5.8 Merksätze und Prüfungswissen zu OSI-Schicht 2

Diese Seite fasst die wichtigsten Inhalte zur OSI-Schicht 2 zusammen.

OSI-Schicht 2 heißt:

```
Sicherungsschicht
```

Sie liegt zwischen:

```
Schicht 1: Bitübertragungsschicht
und
Schicht 3: Vermittlungsschicht / Netzwerkschicht
```

Die Hauptaufgabe von Schicht 2 ist:

```
lokale Datenübertragung im Netzwerk mit Frames und MAC-Adressen.
```

Merksatz:

```
Schicht 2 = Frames, MAC-Adressen, Switches und VLANs.
```

Grundidee von Schicht 2

Schicht 1 überträgt nur Bits als Signale.

Schicht 2 organisiert diese Bits zu Frames.

Ein Frame enthält Informationen für die lokale Übertragung.

Wichtig sind vor allem:

```
- Ziel-MAC-Adresse
- Quell-MAC-Adresse
- Nutzdaten
- Prüfinformation
```

Merksatz:

```
Schicht 2 macht aus Bits nutzbare lokale Datenrahmen.
```

Schicht 1, 2 und 3 unterscheiden

Schicht	Name	Datenform	wichtige Begriffe
1	Bitübertragungsschicht	Bits	Signal, Kabel, Link, Hub
2	Sicherungsschicht	Frame	MAC, Switch, VLAN, ARP
3	Vermittlungsschicht	Paket	IP, Router, Subnetz, Routing

Merksatz:

```
Schicht 1 = Bits.
Schicht 2 = Frames.
Schicht 3 = Pakete.
```

Frame

Ein Frame ist die Datenübertragungseinheit auf Schicht 2.

Bei Ethernet spricht man von:

```
Ethernet-Frame
```

Ein Ethernet-Frame enthält unter anderem:

```
- Ziel-MAC-Adresse
- Quell-MAC-Adresse
- EtherType oder Länge
- Nutzdaten
- FCS
```

Merksatz:

```
Frame = Datenrahmen auf Schicht 2.
```

Frame, Paket und Segment

Diese Begriffe dürfen nicht verwechselt werden.

Begriff	Schicht	Bedeutung
Bit	1	einzelne Informationseinheit
Frame	2	lokale Übertragung
Paket	3	IP-Übertragung zwischen Netzen
Segment	4	TCP-Datenübertragung
Datagramm	4	UDP-Datenübertragung

Prüfungsfalle:

```
Ethernet arbeitet mit Frames.
IP arbeitet mit Paketen.
TCP arbeitet mit Segmenten.
```

Merksatz:

```
Frame ist nicht Paket.
```

MAC-Adresse

MAC steht für:

```
Media Access Control
```

Eine MAC-Adresse ist die lokale Hardwareadresse einer Netzwerkschnittstelle.

Typische Netzwerkschnittstellen:

```
- Ethernet-Port
- WLAN-Adapter
- virtuelle Netzwerkkarte
- Server-Netzwerkkarte
- USB-LAN-Adapter
```

Merksatz:

```
MAC-Adresse = lokale Adresse einer Netzwerkschnittstelle.
```

Aufbau einer MAC-Adresse

Eine klassische MAC-Adresse hat:

```
48 Bit
```

Sie wird meist hexadezimal dargestellt.

Beispiel:

```
00:1A:2B:3C:4D:5E
```

Oder:

```
00-1A-2B-3C-4D-5E
```

Merksatz:

```
MAC-Adresse = 48 Bit, hexadezimal dargestellt.
```

Quell-MAC und Ziel-MAC

Ein Ethernet-Frame enthält normalerweise:

```
Quell-MAC-Adresse
Ziel-MAC-Adresse
```

Die Quell-MAC-Adresse sagt:

```
Von welchem Gerät kommt der Frame?
```

Die Ziel-MAC-Adresse sagt:

```
Zu welchem lokalen Gerät soll der Frame?
```

Merksatz:

```
Quell-MAC = woher.
Ziel-MAC = wohin.
```

MAC-Adresse und IP-Adresse unterscheiden

Adresse	Schicht	Aufgabe
MAC-Adresse	2	lokale Zustellung im LAN
IP-Adresse	3	netzübergreifende Adressierung

Wichtig:

```
MAC-Adressen gelten nur lokal im jeweiligen Netzwerkabschnitt.
IP-Adressen dienen der Kommunikation über Netzgrenzen hinweg.
```

Merksatz:

```
MAC = lokal.
IP = netzübergreifend.
```

MAC-Adresse auf dem Weg durch Router

Wenn Daten über Router laufen, ändern sich die MAC-Adressen auf jedem Abschnitt.

