5.3 Switching, MAC-Adresstabelle und Flooding

Ein Switch ist eines der wichtigsten Geräte auf OSI-Schicht 2.

Er verbindet Geräte in einem lokalen Netzwerk und leitet Ethernet-Frames weiter.

Dabei arbeitet ein Switch nicht mit IP-Adressen, sondern mit MAC-Adressen.

Merksatz:

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

Grundaufgabe eines Switches

Ein Switch soll Frames möglichst gezielt an den richtigen Port weiterleiten.

Beispiel:

```
PC A sendet Daten an PC B.
```

Der Switch soll den Frame nicht unnötig an alle Geräte senden, sondern möglichst nur an den Port, an dem PC B angeschlossen ist.

Dafür nutzt der Switch:

```
- Ziel-MAC-Adresse
- Quell-MAC-Adresse
- MAC-Adresstabelle
- Ports
```

Merksatz:

```
Ein Switch leitet Frames anhand von MAC-Adressen weiter.
```

Switch im OSI-Modell

Ein Switch arbeitet typischerweise auf:

```
OSI-Schicht 2
```

Diese Schicht heißt:

```
Sicherungsschicht
```

Warum?

```
Ein Switch wertet Ethernet-Frames aus.
Ethernet-Frames gehören zu Schicht 2.
MAC-Adressen gehören zu Schicht 2.
```

Wichtig:

```
Ein normaler Switch routet nicht zwischen IP-Netzen.
Routing gehört zu Schicht 3.
```

Merksatz:

```
Switch = Schicht 2.
Router = Schicht 3.
```

Switch und physische Ports

Ein Switch besitzt mehrere physische Anschlüsse.

Diese Anschlüsse nennt man:

```
Ports
```

Beispiele:

```
Port 1
Port 2
Port 3
Port 4
```

An diesen Ports können angeschlossen sein:

- PCs
- Server
- Drucker
- Access Points
- andere Switches
- Router
- Firewalls

Wichtig:

Hier ist mit Port der physische Anschluss gemeint,
nicht ein TCP- oder UDP-Port.

Merksatz:

Switch-Port = physischer Anschluss.
TCP-/UDP-Port = Dienstadresse auf Schicht 4.

MAC-Adresstabelle

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

Diese Tabelle nennt man:

MAC-Adresstabelle

Oder auch:

Switching-Tabelle

Beispiel:

MAC-Adresse	Switch-Port
AA:AA:AA:AA:AA:01	Port 1
BB:BB:BB:BB:BB:02	Port 2
CC:CC:CC:CC:CC:03	Port 3

Mit dieser Tabelle kann der Switch Frames gezielt weiterleiten.

Merksatz:

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

Wie lernt ein Switch MAC-Adressen?

Ein Switch lernt MAC-Adressen automatisch.

Dafür schaut er auf die Quell-MAC-Adresse eingehender Frames.

Beispiel:

```
Ein Frame kommt an Port 1 an.
Die Quell-MAC-Adresse lautet AA:AA:AA:AA:AA:01.
```

Dann lernt der Switch:

```
AA:AA:AA:AA:AA:01 ist an Port 1 erreichbar.
```

Wichtig:

```
Der Switch lernt über die Quell-MAC-Adresse,
nicht über die Ziel-MAC-Adresse.
```

Merksatz:

```
Switch lernt MAC-Adressen über die Quell-MAC.
```

Warum lernt der Switch über die Quell-MAC?

Die Quell-MAC-Adresse zeigt, von welchem Gerät ein Frame kommt.

Wenn ein Frame an einem bestimmten Port eingeht, weiß der Switch:

```
Der Absender dieses Frames befindet sich hinter diesem Port.
```

Dadurch kann der Switch seine MAC-Adresstabelle aufbauen.

Beispiel:

> Frame kommt von PC A an Port 1.
> Also ist PC A über Port 1 erreichbar.

Merksatz:

> Eingangsport + Quell-MAC = Lerninformation für den Switch.

