Netzwerktechnik 1/2

Access Point

Ein Access Point (WLAN-Zugangspunkt) ist ein Gerät, das ein kabelloses Netzwerk bereitstellt. Er wird meist über ein Netzwerkkabel mit einem Router oder Switch verbunden und fungiert als Brücke zwischen drahtlosen Endgeräten (wie Laptops, Smartphones) und einem kabelgebundenen Netzwerk. Moderne Access Points unterstützen mehrere Frequenzbänder (2,4 GHz und 5 GHz), bieten Verschlüsselungsmethoden wie WPA3 und ermöglichen Roaming-Funktionen in großen Netzwerken.

Router

Ein Router ist ein intelligentes Netzwerkgerät, das Datenpakete zwischen verschiedenen Netzwerken weiterleitet. In einem Heimnetzwerk verbindet er interne Geräte mit dem Internet, vergibt IP-Adressen über DHCP, übernimmt NAT (Network Address Translation) und schützt durch integrierte Firewalls. Einige Router beinhalten WLAN-Funktionen, USB-Anschlüsse für Drucker oder Massenspeicher und Quality-of-Service-Regeln (QoS).

Hub

Ein Hub ist ein passives, veraltetes Netzwerkgerät, das alle eingehenden Signale an sämtliche Ports weiterleitet. Dadurch entstehen viele Datenkollisionen im Netzwerk. Er arbeitet auf OSI-Schicht 1 (Bitübertragungsschicht), kennt keine MAC-Adressen und unterscheidet nicht zwischen den angeschlossenen Geräten. Hubs wurden in modernen Netzwerken fast vollständig durch Switches ersetzt.

Switch

Ein Switch ist ein aktives Netzwerkgerät auf OSI-Schicht 2 (Sicherungsschicht), das Daten gezielt basierend auf MAC-Adressen an das richtige Zielgerät weiterleitet. Ein Switch lernt mit der Zeit, an welchem Port sich welches Gerät befindet, und speichert dies in einer MAC-Adresstabelle. Dadurch wird der Netzwerkverkehr effizient und kollisionsfrei.

Repeater

Ein Repeater verlängert die Reichweite eines Netzwerks, indem er empfangene Signale aufbereitet und erneut aussendet. In WLANs wird er eingesetzt, um Funklöcher zu überbrücken. In kabelgebundenen Netzwerken (z. B. bei langen Ethernet-Strecken) kann er ebenfalls zur Verstärkung verwendet werden. Repeater arbeiten auf OSI-Schicht 1.

Patch-Panel

Ein Patch-Panel ist eine passive Netzwerkkomponente, in der viele Netzwerkleitungen zentral zusammenlaufen. Es ermöglicht durch Patchkabel eine flexible Zuordnung der Netzwerkanschlüsse in Gebäuden. Es dient der strukturierten Verkabelung und wird meist in Netzwerkschränken installiert.

TP (Twisted Pair)

Twisted-Pair-Kabel bestehen aus paarweise verdrillten Kupferadern. Die Verdrillung verringert elektromagnetische Störungen. Es gibt ungeschirmte (UTP) und geschirmte Varianten (STP, FTP). TP-Kabel gibt es in verschiedenen Kategorien (Cat 5e, Cat 6, Cat 7, Cat 8), die unterschiedliche Übertragungsraten und Frequenzbereiche unterstützen.

Modem

Ein Modem (Modulator-Demodulator) wandelt digitale Signale eines Computers in analoge Signale für die Übertragung über Telefonleitungen und umgekehrt. Moderne Modems (z. B. DSL-, Kabel- oder LTE-Modems) werden oft mit einem Router kombiniert. Sie bilden die Schnittstelle zwischen Providerleitung und Heimnetzwerk.

WLAN Sicherheit

- **MAC-Filterung**: Erlaubt nur bestimmten Geräten den Netzwerkzugang anhand ihrer MAC-Adresse. Kann leicht umgangen werden.
- **IEEE 802.1X**: Netzwerkzugriffskontrolle über Authentifizierungsserver (meist RADIUS). Wird in Firmen- und Bildungseinrichtungen verwendet.
- **WEP**: Veraltete und unsichere Verschlüsselung. Leicht zu knacken.
- **WPA/WPA2 (802.11i)**: Bessere Sicherheit durch TKIP bzw. AES-Verschlüsselung.
- **WPS**: Erlaubt einfachen Netzwerkzugang durch Knopfdruck oder PIN. Unsicher wegen möglicher Brute-Force-Angriffe.
- **WPA3**: Aktuellster WLAN-Verschlüsselungsstandard mit verbesserter Sicherheit, auch für öffentliche Netzwerke (SAE-Verfahren).

NIC: Aufbau, Funktion

Die Netzwerkkarte (NIC – Network Interface Card) stellt die physische Verbindung zwischen Computer und Netzwerk her. Sie besteht aus:

- einem Controller zur Verarbeitung der Netzwerkdaten
- einem PHY-Transceiver (Physical Layer)
- einer eindeutigen MAC-Adresse Netzwerkkarten gibt es als interne Steckkarten (PCIe) oder extern via USB. Moderne NICs unterstützen Geschwindigkeiten von 1 Gbit/s bis 10 Gbit/s und mehr.

