen,
wenn VLANs miteinander sprechen sollen.

Firewall-Regeln ohne Richtung betrachten.

Rückroute vergessen.

Gateway außerhalb des Subnetzes eintragen.

Any-to-Any als unkritisch ansehen.

VLAN als vollständige Sicherheitsmaßnahme betrachten.

Switch nur als „Verteiler“ ohne MAC-Lernen beschreiben.

Merksatz:

Viele Fehler entstehen,
weil Trennung,
Weiterleitung
und Filterung vermischt werden.

Typische IHK-Fragen

In AP1 und AP2 kann zum Beispiel gefragt werden:

- Was macht ein Switch?
- Was ist eine MAC-Adresstabelle?
- Was bedeutet Flooding?
- Was ist ein VLAN?
- Warum setzt man VLANs ein?
- Was ist eine Broadcast-Domäne?
- Was ist der Unterschied zwischen Access-Port und Trunk-Port?
- Was bedeutet 802.1Q?
- Was ist Inter-VLAN-Routing?
- Was macht ein Router?
- Was ist eine Standardroute?
- Was bedeutet:
  spezifischste Route gewinnt?
- Was macht eine Firewall?
- Was ist Default Deny?

- Warum ist Any-to-Any kritisch?
- Was ist eine DMZ?
- Was ist STP?
- Warum kann eine Rückroute wichtig sein?

IHK-sichere Kurzformulierung

Ein Switch arbeitet hauptsächlich auf OSI-Schicht 2 und leitet Frames anhand von MAC-Adressen weiter. VLANs trennen ein physisches Netzwerk logisch in mehrere Broadcast-Domänen. Access-Ports gehören meist zu einem VLAN, Trunk-Ports transportieren mehrere VLANs mit VLAN-Tagging nach IEEE 802.1Q. Damit Geräte aus unterschiedlichen VLANs kommunizieren können, ist Inter-VLAN-Routing über Router, Layer-3-Switch oder Firewall nötig. Routing verbindet IP-Netze anhand von Routing-Tabellen. Eine Firewall filtert Verkehr anhand von Regeln wie Quelle, Ziel, Port, Protokoll und Aktion. VLANs trennen Netze, Firewalls kontrollieren den erlaubten Verkehr zwischen ihnen.

Merksätze

Switches arbeiten mit MAC-Adressen.

Switch lernt aus Quell-MAC-Adressen.

Unbekannte Ziel-MAC führt zu Flooding.

Broadcast erreicht alle Geräte im gleichen VLAN.

VLAN trennt logisch auf Schicht 2.

VLANs bilden eigene Broadcast-Domänen.

Access-Port = ein VLAN.

Trunk-Port = mehrere VLANs.

802.1Q markiert VLAN-Frames.

Access meist untagged.

Trunk meist tagged.

Managementzugänge gehören nicht ins Clientnetz.

Gast-VLAN vom internen Netz trennen.

VLAN ist keine vollständige Firewall.

Inter-VLAN-Routing verbindet VLANs gezielt.

Routing verbindet IP-Netze.

Standardroute ist 0.0.0.0/0.

Spezifischste Route gewinnt.

Gateway führt aus dem eigenen Netz.

Firewall filtert Verkehr.

Default Deny ist sicherer.

Any-to-Any ist kritisch.

Stateful Firewall kennt Verbindungen.

Stateless Firewall prüft Pakete einzeln.

DMZ trennt öffentliche Dienste.

ACL ist eine Regelliste für Zugriff.

Rückroute nicht vergessen.

STP verhindert Layer-2-Schleifen.

Broadcast-Sturm kann ein Netz lahmlegen.

Port Security kontrolliert MAC-Adressen.

802.1X prüft Netzzugang.

Switch leitet lokal.

Router leitet zwischen Netzen.

Firewall entscheidet,
ob Verkehr erlaubt ist.