

6.1 OSI-Schicht 3 - Vermittlungsschicht / Netzwerkschicht

Die Vermittlungsschicht ist Schicht 3 des OSI-Modells.

Sie wird auch genannt:

Netzwerkschicht

Die wichtigste Aufgabe von Schicht 3 ist:

Daten zwischen verschiedenen Netzwerken weiterleiten.

Dabei geht es vor allem um:

- IP-Adressen
- IP-Pakete
- Subnetze
- Routing
- Router
- Standard-Gateway
- Netzmaske
- IPv4
- IPv6
- ICMP

Merksatz:

Schicht 3 = IP-Adressen, Pakete und Routing.

Grundidee von Schicht 3

Schicht 2 ist für die lokale Übertragung im LAN zuständig.

Schicht 3 geht darüber hinaus.

Schicht 3 ermöglicht Kommunikation zwischen unterschiedlichen Netzwerken.

Beispiel:

PC im LAN
→ Router
→ Internet
→ Webserver

Dabei wird nicht mehr nur lokal mit MAC-Adressen gearbeitet, sondern mit IP-Adressen.

Merksatz:

Schicht 2 verbindet lokal.
Schicht 3 verbindet Netze.

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 / Netzwerkschicht	IP-Adressierung und Routing
2	Sicherungsschicht	Frames, MAC-Adressen, lokale Übertragung
1	Bitübertragungsschicht	Bits als Signale übertragen

Merksatz:

Schicht 3 liegt zwischen lokaler Übertragung und Transport.

Warum braucht man Schicht 3?

Ein lokales Netzwerk allein reicht nicht aus, wenn Geräte in unterschiedlichen Netzen kommunizieren sollen.

Beispiel:

PC A:

192.168.10.20

Server B:

192.168.30.50

Diese Geräte liegen in unterschiedlichen IP-Netzen.

Damit sie kommunizieren können, braucht man Routing.

Routing gehört zu Schicht 3.

Merksatz:

Unterschiedliche IP-Netze brauchen Schicht-3-Vermittlung.

Begriff: IP-Adresse

Eine IP-Adresse ist eine logische Adresse auf Schicht 3.

Sie dient dazu, Geräte in IP-Netzen erreichbar zu machen.

Beispiele:

IPv4:

192.168.10.20

IPv6:

2001:db8::10

IP-Adressen werden für die netzübergreifende Kommunikation verwendet.

Merksatz:

IP-Adresse = logische Adresse auf Schicht 3.

MAC-Adresse und IP-Adresse unterscheiden

Adresse	Schicht	Aufgabe
---------	---------	---------

MAC-Adresse	2	lokale Zustellung im LAN
IP-Adresse	3	logische Adressierung zwischen Netzen

Wichtig:

MAC-Adressen gelten nur lokal auf einem Netzwerkabschnitt.
IP-Adressen dienen der Zustellung über Netzgrenzen hinweg.

Merksatz:

MAC = lokal.
IP = netzübergreifend.

Begriff: IP-Paket

Ein IP-Paket ist die Datenübertragungseinheit auf Schicht 3.

Ein IP-Paket enthält unter anderem:

- Quell-IP-Adresse
- Ziel-IP-Adresse
- Nutzdaten
- Steuerinformationen

Vereinfacht:

Ein IP-Paket ist der Datenbehälter für die Zustellung zwischen IP-Netzen.

Merksatz:

IP-Paket = Datenform auf Schicht 3.

Frame, Paket und Segment unterscheiden

Begriff	Schicht	Bedeutung
Frame	2	lokale Übertragung mit MAC-Adressen

Begriff	Schicht	Bedeutung
Paket	3	IP-Übertragung zwischen Netzen
Segment	4	TCP-Datenübertragung
Datagramm	4	UDP-Datenübertragung

Prüfungsfälle:

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

Merksatz:

Schicht 2 = Frame.
Schicht 3 = Paket.
Schicht 4 = Segment oder Datagramm.

Quell-IP und Ziel-IP

Ein IP-Paket enthält normalerweise:

- Quell-IP-Adresse
- Ziel-IP-Adresse

Die Quell-IP-Adresse gibt an:

Von welchem Gerät stammt das Paket?