Netzwerktopologien

Ring-Topologie

In einem Ringnetzwerk ist jedes Gerät mit zwei Nachbarn verbunden, sodass ein geschlossener Kreis entsteht. Die Daten werden von einem Gerät zum nächsten weitergeleitet, bis sie ihr Ziel erreichen. Vorteile: einfache Verkabelung, keine Kollisionen. Nachteil: Fällt ein Gerät oder eine Verbindung aus, bricht das ganze Netzwerk zusammen.

Vermaschte Topologie

In einer vermaschten Struktur sind die Geräte teilweise oder vollständig direkt miteinander verbunden. Dies erhöht die Redundanz und Ausfallsicherheit, da alternative Wege für die Datenübertragung zur Verfügung stehen. Häufig in Backbone-Netzen oder bei sicherheitskritischen Anwendungen.

Vollvermaschte Topologie

Jedes Gerät ist direkt mit jedem anderen verbunden. Dadurch entsteht maximale Redundanz und minimale Latenz, jedoch mit sehr hohem Verkabelungsaufwand und steigenden Kosten bei zunehmender Anzahl von Geräten.

Stern-Topologie

Alle Geräte sind sternförmig mit einem zentralen Punkt (z. B. einem Switch) verbunden. Die am häufigsten verwendete Topologie in heutigen Netzwerken. Sie ist einfach zu verwalten, erlaubt einfache Fehlerdiagnose und reduziert Kollisionen. Der Ausfall der Zentraleinheit führt jedoch zum Ausfall des gesamten Netzwerks.

Linien-Topologie

Geräte sind linear miteinander verbunden. Einfach in der Umsetzung, jedoch anfällig für Ausfälle: Wenn ein Gerät in der Mitte ausfällt, sind alle nachfolgenden Geräte ebenfalls vom Netz getrennt.

Baum-Topologie

Eine Kombination aus Stern- und Linien-Topologie mit hierarchischem Aufbau. Sie wird oft in großen Gebäuden oder Organisationen verwendet, da sie eine logische Segmentierung erlaubt. Der Ausfall eines Hauptzweigs kann jedoch viele Geräte betreffen.

Bus-Topologie

Alle Geräte sind über ein gemeinsames Übertragungsmedium verbunden. Diese Struktur war früher sehr verbreitet (z. B. mit Koaxialkabeln), ist jedoch heute kaum noch im Einsatz. Sie ist kostengünstig, jedoch störanfällig und schwer skalierbar.

Medien für die Datenübertragung

Koaxialkabel

Koaxialkabel bestehen aus einem Innenleiter, einem Isolator, einer metallischen Abschirmung und einer äußeren Kunststoffhülle. Der Innenleiter überträgt das Signal, während die Abschirmung äußere Störungen minimiert. Sie wurden früher in Computernetzwerken (10Base2, 10Base5) eingesetzt, heute vor allem für Fernsehsignale und Kabelanschlüsse. Vorteile: hohe Störsicherheit und robuste Bauweise. Nachteile: relativ unflexibel und nicht mehr zeitgemäß für moderne Netzwerke.

Twisted-Pair-Kabel (TP)

Twisted-Pair-Kabel sind die am weitesten verbreiteten Netzwerkkabel. Sie bestehen aus paarweise verdrillten Kupferadern, was Störungen durch elektromagnetische Einflüsse reduziert. Es gibt verschiedene Kategorien:

- **Cat 5e**: bis 1 Gbit/s
- **Cat 6**: bis 10 Gbit/s (über kurze Strecken)
- **Cat 7/Cat 8**: bis 40 Gbit/s (spezielle Abschirmung und Stecker erforderlich) Twisted-Pair-Kabel eignen sich für strukturierte Gebäudeverkabelung und sind flexibel, günstig und leicht zu verlegen.

Kabellose Systeme

Datenübertragung ohne physisches Kabel erfolgt z. B. über:

- **WLAN (Wi-Fi)**: Funknetzwerk im 2,4- und 5-GHz-Band, teilweise auch 6 GHz (Wi-Fi 6E)
- **Bluetooth**: Kurzstreckenfunk für Gerätekommunikation
- **Mobilfunk (LTE, 5G)**: Weitreichende Datenübertragung über Mobilfunknetze Kabellose Systeme bieten hohe Flexibilität, jedoch geringere Sicherheit und potenzielle Störanfälligkeit gegenüber Kabelverbindungen.

Glasfaser / FTTH (Fiber To The Home)

Glasfaserkabel übertragen Daten als Lichtsignale durch sehr dünne Glasstränge. Sie ermöglichen extrem hohe Übertragungsraten (bis mehrere 100 Gbit/s) über große Entfernungen ohne Qualitätsverlust. FTTH beschreibt eine Glasfaseranbindung direkt bis in die Wohnung oder das Gebäude des Endnutzers. Vorteile: hohe Geschwindigkeit, keine elektromagnetischen Störungen. Nachteil: hohe Installationskosten.

