

5.1 OSI-Schicht 2 - Sicherungsschicht

Die Sicherungsschicht ist Schicht 2 des OSI-Modells.

Sie liegt direkt über der Bitübertragungsschicht.

Während Schicht 1 nur Bits als Signale überträgt, organisiert Schicht 2 diese Bits zu sinnvollen Übertragungseinheiten im lokalen Netzwerk.

Diese Übertragungseinheiten heißen:

Frames

Bei Ethernet spricht man deshalb auch von:

Ethernet-Frames

Merksatz:

Schicht 2 = Frames und MAC-Adressen.

Grundaufgabe der Sicherungsschicht

Die Hauptaufgabe der Sicherungsschicht ist:

Daten im lokalen Netzwerk zuverlässig von einem Gerät zum nächsten übertragen.

Dabei geht es besonders um:

- Frames
- MAC-Adressen
- lokale Zustellung
- Zugriff auf das Übertragungsmedium
- Fehlererkennung
- Switches
- VLANs
- Broadcasts
- Kollisions- und Broadcast-Domänen

Wichtig:

Schicht 2 arbeitet innerhalb eines lokalen Netzwerks.
Schicht 3 ist für IP und Routing zwischen Netzwerken zuständig.

Merksatz:

Schicht 2 kümmert sich um die lokale Übertragung im LAN.

Einordnung im OSI-Modell

OSI-Schicht	Name	Aufgabe
7	Anwendungsschicht	Netzwerkdienste für Anwendungen
6	Darstellungsschicht	Darstellung, Codierung, Verschlüsselung
5	Sitzungsschicht	Sitzungen verwalten
4	Transportschicht	Transport zwischen Anwendungen
3	Vermittlungsschicht	IP-Adressierung und Routing
2	Sicherungsschicht	Frames, MAC-Adressen, lokale Übertragung
1	Bitübertragungsschicht	Bits als Signale übertragen

Merksatz:

Schicht 1 = Bits.
Schicht 2 = Frames.
Schicht 3 = IP-Pakete.

Warum braucht man Schicht 2?

Schicht 1 überträgt nur einzelne Bits.

Aber ein Netzwerkgerät muss wissen:

Wo beginnt eine Datenübertragung?
Wo endet sie?
Für welches Gerät ist sie bestimmt?

Von welchem Gerät kommt sie?
Ist der Frame beschädigt?
Soll der Frame weitergeleitet werden?

Diese Aufgaben übernimmt Schicht 2.

Merksatz:

Schicht 2 macht aus reiner Bitübertragung eine lokale Datenübertragung.

Begriff: Frame

Ein Frame ist die Datenübertragungseinheit auf Schicht 2.

Bei Ethernet spricht man von:

Ethernet-Frame

Ein Frame enthält unter anderem:

- Ziel-MAC-Adresse
- Quell-MAC-Adresse
- Nutzdaten
- Prüfinformationen

Vereinfacht:

Ein Frame ist ein Datenpaket für das lokale Netzwerk.

Fachlich genauer:

Ein Frame ist die Protocol Data Unit der Sicherungsschicht.

Merksatz:

Frame = Datenrahmen auf Schicht 2.

Frame und Paket unterscheiden

Die Begriffe Frame und Paket werden im Alltag oft vermischt.

Fachlich sollte man unterscheiden:

Begriff	Schicht	Bedeutung
Frame	Schicht 2	lokale Übertragung mit MAC-Adressen
Paket	Schicht 3	IP-Übertragung zwischen Netzwerken
Segment	Schicht 4	TCP-Datenübertragung
Datagramm	Schicht 4	UDP-Datenübertragung

Prüfungsfälle:

Ethernet arbeitet mit Frames,
IP arbeitet mit Paketen.

Merksatz:

Schicht 2 = Frame.
Schicht 3 = Paket.

Begriff: MAC-Adresse

MAC steht für:

Media Access Control

Eine MAC-Adresse ist eine Hardwareadresse einer Netzwerkschnittstelle.