Weiterleitung anhand der Ziel-MAC

Wenn ein Switch einen Frame erhält, prüft er die Ziel-MAC-Adresse.

Dann entscheidet er:

> Kenne ich diese Ziel-MAC-Adresse?
> Wenn ja, an welchem Port ist sie erreichbar?
> Wenn nein, muss ich den Frame fluten?

Merksatz:

> Ziel-MAC entscheidet über die Weiterleitung.

Fall 1: Ziel-MAC ist bekannt

Wenn die Ziel-MAC-Adresse in der MAC-Adresstabelle steht, leitet der Switch den Frame gezielt an den passenden Port weiter.

Beispiel:

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

PC A sendet an PC B.

Frame:

```
Quell-MAC: AA:AA:AA:AA:AA:01
Ziel-MAC: BB:BB:BB:BB:BB:02
```

Der Switch sieht:

```
BB:BB:BB:BB:BB:02 ist an Port 2.
```

Er leitet den Frame nur an Port 2 weiter.

Merksatz:

```
Bekannte Ziel-MAC = gezielte Weiterleitung.
```

Fall 2: Ziel-MAC ist unbekannt

Wenn die Ziel-MAC-Adresse nicht in der MAC-Adresstabelle steht, kennt der Switch den passenden Port noch nicht.

Dann sendet er den Frame an alle passenden Ports außer dem Eingangsport.

Das nennt man:

```
Flooding
```

Beispiel:

```
Frame kommt an Port 1 an.
Ziel-MAC ist unbekannt.
```

Der Switch sendet den Frame an:

```
Port 2
Port 3
Port 4
```

Aber nicht zurück an Port 1.

Merksatz:

```
Unbekannte Ziel-MAC = Flooding.
```

Begriff: Flooding

Flooding bedeutet:

```
Ein Switch verteilt einen Frame an mehrere Ports,
weil er die Ziel-MAC-Adresse nicht kennt.
```

Flooding ist kein Fehler.

Es ist ein normales Verhalten eines Switches, wenn ihm eine Ziel-MAC-Adresse unbekannt ist.

Sobald die Zielstation antwortet, kann der Switch deren MAC-Adresse lernen.

Merksatz:

```
Flooding hilft dem Switch,
unbekannte Ziele trotzdem zu erreichen.
```

Fall 3: Broadcast

Ein Broadcast ist ein Frame an alle Geräte im lokalen Netz.

Die Broadcast-MAC-Adresse lautet:

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

Wenn ein Switch einen Broadcast empfängt, leitet er ihn an alle passenden Ports weiter, außer an den Eingangsport.

Typische Broadcasts:

```
- ARP-Anfragen
- DHCP-Anfragen
```

Merksatz:

Broadcast = absichtlich an alle.

Broadcast und Flooding unterscheiden

Broadcast und Flooding sehen ähnlich aus, weil Frames an mehrere Ports gesendet werden.

Der Unterschied liegt im Grund.

Begriff	Warum wird an mehrere Ports gesendet?
Broadcast	Zieladresse ist ausdrücklich „alle“
Flooding	Ziel-MAC ist dem Switch unbekannt

Wichtig:

Broadcast ist eine Adressierungsart.
Flooding ist ein Verhalten des Switches.

Merksatz:

Broadcast = Ziel ist alle.
Flooding = Ziel ist unbekannt.

Fall 4: Frame geht an denselben Port zurück

Ein Switch leitet einen Frame normalerweise nicht an denselben Port zurück, über den er gekommen ist.

Beispiel:

Frame kommt an Port 1 an.
Ziel-MAC ist ebenfalls über Port 1 bekannt.

Dann verwirft der Switch den Frame für die Weiterleitung.

Warum?

Ziel und Quelle liegen aus Sicht des Switches hinter demselben Port.
Eine Weiterleitung ist nicht nötig.

Merksatz:

> Ein Switch sendet einen Frame nicht zurück auf den Eingangsport.