Kunststofffaser

PNA (Polymer Optical Fiber) ist eine günstigere Alternative zu Glasfaser. Sie besteht aus Kunststoff statt Glas und ist einfacher zu verlegen. Allerdings hat sie eine deutlich geringere Reichweite und Bandbreite, daher eher für kurze Verbindungen innerhalb eines Raumes geeignet.

Aufbau LWL (Lichtwellenleiter)

Ein LWL-Kabel besteht typischerweise aus:

- **Kern** (Core): Führt das Lichtsignal, besteht aus Glas oder Kunststoff
- **Mantel** (Cladding): Umgibt den Kern, sorgt für Totalreflexion
- **Schutzschicht**: Mechanischer Schutz gegen äußere Einflüsse LWLs benötigen spezielle Stecker und eine präzise Verarbeitung.

Signalübertragung im LWL

Lichtimpulse werden durch Laser- oder LED-Lichtquellen erzeugt. Das Licht wird im Kern durch Totalreflexion fortgeleitet. Die Modulation erfolgt digital – Licht an bedeutet 1, Licht aus bedeutet 0. Die Übertragung ist extrem schnell und störungsfrei.

Monomode- / Singlemodefaser

Diese Glasfaser hat einen sehr kleinen Kerndurchmesser (ca. 9 µm), wodurch das Licht nur auf einem Pfad läuft. Sie eignet sich für sehr große Entfernungen (z. B. 100 km und mehr), benötigt aber teurere Laserlichtquellen.

Multimodefaser (MM)

Multimodefasern haben einen größeren Kern (50–62,5 µm), in dem Licht in mehreren Modi gleichzeitig reflektiert wird. Sie sind günstiger, aber anfälliger für Laufzeitunterschiede (Modal Dispersion). Einsatzbereich: kurze bis mittlere Distanzen (z. B. innerhalb von Rechenzentren).

FTTH

FTTH (Fiber To The Home) bezeichnet eine Glasfaserverkabelung, die direkt bis in die Wohnung oder das Gebäude des Endnutzers reicht. Dadurch entfallen verlustreiche Kupferverbindungen. Ergebnis: konstant hohe Bandbreiten, ideal für moderne Anwendungen wie 4K-Streaming, Cloud-Dienste und Home-Office.

Strukturierte Verkabelung

Die strukturierte Verkabelung ist ein standardisiertes System zur physischen Verbindung von Netzwerkkomponenten in Gebäuden. Sie folgt einem hierarchischen Aufbau und besteht aus drei Hauptbereichen, die jeweils spezifische Aufgaben erfüllen:

Primärverkabelung

Die Primärverkabelung verbindet verschiedene Gebäude eines Campus oder Standorts miteinander. Sie ist für die Kommunikation auf dem Gelände zuständig und nutzt in der Regel Glasfaserkabel, da sie große Distanzen überbrücken muss. Diese Verkabelung erfolgt oft unterirdisch oder in Kabelkanälen zwischen Gebäuden.

- **Verbindungsebene**: Gebäudeverteiler zu Gebäudeverteiler
- **Typische Medien**: Singlemode-Glasfaser
- **Merkmale**: Hohe Reichweite, geringe Dämpfung, zukunftssicher

Sekundärverkabelung

Die Sekundärverkabelung verbindet die Etagenverteiler (Stockwerksverteiler) mit dem Gebäudeverteiler. Sie sorgt für die vertikale Kommunikation innerhalb eines Gebäudes, also zwischen den einzelnen Stockwerken.

- **Verbindungsebene**: Gebäudeverteiler zu Etagenverteilern

- **Typische Medien**: Glasfaser oder Twisted-Pair (bei kurzen Strecken)
- **Merkmale**: Mittlere Reichweite, zentral verwaltbar

Tertiärverkabelung

Die Tertiärverkabelung (auch Etagen- oder Horizontalverkabelung genannt) verbindet die Netzwerkanschlussdosen in den Räumen mit dem Etagenverteiler. Sie ist die am häufigsten eingesetzte Form, da sie den direkten Arbeitsplatzanschluss herstellt.

- **Verbindungsebene**: Etagenverteiler zu Anschlussdosen
- **Typische Medien**: Twisted-Pair-Kabel (Cat 5e, Cat 6, Cat 7)
- **Merkmale**: Kurze Strecken, flexible Endgeräte-Anbindung

Vorteile der strukturierten Verkabelung

- Einheitliches, standardisiertes System
- Skalierbarkeit für zukünftige Erweiterungen
- Erleichterte Wartung und Fehlersuche
- Unterstützung verschiedener Netzwerkprotokolle
- Saubere und nachvollziehbare Verkabelung

Komponenten einer strukturierten Verkabelung

- **Patchpanel**: Zentrale Aufnahmepunkte für Kabel
- **Racks / Netzwerkschränke**: Gehäuse für aktive/passive Komponenten
- **Patchkabel**: Flexible Verbindungskabel zwischen Patchpanel und Switch
- **Datendosen / RJ45-Anschlüsse**: Netzwerkzugangspunkte im Raum

Die strukturierte Verkabelung ist die Grundlage für leistungsfähige IT-Infrastrukturen in Unternehmen, öffentlichen Einrichtungen und modernen Gebäuden.