Beispiel:

```
PC → Router → weiterer Router → Server
```

Auf jedem lokalen Abschnitt gibt es neue Frames mit neuen MAC-Adressen.

Die IP-Adressen bleiben grundsätzlich erhalten.

Ausnahme:

```
NAT oder PAT kann IP-Adressen verändern.
```

Merksatz:

MAC ändert sich pro Hop.

IP bleibt grundsätzlich erhalten.

Unicast, Broadcast und Multicast

Art	Bedeutung	Beispiel
Unicast	einer an einen	PC an Server
Broadcast	einer an alle	ARP-Anfrage
Multicast	einer an eine Gruppe	Streaming-Gruppe

Die Broadcast-MAC-Adresse lautet:

```
FF:FF:FF:FF:FF:FF
```

Merksatz:

```
Unicast = einer.
Broadcast = alle.
Multicast = Gruppe.
```

FCS und CRC

FCS steht für:

```
Frame Check Sequence
```

CRC steht für:

```
Cyclic Redundancy Check
```

Die FCS dient zur Fehlererkennung im Ethernet-Frame.

Wenn ein Frame beschädigt ist, kann das erkannt werden.

Wichtig:

Ethernet korrigiert beschädigte Frames normalerweise nicht selbst.
Fehlerhafte Frames werden verworfen.

Merksatz:

FCS/CRC erkennt beschädigte Frames.

MTU

MTU steht für:

Maximum Transmission Unit

Die MTU beschreibt die maximale Nutzdaten-Größe einer Verbindung.

Bei Ethernet ist häufig relevant:

1500 Byte Nutzlast

Wichtig:

Zu große Pakete können Fragmentierung oder Verbindungsprobleme verursachen,
wenn die Strecke sie nicht unterstützt.

Merksatz:

MTU = maximale Nutzdaten-Größe.

Switch

Ein Switch ist ein typisches Gerät auf Schicht 2.

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

Ein Switch nutzt dazu eine Tabelle.

Diese nennt man:

MAC-Adresstabelle

Oder:

Switching-Tabelle

Merksatz:

Switch = Schicht-2-Gerät für Frame-Weiterleitung.

Hub, Switch und Router unterscheiden

Gerät	typische Schicht	Aufgabe
Hub	1	verteilt Signale an alle Ports
Switch	2	leitet Frames anhand von MAC-Adressen weiter
Router	3	leitet IP-Pakete zwischen Netzen weiter

Prüfungsfalle:

Ein Switch ist kein Router.

Ein Hub ist kein Switch.

Merksatz:

Hub = Signal.

Switch = MAC.

Router = IP.

MAC-Adresstabelle

Die MAC-Adresstabelle enthält Zuordnungen wie:

MAC-Adresse	Switch-Port
AA:AA:AA:AA:AA:01	Port 1
BB:BB:BB:BB:BB:02	Port 2

MAC-Adresse	Switch-Port
CC:CC:CC:CC:CC:03	Port 3

Damit kann ein Switch Frames gezielt weiterleiten.

Merksatz:

```
MAC-Adresstabelle = MAC-Adresse zu Port.
```

Wie lernt ein Switch MAC-Adressen?

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

Beispiel:

```
Frame kommt an Port 4 an.
Quell-MAC ist AA:BB:CC:11:22:33.
```

Der Switch lernt:

```
AA:BB:CC:11:22:33 ist über Port 4 erreichbar.
```

Merksatz:

```
Switch lernt über Quell-MAC.
```

Weiterleitung durch den Switch

Ein Switch prüft die Ziel-MAC-Adresse.