Beispiele für Netzwerkschnittstellen:

- Ethernet-Netzwerkkarte
- WLAN-Adapter
- Switch-Port mit eigener Management-Schnittstelle
- virtuelle Netzwerkkarte

Eine MAC-Adresse dient zur lokalen Adressierung im Netzwerk.

Merksatz:

MAC-Adresse = lokale Hardwareadresse einer Netzwerkschnittstelle.

Aufbau einer MAC-Adresse

Eine MAC-Adresse besteht aus 48 Bit.

Sie wird häufig hexadezimal dargestellt.

Beispiel:

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

Oder auch:

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

Hexadezimal bedeutet:

Darstellung mit den Zeichen 0 bis 9 und A bis F.

Merksatz:

MAC-Adresse = 48 Bit, meist hexadezimal dargestellt.

Quell-MAC-Adresse und Ziel-MAC-Adresse

Ein Ethernet-Frame enthält normalerweise:

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

Die Ziel-MAC-Adresse gibt an:

An welches Gerät im lokalen Netzwerk soll der Frame gehen?

Die Quell-MAC-Adresse gibt an:

Von welchem Gerät kommt der Frame?

Beispiel:

PC A sendet an PC B.

Dann enthält der Frame:

Quell-MAC-Adresse: MAC von PC A

Ziel-MAC-Adresse: MAC von PC B

Merksatz:

Ziel-MAC = wohin im lokalen Netz.

Quell-MAC = woher im lokalen Netz.

Lokale Bedeutung der MAC-Adresse

MAC-Adressen gelten für die lokale Übertragung im gleichen Netzwerksegment.

Wichtig:

MAC-Adressen werden nicht über Router hinweg unverändert für die gesamte Strecke verwendet.

Wenn ein IP-Paket über mehrere Router läuft, ändern sich auf jedem lokalen Abschnitt die Schicht-2-Adressen.

Die IP-Adressen bleiben dagegen grundsätzlich Ende-zu-Ende erhalten, außer bei NAT.

Merksatz:

MAC-Adressen gelten lokal.

IP-Adressen gelten netzübergreifend.

Beispiel: MAC und IP

Ein PC möchte eine Webseite im Internet öffnen.

Dabei gibt es mehrere Ebenen:

Schicht 2:

lokale Zustellung zum nächsten Gerät, zum Beispiel Router

Schicht 3:

IP-Zustellung zum Zielnetz

Vereinfacht:

Der PC sendet den Ethernet-Frame lokal an die MAC-Adresse des Routers.

Im IP-Paket steht aber die IP-Adresse des Webserver.

Merksatz:

MAC bringt den Frame zum nächsten lokalen Ziel.

IP bringt das Paket zum Zielnetz.

Schicht 2 im lokalen Netzwerk

Schicht 2 ist besonders wichtig im LAN.

LAN steht für:

Local Area Network

Typische Schicht-2-Techniken im LAN:

- Ethernet
- WLAN
- Switches
- MAC-Adressen
- VLANs
- ARP im Zusammenspiel mit IP
- Broadcasts

Merksatz:

Schicht 2 ist die lokale Ebene im LAN.

Ethernet

Ethernet ist die wichtigste LAN-Technik in kabelgebundenen Netzwerken.

Ethernet beschreibt unter anderem:

- Frame-Aufbau
- MAC-Adressen
- Zugriff auf das Medium
- Übertragungsstandards
- Zusammenarbeit mit Schicht 1

Ethernet betrifft Schicht 1 und Schicht 2.

Schicht 1:

physische Übertragung

Schicht 2:

Frames und MAC-Adressen

Merksatz:

Ethernet verbindet Schicht 1 und Schicht 2.

WLAN und Schicht 2

Auch WLAN arbeitet mit Schicht-2-Konzepten.