Zugriffsverfahren / Zugangsverfahren

Zugriffsverfahren regeln, wie mehrere Teilnehmer auf ein gemeinsames Übertragungsmedium zugreifen dürfen, ohne dass es zu Datenkollisionen kommt. Zwei bedeutende Verfahren sind CSMA/CD und CSMA/CA.

CSMA/CD (Carrier Sense Multiple Access with Collision Detection)

Dieses Verfahren wird im klassischen Ethernet (10Base-T, 100Base-TX) mit Halbduplex verwendet. Geräte "lauschen" zunächst auf dem Medium:

- Ist das Medium frei, darf gesendet werden.
- Tritt eine Kollision auf, erkennen dies die Geräte, brechen die Übertragung ab und senden nach einer zufällig gewählten Wartezeit erneut.

Eigenschaften:

- Arbeitet auf OSI-Schicht 2 (Sicherungsschicht)
- Wird durch Switches und Vollduplex weitgehend ersetzt
- Effizienz nimmt bei hoher Netzlast stark ab

CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance)

Dieses Verfahren kommt bei drahtlosen Netzwerken (z. B. WLAN) zum Einsatz. Kollisionen können hier nicht direkt erkannt werden, da Geräte nicht gleichzeitig senden und empfangen können.

- Vor dem Senden wird überprüft, ob das Medium frei ist
- Zusätzlich wird durch Steuerpakete (RTS/CTS) versucht, Kollisionen zu vermeiden
- Es wird eine Wartezeit eingehalten, bevor gesendet wird (Backoff)

Eigenschaften:

- Eignet sich für Funknetzwerke
- Verringert das Risiko von Datenverlusten durch versteckte Sender
- Kann durch viele Teilnehmer und Störungen beeinträchtigt werden

Beide Verfahren ermöglichen es, dass mehrere Teilnehmer ein gemeinsames Medium nutzen, ohne sich gegenseitig zu stören. Sie unterscheiden sich jedoch erheblich in ihrer Wirkweise und ihrem Einsatzgebiet.

OSI-Modell

Das OSI-Modell (Open Systems Interconnection Model) ist ein konzeptionelles Referenzmodell der Internationalen Organisation für Normung (ISO), das die Kommunikation zwischen Netzwerksystemen in sieben Schichten unterteilt. Es dient dazu, die Funktionsweise von Netzwerken systematisch zu beschreiben, zu standardisieren und Probleme besser analysieren zu können.

Die 7 Schichten des OSI-Modells

1. **Bitübertragungsschicht (Physical Layer)**
    - Überträgt einzelne Bits über das physikalische Medium (Kabel, Funk).
    - Beispiel: Netzwerkkabel, elektrische Signale, Steckverbinder (RJ45).
2. **Sicherungsschicht (Data Link Layer)**
    - Stellt eine fehlerfreie Verbindung zwischen zwei direkt verbundenen Geräten her.
    - Kümmert sich um MAC-Adressen, Frames, Fehlererkennung (z. B. CRC).
    - Beispiel: Ethernet, WLAN (MAC-Teil), Switches.
3. **Vermittlungsschicht (Network Layer)**
    - Verantwortlich für die logische Adressierung (IP) und Routing von Daten.
    - Beispiel: IP-Protokoll, Router.
4. **Transportschicht (Transport Layer)**
    - Stellt eine Ende-zu-Ende-Verbindung zwischen Sender und Empfänger her.
    - Sorgt für Datenflusskontrolle, Fehlerkorrektur und Reihenfolge.

    - Beispiel: TCP, UDP.
5. **Sitzungsschicht (Session Layer)**
    - Erstellt, verwaltet und beendet Sitzungen zwischen Anwendungen.
    - Beispiel: Remote-Prozeduraufrufe (RPC), NetBIOS.
6. **Darstellungsschicht (Presentation Layer)**
    - Wandelt Datenformate um (z. B. Zeichencodierung, Verschlüsselung).
    - Beispiel: JPEG, MP3, TLS/SSL-Verschlüsselung.
7. **Anwendungsschicht (Application Layer)**
    - Stellt Schnittstellen für Anwendungen bereit, um auf Netzwerkdienste zuzugreifen.
    - Beispiel: HTTP, FTP, SMTP, DNS.

Bedeutung des OSI-Modells

- **Vereinfachung komplexer Netzwerktechnologien**
- **Modularisierung von Funktionen**
- **Standardisierung der Netzwerkkommunikation**
- **Fehlerdiagnose durch Schichtenprinzip**

Das OSI-Modell ist heute kein praktisches Protokollstapelmodell, sondern ein theoretisches Modell zur Orientierung und Problemanalyse. In der Praxis ist das TCP/IP-Modell gebräuchlicher, das sich grob auf vier Schichten reduziert, aber sich eng am OSI-Modell orientiert.