Dann gibt es drei typische Fälle:

Situation	Verhalten
Ziel-MAC bekannt	gezielte Weiterleitung
Ziel-MAC unbekannt	Flooding
Broadcast	Weiterleitung an alle passenden Ports

Merksatz:

```
Ziel-MAC entscheidet über die Weiterleitung.
```

Flooding

Flooding bedeutet:

```
Der Switch verteilt einen Frame an mehrere Ports,
weil die Ziel-MAC-Adresse unbekannt ist.
```

Flooding ist normales Switch-Verhalten bei unbekanntem Ziel.

Nicht verwechseln mit Broadcast.

Merksatz:

```
Flooding = Ziel-MAC unbekannt.
```

Broadcast

Broadcast bedeutet:

```
Der Frame ist ausdrücklich an alle Geräte im lokalen Netz adressiert.
```

Broadcast-MAC:

```
FF:FF:FF:FF:FF:FF
```

Typische Beispiele:

```
- ARP-Anfrage
- DHCP-Anfrage
```

Merksatz:

```
Broadcast = Ziel ist alle.
```

Broadcast und Flooding unterscheiden

Begriff	Grund
Broadcast	Zieladresse ist „alle“
Flooding	Ziel-MAC ist unbekannt

Beide können dazu führen, dass Frames an mehrere Ports gehen.

Aber:

```
Der Grund ist unterschiedlich.
```

Merksatz:

```
Broadcast ist eine Adresse.
Flooding ist ein Switch-Verhalten.
```

Broadcast-Domäne

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

Ein VLAN bildet normalerweise eine eigene Broadcast-Domäne.

Router trennen Broadcast-Domänen.

Merksatz:

```
Broadcast-Domäne = Bereich für Broadcasts.
```

Kollisionsdomäne

Eine Kollisionsdomäne ist ein Bereich, in dem Kollisionen auftreten können.

Bei einem Hub:

```
alle Ports in einer Kollisionsdomäne
```

Bei einem Switch:

```
normalerweise jeder Port eigene Kollisionsdomäne
```

In modernen Vollduplex-Switch-Netzen spielen klassische Kollisionen praktisch keine Rolle mehr.

Merksatz:

```
Hub = eine Kollisionsdomäne.
Switch = getrennte Kollisionsbereiche.
```

VLAN

VLAN steht für:

```
Virtual Local Area Network
```

Ein VLAN ist ein logisch getrenntes LAN auf Schicht 2.

VLANs ermöglichen mehrere logische Netze auf derselben physischen Switch-Infrastruktur.

Beispiel:

VLAN	Zweck
10	Mitarbeiter
20	Gäste
30	Server
40	VoIP
99	Management

Merksatz:

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

VLAN und Subnetz unterscheiden

Begriff	Schicht	Aufgabe
VLAN	2	logische Trennung im LAN
IP-Subnetz	3	logischer IP-Adressbereich

In der Praxis wird häufig pro VLAN ein eigenes IP-Subnetz verwendet.

Beispiel:

VLAN	Subnetz
VLAN 10	192.168.10.0/24
VLAN 20	192.168.20.0/24

Merksatz:

```
VLAN ist nicht Subnetz.
VLAN = Schicht 2.
Subnetz = Schicht 3.
```

Access-Port

Ein Access-Port gehört normalerweise zu genau einem VLAN.

Typischer Einsatz:

```
- PC
- Drucker
- Kamera
- einzelnes Endgerät
```

Das Endgerät sendet meist untagged Frames.

Der Switch ordnet diese Frames dem VLAN des Ports zu.

Merksatz:

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

Trunk-Port

Ein Trunk-Port kann mehrere VLANs über eine Verbindung transportieren.

Typischer Einsatz:

```
- Switch zu Switch
- Switch zu Router
- Switch zu Firewall
- Switch zu Access Point mit mehreren SSIDs
- Switch zu Virtualisierungshost
```

Merksatz:

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

VLAN-Tagging

VLAN-Tagging markiert Frames mit einer VLAN-ID.

Der Standard dafür heißt:

```
IEEE 802.1Q
```

Tagged bedeutet:

```
Frame enthält VLAN-Tag.
```

Untagged bedeutet:

```
Frame enthält keinen VLAN-Tag.
```

Merksatz:

```
802.1Q = VLAN-Tagging.
```

Native VLAN

Das Native VLAN ist bei bestimmten Trunk-Konzepten das untagged VLAN auf einem Trunk.

