4 Netzwerketechnologie und -konfiguration

- 01 Netzwerkarten und -komponenten
- 02 Netzwerkprotokolle und Standards
- 03 IP
- 04 Übertragungsmedien
- 05 Netzwerkdokumentation
- 06 Netzwerkkonfiguration
- 07 Barcode, QR-Code, RFID-Chip
- 08 Störungen
- 09 Wichtige Serverarten

01 Netzwerkarten und -komponenten

- Netzwerkarten
- Netzwerktopologien
- Gateway
- Router
- Switch
- Repeater und Access Point
- Übertragungsgeschwindigkeit berechnen
- CPS

Netzwerkarten

Personal Area Network (PAN)

Verbund von Geräten in unmittelbarer Nähe, z. B. mit Bluetooth verbundene Geräte

Local Area Networks (LAN)

Begrenzt, z. B. auf ein Unternehmen

Metropolitan Area Networks (MAN)

Zusammenschluss kleinerer NW zu einem größerem Netzwerk, z. B. Stadtnetz

Wide Area Networks (WAN)

Räumlich größeres NW, z. B. über mehrere Firmenstandorte hinweg

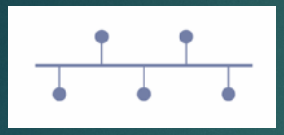
Global Area Networks (GAN)

Weltumspannendes NW, z. B. das Internet, Netzwerk international tätiger Firmen

Virtual Private Network (VPN)

Geschütztes, in sich geschlossenes Netzwerk, z. B. zum Zugriff auf das Firmen-NW von zu Hause aus

Netzwerktopologien



Bustopologie

- ⊕ Einfach & kostengünstig
- ⊕ Geringer Kabelbedarf
- ⊖ Störungen legen das ganze Netz lahm
- ⊖ Begrenzte Anzahl an Geräten

Ringtopologie

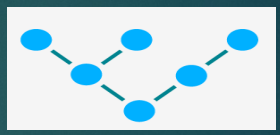
- ⊕ Vorhersehbare Paketlaufwege
- ⊕ Gute Lastverteilung
- ⊖ Ein Fehler → Netzunterbrechung
- ⊖ Aufwendige Fehlerbehandlung

Sterntopologie

- ⊕ Einfache Verwaltung
- ⊕ Fehler leicht lokalisierbar
- ⊕ Sehr verbreitet und skalierbar
- ⊖ Zentraler Punkt ist Single Point of Failure
- ⊖ Höherer Kabelaufwand

Mesh-Topologie

- ⊕ Höchste Ausfallsicherheit
- ⊕ Redundante Wege für jeden Pfad
- ⊖ Sehr hoher Verkabelungs-aufwand
- ⊖ Teuer und komplex



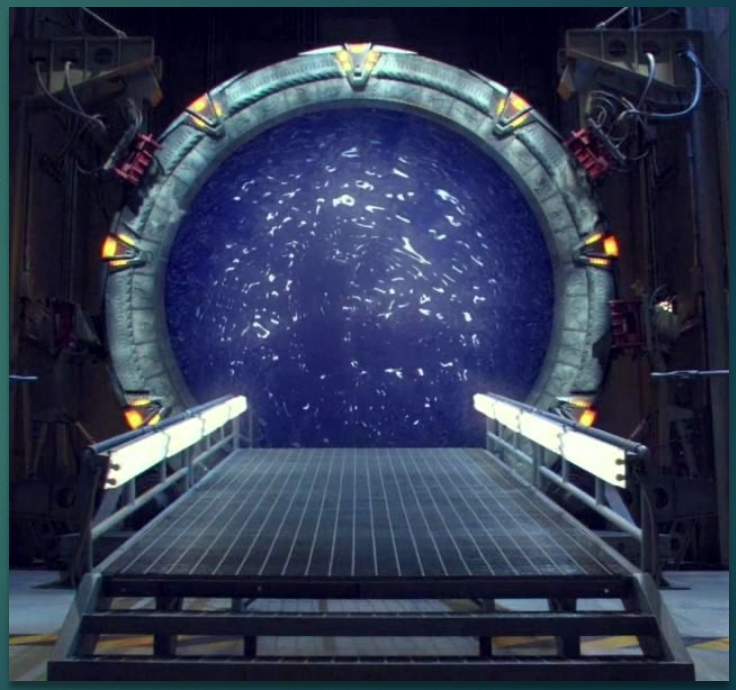
Baumtopologie

- ⊕ Gut erweiterbar
- ⊕ Übersichtliche Struktur
- ⊖ Fehler in oberen Ebenen → große Auswirkungen
- ⊖ Höhere Komplexität bei Planung

