2.6 Datenweg durch die Schichten

Beim Senden und Empfangen von Daten arbeiten mehrere Netzwerkschichten zusammen.

Ein einzelner Webseitenaufruf besteht nicht nur aus „Browser fragt Server“. Technisch laufen viele Schritte ab:

- Anwendung erzeugt Daten
- Transportprotokoll bereitet die Übertragung vor
- IP sorgt für Adressierung und Weiterleitung
- Ethernet oder WLAN überträgt im lokalen Netzwerk
- Bits werden über Kabel, Glasfaser oder Funk gesendet
- beim Empfänger wird alles wieder entpackt

Das nennt man auch:

Kapselung beim Sender
Entkapselung beim Empfänger

Grundidee

Beim Sender laufen die Daten im OSI-Modell von oben nach unten.

Beim Empfänger laufen die Daten wieder von unten nach oben.

Vereinfacht:

Sender:
Anwendung → Transport → Vermittlung → Sicherung → Bitübertragung

Empfänger:
Bitübertragung → Sicherung → Vermittlung → Transport → Anwendung

Das bedeutet:

Beim Senden werden Daten verpackt.
Beim Empfangen werden Daten wieder ausgepackt.

Begriff: Datenweg

Der Datenweg beschreibt, welchen Weg Daten durch die einzelnen Schichten nehmen.

Dabei kann man zwei Arten von Wegen unterscheiden:

Begriff	Bedeutung
logischer Datenweg	Kommunikation zwischen den passenden Schichten von Sender und Empfänger
physischer Datenweg	tatsächliche Übertragung über Kabel, Glasfaser oder Funk

Vereinfacht:

```
Logisch spricht Schicht 4 mit Schicht 4.
Physisch laufen die Daten aber durch alle unteren Schichten und über das Medium.
```

Beispiel: Webseite aufrufen

Ein Client ruft eine Webseite auf.

Beispiel:

```
Der Benutzer öffnet im Browser eine Webseite.
```

Dafür arbeiten mehrere Protokolle und Schichten zusammen.

Vereinfacht:

```
Browser
HTTPS
TCP
IP
Ethernet oder WLAN
Bits / Signale
```

Als Schichtenfolge:

Schritt	Schicht	Aufgabe
1	Anwendungsschicht	Browser erzeugt eine Anfrage

Schritt	Schicht	Aufgabe
2	Transportschicht	TCP transportiert die Daten zuverlässig
3	Vermittlungsschicht	IP adressiert das Ziel
4	Sicherungsschicht	Ethernet oder WLAN überträgt lokal
5	Bitübertragungsschicht	Bits werden als Signale übertragen

Schritt 1: Anwendung erzeugt Daten

Der Browser erzeugt eine Anfrage an den Webserver.

Beispiel:

```
Der Browser möchte eine Webseite laden.
```

Auf Anwendungsebene wird dafür ein Anwendungsprotokoll genutzt.

Typische Beispiele:

```
HTTP
HTTPS
DNS
SMTP
IMAP
```

Bei einer Webseite ist es meistens:

```
HTTP oder HTTPS
```

Wichtig:

```
Der Browser ist das Programm.
HTTP oder HTTPS ist das Anwendungsprotokoll.
```

Merksatz:

```
Anwendungsschicht = Netzwerkdienste für Anwendungen
```

Schritt 2: Namensauflösung durch DNS

Bevor der Client eine Webseite aufrufen kann, muss oft zuerst der Name in eine IP-Adresse aufgelöst werden.

Beispiel:

```
www.example.org
```

Der Computer braucht aber eine IP-Adresse, um das Ziel im Netzwerk zu erreichen.

Dafür wird DNS verwendet.

DNS steht für:

```
Domain Name System
```

DNS löst Namen in IP-Adressen auf.

Beispiel:

```
www.example.org → 93.184.216.34
```

Wichtig:

```
DNS ist ein Anwendungsprotokoll,
hat aber einen starken Bezug zur IP-Kommunikation,
weil am Ende eine IP-Adresse benötigt wird.
```

DNS-Anfrage als eigener Datenweg

Auch die DNS-Anfrage läuft durch die Schichten.