Protokolle: DHCP, Mail

Netzwerkprotokolle definieren, wie Daten über ein Netzwerk ausgetauscht werden. Zwei wichtige Bereiche sind die automatische IP-Vergabe und die E-Mail-Kommunikation.

DHCP (Dynamic Host Configuration Protocol)

DHCP ist ein Netzwerkprotokoll, das Clients automatisch mit IP-Adressen und weiteren Netzwerkeinstellungen (z. B. Subnetzmaske, Gateway, DNS-Server) versorgt. Es arbeitet nach dem Client-Server-Prinzip:

1. **DHCPDISCOVER**: Der Client sucht per Broadcast nach einem DHCP-Server.
2. **DHCPOFFER**: Der Server antwortet mit einem Adressangebot.
3. **DHCPREQUEST**: Der Client akzeptiert das Angebot.
4. **DHCPACK**: Der Server bestätigt und vergibt die Adresse.

Vorteile:

- Zentrale Verwaltung der IP-Adressen
- Fehlerreduktion durch automatische Konfiguration
- Effiziente Nutzung des Adresspools durch Leases

Mailprotokolle

Zur E-Mail-Kommunikation kommen verschiedene Protokolle zum Einsatz, abhängig vom Zweck:

SMTP (Simple Mail Transfer Protocol)

- Wird zum **Versenden** von E-Mails verwendet
- Arbeitet auf Port 25, 465 (SSL) oder 587 (TLS)
- Funktioniert zwischen Mail-Client und Server sowie zwischen Servern

POP3 (Post Office Protocol Version 3)

- Dient dem **Abrufen** von E-Mails
- Lädt Mails vom Server herunter und löscht sie (Standardverhalten)
- Arbeitet meist auf Port 110 (oder 995 mit SSL)
- Vorteil: Offline-Zugriff möglich

IMAP (Internet Message Access Protocol)

- Ermöglicht den **Zugriff auf E-Mails direkt auf dem Server**
- Nachrichten bleiben gespeichert, ideal für Zugriff von mehreren Geräten
- Arbeitet auf Port 143 (oder 993 mit SSL)

Zusammenfassung:

- **SMTP**: Senden von E-Mails
- **POP3/IMAP**: Empfangen von E-Mails (POP3: Download, IMAP: Synchronisierung)

Mailprotokolle sind essenziell für den reibungslosen E-Mail-Verkehr im Internet und werden in den Anwendungsschichten von Netzwerkmodellen angesiedelt.

IP-Adressen: IPv4, IPv6 – Aufbau, besondere Adressen

IP-Adressen (Internet Protocol Addresses) dienen der eindeutigen Identifikation von Geräten in einem Netzwerk. Sie sind notwendig, damit Datenpakete korrekt zugestellt werden können.

IPv4 (Internet Protocol Version 4)

- Besteht aus **32 Bit**, dargestellt in vier Blöcken (Oktetten) mit Dezimalzahlen.
- Beispiel: 192.168.0.1
- Es gibt ca. 4,3 Milliarden eindeutige Adressen – heute nahezu ausgeschöpft.

Adressklassen:

- Klasse A: 1.0.0.0 – 126.255.255.255
- Klasse B: 128.0.0.0 – 191.255.255.255

- Klasse C: 192.0.0.0 – 223.255.255.255

Private Adressbereiche (nicht öffentlich erreichbar):

- 10.0.0.0 – 10.255.255.255 (Klasse A)
- 172.16.0.0 – 172.31.255.255 (Klasse B)
- 192.168.0.0 – 192.168.255.255 (Klasse C)

Besondere IPv4-Adressen:

- 127.0.0.1: Loopback-Adresse (localhost)
- 255.255.255.255: Broadcast an alle im lokalen Netz
- 0.0.0.0: Nicht spezifiziert oder unbekannt
- 169.254.x.x: APIPA (automatisch zugewiesene Adresse ohne DHCP)

IPv6 (Internet Protocol Version 6)

- Besteht aus **128 Bit**, dargestellt als acht Gruppen aus vier hexadezimalen Ziffern.
- Beispiel: 2001:0db8:85a3:0000:0000:8a2e:0370:7334
- Bietet 2^128 Adressen – genug für jedes Gerät weltweit

Vorteile gegenüber IPv4:

- Größerer Adressraum
- Integrierte Sicherheitsmechanismen (IPSec)
- Vereinfachtes Routing durch Hierarchie
- Keine NAT nötig, da jeder Client eine globale Adresse haben kann

Besondere IPv6-Adressen:

- ::1: Loopback-Adresse (entspricht 127.0.0.1 in IPv4)
- fe80::/10: Link-Local-Adresse (lokales Netzwerk, nicht geroutet)
- ff00::/8: Multicast-Adressen

Darstellung und Kürzung von IPv6

IPv6-Adressen können gekürzt werden:

- Führende Nullen können entfernt werden: 03f → 3f
- Längere Null-Blöcke können durch :: ersetzt werden (nur einmal pro Adresse):
  - z. B. 2001:0db8:0000:0000:0000:0000:0000:0001 → 2001:db8::1

IP-Adressen sind zentrale Bausteine des Internets und Grundlage für die Kommunikation in Netzwerken.