Aging der MAC-Adresstabelle

Einträge in der MAC-Adresstabelle bleiben nicht für immer gespeichert.

Nach einer gewissen Zeit ohne neue Frames können Einträge gelöscht werden.

Das nennt man:

> Aging

Warum ist das sinnvoll?

> Geräte können umgesteckt werden.
> Geräte können ausgeschaltet werden.
> Netzwerke können sich verändern.

Der Switch muss seine Tabelle aktuell halten.

Merksatz:

> Aging entfernt alte MAC-Einträge aus der Tabelle.

MAC-Adresse wandert auf einen anderen Port

Wenn ein Gerät umgesteckt wird, kann seine MAC-Adresse an einem anderen Port auftauchen.

Beispiel:

> PC war vorher an Port 1.
> PC wird an Port 5 gesteckt.

Sobald der Switch einen Frame von diesem PC an Port 5 sieht, aktualisiert er die MAC-Adresstabelle.

Merksatz:

Der Switch aktualisiert MAC-Einträge durch neue Quell-MAC-Informationen.

MAC-Adresstabelle und Sicherheit

Die MAC-Adresstabelle hilft beim gezielten Weiterleiten.

Sie ist aber kein starker Sicherheitsmechanismus.

Warum?

MAC-Adressen können gefälscht werden.
Geräte können umgesteckt werden.
Ein Angreifer kann viele gefälschte MAC-Adressen erzeugen.

Für zusätzliche Sicherheit nutzt man zum Beispiel:

- Port Security
- 802.1X
- VLANs
- Firewall-Regeln
- Monitoring

Merksatz:

MAC-Adresstabelle dient der Weiterleitung,
nicht als alleiniger Sicherheitsnachweis.

MAC-Flooding als Angriff

MAC-Flooding ist ein Angriff auf die MAC-Adresstabelle eines Switches.

Dabei sendet ein Angreifer sehr viele Frames mit verschiedenen gefälschten Quell-MAC-Adressen.

Ziel:

Die MAC-Adresstabelle des Switches soll überfüllt werden.

Mögliche Folge:

```
Der Switch kennt viele Ziel-MAC-Adressen nicht mehr zuverlässig
und flutet mehr Frames.
```

Schutzmaßnahmen:

```
- Port Security
- Begrenzung erlaubter MAC-Adressen pro Port
- Monitoring
- 802.1X
```

Merksatz:

```
MAC-Flooding versucht,
die MAC-Adresstabelle zu überlasten.
```

Port Security

Port Security ist eine Sicherheitsfunktion auf Switches.

Damit kann festgelegt werden, welche oder wie viele MAC-Adressen an einem Port erlaubt sind.

Beispiel:

```
An Port 5 ist nur eine MAC-Adresse erlaubt.
```

Wenn dort plötzlich mehrere MAC-Adressen auftauchen, kann der Switch reagieren.

Mögliche Reaktionen:

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

Merksatz:

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

Switching und Broadcast-Domäne

Ein normaler Switch trennt Kollisionsdomänen, aber nicht automatisch Broadcast-Domänen.

Das bedeutet:

> Broadcasts werden innerhalb desselben VLANs weitergeleitet.

Alle Ports im gleichen VLAN gehören zur gleichen Broadcast-Domäne.

Router oder Layer-3-Grenzen trennen Broadcast-Domänen.

Merksatz:

> Switch trennt Kollisionsdomänen.
> VLAN oder Router trennen Broadcast-Domänen.

Switching und Kollisionsdomäne

Bei modernen Switches ist jeder Port normalerweise eine eigene Kollisionsdomäne.

Das ist ein wichtiger Unterschied zum Hub.

Gerät	Kollisionsdomäne
Hub	alle Ports gemeinsam
Switch	jeder Port separat

Bei Vollduplex-Verbindungen treten klassische Kollisionen praktisch nicht mehr auf.

Merksatz:

> Switch reduziert Kollisionsprobleme durch getrennte Ports.