Bei WLAN gibt es ebenfalls:

- MAC-Adressen
- Frames
- Zugriff auf das Medium

- Authentifizierung und Assoziation
- SSID
- Access Points

WLAN unterscheidet sich technisch von Ethernet, erfüllt aber ebenfalls Aufgaben der Sicherungsschicht.

Merksatz:

WLAN hat ebenfalls Schicht-2-Funktionen.

Begriff: Switch

Ein Switch ist ein Netzwerkgerät, das auf Schicht 2 arbeitet.

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

Er merkt sich, an welchem Port welche MAC-Adresse erreichbar ist.

Diese Informationen speichert er in einer Tabelle.

Diese Tabelle nennt man häufig:

MAC-Adresstabelle

Oder:

Switching-Tabelle

Merksatz:

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

Hub und Switch unterscheiden

Ein Hub arbeitet auf Schicht 1.

Ein Switch arbeitet typischerweise auf Schicht 2.

Gerät	Schicht	Arbeitsweise
-------	---------	--------------

Hub	1	verteilt Signale an alle Ports
Switch	2	leitet Frames anhand von MAC-Adressen weiter

Wichtig:

Ein Switch ist intelligenter als ein Hub,
weil er MAC-Adressen auswertet.

Merksatz:

Hub verteilt blind.
Switch entscheidet anhand von MAC-Adressen.

MAC-Adresstabelle

Ein Switch lernt MAC-Adressen automatisch.

Wenn ein Frame an einem Switch-Port eingeht, merkt sich der Switch:

Diese Quell-MAC-Adresse ist an diesem Port erreichbar.

Beispiel:

Frame kommt an Port 3 an.
Quell-MAC-Adresse ist AA:BB:CC:11:22:33.

Der Switch merkt sich:

AA:BB:CC:11:22:33 → Port 3

Merksatz:

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

Frame-Weiterleitung durch den Switch

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

Dann gibt es drei typische Fälle:

Fall	Verhalten
Ziel-MAC bekannt	Frame wird gezielt an passenden Port weitergeleitet
Ziel-MAC unbekannt	Frame wird an mehrere Ports geflutet
Ziel-MAC ist Broadcast	Frame wird an alle relevanten Ports gesendet

Dieses Fluten nennt man:

Flooding

Merksatz:

Bekannte MAC = gezielt.
Unbekannte MAC = Flooding.

Broadcast

Ein Broadcast ist eine Nachricht an alle Geräte im lokalen Netz.

Die Broadcast-MAC-Adresse lautet:

FF:FF:FF:FF:FF:FF

Broadcasts werden zum Beispiel verwendet bei:

- ARP-Anfragen
- DHCP-Anfragen
- bestimmten lokalen Such- und Steuerdiensten

Wichtig:

Broadcasts bleiben normalerweise innerhalb einer Broadcast-Domäne.

Merksatz:

Broadcast = Nachricht an alle im lokalen Netz.

Broadcast-Domäne

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

Alle Geräte in derselben Broadcast-Domäne können Broadcasts voneinander empfangen.

Typisch:

Ein VLAN bildet eine eigene Broadcast-Domäne.

Router trennen Broadcast-Domänen.

Merksatz:

Broadcast-Domäne = Bereich, in dem Broadcasts weitergegeben werden.

Kollisionsdomäne

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

Bei einem Hub:

alle Ports gehören zu einer gemeinsamen Kollisionsdomäne.

Bei einem Switch:

jeder Port ist normalerweise eine eigene Kollisionsdomäne.

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

Merksatz:

Hub = eine Kollisionsdomäne.

Switch = getrennte Kollisionsbereiche pro Port.

Fehlererkennung auf Schicht 2

Schicht 2 kann Übertragungsfehler erkennen.

Dazu enthält ein Ethernet-Frame eine Prüfinformation.

Diese nennt man:

FCS

FCS steht für:

Frame Check Sequence

Die FCS basiert auf einer Prüfsumme.

Häufig wird dabei der Begriff CRC verwendet.