MAC-Adressen

Die MAC-Adresse (Media Access Control Address) ist eine weltweit eindeutige Kennung für jedes netzwerkfähige Gerät, das auf der Sicherungsschicht (Schicht 2) des OSI-Modells arbeitet. Sie ist fest in den Netzwerkadapter (z. B. LAN- oder WLAN-Karte) eingebrannt.

Aufbau

- Besteht aus **48 Bit**, dargestellt in 6 Byte (jeweils zwei hexadezimale Zeichen)
- Beispiel: 00:1A:2B:3C:4D:5E

Die ersten drei Byte (24 Bit) stehen für den Hersteller (OUI – Organizationally Unique Identifier), die letzten drei Byte (24 Bit) sind gerätespezifisch und werden vom Hersteller vergeben.

Funktion

- Wird im lokalen Netzwerk verwendet, um Geräte eindeutig zu identifizieren
- Switches verwenden MAC-Adressen, um Datenpakete gezielt an den richtigen Port weiterzuleiten
- DHCP-Server können MAC-Adressen zur Zuordnung fester IPs verwenden (Statische IP-Zuweisung)

Eigenschaften

- Bleibt bei jedem Gerät gleich, unabhängig vom Netzwerk
- Kann in einigen Betriebssystemen temporär geändert („gespooft“) werden

Vergleich zu IP-Adresse

- **MAC-Adresse**: Hardwareadresse, lokal eindeutig, unverändert (fest im Gerät)
- **IP-Adresse**: Logische Adresse, netzwerkabhängig, kann sich ändern

MAC-Adressen sind essenziell für den Betrieb lokaler Netzwerke und Grundlage für viele Sicherheits- und Verwaltungsfunktionen wie MAC-Filterung, Netzwerkzugriffskontrolle und Gerätetracking.

Angewandte Mathematik

Mathematische Grundlagen sind in der IT essenziell, um technische Zusammenhänge zu verstehen, Systemressourcen zu planen und Fehler zu analysieren. Im Prüfungsbereich IT-Systemtechnik sind besonders folgende Themen relevant:

Dateigröße eines Bildes berechnen

Zur Berechnung der Dateigröße eines unkomprimierten Bildes:

Formel: Breite × Höhe × Farbtiefe (in Bit) ÷ 8 = Größe in Byte

Beispiel: Ein Bild mit 1920 × 1080 Pixeln und 24 Bit Farbtiefe: 1920 × 1080 × 24 ÷ 8 = 6.220.800 Byte ≈ 5,93 MB

Datendurchsatz / Download-Dauer berechnen

Zur Berechnung der benötigten Zeit für einen Download:

Formel: Datenmenge (in Bit) ÷ Bandbreite (in Bit/s) = Dauer (in Sekunden)

Beispiel: Ein 1 GB (8.000.000.000 Bit) großer Download bei 100 Mbit/s: 8.000.000.000 ÷ 100.000.000 = 80 Sekunden

Zahlensysteme: Konvertieren und Rechnen

Zahlensysteme wie Binär, Dezimal, Hexadezimal und Oktal sind wichtig für die Darstellung und Verarbeitung von Daten im Computer.

Beispiele:

- Dezimal → Binär: 13 → 1101
- Hexadezimal → Binär: 1A → 00011010
- Binär-Addition: 1101 + 1010 = 10111

Grundoperationen:

- Addition, Subtraktion, Multiplikation und Division im Binärsystem
- Umwandlung von Zahlen zwischen den Systemen

Leistungsberechnung – Strom, Spannung, Leistung

In elektronischen Schaltungen wichtig zur Auslegung und Fehlerdiagnose.

Formeln:

- U = R × I (Ohm’sches Gesetz)
- P = U × I (Leistung in Watt)

Beispiel:

- Spannung: 12 V, Strom: 2 A → Leistung: 12 V × 2 A = 24 W

Akkulaufzeit, Stromdichte, Widerstand

Akkulaufzeit: Kapazität (mAh) ÷ Stromaufnahme (mA) = Laufzeit (h)

Beispiel: 3000 mAh Akku, Verbrauch 500 mA → 3000 ÷ 500 = 6 Stunden

Stromdichte (J): J = I / A (Strom pro Querschnittsfläche)

Widerstand (R): $R = \rho \times (l / A)$, wobei ρ der spezifische Widerstand, l die Länge und A die Querschnittsfläche des Leiters ist

Reihenschaltung, Parallelschaltung, Kirchhoff'sche Regeln

Reihenschaltung:

- Strom ist überall gleich: $I_1 = I_2 = I_3$
- Gesamtwiderstand: $Rges = R_1 + R_2 + R_3$

Parallelschaltung:

- Spannung ist überall gleich: $U_1 = U_2 = U_3$
- Gesamtwiderstand: $1/Rges = 1/R_1 + 1/R_2 + 1/R_3$

Kirchhoff'sche Gesetze:

1. **Knotenregel** (Strom): Summe der zufließenden Ströme = Summe der abfließenden Ströme
2. **Maschenregel** (Spannung): Summe aller Spannungen in einer Masche = 0

Diese Grundlagen sind in der Praxis unerlässlich für Fehlerdiagnose, Schaltungsplanung und die richtige Dimensionierung elektrischer Komponenten.