Wichtig:

```
Das Native VLAN muss auf beiden Seiten korrekt zusammenpassen.
```

Falsche Native-VLAN-Konfiguration kann zu Problemen und Sicherheitsrisiken führen.

Merksatz:

```
Native VLAN = untagged VLAN auf dem Trunk.
```

Inter-VLAN-Routing

Geräte in unterschiedlichen VLANs können nicht nur über Schicht 2 miteinander kommunizieren.

Für Kommunikation zwischen VLANs braucht man Routing.

Das nennt man:

```
Inter-VLAN-Routing
```

Dafür nutzt man zum Beispiel:

```
- Router
- Layer-3-Switch
- Firewall
```

Merksatz:

```
VLAN zu VLAN braucht Routing.
```

ARP

ARP steht für:

```
Address Resolution Protocol
```

ARP wird in IPv4-Netzen verwendet, um zu einer IP-Adresse die passende MAC-Adresse im lokalen Netz zu finden.

ARP-Anfrage:

```
Broadcast
```

ARP-Antwort:

```
meistens Unicast
```

Merksatz:

```
ARP findet MAC zu IP im lokalen Netz.
```

ARP im gleichen Subnetz

Wenn sich das Ziel im gleichen Subnetz befindet, sucht ARP die MAC-Adresse des Zielgeräts.

Beispiel:

```
PC A sucht MAC von PC B.
```

Dann sendet PC A eine ARP-Anfrage ins lokale Netz.

Merksatz:

```
Gleiches Subnetz:
ARP sucht Ziel-MAC.
```

ARP bei anderem Subnetz

Wenn das Ziel in einem anderen Netz liegt, sucht ARP nicht die MAC-Adresse des entfernten Servers.

Stattdessen sucht ARP die MAC-Adresse des Standard-Gateways.

Beispiel:

```
Ziel-IP ist im Internet.
Ziel-MAC im lokalen Frame ist das Gateway.
```

Merksatz:

Anderes Netz:

ARP sucht Gateway-MAC.

ARP, DNS und DHCP unterscheiden

Protokoll	Aufgabe
ARP	IP-Adresse zu MAC-Adresse
DNS	Name zu IP-Adresse
DHCP	IP-Konfiguration automatisch vergeben

Prüfungsfalle:

ARP ist keine Namensauflösung.

DNS ist keine MAC-Auflösung.

Merksatz:

ARP = MAC zu IP.

DNS = IP zu Name.

DHCP = IP vergeben.

IPv4 und IPv6

ARP wird bei IPv4 verwendet.

IPv6 nutzt nicht ARP.

IPv6 verwendet stattdessen:

NDP

NDP steht für:

Neighbor Discovery Protocol

Merksatz:

```
IPv4 nutzt ARP.
IPv6 nutzt NDP.
```

STP

STP steht für:

```
Spanning Tree Protocol
```

STP verhindert Schleifen in Layer-2-Netzen.

Warum ist das wichtig?

```
Ethernet-Frames haben keine TTL wie IP-Pakete.
Frames können bei einer Schleife immer weiterlaufen.
Broadcasts können sich stark vervielfachen.
```

Merksatz:

```
STP schützt vor Layer-2-Schleifen.
```

Root Bridge

Die Root Bridge ist der zentrale Bezugspunkt im STP-Netz.

Switches berechnen ihre besten Wege zur Root Bridge.

Die Root Bridge wird über die Bridge-ID bestimmt.

Merksatz:

```
Root Bridge = zentraler STP-Bezugspunkt.
```

BPDU

BPDU steht für:

Bridge Protocol Data Unit

BPDUs sind STP-Nachrichten zwischen Switches.

Damit tauschen Switches Informationen über die STP-Topologie aus.

Merksatz:

BPDU = STP-Nachricht.

STP-Portrollen

Rolle	Bedeutung
Root Port	bester Weg zur Root Bridge
Designated Port	aktiver Port für ein Segment
Blocked Port	blockierter Port zur Schleifenvermeidung

Merksatz:

Root und Designated leiten weiter.
Blocked verhindert Schleifen.