Store-and-Forward

Store-and-Forward ist eine typische Weiterleitungsmethode bei Switches.

Dabei empfängt der Switch den gesamten Frame.

Dann prüft er den Frame, zum Beispiel anhand der FCS.

Erst danach leitet er den Frame weiter.

Vorteil:

Fehlerhafte Frames können erkannt und verworfen werden.

Nachteil:

etwas mehr Verzögerung als bei sofortiger Weiterleitung.

Merksatz:

Store-and-Forward prüft den Frame vor der Weiterleitung.

Cut-Through

Cut-Through ist eine andere Weiterleitungsmethode.

Dabei beginnt der Switch mit der Weiterleitung, sobald er die Ziel-MAC-Adresse gelesen hat.

Vorteil:

geringere Verzögerung

Nachteil:

Fehlerhafte Frames können eventuell weitergeleitet werden,
bevor der gesamte Frame geprüft wurde.

Merksatz:

Cut-Through ist schneller,
prüft aber weniger vollständig vor der Weiterleitung.

Store-and-Forward und Cut-Through im Vergleich

Methode	Arbeitsweise	Vorteil	Nachteil

Store-and-Forward	ganzer Frame wird empfangen und geprüft	Fehlererkennung vor Weiterleitung	etwas mehr Latenz
Cut-Through	Weiterleitung beginnt früh	geringe Latenz	fehlerhafte Frames können weitergehen

Für die Prüfung ist vor allem wichtig:

```
Store-and-Forward prüft vollständiger.
Cut-Through ist schneller.
```

Switching und VLANs

Ein Switch kann Ports verschiedenen VLANs zuordnen.

Beispiel:

Port	VLAN	Gerät
1	VLAN 10	Mitarbeiter-PC
2	VLAN 10	Mitarbeiter-PC
3	VLAN 20	Gastgerät
4	VLAN 30	Server

Frames werden normalerweise nur innerhalb desselben VLANs weitergeleitet.

Dadurch entstehen getrennte logische Netze.

Merksatz:

```
VLANs trennen Switching-Bereiche logisch.
```

Access-Port

Ein Access-Port gehört normalerweise zu genau einem VLAN.

Typischer Einsatz:

```
- PC
- Drucker
- IP-Telefon
```

```
- Access Point mit einfacher Konfiguration
```

Beispiel:

```
Port 1 ist Access-Port in VLAN 10.
```

Ein Gerät an diesem Port gehört dann logisch zu VLAN 10.

Merksatz:

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

Trunk-Port

Ein Trunk-Port kann mehrere VLANs transportieren.

Typischer Einsatz:

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

Bei Ethernet wird dafür häufig VLAN-Tagging verwendet.

Merksatz:

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

Switching-Schleifen

Eine Switching-Schleife entsteht, wenn Frames im Netzwerk endlos im Kreis laufen können.

Das kann passieren, wenn Switches mehrfach miteinander verbunden sind und keine Schutzmechanismen aktiv sind.

Folgen:

```
- Broadcast-Sturm
- hohe Switch-Last
- Netzwerk wird langsam oder fällt aus
- MAC-Adresstabelle wird instabil
```

Merksatz:

```
Schleifen im Layer-2-Netz können sehr gefährlich sein.
```

Spanning Tree Protocol

STP steht für:

```
Spanning Tree Protocol
```

STP verhindert Schleifen in Layer-2-Netzen.

Es blockiert bestimmte redundante Wege, damit keine Schleife entsteht.

Wenn eine Verbindung ausfällt, kann STP einen anderen Weg aktivieren.

Merksatz:

```
STP schützt vor Switching-Schleifen.
```

Broadcast-Sturm

Ein Broadcast-Sturm entsteht, wenn sehr viele Broadcasts im Netzwerk unterwegs sind.