Gateway

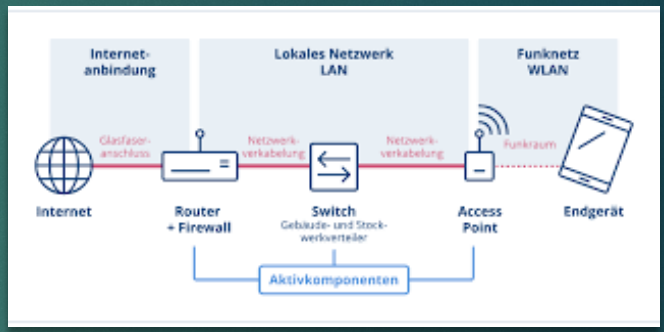
- Verbindet die netzwerkfähigen Geräte eines Netzwerks mit den netzwerkfähigen Geräten eines anderen Netzwerks
- Definiert Netzwerkgrenzen
- Verbindung verschiedener Systeme

- Mögliche Geräte
  - Router
  - Switch
  - PC



Router

- Weiterleitung von Netzwerkpakete
  zwischen mehreren Rechnernetzen

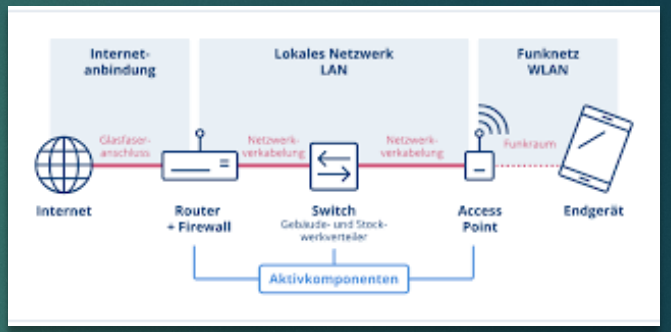


Quelle

- Meist genutzt zur
  - Internetanbindung
  - sicheren Kopplung mehrerer Standorte (VPN)
  - zur direkten Kopplung mehrerer lokaler Netzwerksegmente

Switch 1/2

- Verbindung von Geräten untereinander



Quelle

- Layer 2-Switch
  - Arbeitet auf OSI - Layer 2 (Datenverbindungs-Layer)
  - Datenweiterleitung anhand der MAC-Zieladresse
- Layer 3 Switch
  - Arbeitet auf OSI - Layer 3 (Netzwerk-Layer)
  - Datenweiterleitung anhand der IP-Zieladresse

Switch 2/2

Unverwalteter/Unmanaged Switch

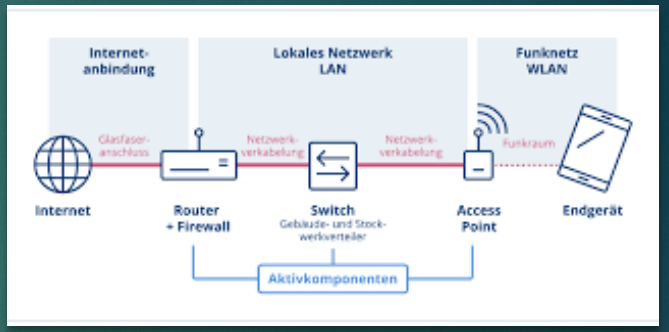
- Einfaches Plug-and-Play-Gerät, das keine Konfiguration erfordert.
- einfacher zu bedienen als Managed Switch
- Für kleine Unternehmen oder Heimnetzwerke, die keine erweiterten Funktionen benötigen

