6.8 Merksätze und Prüfungswissen zu OSI-Schicht 3

Diese Seite fasst die wichtigsten Inhalte zur OSI-Schicht 3 zusammen.

OSI-Schicht 3 heißt:

```
Vermittlungsschicht
```

Sie wird auch genannt:

```
Netzwerkschicht
```

Die Hauptaufgabe von Schicht 3 ist:

```
IP-Pakete zwischen verschiedenen Netzwerken weiterleiten.
```

Merksatz:

```
Schicht 3 = IP-Adressen, Pakete und Routing.
```

Grundidee von Schicht 3

Schicht 2 arbeitet lokal im LAN.

Schicht 3 verbindet unterschiedliche IP-Netze.

Beispiel:

```
Client im LAN
→ Router
→ anderes Netz
→ Server
```

Dafür werden IP-Adressen und Routing verwendet.

Merksatz:

Schicht 2 bringt Frames lokal weiter.

Schicht 3 bringt IP-Pakete in andere Netze.

Schicht 1, 2, 3 und 4 unterscheiden

Schicht	Name	Datenform	wichtige Begriffe
1	Bitübertragungsschicht	Bits	Signal, Link, Kabel
2	Sicherungsschicht	Frame	MAC, Switch, VLAN
3	Vermittlungsschicht / Netzwerkschicht	Paket	IP, Router, Routing
4	Transportschicht	Segment / Datagramm	TCP, UDP, Port

Merksatz:

Bit = Schicht 1.

Frame = Schicht 2.

Paket = Schicht 3.

Segment oder Datagramm = Schicht 4.

IP-Adresse

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

Sie dient dazu, Geräte in IP-Netzen zu adressieren.

Beispiele:

IPv4:

192.168.10.20

IPv6:

2001:db8::20

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	netzübergreifende Adressierung

Wichtig:

MAC-Adressen gelten lokal.
IP-Adressen gelten netzübergreifend.

Merksatz:

MAC = lokal.
IP = netzübergreifend.

IP-Paket

Ein IP-Paket ist die Datenform auf Schicht 3.

Ein IP-Paket enthält unter anderem:

- Quell-IP-Adresse
- Ziel-IP-Adresse
- Steuerinformationen
- Nutzdaten höherer Schichten

Merksatz:

IP-Paket = Datenbehälter auf Schicht 3.

Quell-IP und Ziel-IP

Ein IP-Paket enthält normalerweise:

Quell-IP-Adresse
Ziel-IP-Adresse

Die Quell-IP sagt:

```
Von welchem Gerät stammt das Paket?
```

Die Ziel-IP sagt:

```
Zu welchem Gerät soll das Paket?
```

Merksatz:

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

MAC ändert sich, IP bleibt grundsätzlich erhalten

Wenn ein IP-Paket über Router läuft, wird auf jedem Netzwerkabschnitt ein neuer Schicht-2-Frame erstellt.

Dabei ändern sich:

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

Grundsätzlich gleich bleiben:

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

Ausnahme:

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

Merksatz:

```
MAC ändert sich pro Abschnitt.
IP bleibt grundsätzlich Ende-zu-Ende.
```

Router

Ein Router ist ein typisches Gerät auf Schicht 3.

Ein Router verbindet verschiedene IP-Netze.

Er entscheidet anhand der Ziel-IP-Adresse, wohin ein IP-Paket weitergeleitet wird.

Dafür verwendet er eine Routing-Tabelle.

Merksatz:

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

Switch und Router unterscheiden

Gerät	typische Schicht	Entscheidung nach
Hub	1	Signal
Switch	2	MAC-Adresse
Router	3	IP-Adresse

Merksatz:

```
Hub = Signal.
Switch = MAC.
Router = IP.
```

Subnetz

Ein Subnetz ist ein logischer IP-Adressbereich.

Beispiel:

```
192.168.10.0/24
```

Zu einem Subnetz gehören:

```
- Netzadresse
- nutzbare Host-Adressen
```

```
- Broadcast-Adresse bei IPv4
- Subnetzmaske oder Präfix
```

Merksatz:

```
Subnetz = IP-Adressbereich auf Schicht 3.
```

Netzadresse

Die Netzadresse bezeichnet das Netzwerk selbst.

Beispiel:

```
192.168.10.0/24
```

Netzadresse:

```
192.168.10.0
```

Sie wird normalerweise nicht einem Endgerät zugewiesen.