Mögliche Ursachen:

```
- Layer-2-Schleife
- fehlerhafte Geräte
- falsch konfigurierte Switches
- Angriffe
- sehr viele Broadcast-Anfragen
```

Folgen:

```
- hohe Netzwerklast
- hohe CPU-Last auf Geräten
- Verbindungsprobleme
- Netzwerkausfall
```

Merksatz:

```
Broadcast-Sturm = zu viele Broadcasts im lokalen Netz.
```

Switching und Fehlersuche

Bei Schicht-2-Problemen prüft man zum Beispiel:

```
- Ist der richtige Switch-Port verwendet?
- Ist der Port aktiv?
- Wird die MAC-Adresse gelernt?
- Ist das richtige VLAN konfiguriert?
- Ist der Port Access oder Trunk?
- Gibt es Fehler am Port?
- Gibt es STP-Blockierungen?
- Gibt es Broadcast-Stürme?
- Gibt es doppelte MAC-Adressen?
- Wurde das Gerät umgesteckt?
```

Merksatz:

```
Bei Schicht 2 prüft man MAC-Adressen, VLANs und Switch-Ports.
```

Beispiel: MAC-Adresse wird nicht gelernt

Fehlerbild:

```
Ein Gerät ist physisch verbunden,
aber der Switch lernt keine MAC-Adresse.
```

Mögliche Ursachen:

- Gerät sendet keine Frames
- falscher Port
- Port deaktiviert
- Link ist doch nicht aktiv
- VLAN falsch
- Netzwerkkarte deaktiviert
- Kabelproblem
- Port Security blockiert
- Gerät hängt an falscher Stelle

Merksatz:

Keine gelernte MAC kann auf Schicht 1 oder Schicht 2 hinweisen.

Beispiel: Gerät im falschen VLAN

Fehlerbild:

Ein PC bekommt keine passende IP-Adresse
oder erreicht die erwarteten Server nicht.

Mögliche Ursache:

Der Switch-Port ist im falschen VLAN.

Beispiel:

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

Folge:

Der PC befindet sich logisch im falschen Netz.

Merksatz:

Falsches VLAN kann wie ein IP-Problem aussehen.

Beispiel: Trunk falsch konfiguriert

Fehlerbild:

Mehrere VLANs funktionieren über eine Switch-Verbindung nicht.

Mögliche Ursachen:

- Port ist kein Trunk
- VLAN nicht auf dem Trunk erlaubt
- falsches Native VLAN
- Gegenstelle anders konfiguriert
- Tagging stimmt nicht
- STP blockiert den Port

Merksatz:

Trunk-Probleme betreffen oft mehrere VLANs gleichzeitig.

Was ein Switch nicht macht

Ein normaler Layer-2-Switch macht nicht:

- Routing zwischen IP-Netzen
- NAT oder PAT
- DNS-Auflösung
- TCP-Verbindungsaufbau
- Anwendungsschutz
- Internetzugang allein
- Firewall-Regeln auf Anwendungsebene

Dafür braucht man andere Funktionen oder Geräte, zum Beispiel:

- Router
- Layer-3-Switch
- Firewall
- DNS-Server

Merksatz:

Ein Layer-2-Switch verbindet lokal,
routet aber nicht zwischen Netzen.

Typische IHK-Fragen

In AP1 und AP2 kann zum Beispiel gefragt werden:

- Was macht ein Switch?
- Auf welcher OSI-Schicht arbeitet ein Switch?
- Wie lernt ein Switch MAC-Adressen?
- Was ist eine MAC-Adresstabelle?
- Was passiert bei bekannter Ziel-MAC?
- Was passiert bei unbekannter Ziel-MAC?
- Was bedeutet Flooding?
- Was ist der Unterschied zwischen Broadcast und Flooding?
- Was ist Port Security?
- Was ist eine Kollisionsdomäne?
- Was ist eine Broadcast-Domäne?
- Was ist der Unterschied zwischen Access-Port und Trunk-Port?
- Was ist STP?
- Warum sind Layer-2-Schleifen gefährlich?