Die Ziel-IP-Adresse gibt an:

Zu welchem Gerät soll das Paket?

Beispiel:

PC sendet an Webserver.

Quell-IP:

IP-Adresse des PCs

Ziel-IP:

IP-Adresse des Webservers

Merksatz:

Quell-IP = woher.

Ziel-IP = wohin.

IP-Adresse bleibt über Router hinweg erhalten

Wenn ein IP-Paket über mehrere Router läuft, bleibt die Ziel-IP-Adresse grundsätzlich gleich.

Beispiel:

PC → Router 1 → Router 2 → Server

Die Ethernet-Frames ändern sich auf jedem Abschnitt.

Die IP-Adressen im IP-Paket bleiben grundsätzlich erhalten.

Ausnahme:

NAT oder PAT kann IP-Adressen verändern.

Merksatz:

MAC ändert sich pro Abschnitt.

IP bleibt grundsätzlich Ende-zu-Ende erhalten.

Router

Ein Router ist ein typisches Gerät auf Schicht 3.

Aufgabe:

IP-Pakete zwischen unterschiedlichen Netzwerken weiterleiten.

Ein Router entscheidet anhand der Ziel-IP-Adresse, wohin ein Paket weitergeleitet werden soll.

Dafür nutzt er eine Routing-Tabelle.

Merksatz:

Router = Schicht-3-Gerät für IP-Weiterleitung.

Switch und Router unterscheiden

Gerät	typische Schicht	Arbeitsweise
Switch	2	leitet Frames anhand von MAC-Adressen weiter
Router	3	leitet IP-Pakete anhand von IP-Adressen weiter

Wichtig:

Ein Switch verbindet Geräte im lokalen Netz.

Ein Router verbindet verschiedene IP-Netze.

Merksatz:

Switch = MAC.

Router = IP.

Standard-Gateway

Das Standard-Gateway ist der Router, den ein Gerät verwendet, wenn das Ziel nicht im eigenen IP-Netz liegt.

Beispiel:

PC:

192.168.10.20/24

Gateway:

192.168.10.1

Wenn der PC ein Ziel außerhalb von 192.168.10.0/24 erreichen möchte, sendet er das Paket an das Standard-Gateway.

Merksatz:

Standard-Gateway = Ausgang in andere Netze.

Wann braucht ein Gerät das Gateway?

Ein Gerät braucht das Gateway, wenn die Ziel-IP-Adresse nicht im eigenen Subnetz liegt.

Beispiel:

PC:
192.168.10.20/24

Ziel:
192.168.10.30

Das Ziel liegt im gleichen Netz.

Kein Gateway nötig.

Beispiel:

PC:
192.168.10.20/24

Ziel:
8.8.8.8

Das Ziel liegt nicht im gleichen Netz.

Gateway nötig.

Merksatz:

Gleiches Subnetz = direkt.

Anderes Subnetz = über Gateway.

Subnetz

Ein Subnetz ist ein Teilbereich eines IP-Netzes.

Beispiel:

192.168.10.0/24

Dieses Subnetz enthält IP-Adressen von:

192.168.10.1

bis

192.168.10.254

Die Netzadresse ist:

192.168.10.0

Die Broadcast-Adresse ist:

192.168.10.255

Merksatz:

Subnetz = logischer IP-Adressbereich.

Netzadresse

Die Netzadresse bezeichnet das Netzwerk selbst.

Beispiel:

192.168.10.0/24

Die Netzadresse ist:

192.168.10.0

Diese Adresse wird normalerweise nicht einem Endgerät zugewiesen.

Merksatz:

Netzadresse = Adresse des Netzes.

Broadcast-Adresse

Die Broadcast-Adresse ist die Adresse für alle Geräte im Subnetz.

Beispiel:

192.168.10.0/24

Broadcast-Adresse:

192.168.10.255

Diese Adresse wird normalerweise nicht einem einzelnen Endgerät zugewiesen.

Merksatz:

Broadcast-Adresse = alle Geräte im Subnetz.

Host-Adresse

Host-Adressen sind die nutzbaren Adressen für Geräte im Subnetz.