Vereinfacht:

```
DNS → UDP → IP → Ethernet/WLAN → Bits
```

Typischer Ablauf:

```
1. Client fragt den DNS-Server nach der IP-Adresse.
2. DNS-Anfrage wird häufig über UDP gesendet.
3. IP adressiert die Anfrage zum DNS-Server.
4. Ethernet oder WLAN überträgt die Daten im lokalen Netzwerk.
5. DNS-Server antwortet mit der passenden IP-Adresse.
```

Merksatz:

```
Vor vielen Verbindungen kommt zuerst die Namensauflösung.
```

Schritt 3: Transportschicht bereitet die Verbindung vor

Wenn die Ziel-IP-Adresse bekannt ist, kann die eigentliche Verbindung zum Webserver vorbereitet werden.

Bei HTTPS wird meistens TCP verwendet.

TCP steht für:

```
Transmission Control Protocol
```

TCP ist verbindungsorientiert und zuverlässig.

Bei TCP wird vor der eigentlichen Nutzdatenübertragung eine Verbindung aufgebaut.

Das nennt man:

```
3-Wege-Handshake
```

Ablauf:

```
Client                    Server

1. SYN  ---------------------->   Verbindungswunsch
2. SYN-ACK <------------------   Bestätigung + eigene Start-Sequenznummer
3. ACK  ---------------------->   Bestätigung

Danach ist die TCP-Verbindung aufgebaut.
```

Wichtig:

> Erst nach dem TCP-Verbindungsaufbau werden die eigentlichen Nutzdaten übertragen.

Merksatz:

> TCP = erst Verbindung aufbauen, dann Nutzdaten senden

Schritt 4: Ports bestimmen den Dienst

Auf Schicht 4 werden Ports verwendet.

Ein Port zeigt, welcher Dienst oder welche Anwendung auf einem Host gemeint ist.

Beispiel:

> Ziel-IP-Adresse: 93.184.216.34
> Ziel-Port: 443

Bedeutung:

> Sende die Daten an den Host 93.184.216.34
> und dort an den Dienst HTTPS auf Port 443.

Typische Ports:

Port	Protokoll / Dienst
80	HTTP
443	HTTPS
53	DNS
22	SSH
25	SMTP
110	POP3
143	IMAP

Merksatz:

```
IP-Adresse = welcher Host?
Port = welcher Dienst?
```

Schritt 5: IP adressiert das Ziel

Auf Schicht 3 wird IP verwendet.

IP steht für:

```
Internet Protocol
```

IP sorgt für die logische Adressierung und Weiterleitung von Paketen.

Ein IP-Paket enthält unter anderem:

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

Beispiel:

```
Quell-IP-Adresse: 192.168.1.20
Ziel-IP-Adresse: 93.184.216.34
```

Die IP-Adresse sagt:

```
Von welchem Host kommt das Paket?
Zu welchem Host soll das Paket?
```

Merksatz:

```
IP-Adresse = logische Adresse für Netzwerkkommunikation
```

Schritt 6: Routing entscheidet den Weg

Wenn Ziel und Quelle nicht im selben lokalen Netzwerk liegen, muss ein Router das Paket weiterleiten.

Routing bedeutet:

```
Weiterleitung von Paketen zwischen Netzwerken
```

Ein Router betrachtet die Ziel-IP-Adresse und entscheidet, wohin das Paket als Nächstes gesendet wird.

Beispiel:

```
Client → Standard-Gateway → Internet → Zielserver
```

Das Standard-Gateway ist meistens der Router im lokalen Netzwerk.

Merksatz:

```
Router verbinden Netzwerke.
Switches verbinden Geräte im lokalen Netzwerk.
```

Schritt 7: Ethernet oder WLAN überträgt lokal

Auf Schicht 2 wird das IP-Paket in einen Frame verpackt.

Bei kabelgebundenem LAN ist das häufig ein Ethernet-Frame.

Ein Ethernet-Frame enthält unter anderem:

```
- Ziel-MAC-Adresse
- Quell-MAC-Adresse
- Typfeld
- Nutzdaten
- FCS-Prüfsumme
```

Die MAC-Adresse wird für die lokale Zustellung im aktuellen Netzwerkabschnitt verwendet.