Merksatz:

```
Netzadresse = Adresse des Netzes.
```

Broadcast-Adresse bei IPv4

Die Broadcast-Adresse ist die letzte Adresse im IPv4-Subnetz.

Beispiel:

```
192.168.10.0/24
```

Broadcast-Adresse:

```
192.168.10.255
```

Sie adressiert alle Geräte im Subnetz.

Merksatz:

```
Broadcast-Adresse = letzte Adresse im IPv4-Subnetz.
```

Hostbereich

Der Hostbereich enthält die nutzbaren Adressen für Geräte.

Beispiel:

```
Netz:
192.168.10.0/24

Netzadresse:
192.168.10.0

Hostbereich:
192.168.10.1 bis 192.168.10.254

Broadcast-Adresse:
192.168.10.255
```

Merksatz:

```
Hostbereich = nutzbare Geräteadressen.
```

Subnetzmaske

Die Subnetzmaske trennt Netzanteil und Hostanteil.

Beispiel:

```
IP-Adresse:
192.168.10.20

Subnetzmaske:
255.255.255.0
```

Das entspricht:

```
/24
```

Merksatz:

```
Subnetzmaske trennt Netz und Host.
```

CIDR

CIDR steht für:

```
Classless Inter-Domain Routing
```

CIDR gibt an, wie viele Bits zum Netzanteil gehören.

Beispiel:

```
192.168.10.20/24
```

Bedeutung:

```
24 Bit Netzanteil
```

Merksatz:

```
CIDR-Präfix = Anzahl der Netz-Bits.
```

Host-Bits und nutzbare Hosts

IPv4 hat insgesamt:

```
32 Bit
```

Host-Bits berechnet man mit:

```
32 minus CIDR-Präfix
```

Beispiel /24:

```
32 - 24 = 8 Host-Bits
```

Alle Adressen:

```
2 hoch 8 = 256
```

Nutzbare Hosts:

```
256 - 2 = 254
```

Merksatz:

```
Nutzbare Hosts = 2 hoch Host-Bits minus 2.
```

Wichtige IPv4-Präfixe

CIDR	Subnetzmaske	alle Adressen	nutzbare Hosts
/24	255.255.255.0	256	254
/25	255.255.255.128	128	126
/26	255.255.255.192	64	62
/27	255.255.255.224	32	30
/28	255.255.255.240	16	14
/29	255.255.255.248	8	6
/30	255.255.255.252	4	2

Merksatz:

```
Je größer die CIDR-Zahl,
desto kleiner das Netz.
```

Schrittweite

Die Schrittweite zeigt, in welchen Abständen neue Subnetze beginnen.

Beispiele:

CIDR	Schrittweite
/25	128
/26	64
/27	32
/28	16
/29	8
/30	4

Schnelle Regel:

```
Schrittweite = 256 minus Maskenwert im interessanten Oktett
```

Merksatz:

```
Schrittweite = Größe des Subnetzes im betroffenen Oktett.
```

Private IPv4-Adressen

Private IPv4-Adressen werden in internen Netzen 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 IPv4-Adressen sind im öffentlichen Internet nicht direkt geroutet.

Merksatz:

```
Private IPv4-Adressen = interne Adressen.
```

Besondere IPv4-Adressen

Adresse / Bereich	Bedeutung

127.0.0.1	Loopback, eigenes Gerät
127.0.0.0/8	Loopback-Bereich
169.254.0.0/16	APIPA, häufig DHCP-Problem
0.0.0.0/0	Default Route
255.255.255.255	lokaler Broadcast
100.64.0.0/10	häufig Carrier-Grade NAT

Merksatz:

```
127.0.0.1 = eigenes Gerät.
169.254.x.x = oft DHCP-Problem.
0.0.0.0/0 = Default Route.
```

Standard-Gateway

Das Standard-Gateway ist der Router für Ziele außerhalb des eigenen Subnetzes.

Beispiel:

```
Client:
192.168.10.20/24

Gateway:
192.168.10.1
```

Wenn das Ziel nicht in 192.168.10.0/24 liegt, sendet der Client an das Gateway.

Merksatz:

```
Standard-Gateway = Ausgang in andere Netze.
```

Gateway muss erreichbar sein

Das Standard-Gateway muss im eigenen lokalen Subnetz liegen.

Falsch:

Client:
192.168.10.20/24

Gateway:
192.168.20.1

Warum falsch?

Das Gateway liegt nicht im Netz 192.168.10.0/24.

Merksatz:

Gateway muss im eigenen Subnetz erreichbar sein.