Beispiel:

192.168.10.0/24

Nutzbare Host-Adressen:

192.168.10.1
bis
192.168.10.254

Diese Adressen können Geräten zugewiesen werden.

Beispiele:

PC
Server
Drucker
Router-Interface
Access Point

Merksatz:

Host-Adresse = nutzbare Adresse für ein Gerät.

Subnetzmaske

Die Subnetzmaske legt fest, welcher Teil einer IP-Adresse zum Netz gehört und welcher Teil zum Host gehört.

Beispiel:

IP-Adresse:
192.168.10.20

Subnetzmaske:
255.255.255.0

Das entspricht:

/24

Merksatz:

Subnetzmaske trennt Netzanteil und Hostanteil.

CIDR-Schreibweise

CIDR steht für:

Classless Inter-Domain Routing

Die CIDR-Schreibweise gibt an, wie viele Bits zur Netzadresse gehören.

Beispiel:

192.168.10.20/24

Das bedeutet:

Die ersten 24 Bit gehören zum Netzanteil.

Häufige Beispiele:

	CIDR	Subnetzmaske
	/24	255.255.255.0
	/25	255.255.255.128
	/26	255.255.255.192
	/27	255.255.255.224
	/28	255.255.255.240
	/30	255.255.255.252

Merksatz:

/24 bedeutet:
24 Bit Netzanteil.

Netzanteil und Hostanteil

Eine IP-Adresse besteht aus:

Netzanteil
und

Hostanteil

Beispiel:

192.168.10.20/24

Bei /24 ist vereinfacht:

Netzanteil:

192.168.10

Hostanteil:

20

Das Netz ist:

192.168.10.0/24

Merksatz:

Netzanteil bestimmt das Netzwerk.

Hostanteil bestimmt das Gerät im Netzwerk.

Routing

Routing bedeutet:

IP-Pakete zwischen Netzwerken weiterleiten.

Ein Router prüft die Ziel-IP-Adresse und entscheidet anhand seiner Routing-Tabelle, wohin das Paket weitergeleitet wird.

Dabei interessiert ihn nicht die Ziel-MAC-Adresse des ursprünglichen Frames.

Der Router arbeitet auf Schicht 3.

Merksatz:

Routing = Wegentscheidung für IP-Pakete.

Routing-Tabelle

Eine Routing-Tabelle enthält Informationen darüber, welche Netze über welchen Weg erreichbar sind.

Vereinfacht enthält sie:

- Zielnetz
- Netzmaske oder Präfix
- nächster Hop
- Ausgangsschnittstelle
- Metrik

Beispiel:

Zielnetz	Nächster Hop	Schnittstelle
192.168.10.0/24	direkt verbunden	LAN
192.168.20.0/24	192.168.10.1	LAN
0.0.0.0/0	Provider-Router	WAN

Merksatz:

Routing-Tabelle = Wegweiser für IP-Pakete.

Nächster Hop

Der nächste Hop ist das nächste Gerät, an das ein Router ein Paket weitergibt.

Meist ist das ein anderer Router.

Beispiel:

Zielnetz:
10.20.30.0/24

nächster Hop:

192.168.1.1

Der Router sendet das Paket an den nächsten Hop, damit es dem Ziel näherkommt.

Merksatz:

Nächster Hop = nächster Router auf dem Weg zum Ziel.

Direkt verbundenes Netz

Ein Router kennt Netze, die direkt an seinen Schnittstellen angeschlossen sind.

Beispiel:

Router-Interface:

192.168.10.1/24

Dann kennt der Router direkt:

192.168.10.0/24

Für direkt verbundene Netze braucht der Router keinen weiteren Router als nächsten Hop.

Merksatz:

Direkt verbunden = Netz liegt an eigener Schnittstelle.

Default Route

Eine Default Route ist eine Standardroute für alle Ziele, für die keine genauere Route vorhanden ist.

IPv4-Schreibweise:

0.0.0.0/0

Bedeutung:

alle IPv4-Ziele

Beispiel:

Alles Unbekannte geht zum Provider-Router.

Merksatz:

Default Route = Route für alles, was nicht genauer bekannt ist.

Longest Prefix Match

Ein Router wählt bei mehreren passenden Routen die genaueste Route.