Wichtig:

```
MAC-Adressen gelten nur im lokalen Netzwerkabschnitt.
IP-Adressen sind für die logische Kommunikation über Netzwerke hinweg wichtig.
```

Merksatz:

```
MAC-Adresse = lokale Zustellung im LAN
```

Schritt 8: ARP findet die passende MAC-Adresse

Wenn ein Gerät eine IP-Adresse im lokalen Netzwerk erreichen möchte, braucht es die passende MAC-Adresse.

Dafür wird bei IPv4 ARP verwendet.

ARP steht für:

```
Address Resolution Protocol
```

ARP fragt sinngemäß:

```
Wer hat diese IP-Adresse?
Ich brauche die passende MAC-Adresse.
```

Beispiel:

```
Wer hat 192.168.1.1?
Antwort: 192.168.1.1 hat die MAC-Adresse aa:bb:cc:dd:ee:ff
```

Wichtig:

```
ARP löst IPv4-Adressen zu MAC-Adressen auf.
ARP ist für die lokale Kommunikation im LAN wichtig.
```

Merksatz:

```
ARP verbindet IP-Adresse und MAC-Adresse im lokalen Netzwerk.
```

Schritt 9: Schicht 1 überträgt Bits

Auf Schicht 1 werden die Daten als Bits übertragen.

Ein Bit kann zwei Zustände haben:

```
0
1
```

Je nach Übertragungsmedium werden diese Bits übertragen als:

```
- elektrische Signale über Kupferkabel
- Lichtsignale über Glasfaser
- Funksignale über WLAN
```

Wichtig:

```
Schicht 1 interessiert sich nicht für IP-Adressen, Ports oder Anwendungen.
Schicht 1 überträgt nur Bits als Signale.
```

Merksatz:

```
Schicht 1 = Bits und Signale
```

Der Datenweg beim Sender

Beim Sender werden die Daten schrittweise verpackt.

Vereinfacht:

```
Anwendung:
HTTPS-Daten

Transportschicht:
TCP-Header + HTTPS-Daten

Vermittlungsschicht:
IP-Header + TCP-Header + HTTPS-Daten

Sicherungsschicht:
Ethernet-Header + IP-Header + TCP-Header + HTTPS-Daten + Ethernet-Trailer

Bitübertragungsschicht:
Bits werden als Signale übertragen
```

Fachbegriffe:

Schicht	Ergebnis
Anwendungsschicht	Daten
Transportschicht	TCP-Segment
Vermittlungsschicht	IP-Paket
Sicherungsschicht	Ethernet-Frame
Bitübertragungsschicht	Bits

Der Datenweg beim Empfänger

Beim Empfänger passiert der Vorgang umgekehrt.

Die Daten werden Schicht für Schicht entpackt.

Vereinfacht:

```
Schicht 1:
Signale werden als Bits empfangen.

Schicht 2:
Ethernet-Frame wird geprüft.
Ethernet-Header und Trailer werden ausgewertet.

Schicht 3:
IP-Paket wird ausgewertet.
Ziel-IP-Adresse wird geprüft.

Schicht 4:
TCP-Segment wird ausgewertet.
Port und Sequenzinformationen werden geprüft.

Schicht 7:
Die Anwendung erhält die Nutzdaten.
```

Das nennt man:

```
Entkapselung
```

Merksatz:

```
Sender kapselt ein.
Empfänger kapselt aus.
```

Beispiel mit TCP/IP-Modell

Im TCP/IP-Modell sieht der gleiche Ablauf kompakter aus.

Beispiel HTTPS:

TCP/IP-Schicht	Beispiel
Anwendungsschicht	HTTPS
Transportschicht	TCP
Internetschicht	IP
Netzzugangsschicht	Ethernet oder WLAN

Vereinfacht:

```
HTTPS → TCP → IP → Ethernet/WLAN
```

Oder allgemein:

```
Anwendung → Transport → Internet → Netzzugang
```

Beispiel mit DNS

Eine DNS-Anfrage hat einen ähnlichen Weg, nutzt aber häufig UDP statt TCP.