Gleiches oder anderes Subnetz

Ein Gerät entscheidet:

Ziel im eigenen Subnetz?
Dann direkt lokal senden.

Ziel in anderem Subnetz?
Dann zum Gateway senden.

Beispiel:

192.168.10.20/24 zu 192.168.10.50
= gleiches Subnetz

192.168.10.20/24 zu 192.168.20.50
= anderes Subnetz

Merksatz:

Gleiches Subnetz = direkt.
Anderes Subnetz = Gateway.

Routing

Routing bedeutet:

```
IP-Pakete zwischen Netzwerken weiterleiten.
```

Ein Router prüft die Ziel-IP-Adresse und sucht eine passende Route.

Merksatz:

```
Routing = Wegentscheidung für IP-Pakete.
```

Routing-Tabelle

Eine Routing-Tabelle enthält Wege zu Zielnetzen.

Typische Bestandteile:

```
- Zielnetz
- Präfix
- nächster Hop
- Ausgangsschnittstelle
- Metrik
```

Merksatz:

```
Routing-Tabelle = Wegweiser für IP-Pakete.
```

Direkt verbundene Route

Eine direkt verbundene Route entsteht, wenn ein Router mit einer Schnittstelle direkt in einem Netz hängt.

Beispiel:

```
Router-Interface:
192.168.10.1/24
```

Direkt verbundenes Netz:

```
192.168.10.0/24
```

Merksatz:

```
Direkt verbunden = Netz liegt an eigener Schnittstelle.
```

Statische Route

Eine statische Route wird manuell eingetragen.

Vorteile:

```
- einfach bei kleinen Netzen
- gut kontrollierbar
```

Nachteile:

```
- manuelle Pflege
- keine automatische Anpassung bei Ausfällen
```

Merksatz:

```
Statische Route = manuell eingetragener Weg.
```

Dynamische Route

Dynamische Routen werden automatisch über Routing-Protokolle gelernt.

Beispiele:

```
- RIP
- OSPF
- BGP
```

Merksatz:

```
Dynamische Route = automatisch gelernter Weg.
```

Routing-Protokolle

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

Merksatz:

```
OSPF intern.
BGP im Internet zwischen großen Netzen.
```

Default Route

Die Default Route wird verwendet, wenn keine genauere Route vorhanden ist.

IPv4:

```
0.0.0.0/0
```

Bedeutung:

```
alle IPv4-Ziele
```

Merksatz:

```
Default Route = Route für alles Unbekannte.
```

Longest Prefix Match

Wenn mehrere Routen passen, gewinnt die genaueste Route.

Beispiel:

Route	Präfix
192.168.0.0/16	/16
192.168.10.0/24	/24

Route	Präfix
0.0.0.0/0	/0

Ziel:

```
192.168.10.50
```

Gewählt wird:

```
192.168.10.0/24
```

Merksatz:

```
Genaueste passende Route gewinnt.
```

Nächster Hop

Der nächste Hop ist der nächste Router auf dem Weg zum Ziel.

Beispiel:

```
Zielnetz:
10.10.0.0/16

nächster Hop:
192.168.20.254
```

Merksatz:

```
Nächster Hop = nächster Router.
```

Rückroute

Kommunikation braucht Hinweg und Rückweg.

Wenn der Rückweg fehlt, kommt keine Antwort zurück.

Beispiel:

Netz A erreicht Netz B.

Netz B kennt aber keinen Weg zurück zu Netz A.

Folge:

Verbindung funktioniert nicht.

Merksatz:

Ohne Rückroute keine Antwort.

Asymmetrisches Routing

Asymmetrisches Routing bedeutet:

Hinweg und Rückweg nehmen unterschiedliche Pfade.

Das kann funktionieren, aber bei Firewalls oder NAT problematisch sein.

Warum?

Stateful Firewalls und NAT-Geräte müssen die Verbindung kennen.

Merksatz:

Asymmetrisches Routing kann Firewalls und NAT stören.

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.

Merksatz:

```
TTL verhindert endloses Kreisen von IP-Paketen.
```

ICMP

ICMP steht für:

```
Internet Control Message Protocol
```

ICMP wird für Kontroll- und Fehlermeldungen im IP-Netz verwendet.

Wichtig:

```
ICMP nutzt keine TCP- oder UDP-Ports.
ICMP nutzt Typ und Code.
```

Merksatz:

```
ICMP = Kontrollmeldungen für IP.
```

Ping

Ping nutzt typischerweise ICMP Echo Request und Echo Reply.