RSTP und MSTP

Protokoll	Bedeutung
STP	verhindert Schleifen
RSTP	schnellere Weiterentwicklung von STP
MSTP	mehrere Spanning-Tree-Instanzen

Merksatz:

STP verhindert Schleifen.
RSTP ist schneller.
MSTP ist flexibler für VLAN-Umgebungen.

Layer-2-Schleife

Eine Layer-2-Schleife entsteht, wenn Frames in einem Switch-Netz im Kreis laufen können.

Typische Ursachen:

- falsch gesteckte Kabel
- redundante Verbindungen ohne STP
- unmanaged Switches
- falsch konfigurierte Link Aggregation
- STP deaktiviert

Mögliche Folgen:

- Broadcast-Sturm
- MAC Flapping
- hohe Switch-Last
- Netzwerkausfall

Merksatz:

Layer-2-Schleifen können ein LAN lahmlegen.

Broadcast-Sturm

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

Eine Layer-2-Schleife kann Broadcasts stark vervielfachen.

Typische Symptome:

- Netzwerk plötzlich extrem langsam
- Switch-LEDs blinken stark
- viele Broadcasts im Mitschnitt
- Geräte verlieren Verbindung
- MAC-Adressen wechseln Ports

Merksatz:

Broadcast-Sturm = zu viele Broadcasts im LAN.

MAC Flapping

MAC Flapping bedeutet:

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

Mögliche Ursachen:

```
- Layer-2-Schleife
- falsche Link Aggregation
- falsche Verkabelung
- virtuelle Umgebung
- doppelte MAC-Adresse
```

Merksatz:

```
MAC Flapping ist ein Warnsignal.
```

Port Security

Port Security ist eine Switch-Sicherheitsfunktion.

Damit kann man festlegen:

```
welche MAC-Adressen
oder wie viele MAC-Adressen
an einem Port erlaubt sind.
```

Mögliche Reaktionen bei Verstoß:

```
- Frames verwerfen
- Port sperren
- Warnung erzeugen
- Ereignis protokollieren
```

Merksatz:

```
Port Security begrenzt MAC-Adressen pro Port.
```

ARP-Spoofing und ARP-Poisoning

ARP-Spoofing bedeutet:

```
Ein Angreifer sendet falsche ARP-Informationen.
```

ARP-Poisoning bedeutet:

```
ARP-Caches werden mit falschen Zuordnungen manipuliert.
```

Mögliche Folge:

```
Datenverkehr wird zum Angreifer umgeleitet.
```

Schutzmaßnahmen:

```
- VLAN-Trennung
- 802.1X
- Port Security
- DHCP Snooping
- Dynamic ARP Inspection
- Monitoring
```

Merksatz:

```
ARP-Spoofing manipuliert IP-MAC-Zuordnungen.
```

DHCP Snooping

DHCP Snooping ist eine Switch-Sicherheitsfunktion.

Ziele:

```
- unerlaubte DHCP-Server verhindern
- IP-MAC-Zuordnungen erfassen
- Dynamic ARP Inspection unterstützen
```

Merksatz:

```
DHCP Snooping schützt vor falschen DHCP-Servern.
```

Dynamic ARP Inspection

Dynamic ARP Inspection prüft ARP-Nachrichten auf dem Switch.

Ziel:

```
gefälschte ARP-Informationen erkennen und blockieren.
```

Häufig arbeitet diese Funktion mit DHCP Snooping zusammen.

Merksatz:

```
Dynamic ARP Inspection schützt vor ARP-Manipulation.
```

BPDU Guard

BPDU Guard schützt Access-Ports vor unerwarteten STP-Nachrichten.

Wenn an einem Endgeräte-Port plötzlich BPDUs auftauchen, könnte dort ein unerlaubter Switch angeschlossen sein.

Mögliche Reaktion:

```
Port wird deaktiviert.
```

Merksatz:

```
BPDU Guard schützt Access-Ports.
```

Root Guard

Root Guard verhindert, dass ein unerwünschter Switch Root Bridge wird.

Dadurch bleibt die geplante STP-Struktur erhalten.

Merksatz:

```
Root Guard schützt die geplante Root Bridge.
```

Storm Control

Storm Control begrenzt übermäßigen Broadcast-, Multicast- oder unbekannten Unicast-Verkehr.