Verwalteter/Managed Switch

- Kann von einem Netzwerkadministrator konfiguriert und gesteuert werden
- Funktionen u. a.:
  - Datenverkehr verwalten
  - Quality of Service (QoS) einrichten
  - Portsicherheit einrichten
  - VLANs einrichten
- Geeignet für große Unternehmen

Repeater und Access Point

- Repeater
  - Verstärkt bestehendes WLAN-Signal eines Routers
  - Empfängt WLAN Funksignal eines Routers gibt dies und verstärkt wieder ab
  - Dient der Erweiterung eines Netzwerkes



Quelle

- Access Point
  - Ist über LAN-Kabel mit dem Router oder Switch verbunden
  - Generiert ein eigenes WLAN-Netz mit eigener SSID
  - Router verfügen über die Funktion eines Access Points

Übertragungsraten berechnen

C = D/t

C = Datenübertragungsrate

D = Datenmenge

t = Zeit

Übliche Maßeinheiten;

Bit/s, kBit/s, MBit/s, GBit/s

1.000 oder 1.024?

1.024 ist binärer Wert

Als Multiplikator von Bit und Byte verwendet, um die Kapazität von Speichergeräten oder die Größe von Computerdateien auszudrücken

Kibi, Mebi und Gibi etc., durch Ki, Mi, Gi abgekürzt

Cyber-physische Systeme (CBS)

- System, in dem rechnergestützte Steuerung (Software) mit physischen Prozessen (Sensoren, Aktoren, Maschinen) eng gekoppelt ist – in Echtzeit und oft über ein Netzwerk verbunden

- Ein CPS besteht typischerweise aus:
  - **Sensoren** (erfassen Daten)
  - **Aktorik** (wirkt auf die Umwelt ein)
  - **Software** (verarbeitet Daten, trifft Entscheidungen)
  - **Kommunikation** (z. B. WLAN)

CPS Software

- verarbeitet Sensordaten
- trifft Entscheidungen (z. B. per Regelalgorithmus)
- steuert Aktoren
- kommuniziert mit anderen Systemen (z. B. über APIs)
- Echtzeitfähigkeit
- **Plattformen**: Raspberry Pi, Microcontroller etc.
- **Programmiersprachen**: Python, C/C++ etc.