Ping prüft:

```
grundlegende IP-Erreichbarkeit
```

Aber Ping beweist nicht:

```
dass ein bestimmter Dienst funktioniert.
```

Merksatz:

```
Ping prüft IP-Erreichbarkeit,
nicht die Anwendung.
```

Traceroute

Traceroute zeigt den Weg zu einem Ziel über mehrere Router.

Je nach System heißt der Befehl:

```
tracert
traceroute
tracepath
```

Traceroute nutzt das TTL-Verhalten von IP-Paketen.

Merksatz:

```
Traceroute zeigt Router-Hops.
```

NAT

NAT steht für:

```
Network Address Translation
```

NAT verändert IP-Adressen beim Übergang zwischen Netzen.

Typischer Einsatz:

```
private IPv4-Adresse
→ öffentliche IPv4-Adresse
```

Merksatz:

```
NAT = IP-Adressen übersetzen.
```

PAT

PAT steht für:

```
Port Address Translation
```

PAT ist eine Form von NAT mit Port-Zuordnung.

Dadurch können viele interne Geräte eine öffentliche IPv4-Adresse gemeinsam nutzen.

Merksatz:

```
PAT = NAT mit Ports.
```

Source NAT und Destination NAT

Art	Bedeutung	typischer Einsatz
Source NAT	Quell-IP wird verändert	internes Gerät ins Internet
Destination NAT	Ziel-IP wird verändert	Portweiterleitung nach innen

Merksatz:

```
Source NAT verändert Quelle.
Destination NAT verändert Ziel.
```

Portweiterleitung

Portweiterleitung bedeutet:

```
Ein externer Port wird an einen internen Dienst weitergeleitet.
```

Beispiel:

```
öffentlich:
93.184.100.10:443

intern:
192.168.10.50:443
```

Merksatz:

```
Portweiterleitung macht interne Dienste von außen erreichbar.
```

CGNAT

CGNAT steht für:

```
Carrier-Grade NAT
```

Dabei macht der Provider NAT.

Mögliche Folge:

```
Der eigene Router hat keine echte öffentliche IPv4-Adresse.
```

Typischer Hinweis:

```
WAN-Adresse am Router liegt im Bereich 100.64.0.0/10
oder unterscheidet sich von der öffentlich angezeigten Adresse.
```

Merksatz:

```
CGNAT erschwert eingehende Verbindungen von außen.
```

IPv6

IPv6 ist ebenfalls Schicht 3.

Eine IPv6-Adresse hat:

```
128 Bit
```

Beispiel:

```
2001:db8::10
```

Merksatz:

IPv6 = 128 Bit.

IPv6-Adressarten

Art	Bereich / Beispiel	Bedeutung
Link-Local	fe80::/10	nur lokaler Link
Global Unicast	2000::/3	weltweit routbar
Unique Local	fc00::/7	interne Nutzung
Multicast	ff00::/8	Gruppe von Empfängern
Loopback	::1	eigenes Gerät
Unspecified	::	keine konkrete Adresse

Merksatz:

fe80 lokal.
2000 global.
fd intern.
ff Multicast.

IPv6-Abkürzungen

Bei IPv6 gilt:

Führende Nullen dürfen weggelassen werden.
Zusammenhängende Nullblöcke dürfen mit :: ersetzt werden.
:: darf nur einmal pro Adresse vorkommen.

Beispiel:

```
2001:0db8:0000:0000:0000:0000:0000:0010
```

wird zu:

```
2001:db8::10
```

Merksatz:

```
:: darf nur einmal vorkommen.
```

IPv6 nutzt kein ARP

IPv4 nutzt ARP.

IPv6 nutzt kein ARP.

IPv6 nutzt stattdessen:

```
NDP
```

NDP steht für:

```
Neighbor Discovery Protocol
```

NDP basiert auf ICMPv6.

Merksatz:

```
IPv6 nutzt NDP statt ARP.
```

ICMPv6

ICMPv6 ist für IPv6 besonders wichtig.

Es wird benötigt für:

```
- Neighbor Discovery
- Router Discovery
- Router Advertisements
- Fehler- und Kontrollmeldungen
```

Wichtig:

```
ICMPv6 nicht pauschal blockieren.
```

Merksatz:

IPv6 braucht ICMPv6 für Grundfunktionen.

SLAAC und DHCPv6

SLAAC steht für:

Stateless Address Autoconfiguration

Der Client bildet seine IPv6-Adresse anhand von Router Advertisements.

DHCPv6 kann zusätzlich oder alternativ Konfigurationsinformationen liefern.