Systemmanagement 1/2

Systemmanagement umfasst die Verwaltung, Konfiguration, Wartung und Überwachung von IT-Systemen – sowohl im Client- als auch im Serverbereich. Dazu gehören unter anderem Virtualisierungskonzepte, Befehlszeilensteuerung, Authentifizierungsmethoden und Speichertechnologien.

VM-Konzepte (Virtuelle Maschinen)

Virtuelle Maschinen (VMs) sind softwarebasierte Nachbildungen von Computersystemen. Sie laufen auf einem sogenannten **Hypervisor**, der die Ressourcen des physischen Systems (Host) den VMs (Guests) zuweist.

- **Typ-1-Hypervisor**: Läuft direkt auf der Hardware (z. B. VMware ESXi, Microsoft Hyper-V Server)
- **Typ-2-Hypervisor**: Läuft auf einem Betriebssystem (z. B. Oracle VirtualBox, VMware Workstation)

Vorteile:

- Mehrere Betriebssysteme auf einem Host
- Ressourceneffizienz
- Snapshot-Funktion, einfache Sicherung und Wiederherstellung
- Isolierung der Systeme für mehr Sicherheit

Client-Befehle (Windows)

Typische Windows-Befehle zur Netzwerk- und Systemdiagnose:

- ipconfig – Zeigt IP-Konfiguration des Systems
- ping – Prüft die Erreichbarkeit eines Hosts
- tracert – Zeigt den Weg eines Datenpakets
- netstat – Zeigt aktive Netzwerkverbindungen
- tasklist / taskkill – Listet laufende Prozesse, beendet Prozesse
- shutdown – Herunterfahren/Neustart des Systems

Linux-Befehle

Wichtige Terminalbefehle in Linux-Systemen:

- ls, cd, pwd – Navigation im Dateisystem
- sudo – Ausführen mit Administratorrechten
- apt-get / dnf / zypper – Paketverwaltung
- nano, vi – Texteditoren
- chmod, chown – Rechte ändern
- systemctl – Dienste verwalten

Serverdienste

Ein Server bietet Netzwerkdienste an, die von Clients verwendet werden:

- **DHCP-Server**: Vergibt automatisch IP-Adressen
- **DNS-Server**: Wandelt Domainnamen in IP-Adressen um
- **Webserver**: Hosten von Webseiten (z. B. Apache, NGINX)
- **Fileserver**: Bereitstellung von Dateien (z. B. über SMB, NFS)
- **Mailserver**: Abwicklung von E-Mail-Kommunikation (z. B. Postfix, Exchange)
- **Druckserver**: Gemeinsame Nutzung von Druckern

2FA / MFA (Zwei-/Mehrfaktor-Authentifizierung)

Sicherheitsverfahren zur Absicherung von Logins:

- **Etwas, das man weiß** (Passwort)
- **Etwas, das man hat** (Smartphone, Token)
- **Etwas, das man ist** (biometrische Merkmale)

Bei 2FA sind zwei dieser Faktoren nötig, bei MFA mindestens zwei. Einsatzgebiete: Online-Banking, E-Mail-Zugänge, VPN-Zugänge, Firmenportale.

RAID (Redundant Array of Independent Disks)

RAID ist eine Technik zur Kombination mehrerer physischer Festplatten zu einem logischen Laufwerk, um Ausfallsicherheit und/oder Geschwindigkeit zu erhöhen.

Wichtige RAID-Level:

- **RAID 0** – Striping, keine Redundanz, hohe Geschwindigkeit
- **RAID 1** – Mirroring, Daten werden gespiegelt (hohe Sicherheit)
- **RAID 5** – Striping mit Parität, Ausfall einer Platte möglich
- **RAID 10** – Kombination aus RAID 1 + RAID 0: gespiegelt und gestreift

RAID schützt nicht vor versehentlichem Löschen – es ist kein Backup-Ersatz.

Systemmanagement 2/2

Sicherungskonzepte und Speichermedien

Datensicherungen sind essenziell, um Datenverlust durch Fehler, Manipulation oder Hardwareausfälle zu vermeiden. Es gibt unterschiedliche Strategien und Speichermedien:

Sicherungsarten:

- **Vollsicherung**: Es werden alle Daten gesichert. Einfach in der Wiederherstellung, benötigt aber viel Speicher.
- **Differenzielle Sicherung**: Sichert alle Änderungen seit der letzten Vollsicherung. Schnelle Wiederherstellung, moderater Speicherbedarf.
- **Inkrementelle Sicherung**: Sichert nur die Änderungen seit der letzten Sicherung (egal ob voll oder inkrementell). Spart Speicherplatz, aber längere Wiederherstellung.