Vereinfacht:

```
DNS → UDP → IP → Ethernet/WLAN
```

Schichtbezug:

Bestandteil	Schicht
DNS	OSI-Schicht 7
UDP	OSI-Schicht 4

Bestandteil	Schicht
IP	OSI-Schicht 3
Ethernet/WLAN	OSI-Schicht 1/2

Wichtig:

DNS ist ein Anwendungsprotokoll.
UDP ist das Transportprotokoll.
IP sorgt für Adressierung und Routing.
Ethernet oder WLAN sorgt für lokale Übertragung.

Beispiel mit Ping

Ping nutzt klassisch ICMP.

ICMP steht für:

Internet Control Message Protocol

Ping verwendet normalerweise:

ICMP Echo Request
ICMP Echo Reply

Schichtbezug:

Bestandteil	Schicht
ICMP	OSI-Schicht 3
IP	OSI-Schicht 3
Ethernet/WLAN	OSI-Schicht 1/2

Wichtig:

ICMP nutzt keine Ports.
ICMP gehört nicht zu TCP oder UDP.
ICMP verwendet Typen und Codes.

Merksatz:

Ping prüft Erreichbarkeit.

ICMP meldet, prüft und diagnostiziert.

Was passiert beim Weg über einen Router?

Wenn ein Paket über einen Router weitergeleitet wird, ändert sich der Ethernet-Frame.

Wichtig:

Das IP-Paket bleibt grundsätzlich erhalten.

Der Ethernet-Frame wird pro Netzwerkabschnitt neu erstellt.

Beispiel:

PC → Router:

Ethernet-Frame mit Ziel-MAC des Routers

Router → nächster Router:

neuer Ethernet-Frame mit neuer Ziel-MAC

letzter Router → Server:

Ethernet-Frame mit Ziel-MAC des Servers

Das bedeutet:

MAC-Adressen ändern sich pro Netzwerkabschnitt.

IP-Adressen bleiben für die Ende-zu-Ende-Kommunikation wichtig.

Merksatz:

MAC-Adresse = nächster lokaler Schritt

IP-Adresse = logisches Ziel über Netzwerke hinweg

Was bleibt gleich und was ändert sich?

Information	Bleibt auf dem Weg grundsätzlich gleich?	Erklärung

Ziel-IP-Adresse	ja	Zielhost bleibt derselbe
Quell-IP-Adresse	meistens ja	außer bei NAT/PAT
Ziel-Port	ja	Dienst bleibt derselbe
Quell-Port	ja	Client-Verbindung bleibt zuordenbar
Ziel-MAC-Adresse	nein	ändert sich je Netzwerkabschnitt
Quell-MAC-Adresse	nein	ändert sich je Netzwerkabschnitt

Wichtig:

NAT/PAT kann IP-Adressen und Ports verändern.
Ohne NAT bleiben Quell- und Ziel-IP grundsätzlich erhalten.

NAT/PAT als Sonderfall

Bei NAT/PAT kann sich die Quell-IP-Adresse verändern.

NAT steht für:

Network Address Translation

PAT steht für:

Port Address Translation

Typischer Fall:

Ein interner Client nutzt eine private IP-Adresse.
Der Router ersetzt diese private Quell-IP durch seine öffentliche IP-Adresse.

Beispiel:

intern:
192.168.1.20:51544

extern:
84.10.20.30:40001

Dadurch können mehrere interne Geräte über eine gemeinsame öffentliche IP-Adresse ins Internet.

Merksatz:

```
NAT/PAT verändert Adressen oder Ports an der Router-/Firewall-Grenze.
```

Datenweg und Firewall

Eine Firewall kann den Datenweg kontrollieren.

Sie kann zum Beispiel prüfen:

```
- Quell-IP-Adresse
- Ziel-IP-Adresse
- Quell-Port
- Ziel-Port
- Protokoll
- Verbindungszustand
- teilweise auch Anwendungsdaten
```

Beispiel:

```
Port 443 erlaubt
Port 22 blockiert
```

Wichtig:

```
Eine Firewall kann je nach Art auf mehreren OSI-Schichten arbeiten.
```

Merksatz:

```
Firewall = kontrolliert erlaubte und verbotene Kommunikation
```

Warum ist der Datenweg für die Fehlersuche wichtig?