Merksatz:

SLAAC = automatische IPv6-Adresse.
DHCPv6 = IPv6-Konfigurationsdienst.

Dual Stack

Dual Stack bedeutet:

IPv4 und IPv6 laufen gleichzeitig.

Ein Gerät kann dann beide Protokolle nutzen.

Wichtig:

Bei Problemen IPv4 und IPv6 getrennt prüfen.

Merksatz:

Dual Stack = IPv4 und IPv6 gleichzeitig.

DNS bei IPv4 und IPv6

DNS kann IPv4- und IPv6-Adressen liefern.

DNS-Record	Bedeutung

A	Name zu IPv4-Adresse
AAAA	Name zu IPv6-Adresse

Merksatz:

```
A = IPv4.
AAAA = IPv6.
```

Schicht 3 und VLANs

VLANs gehören zu Schicht 2.

IP-Subnetze gehören zu Schicht 3.

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

Beispiel:

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

Merksatz:

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

Inter-VLAN-Routing

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

Dafür nutzt man zum Beispiel:

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

Merksatz:

VLAN zu VLAN braucht Routing.

Schicht-3-Fehlersuche

Typische Prüfpunkte:

- IP-Adresse korrekt?
- Subnetzmaske korrekt?
- Gateway korrekt?
- Gateway erreichbar?
- Routing-Tabelle korrekt?
- Default Route vorhanden?
- Rückroute vorhanden?
- NAT korrekt?
- Firewall-Regel passend?
- IPv4 und IPv6 getrennt geprüft?

Merksatz:

Schicht-3-Fehlersuche = IP, Gateway, Routing und NAT prüfen.

Typische Schicht-3-Fehler

Fehlerbild	mögliche Ursache
keine IP-Adresse	DHCP, VLAN, Link
169.254.x.x	DHCP nicht erreichbar
falsche IP-Adresse	falsches VLAN oder falscher DHCP-Bereich
Gateway nicht erreichbar	falsches Gateway, VLAN, ARP
Internet geht nicht	Gateway, Default Route, NAT, DNS
IP geht, Name nicht	DNS-Problem
Ping geht, Dienst nicht	Schicht 4 oder 7 prüfen
VLAN zu VLAN geht nicht	Inter-VLAN-Routing oder Firewall
extern nicht erreichbar	NAT, Firewall, CGNAT, DNS
IPv6 geht nicht	RA, NDP, ICMPv6, Firewall

Merksatz:

Viele sichtbare IP-Probleme haben Ursachen in Gateway, VLAN, Routing oder DNS.

Was Schicht 3 nicht macht

Schicht 3 macht nicht:

- Ethernet-Frames anhand von MAC-Adressen switchen
- VLAN-Tags setzen
- TCP-Verbindungen aufbauen
- UDP-Ports auswerten
- DNS-Namen auflösen
- Webseiten bereitstellen
- Benutzer authentifizieren
- Zertifikate prüfen

Merksatz:

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

Prüfungswissen: wichtigste Zuordnungen

Begriff	richtige Einordnung
IP-Adresse	Schicht 3
IP-Paket	Schicht 3
Router	Schicht 3
Routing	Schicht 3
Standard-Gateway	Schicht 3
Subnetzmaske	Schicht 3
ICMP	Schicht 3
Ping	Schicht 3
Traceroute	Schicht 3
TTL	Schicht 3
NAT	Schicht 3
PAT	Schicht 3 / 4

Begriff	richtige Einordnung
VLAN	Schicht 2
MAC-Adresse	Schicht 2
TCP-Port	Schicht 4
DNS	Schicht 7

Merksatz:

> IP, Router, Routing, ICMP = Schicht 3.

Typische IHK-Fragen

In AP1 und AP2 kann zum Beispiel gefragt werden:

- Welche Aufgabe hat OSI-Schicht 3?
- Was ist eine IP-Adresse?
- Was ist ein IP-Paket?
- Was ist der Unterschied zwischen MAC und IP?
- Was macht ein Router?
- Was ist ein Standard-Gateway?
- Wann wird ein Gateway benötigt?
- Was ist ein Subnetz?
- Was bedeutet CIDR?
- Wie berechnet man nutzbare Hosts?
- Was ist eine Routing-Tabelle?
- Was ist eine Default Route?
- Was bedeutet Longest Prefix Match?
- Was macht ICMP?
- Warum nutzt ICMP keine Ports?
- Was prüfen Ping und Traceroute?
- Was ist NAT?
- Was ist PAT?
- Was ist der Unterschied zwischen IPv4 und IPv6?
- Warum nutzt IPv6 kein ARP?