Ziel:

```
Schutz vor Überlastung durch zu viel Layer-2-Verkehr.
```

Merksatz:

```
Storm Control begrenzt Broadcast-Stürme.
```

Schicht-2-Fehlersuche

Typische Prüfpunkte:

```
- MAC-Adresse gelernt?
- richtiger Switch-Port?
- richtiges VLAN?
- Access oder Trunk?
- VLAN auf Trunk erlaubt?
- Native VLAN korrekt?
- ARP zum Gateway vorhanden?
- STP blockiert Port?
- MAC Flapping sichtbar?
- Broadcast-Sturm vorhanden?
- Port Security aktiv?
```

Merksatz:

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

Typische Schicht-2-Fehler

Fehlerbild	mögliche Ursache
keine IP-Adresse	falsches VLAN, Trunk-Fehler
falsche IP-Adresse	falsches VLAN
Gateway nicht per ARP erreichbar	VLAN- oder ARP-Problem
Netzwerk plötzlich langsam	Broadcast-Sturm oder Schleife
MAC wechselt ständig Port	MAC Flapping
einzelne SSID funktioniert nicht	falsche SSID-VLAN-Zuordnung
Gerät nach Tausch blockiert	Port Security
VLAN kommt nicht durch	Trunk erlaubt VLAN nicht

Merksatz:

> Viele IP-Probleme beginnen auf Schicht 2.

Was Schicht 2 nicht macht

Schicht 2 macht nicht:

- Routing zwischen IP-Netzen
- NAT oder PAT
- TCP-Verbindungen aufbauen
- UDP-Ports auswerten
- DNS-Namen auflösen
- Webseiten bereitstellen
- Benutzer authentifizieren
- Internetzugang allein herstellen

Diese Aufgaben liegen auf höheren Schichten.

Merksatz:

> Schicht 2 leitet lokal weiter,
> routet aber nicht zwischen IP-Netzen.

Prüfungswissen: wichtigste Zuordnungen

Begriff	richtige Einordnung

Ethernet-Frame	Schicht 2
MAC-Adresse	Schicht 2
Switch	Schicht 2
VLAN	Schicht 2
Access-Port	Schicht 2
Trunk-Port	Schicht 2
ARP	Schicht 2 / 3-Bezug
STP	Schicht 2
Broadcast-Domäne	Schicht 2
IP-Adresse	Schicht 3
Router	Schicht 3
TCP-Port	Schicht 4
DNS	Schicht 7

Merksatz:

```
Frame, MAC, Switch, VLAN = Schicht 2.
```

Typische IHK-Fragen

In AP1 und AP2 kann zum Beispiel gefragt werden:

```
- Welche Aufgabe hat die Sicherungsschicht?
- Was ist ein Ethernet-Frame?
- Was ist eine MAC-Adresse?
- Wie lernt ein Switch MAC-Adressen?
- Was passiert bei unbekannter Ziel-MAC?
- Was ist Flooding?
- Was ist ein Broadcast?
- Was ist eine Broadcast-Domäne?
- Was ist ein VLAN?
- Was ist der Unterschied zwischen Access-Port und Trunk-Port?
- Was bedeutet IEEE 802.1Q?
- Was macht ARP?
- Warum wird eine ARP-Anfrage als Broadcast gesendet?
- Was ist STP?
```

- Warum sind Layer-2-Schleifen gefährlich?
- Was bedeutet MAC Flapping?
- Wie grenzt man Schicht-2-Fehler ein?

Typische Prüfungsfallen

Schicht 2 arbeitet mit Frames.

IP-Pakete gehören zu Schicht 3.

MAC-Adressen gehören zu Schicht 2.

IP-Adressen gehören zu Schicht 3.

Switches lernen über Quell-MAC-Adressen.

Die Ziel-MAC entscheidet über die Weiterleitung.

Unbekannte Ziel-MAC führt zu Flooding.

Broadcast und Flooding sind nicht dasselbe.

Ein VLAN ist kein IP-Subnetz.

VLAN gehört zu Schicht 2.

Subnetz gehört zu Schicht 3.

Access-Port = ein VLAN.

Trunk-Port = mehrere VLANs.

IEEE 802.1Q = VLAN-Tagging.

ARP ist nicht DNS.

ARP ist nicht DHCP.

IPv4 nutzt ARP.

IPv6 nutzt NDP.