Wenn man den Datenweg versteht, kann man Netzwerkfehler systematisch eingrenzen.

Man prüft am besten von unten nach oben.

Beispiel:

1. Gibt es eine physische Verbindung?
2. Funktioniert die lokale Verbindung?
3. Stimmt die IP-Konfiguration?
4. Ist das Gateway erreichbar?
5. Funktioniert DNS?
6. Ist der Zielhost erreichbar?
7. Ist der Zielport erreichbar?
8. Antwortet die Anwendung?

Das nennt man häufig:

schichtweise Fehlersuche

Beispielhafte Fehlersuche nach Schichten

Fehlerbild	mögliche Schicht	Beispiel
kein Link-Licht	Schicht 1	Kabel, Port, Netzwerkkarte
falsches VLAN	Schicht 2	Client im falschen Netz
falsche IP-Adresse	Schicht 3	kein Routing möglich
falsches Gateway	Schicht 3	Internet nicht erreichbar
DNS funktioniert nicht	Schicht 7 mit Schicht-3-Bezug	Name wird nicht aufgelöst
Port blockiert	Schicht 4 / Firewall	Dienst nicht erreichbar
Webserver antwortet nicht	Schicht 7	Anwendung oder Dienstproblem

Wichtig:

Ein Fehler auf einer unteren Schicht kann alle höheren Schichten beeinflussen.

Beispiel:

Wenn das Kabel defekt ist,
funktionieren IP, TCP, DNS und HTTP ebenfalls nicht.

Typischer Ablauf: Webseite funktioniert nicht

Wenn eine Webseite nicht funktioniert, kann man prüfen:

```
1. Link vorhanden?
2. IP-Adresse vorhanden?
3. Standard-Gateway vorhanden?
4. DNS-Auflösung möglich?
5. Ziel-IP erreichbar?
6. Zielport erreichbar?
7. Webserver antwortet?
```

Beispiele für Werkzeuge:

Prüfung	Werkzeug
IP-Konfiguration	ipconfig, ip addr
Erreichbarkeit	ping
Weg zum Ziel	tracert, traceroute
DNS-Auflösung	nslookup, dig
Port erreichbar	Test-NetConnection, nc
Paketanalyse	Wireshark, tcpdump

Begriff: Standard-Gateway

Das Standard-Gateway ist der Router, an den ein Host Pakete sendet, wenn das Ziel nicht im eigenen lokalen Netzwerk liegt.

Beispiel:

```
Client: 192.168.1.20
Gateway: 192.168.1.1
```

Wenn der Client eine externe IP-Adresse erreichen möchte, sendet er das Paket an das Standard-Gateway.

Merksatz:

```
Standard-Gateway = Ausgang aus dem eigenen Netzwerk
```

Begriff: Ende-zu-Ende-Kommunikation

Ende-zu-Ende-Kommunikation beschreibt die logische Kommunikation zwischen Sender und Empfänger.

Beispiel:

```
Client-Anwendung ↔ Server-Anwendung
```

Bei TCP bedeutet das:

```
Die TCP-Verbindung besteht logisch zwischen Client und Server.
```

Dazwischen können aber mehrere Router liegen.

Merksatz:

```
Ende-zu-Ende = vom ursprünglichen Sender bis zum endgültigen Empfänger
```

Begriff: Hop

Ein Hop ist ein Zwischenschritt auf dem Weg durch ein Netzwerk.

Meist ist damit ein Router gemeint.

Beispiel:

```
Client → Router 1 → Router 2 → Zielserver
```

Hier gibt es mehrere Hops.

Traceroute zeigt solche Zwischenschritte an.

Merksatz:

```
Hop = ein Netzwerksprung über ein Zwischengerät
```

Typische Prüfungsfragen

In AP1 oder AP2 kann zum Beispiel gefragt werden:

- Beschreiben Sie den Weg eines Datenpakets durch die Schichten.
- Welche Schicht fügt welche Informationen hinzu?
- Was passiert beim Empfänger?
- Was ist Kapselung?
- Was ist Entkapselung?
- Welche Dateneinheit gehört zu welcher Schicht?
- Warum ändert sich die MAC-Adresse auf dem Weg?
- Warum bleibt die IP-Adresse grundsätzlich erhalten?
- Welche Rolle spielt das Standard-Gateway?
- Auf welcher Schicht liegt ein bestimmter Fehler?