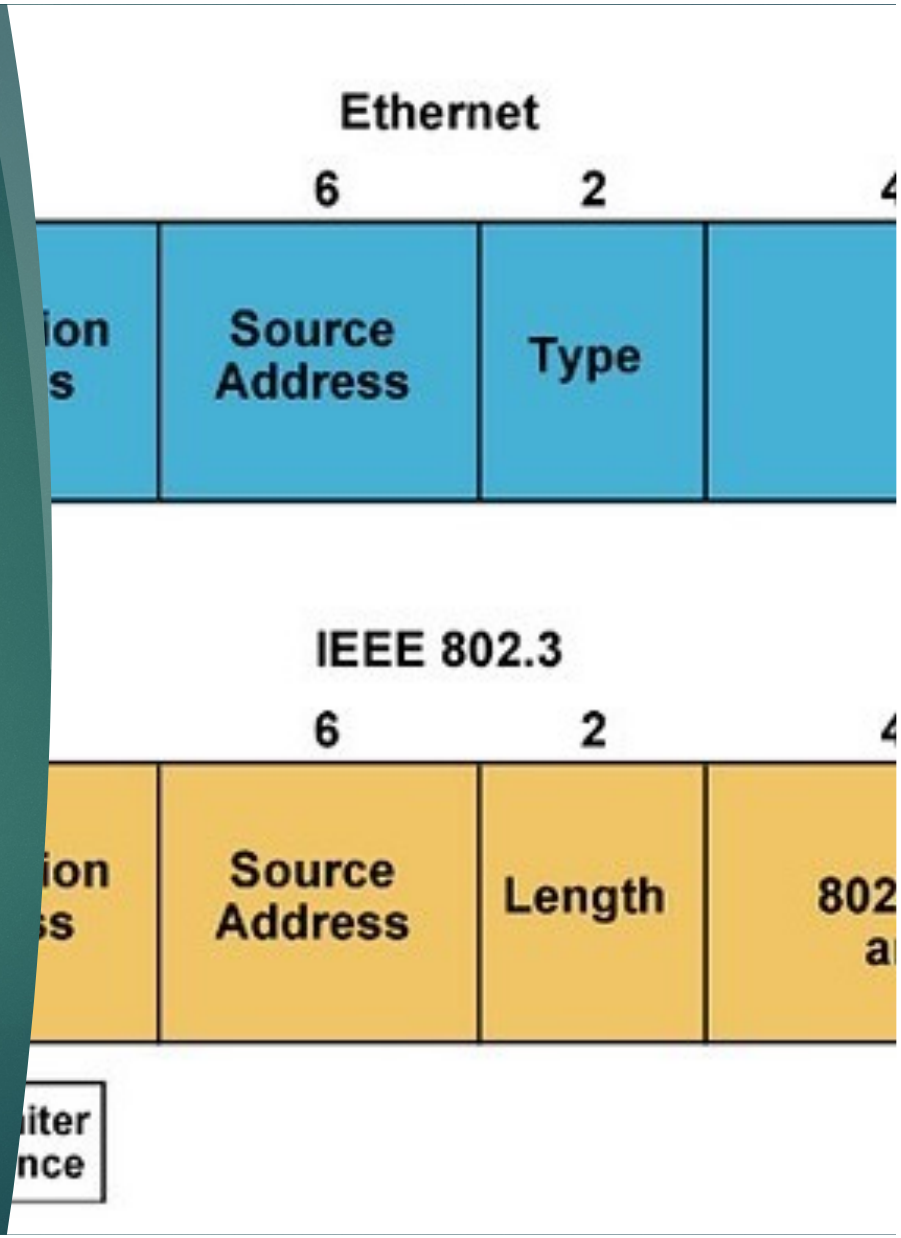
CPS – wichtige Faktoren

- Auswahl von geeigneten Sensoren/Aktoren
- Nutzung von Bibliotheken zur Ansteuerung der Hardware
- Abfragerhythmus planen
- Kenntnis des Zugriffs auf Sensoren und Aktoren
  - Protokolle
  - Register
  - Schnittstellen

Anwendung	Beispiel Abfragefrequenz
Temperaturmessung	alle 30 Sekunden
Bewegungserkennung	< 1 Sekunde
Sicherheitsabschaltung	Echtzeit (10 ms)

02 Netzwerkprotokolle und Standards

- Überblick Netzwerkprotokolle
- Protokolle zur Fernwartung
- Ethernet
- Ethernet Standards (Auswahl)
- Ethernet und TCP
- TCP
- UDP
- Echtzeitkommunikation
- FibreChannel
- HTTPS
- SSL und TLS
- Mail Protokolle
- LDAP
- SNMP
- WLAN Standards
- Bluetooth



Überblick Netzwerkprotokolle 1/3

Protokoll	Port-Nummern	Beschreibung
CSMA/CD	–	Carrier Sense Multiple Access with Collision Detection ist ein Protokoll für den Zugriff auf einen gemeinsam genutzten Übertragungskanal. Dabei werden Kollisionen bei Datenübertragungen vermieden bzw. erkannt.
DNS	53/UDP	Domain Name System ist ein Protokoll, das es ermöglicht, leicht lesbare Domainnamen in IP-Adressen umzuwandeln.
DHCP	67/UDP, 68/UDP	Dynamic Host Configuration Protocol ist ein Protokoll, das es ermöglicht, Netzwerkgeräten automatisch IP-Adressen zuzuweisen und weitere Netzwerkeinstellungen zu konfigurieren.
ARP	–	Address Resolution Protocol ist ein Protokoll, das es ermöglicht, die MAC-Adresse eines Geräts anhand seiner IP-Adresse zu ermitteln.
IP	–	Internet Protocol ist das Grundprotokoll für die Übertragung von Datenpaketen in IP-basierten Netzwerken.
TCP	–	Transmission Control Protocol ist ein verbindungsorientiertes Protokoll, das sicherstellt, dass Daten in der richtigen Reihenfolge ankommen und vollständig übertragen werden.
UDP	–	User Datagram Protocol ist ein verbindungsloses Protokoll, das es ermöglicht, Datenpakete ohne Verbindungsaufbau zu senden.
SMB	137, 138, 139	Server Message Block (SMB) ist ein Protokoll, das es ermöglicht, Dateien, Drucker und andere Ressourcen in einem Netzwerk zu teilen.