Das nennt man:

Longest Prefix Match

Beispiel:

Route A:

192.168.0.0/16

Route B:

192.168.10.0/24

Ziel:

192.168.10.50

Beide Routen passen.

Die /24-Route ist genauer und wird gewählt.

Merksatz:

Genaueste passende Route gewinnt.

Statisches Routing

Beim statischen Routing werden Routen manuell eingetragen.

Vorteile:

- einfach bei kleinen Netzen
- gut kontrollierbar
- wenig Protokoll-Overhead

Nachteile:

- hoher Aufwand bei großen Netzen
- Änderungen müssen manuell gepflegt werden
- Ausfälle werden nicht automatisch umgangen

Merksatz:

Statische Route = manuell eingetragener Weg.

Dynamisches Routing

Beim dynamischen Routing tauschen Router automatisch Routing-Informationen aus.

Dafür werden Routing-Protokolle verwendet.

Beispiele:

- OSPF
- RIP
- BGP

Vorteile:

- automatische Anpassung
- besser für größere Netze
- alternative Wege möglich

Nachteile:

- komplexer
- muss geplant und abgesichert werden

Merksatz:

Dynamisches Routing = Router lernen Wege automatisch.

Routing-Protokolle kurz eingeordnet

Protokoll	typischer Einsatz
RIP	einfach, älter, kleine Netze
OSPF	interne Unternehmensnetze
BGP	Internet und Provider-Routing

Für AP1/AP2 ist besonders wichtig:

OSPF wird häufig in internen Netzen verwendet.
BGP ist zentral für das Routing im Internet.

Merksatz:

OSPF intern.
BGP zwischen großen Netzen im Internet.

ICMP

ICMP steht für:

Internet Control Message Protocol

ICMP gehört zum IP-Umfeld und wird für Kontroll- und Fehlermeldungen verwendet.

Typische Nutzung:

- Ping
- Traceroute

- Fehlermeldungen im IP-Netz

Wichtig:

ICMP nutzt keine TCP- oder UDP-Ports.

Merksatz:

ICMP = Kontrollmeldungen für IP.

Ping

Ping prüft, ob ein Ziel grundsätzlich per IP erreichbar ist.

Dazu wird häufig ICMP Echo Request und Echo Reply verwendet.

Vereinfacht:

Echo Request:

Bist du erreichbar?

Echo Reply:

Ja, ich antworte.

Wichtig:

Wenn Ping nicht funktioniert,
heißt das nicht automatisch,
dass das Ziel komplett unerreichbar ist.

ICMP kann durch Firewalls blockiert werden.

Merksatz:

Ping prüft IP-Erreichbarkeit,
aber ist kein vollständiger Diensttest.

Traceroute

Traceroute zeigt den Weg zu einem Ziel über mehrere Router.

Je nach Betriebssystem heißt der Befehl zum Beispiel:

```
tracert  
traceroute  
tracpath
```

Traceroute hilft zu erkennen:

über welche Router ein Paket läuft
und
wo die Verbindung möglicherweise stoppt.

Merksatz:

Traceroute zeigt den Weg durch das IP-Netz.

TTL

TTL steht für:

Time To Live

TTL begrenzt die Lebensdauer eines IP-Pakets.

Jeder Router verringert den TTL-Wert.

Wenn TTL 0 erreicht, wird das Paket verworfen.

Zweck:

Pakete sollen nicht endlos im Netz kreisen.

Merksatz:

TTL verhindert endloses Kreisen von IP-Paketen.

IPv4 und IPv6

Schicht 3 kann mit IPv4 oder IPv6 arbeiten.

Version	Beispiel
IPv4	192.168.10.20
IPv6	2001:db8::10

IPv4 verwendet 32-Bit-Adressen.

IPv6 verwendet 128-Bit-Adressen.

Merksatz:

IPv4 = 32 Bit.
IPv6 = 128 Bit.

Private IPv4-Adressen

Private IPv4-Adressen werden in lokalen Netzwerken verwendet.

Wichtige Bereiche:

Bereich	CIDR
10.0.0.0 - 10.255.255.255	10.0.0.0/8
172.16.0.0 - 172.31.255.255	172.16.0.0/12
192.168.0.0 - 192.168.255.255	192.168.0.0/16

Private Adressen sind im öffentlichen Internet nicht direkt geroutet.