Typische Prüfungsfallen

Ein Switch lernt über die Quell-MAC-Adresse.

Die Ziel-MAC entscheidet über die Weiterleitung.

Bekannte Ziel-MAC = gezielte Weiterleitung.

Unbekannte Ziel-MAC = Flooding.

Broadcast und Flooding sind nicht dasselbe.

Ein normaler Switch arbeitet auf Schicht 2.

Ein Hub arbeitet auf Schicht 1.

Ein Router arbeitet auf Schicht 3.

Ein Switch trennt Kollisionsdomänen.

Ein Switch trennt Broadcast-Domänen nur durch VLANs.

Ein Access-Port gehört normalerweise zu einem VLAN.

Ein Trunk-Port transportiert mehrere VLANs.

STP schützt vor Layer-2-Schleifen.

Falsches VLAN kann wie ein IP-Problem aussehen.

Wichtige Begriffe kurz erklärt

Begriff	Kurze Erklärung
Switch	Schicht-2-Gerät zur Frame-Weiterleitung
Switch-Port	physischer Anschluss am Switch
MAC-Adresstabelle	Zuordnung von MAC-Adresse zu Switch-Port
Quell-MAC	Absenderadresse im Frame
Ziel-MAC	Empfängeradresse im Frame
Learning	Lernen von MAC-Adressen über Quell-MAC
Forwarding	gezielte Weiterleitung an bekannten Port
Flooding	Weiterleitung an mehrere Ports bei unbekannter Ziel-MAC
Broadcast	Nachricht an alle Geräte im lokalen Netz
Aging	automatisches Entfernen alter MAC-Einträge
Port Security	Begrenzung erlaubter MAC-Adressen pro Port
MAC-Flooding	Angriff auf die MAC-Adresstabelle

Begriff	Kurze Erklärung
Kollisionsdomäne	Bereich möglicher Kollisionen
Broadcast-Domäne	Bereich, in dem Broadcasts verteilt werden
Access-Port	Switch-Port für ein VLAN
Trunk-Port	Switch-Port für mehrere VLANs
STP	Spanning Tree Protocol zur Schleifenvermeidung
Broadcast-Sturm	übermäßige Broadcast-Last im Netz

IHK-sichere Kurzformulierung

Ein Switch arbeitet typischerweise auf OSI-Schicht 2 und leitet Ethernet-Frames anhand von MAC-Adressen weiter. Er lernt MAC-Adressen über die Quell-MAC-Adresse eingehender Frames und speichert die Zuordnung von MAC-Adresse zu Switch-Port in einer MAC-Adresstabelle. Ist die Ziel-MAC-Adresse bekannt, wird der Frame gezielt an den passenden Port weitergeleitet. Ist die Ziel-MAC-Adresse unbekannt, wird der Frame an mehrere Ports geflutet. Broadcasts werden innerhalb der Broadcast-Domäne verteilt. VLANs können Broadcast-Domänen logisch trennen. STP verhindert Schleifen in Layer-2-Netzen.

Merksätze

Switch = Schicht 2.

Switch arbeitet mit Frames.

Switch arbeitet mit MAC-Adressen.

Switch lernt über Quell-MAC.

Ziel-MAC entscheidet über Weiterleitung.

MAC-Adresstabelle = MAC zu Port.

Bekannte Ziel-MAC = gezielte Weiterleitung.

Unbekannte Ziel-MAC = Flooding.

Broadcast = an alle.

Flooding = Ziel unbekannt.

Broadcast und Flooding sind nicht dasselbe.

Hub = Schicht 1.

Switch = Schicht 2.

Router = Schicht 3.

Switch trennt Kollisionsdomänen.

VLAN trennt Broadcast-Domänen.

Access-Port = ein VLAN.

Trunk-Port = mehrere VLANs.

STP schützt vor Schleifen.

Layer-2-Schleifen können Broadcast-Stürme verursachen.

Falsches VLAN kann wie ein IP-Problem aussehen.