CRC steht für:

Cyclic Redundancy Check

Merksatz:

FCS/CRC erkennt beschädigte Frames.

Wichtig: Fehlererkennung ist nicht Fehlerkorrektur

Schicht 2 kann beschädigte Frames erkennen.

Aber:

Ethernet korrigiert fehlerhafte Frames normalerweise nicht.

Wenn ein Frame fehlerhaft ist, wird er verworfen.

Eine erneute Übertragung erfolgt dann gegebenenfalls durch höhere Schichten, zum Beispiel durch TCP.

Merksatz:

Schicht 2 erkennt viele Fehler,
korrigiert sie aber normalerweise nicht selbst.

VLAN kurz eingeordnet

VLAN steht für:

Virtual Local Area Network

Ein VLAN ist ein logisch getrenntes Netzwerk auf Schicht 2.

VLANs ermöglichen es, mehrere logische Netze über dieselbe physische Switch-Infrastruktur zu betreiben.

Beispiel:

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

Merksatz:

VLAN = logische Netztrennung auf Schicht 2.

Schicht 2 und ARP

ARP steht für:

Address Resolution Protocol

ARP verbindet Schicht 3 und Schicht 2.

Aufgabe:

Zu einer bekannten IP-Adresse wird die passende MAC-Adresse im lokalen Netzwerk gesucht.

Beispiel:

PC kennt IP-Adresse des Routers.
PC braucht MAC-Adresse des Routers.
ARP fragt im lokalen Netz nach der passenden MAC-Adresse.

Merksatz:

ARP findet zur IP-Adresse die passende MAC-Adresse im lokalen Netz.

Schicht 2 und IP unterscheiden

Thema	Schicht
MAC-Adresse	Schicht 2
Ethernet-Frame	Schicht 2
Switch	Schicht 2
VLAN	Schicht 2
IP-Adresse	Schicht 3
IP-Paket	Schicht 3
Router	Schicht 3
Routing	Schicht 3

Merksatz:

MAC = lokal.

IP = netzübergreifend.

Was Schicht 2 nicht macht

Schicht 2 macht nicht:

- Routing zwischen IP-Netzen
- Auswahl des besten IP-Wegs
- TCP-Verbindungsaufbau
- UDP-Port-Auswertung
- DNS-Auflösung
- HTTP-Anfragen
- Benutzeranmeldung in Anwendungen

Diese Aufgaben gehören zu höheren Schichten.

Merksatz:

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

Typische Schicht-2-Fehler

Typische Fehler auf Schicht 2 sind:

- falsches VLAN
- MAC-Adresse nicht gelernt
- Broadcast-Stürme
- Schleifen im Switch-Netz
- STP-Probleme
- Port im falschen Modus
- fehlerhafte Trunk-Konfiguration
- doppelte MAC-Adressen
- falsche Access-Point- oder SSID-VLAN-Zuordnung

Wichtig:

Schicht-2-Probleme können so wirken,
als wäre IP falsch,
obwohl die Ursache im lokalen Netz liegt.

Merksatz:

Schicht-2-Fehler betreffen Frames, MACs, VLANs und lokale Weiterleitung.

Einordnung bei der Fehlersuche

Eine sinnvolle Reihenfolge:

1. Schicht 1 prüfen:
Link, Kabel, Signal, Port
2. Schicht 2 prüfen:
MAC-Adresse, VLAN, Switch-Port, Frames

3. Schicht 3 prüfen:

IP-Adresse, Gateway, Routing

4. höhere Schichten prüfen:

DNS, Ports, Anwendung

Merksatz:

Erst Link,

dann MAC/VLAN,

dann IP.