Merksatz:

Private IPv4-Adressen werden im LAN genutzt.

NAT kurz eingeordnet

NAT steht für:

Network Address Translation

NAT verändert IP-Adressen beim Übergang zwischen Netzen.

Typisches Beispiel:

viele private Geräte im LAN
teilen sich eine öffentliche IPv4-Adresse

NAT wird besonders häufig am Internet-Router eingesetzt.

Merksatz:

NAT übersetzt IP-Adressen.

PAT kurz eingeordnet

PAT steht für:

Port Address Translation

PAT ist eine Form von NAT.

Dabei teilen sich mehrere interne Geräte eine öffentliche IP-Adresse und werden über Port-Zuordnungen unterschieden.

Typisch im Heimnetz:

viele Geräte
eine öffentliche IPv4-Adresse

Merksatz:

PAT = viele interne Geräte über eine öffentliche IP mit Ports unterscheiden.

Schicht 3 und VLANs

VLANs gehören zu Schicht 2.

Wenn Geräte in unterschiedlichen VLANs kommunizieren sollen, braucht man Routing auf Schicht 3.

Das nennt man:

Inter-VLAN-Routing

Dafür nutzt man:

- Router
- Layer-3-Switch
- Firewall

Merksatz:

VLAN trennt auf Schicht 2.
Routing verbindet auf Schicht 3.

Was Schicht 3 nicht macht

Schicht 3 macht nicht:

- Ethernet-Frames lokal anhand von MAC-Adressen switchen
- TCP-Verbindungen aufbauen
- UDP-Ports auswerten
- DNS-Namen auflösen
- Webseiten bereitstellen
- Benutzer anmelden
- Dateifreigaben bereitstellen

Diese Aufgaben liegen auf anderen Schichten.

Merksatz:

Schicht 3 routet IP-Pakete,
aber stellt keine Anwendung bereit.

Typische Schicht-3-Fehler

Typische Fehler auf Schicht 3 sind:

- falsche IP-Adresse
- falsche Subnetzmaske
- falsches Standard-Gateway
- fehlende Route
- falsche Route
- doppelte IP-Adresse
- NAT-Problem
- Routing-Schleife
- Firewall-Regel auf IP-Ebene
- falsches VLAN-Subnetz-Zusammenspiel

Merksatz:

Schicht-3-Fehler betreffen IP, Subnetze, Gateway und Routing.

Einordnung bei der Fehlersuche

Eine sinnvolle Reihenfolge:

1. Schicht 1:
Link, Kabel, Signal
2. Schicht 2:
MAC, VLAN, ARP
3. Schicht 3:
IP-Adresse, Subnetzmaske, Gateway, Route
4. Schicht 4:
TCP-/UDP-Port
5. Schicht 7:
Anwendung, DNS, Dienst

Merksatz:

Erst Link,
dann MAC/VLAN,

dann IP/Routing.

Typische IHK-Fragen

In AP1 und AP2 kann zum Beispiel gefragt werden:

- Welche Aufgabe hat die Vermittlungsschicht?
- Was ist eine IP-Adresse?
- Was ist ein IP-Paket?
- Was macht ein Router?
- Was ist ein Standard-Gateway?
- Wann wird ein Gateway benötigt?
- Was ist ein Subnetz?
- Was bedeutet CIDR?
- Was ist eine Routing-Tabelle?
- Was bedeutet Default Route?
- Was bedeutet Longest Prefix Match?
- Was ist der Unterschied zwischen statischem und dynamischem Routing?
- Was ist ICMP?
- Wofür wird Ping verwendet?
- Was zeigt Traceroute?
- Was ist TTL?
- Was ist der Unterschied zwischen MAC-Adresse und IP-Adresse?

Typische Prüfungsfallen

Schicht 3 arbeitet mit IP-Paketen.

Schicht 2 arbeitet mit Frames.

MAC-Adressen gehören zu Schicht 2.

IP-Adressen gehören zu Schicht 3.

Switch = Schicht 2.

Router = Schicht 3.

Gateway wird benötigt,
wenn das Ziel nicht im eigenen Subnetz liegt.