Speicherlösungen:

- **Externe Festplatten (HDD/SSD)**
- **Netzwerkspeicher (NAS)**
- **Magnetbänder (z. B. LTO)** – langlebig, aber langsam
- **Cloud-Backups** – flexibel, extern gespeichert, abhängig von Internetverbindung

Eine gute Backup-Strategie berücksichtigt die 3-2-1-Regel: 3 Kopien, auf 2 verschiedenen Medien, 1 Kopie extern ausgelagert.

Rechtliche Grundlagen: EULA, Urheberrecht, Recht am eigenen Bild

EULA (End User License Agreement)

Ein Endnutzer-Lizenzvertrag, der regelt, wie Software verwendet werden darf. Enthält Bestimmungen zu Nutzungsrechten, Einschränkungen, Haftung etc.

Urheberrecht

Schützt geistige Schöpfungen wie Software, Texte, Bilder oder Musik. Der Urheber hat das Recht zu bestimmen, wer und wie sein Werk genutzt werden darf. Verstöße können zivil- und strafrechtliche Konsequenzen haben.

Recht am eigenen Bild

Regelt, dass Bilder einer Person nur mit deren Zustimmung veröffentlicht oder verbreitet werden dürfen. Ausnahmen gelten z. B. bei Personen des öffentlichen Interesses oder bei Veranstaltungen.

Datenschutz: DSGVO (Datenschutz-Grundverordnung)

Die DSGVO ist eine EU-weite Verordnung zum Schutz personenbezogener Daten. Sie definiert Grundsätze und Rechte im Umgang mit Daten:

- **Personenbezogene Daten**: Daten, die eine Person identifizierbar machen (z. B. Name, IP-Adresse, E-Mail)
- **Besonders schützenswerte Daten**: z. B. Gesundheitsdaten, religiöse Überzeugung
- **Betroffenenrechte**: Auskunft, Berichtigung, Löschung, Datenübertragbarkeit
- **Rechtmäßigkeit**: Verarbeitung nur mit Einwilligung oder Rechtsgrundlage
- **Datensicherheit**: Pflicht zu technischen und organisatorischen Maßnahmen

Speichertechnologien: HDD, SSD

HDD (Hard Disk Drive)

- Mechanischer Speicher mit rotierenden Magnetscheiben
- Große Kapazitäten (bis 20 TB)
- Günstig, aber empfindlich gegen Erschütterung
- Langsamer als SSD

SSD (Solid State Drive)

- Keine beweglichen Teile, basiert auf Flash-Speicher
- Sehr schnell beim Lesen/Schreiben
- Teurer pro GB, aber zuverlässiger im Alltag
- Ideal für Betriebssysteme, Programme und schnelle Datenzugriffe

Grafikkarten (GPU) und Anschlüsse

Eine Grafikkarte verarbeitet visuelle Daten und gibt sie an einen Bildschirm aus. Moderne GPUs unterstützen hohe Auflösungen, 3D-Berechnungen und Hardwarebeschleunigung (z. B. für Video-Encoding, KI-Anwendungen).

Anschlüsse:

- **HDMI (High Definition Multimedia Interface)**: Überträgt Bild & Ton, Standard bei Monitoren/TVs
- **DisplayPort**: Für hohe Auflösungen und Bildwiederholraten, professioneller Einsatz
- **DVI**: Digitaler Anschluss, älter, ohne Ton
- **VGA**: Veraltet, analoger Standard

Aufbau & Schnittstellen Mainboard

Das Mainboard (Hauptplatine) verbindet alle Komponenten miteinander. Es enthält:

- **CPU-Sockel**: Aufnahme für Prozessor
- **RAM-Bänke**: Steckplätze für Arbeitsspeicher
- **PCIe-Steckplätze**: Für Erweiterungskarten (z. B. GPU, Soundkarte)
- **M.2- und SATA-Anschlüsse**: Für SSDs und Festplatten
- **USB-Ports, Audio, LAN, ggf. WLAN onboard**

CPU und RAM

CPU (Central Processing Unit)

Die zentrale Verarbeitungseinheit, auch Prozessor genannt. Sie führt Rechenbefehle aus und steuert die Abläufe im System. Merkmale:

- Taktfrequenz (GHz)
- Anzahl der Kerne/Threads
- Cache-Größen

RAM (Random Access Memory)

Der Arbeitsspeicher speichert temporär Daten und Programme, die aktuell genutzt werden.

- Flüchtig: Inhalte gehen beim Ausschalten verloren
- Je mehr RAM, desto besser Multitasking und Performance
- Moderne Standards: DDR4, DDR5

CPU und RAM bestimmen maßgeblich die Rechenleistung und Geschwindigkeit eines Systems – sowohl im Alltag als auch im Serverbetrieb.