Typische Prüfungsfallen

Ein Switch leitet normalerweise anhand von MAC-Adressen weiter.
Das ist Schicht 2.

Ein Router leitet anhand von IP-Adressen weiter.
Das ist Schicht 3.

TCP und UDP nutzen Ports.
Das ist Schicht 4.

ICMP nutzt keine Ports.
ICMP gehört in den IP-/Netzwerkbereich.

DNS ist ein Anwendungsprotokoll,
auch wenn es für IP-Adressen wichtig ist.

Die MAC-Adresse gilt nur im lokalen Netzwerkabschnitt.

Die IP-Adresse beschreibt das logische Ziel.

Ein Port beschreibt den Dienst auf einem Host.

NAT/PAT kann IP-Adressen und Ports verändern.

Wichtige Begriffe kurz erklärt

Begriff	Kurze Erklärung
Datenweg	Weg der Daten durch Schichten und Netzwerkgeräte
Kapselung	Daten werden beim Senden Schicht für Schicht verpackt
Entkapselung	Daten werden beim Empfangen Schicht für Schicht ausgepackt
Nutzdaten	eigentlicher Inhalt der Anwendung
Header	Steuerinformationen vor den Nutzdaten
Frame	Dateneinheit auf Schicht 2
Paket	Dateneinheit auf Schicht 3
Segment	TCP-Dateneinheit auf Schicht 4
Datagramm	UDP-Dateneinheit auf Schicht 4
MAC-Adresse	lokale Hardwareadresse im LAN
IP-Adresse	logische Adresse für Netzwerkkommunikation
Port	Dienstadresse auf einem Host
Router	Gerät zur Verbindung verschiedener Netzwerke
Switch	Gerät zur Weiterleitung im lokalen Netzwerk anhand von MAC-Adressen
Standard-Gateway	Router für Ziele außerhalb des eigenen Netzes
Hop	Zwischenschritt über ein Netzwerkgerät
Routing	Weiterleitung von Paketen zwischen Netzwerken
ARP	Auflösung von IPv4-Adresse zu MAC-Adresse
DNS	Namensauflösung von Namen zu IP-Adressen

IHK-sichere Kurzformulierung

Beim Senden von Daten werden die Nutzdaten durch die Schichten eines Netzwerkmodells verarbeitet und jeweils um Steuerinformationen ergänzt. Dieser Vorgang heißt Kapselung. Auf der Transportschicht entstehen zum Beispiel TCP-Segmente oder UDP-Datagramme, auf der Vermittlungsschicht IP-Pakete und auf der Sicherungsschicht Ethernet-Frames. Auf der Bitübertragungsschicht werden die Daten als Bits über ein Medium übertragen. Beim Empfänger werden die Informationen in umgekehrter Reihenfolge ausgewertet und entfernt. Dieser Vorgang heißt Entkapselung.

Merksätze

Sender kapselt ein.
Empfänger kapselt aus.

Anwendung erzeugt Daten.

TCP oder UDP transportiert zwischen Anwendungen.

IP adressiert und routet zwischen Netzwerken.

Ethernet oder WLAN überträgt im lokalen Netzwerk.

Schicht 1 überträgt Bits als Signale.

Port = welcher Dienst?

IP-Adresse = welcher Host oder welches Netz?

MAC-Adresse = welches Gerät im lokalen Netzwerkabschnitt?

Switch = Schicht 2

Router = Schicht 3

TCP und UDP = Schicht 4

ICMP = Schicht 3

DNS = Anwendungsschicht mit starkem IP-Bezug

MAC-Adressen können sich auf dem Weg ändern.

IP-Adressen bleiben grundsätzlich für die Ende-zu-Ende-Kommunikation erhalten.

NAT/PAT ist ein Sonderfall,
weil dabei IP-Adressen oder Ports verändert werden können.

Bei der Fehlersuche zuerst die unteren Schichten prüfen.