STP verhindert Layer-2-Schleifen.

Ethernet-Frames haben keine TTL.

Falsches VLAN kann wie ein IP-Problem aussehen.

Wichtige Begriffe kurz erklärt

Begriff	Kurze Erklärung
Sicherungsschicht	OSI-Schicht 2
Frame	Datenrahmen auf Schicht 2
Ethernet-Frame	Frame im Ethernet-LAN
MAC-Adresse	lokale Hardwareadresse
Quell-MAC	Absenderadresse im Frame
Ziel-MAC	Empfängeradresse im Frame
Switch	Schicht-2-Gerät
MAC-Adresstabelle	Zuordnung MAC-Adresse zu Port
Learning	Lernen über Quell-MAC
Forwarding	gezielte Weiterleitung
Flooding	Weiterleitung bei unbekannter Ziel-MAC
Broadcast	Nachricht an alle
Broadcast-Domäne	Bereich, in dem Broadcasts verteilt werden
Kollisionsdomäne	Bereich möglicher Kollisionen
VLAN	logisches LAN auf Schicht 2
Access-Port	Port für ein VLAN
Trunk-Port	Port für mehrere VLANs
802.1Q	VLAN-Tagging
ARP	IP-Adresse zu MAC-Adresse
STP	Schleifenvermeidung auf Schicht 2
BPDU	STP-Nachricht
Broadcast-Sturm	sehr viele Broadcasts im LAN

Begriff	Kurze Erklärung
MAC Flapping	MAC-Adresse wechselt ständig Ports
Port Security	Begrenzung erlaubter MAC-Adressen
DHCP Snooping	Schutz vor unerlaubten DHCP-Servern
Dynamic ARP Inspection	Schutz vor ARP-Manipulation

IHK-sichere Gesamtformulierung

Die Sicherungsschicht ist Schicht 2 des OSI-Modells. Sie ist für die lokale Datenübertragung in Form von Frames zuständig. Im Ethernet-LAN werden MAC-Adressen verwendet, um Frames lokal zuzustellen. Switches arbeiten typischerweise auf Schicht 2, lernen MAC-Adressen über die Quell-MAC-Adresse eingehender Frames und leiten Frames anhand der Ziel-MAC-Adresse weiter. VLANs ermöglichen eine logische Trennung von Broadcast-Domänen auf Schicht 2. ARP wird in IPv4-Netzen verwendet, um zu einer IP-Adresse die passende MAC-Adresse im lokalen Netz zu ermitteln. STP verhindert Layer-2-Schleifen, die sonst Broadcast-Stürme und Netzwerkausfälle verursachen können.

Wichtigste Merksätze

Schicht 2 = Sicherungsschicht.

Schicht 2 arbeitet mit Frames.

Ethernet-Frame = lokaler Datenrahmen.

MAC-Adresse = lokale Hardwareadresse.

MAC = Schicht 2.

IP = Schicht 3.

MAC gilt lokal.

IP gilt netzübergreifend.

Switch = Schicht 2.

Router = Schicht 3.

Hub = Schicht 1.

Switch lernt über Quell-MAC.

Ziel-MAC entscheidet über Weiterleitung.

Bekannte Ziel-MAC = gezielte Weiterleitung.

Unbekannte Ziel-MAC = Flooding.

Broadcast = an alle.

Broadcast-MAC = FF:FF:FF:FF:FF:FF.

Broadcast und Flooding sind nicht dasselbe.

VLAN = logische Trennung auf Schicht 2.

VLAN ist nicht Subnetz.

Access-Port = ein VLAN.

Trunk-Port = mehrere VLANs.

802.1Q = VLAN-Tagging.

VLAN zu VLAN braucht Routing.

ARP findet MAC zu IP.

ARP-Anfrage = Broadcast.

ARP-Antwort = meistens Unicast.

IPv4 nutzt ARP.

IPv6 nutzt NDP.

STP verhindert Layer-2-Schleifen.

Ethernet-Frames haben keine TTL.

Broadcast-Sturm kann ein LAN lahmlegen.

MAC Flapping kann auf eine Schleife hinweisen.

Falsches VLAN kann wie ein IP-Problem aussehen.

Erst Link,
dann MAC/VLAN,
dann IP.