Typische Prüfungsfallen

Schicht 3 arbeitet mit IP-Paketen.

Schicht 2 arbeitet mit Frames.

MAC-Adresse gehört zu Schicht 2.

IP-Adresse gehört zu Schicht 3.

Switch = Schicht 2.

Router = Schicht 3.

Gleiches Subnetz = direkt.

Anderes Subnetz = Gateway.

Gateway muss im eigenen Subnetz liegen.

Default Route = 0.0.0.0/0.

Genaueste passende Route gewinnt.

Kommunikation braucht Hinweg und Rückweg.

Ping nutzt ICMP.

ICMP nutzt keine TCP- oder UDP-Ports.

Ping-Erfolg bedeutet nicht,
dass eine Anwendung funktioniert.

NAT ist nicht Routing.

NAT ist nicht Firewall.

PAT nutzt Ports.

IPv4 hat 32 Bit.

IPv6 hat 128 Bit.

IPv6 hat keinen Broadcast.

IPv6 nutzt NDP statt ARP.

ICMPv6 ist für IPv6 wichtig.

VLAN ist nicht Subnetz.

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
Subnetz	logischer IP-Adressbereich
Subnetzmaske	trennt Netzanteil und Hostanteil
CIDR	Schreibweise mit Präfixlänge
Standard-Gateway	Router für Ziele außerhalb des eigenen Subnetzes
Router	Gerät zur Weiterleitung zwischen IP-Netzen
Routing	Weiterleitung von IP-Paketen
Routing-Tabelle	Tabelle mit Wegen zu Zielnetzen
Default Route	Route für unbekannte Ziele
Longest Prefix Match	genaueste passende Route gewinnt
Nächster Hop	nächster Router auf dem Weg
Rückroute	Weg zurück zum Absender
TTL	Lebensdauerbegrenzung von IP-Paketen
ICMP	Kontrollmeldungen für IP
Ping	ICMP-Erreichbarkeitstest
Traceroute	Weganzeige über Router
NAT	Übersetzung von IP-Adressen
PAT	NAT mit Port-Zuordnung

Begriff	Kurze Erklärung
IPv6	Internet Protocol Version 6
NDP	Neighbor Discovery Protocol
SLAAC	automatische IPv6-Adressbildung
Dual Stack	IPv4 und IPv6 gleichzeitig

IHK-sichere Gesamtformulierung

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. Dazu werden IP-Adressen, Subnetzmasken, Standard-Gateways, Routing-Tabellen und Router verwendet. Ein Router 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 wird für Kontroll- und Fehlermeldungen verwendet, NAT übersetzt IP-Adressen und IPv6 erweitert den Adressraum auf 128 Bit.

Wichtigste Merksätze

```
Schicht 3 = Vermittlungsschicht / Netzwerkschicht.

Schicht 3 = IP, Pakete und Routing.

IP-Adresse = logische Adresse.

IP-Paket = Datenform auf Schicht 3.

MAC = lokal.

IP = netzübergreifend.

MAC-Adresse = Schicht 2.

IP-Adresse = Schicht 3.

Switch = Schicht 2.

Router = Schicht 3.

Router entscheidet anhand der Ziel-IP.
```

Routing = Wegentscheidung für IP-Pakete.

Gleiches Subnetz = direkt.

Anderes Subnetz = Gateway.

Gateway muss im eigenen Subnetz liegen.

Subnetzmaske trennt Netz und Host.

CIDR gibt Netz-Bits an.

Host-Bits = 32 minus Präfix.

Nutzbare Hosts = 2 hoch Host-Bits minus 2.

Default Route = 0.0.0.0/0.

Longest Prefix Match = genaueste Route gewinnt.

Kommunikation braucht Hinweg und Rückweg.

TTL verhindert endloses Kreisen von IP-Paketen.

ICMP = Kontrollmeldungen für IP.

ICMP nutzt Typ und Code,
keine Ports.

Ping prüft IP-Erreichbarkeit.

Traceroute zeigt Router-Hops.

NAT übersetzt IP-Adressen.

PAT nutzt zusätzlich Ports.

IPv4 = 32 Bit.

IPv6 = 128 Bit.

IPv6 nutzt NDP statt ARP.

ICMPv6 ist für IPv6 wichtig.

VLAN = Schicht 2.

Subnetz = Schicht 3.

Inter-VLAN-Routing = Schicht 3.

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