Typische IHK-Fragen

In AP1 und AP2 kann zum Beispiel gefragt werden:

- Welche Aufgabe hat die Sicherungsschicht?
- Was ist ein Frame?
- Was ist eine MAC-Adresse?
- Wofür wird eine MAC-Adresse verwendet?
- Was macht ein Switch?
- Wie lernt ein Switch MAC-Adressen?
- Was ist eine MAC-Adresstabelle?
- Was ist ein Broadcast?
- Was ist eine Broadcast-Domäne?
- Was ist der Unterschied zwischen Hub und Switch?
- Was ist ein VLAN?
- Was ist der Unterschied zwischen MAC-Adresse und IP-Adresse?
- Was macht ARP?
- Was bedeutet FCS oder CRC?

Typische Prüfungsfallen

Schicht 2 arbeitet mit Frames,
nicht mit IP-Paketen.

MAC-Adressen sind Schicht 2.

IP-Adressen sind Schicht 3.

Ein Switch arbeitet typischerweise auf Schicht 2.

Ein Router arbeitet typischerweise auf Schicht 3.

Ein Hub arbeitet auf Schicht 1.

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

Broadcast-MAC-Adresse ist FF:FF:FF:FF:FF:FF.

VLANs trennen logisch auf Schicht 2.

Ein VLAN ist nicht dasselbe wie ein IP-Subnetz,
wird aber häufig zusammen damit geplant.

ARP fragt nach der MAC-Adresse zu einer IP-Adresse im lokalen Netz.

FCS/CRC erkennt beschädigte Frames,
korrigiert sie aber normalerweise nicht.

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 einer Netzwerkschnittstelle
Ziel-MAC	Empfängeradresse im lokalen Netz
Quell-MAC	Absenderadresse im lokalen Netz
Switch	Schicht-2-Gerät für Frame-Weiterleitung
MAC-Adresstabelle	Tabelle mit MAC-Adresse und Switch-Port
Flooding	Weiterleitung an mehrere Ports bei unbekannter Ziel-MAC
Broadcast	Nachricht an alle Geräte im lokalen Netz
Broadcast-Domäne	Bereich, in dem Broadcasts verteilt werden

Begriff	Kurze Erklärung
Kollisionsdomäne	Bereich, in dem Kollisionen auftreten können
VLAN	logisches LAN auf Schicht 2
ARP	sucht MAC-Adresse zu einer IP-Adresse im lokalen Netz
FCS	Frame Check Sequence
CRC	Prüfsummenverfahren zur Fehlererkennung

IHK-sichere Kurzformulierung

Die Sicherungsschicht ist Schicht 2 des OSI-Modells. Sie ist für die lokale Übertragung von Daten in Form von Frames zuständig. Im Ethernet-LAN werden dafür MAC-Adressen verwendet. Ein Ethernet-Frame enthält unter anderem eine Quell-MAC-Adresse und eine Ziel-MAC-Adresse. Switches arbeiten typischerweise auf Schicht 2 und leiten Frames anhand von MAC-Adressen weiter. Sie lernen MAC-Adressen über die Quelladresse eingehender Frames und speichern diese in einer MAC-Adresstabelle. VLANs ermöglichen eine logische Trennung von Netzbereichen auf Schicht 2. Fehlerhafte Frames können über FCS/CRC erkannt und verworfen werden.

Merksätze

Schicht 2 = Sicherungsschicht.

Schicht 2 arbeitet mit Frames.

Ethernet-Frame = Datenrahmen im LAN.

MAC-Adresse = lokale Hardwareadresse.

Ziel-MAC = wohin lokal.

Quell-MAC = woher lokal.

MAC ist Schicht 2.

IP ist Schicht 3.

Switch = Schicht 2.

Hub = Schicht 1.

Router = Schicht 3.

Switch lernt über Quell-MAC-Adressen.

Bekannte Ziel-MAC = gezielte Weiterleitung.

Unbekannte Ziel-MAC = Flooding.

Broadcast = an alle.

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

VLAN = logische Trennung auf Schicht 2.

ARP verbindet IP-Adresse mit MAC-Adresse im lokalen Netz.

FCS/CRC erkennt beschädigte Frames.

Schicht 2 routet nicht zwischen IP-Netzen.