Gleiches Subnetz = direkte lokale Zustellung.

Anderes Subnetz = über Gateway.

Default Route = 0.0.0.0/0.

Genaueste passende Route gewinnt.

Ping nutzt ICMP,
nicht TCP oder UDP.

ICMP hat keine TCP- oder UDP-Ports.

IPv4 hat 32 Bit.

IPv6 hat 128 Bit.

VLAN ist Schicht 2.

Inter-VLAN-Routing ist Schicht 3.

Wichtige Begriffe kurz erklärt

Begriff	Kurze Erklärung
Vermittlungsschicht	OSI-Schicht 3
Netzwerkschicht	anderer Begriff für Schicht 3
IP-Adresse	logische Adresse auf Schicht 3
IP-Paket	Datenform auf Schicht 3
Quell-IP	Absender-IP-Adresse
Ziel-IP	Empfänger-IP-Adresse
Router	Gerät zur Weiterleitung zwischen Netzen
Standard-Gateway	Router für Ziele außerhalb des eigenen Netzes
Subnetz	logischer IP-Adressbereich
Netzadresse	Adresse des Netzes

Begriff	Kurze Erklärung
Broadcast-Adresse	Adresse für alle Hosts im Subnetz
Host-Adresse	nutzbare Adresse für ein Gerät
Subnetzmaske	trennt Netzanteil und Hostanteil
CIDR	Schreibweise für Präfixlänge
Routing	Weiterleitung zwischen IP-Netzen
Routing-Tabelle	Tabelle mit Wegen zu Zielnetzen
Nächster Hop	nächster Router auf dem Weg
Default Route	Standardroute für unbekannte Ziele
Longest Prefix Match	genaueste passende Route gewinnt
ICMP	Kontroll- und Fehlermeldungen für IP
Ping	ICMP-Erreichbarkeitstest
Traceroute	zeigt Weg über Router
TTL	begrenzt Lebensdauer eines IP-Pakets
NAT	Übersetzung von IP-Adressen
PAT	Übersetzung mit Port-Zuordnung

IHK-sichere Kurzformulierung

Die Vermittlungsschicht beziehungsweise Netzwerkschicht ist Schicht 3 des OSI-Modells. Sie ist für die logische Adressierung und Weiterleitung von IP-Paketen zwischen verschiedenen Netzwerken zuständig. Dafür werden IP-Adressen, Subnetzmasken, Gateways und Routing-Tabellen verwendet. Ein Router arbeitet typischerweise auf Schicht 3 und entscheidet anhand der Ziel-IP-Adresse, wohin ein Paket weitergeleitet wird. Befindet sich ein Ziel nicht im eigenen Subnetz, wird das Paket an das Standard-Gateway gesendet. ICMP gehört zum IP-Umfeld und wird unter anderem für Ping und Traceroute verwendet.

Merksätze

Schicht 3 = Vermittlungsschicht / Netzwerkschicht.

Schicht 3 = IP-Adressen, Pakete und Routing.

IP-Adresse = logische Adresse.

IP-Paket = Datenform auf Schicht 3.

MAC = Schicht 2.

IP = Schicht 3.

MAC gilt lokal.

IP gilt netzübergreifend.

Switch = MAC.

Router = IP.

Gateway = Ausgang in andere Netze.

Gleiches Subnetz = direkt.

Anderes Subnetz = über Gateway.

Subnetzmaske trennt Netzanteil und Hostanteil.

CIDR gibt die Präfixlänge an.

Routing = Weiterleitung zwischen IP-Netzen.

Routing-Tabelle = Wegweiser für Pakete.

Default Route = 0.0.0.0/0.

Genaueste passende Route gewinnt.

ICMP = Kontrollmeldungen für IP.

Ping nutzt ICMP.

ICMP nutzt keine TCP- oder UDP-Ports.

Traceroute zeigt den Weg durch das IP-Netz.

TTL verhindert endloses Kreisen von IP-Paketen.

IPv4 = 32 Bit.

IPv6 = 128 Bit.

VLAN = Schicht 2.

Inter-VLAN-Routing = Schicht 3.

Erst Link,
dann MAC/VLAN,
dann IP/Routing.