Überblick Netzwerkprotokolle 2/3

Protokoll	Port-Nummern	Beschreibung
NFS	2049	Network File System (NFS) ist ein Protokoll, das es ermöglicht ganze Dateisysteme über das Netzwerk zu mounten und Dateien zwischen verschiedenen Computern auszutauschen. Es wird unter Linux verwendet.
SMTP/S	25, 587	Simple Mail Transfer Protocol ist ein Protokoll, das es ermöglicht, E-Mails zwischen Mail-Servern auszutauschen, also E-Mails zu versenden.
IMAP/S	143, 993	Internet Message Access Protocol ist ein Protokoll, das es ermöglicht, E-Mails auf einem Mail-Server zu lesen und zu verwalten.
POP3/S	110, 995	Post Office Protocol Version 3 ist ein Protokoll, das es ermöglicht, E-Mails von einem Mail-Server abzurufen und lokal zu speichern.
HTTP	80	Hypertext Transfer Protocol ist das Protokoll, das verwendet wird, um Webseiten im Internet zu übertragen. Es ist jedoch prinzipiell nicht darauf beschränkt, Webseiten zu übertragen.
HTTPS	443	Hypertext Transfer Protocol Secure ist eine sichere Variante des HTTP-Protokolls, die SSL/TLS-Verschlüsselung verwendet.
FTP	20,21	File Transfer Protocol ist ein Protokoll, das es ermöglicht, Dateien zwischen Computern auszutauschen
IPsec	–	Internet Protocol Security ist ein Protokoll, das es ermöglicht, IP-basierte Netzwerke sicher zu kommunizieren
TLS/SSL	–	Transport Layer Security/Secure Sockets Layer ist ein Protokoll, das es ermöglicht, sichere Verbindungen im Internet herzustellen. Es wird hauptsächlich verwendet, um Datenübertragungen über HTTPS, FTP, Telnet und andere Anwendungen zu verschlüsseln.

Überblick Netzwerkprotokolle 3/3

Protokoll	Port-Nummern	Beschreibung
SNMP	161/UDP, 162/UDP	Simple Network Management Protocol ist ein Protokoll, das es ermöglicht, Netzwerkgeräte zu verwalten und Informationen über deren Status zu erhalten.
LDAP/S	389 636	Lightweight Directory Access Protocol ist ein Protokoll, das es ermöglicht, auf Verzeichnisdienste zuzugreifen und Informationen darin zu suchen und zu verwalten.
NTP	123	Network Time Protocol ist ein Protokoll, das es ermöglicht, die Systemzeit von Netzwerkgeräten synchron zu halten. Wichtig ist dies z.B. bei Logs oder Diensten wie Kerberos.
Telnet	23	Telnet ist ein Protokoll, das es ermöglicht, sich per Fernzugriff mit einem entfernten Computer zu verbinden und diesen zu steuern.
SSH	22	Secure Shell ist ein Protokoll, das es ermöglicht, sichere Fernzugriffe auf einen entfernten Computer durchzuführen und diesen zu steuern.
RDP	3389	Remote Desktop Protocol ist ein Protokoll, das es ermöglicht, sich per Fernzugriff mit einem entfernten Computer zu verbinden und die Benutzeroberfläche des Computers anzuzeigen.
ICA	1494	Independent Computing Architecture ist ein Protokoll, das ähnlich wie RDP funktioniert, aber von Citrix Systems entwickelt wurde.
VNC	5900	Virtual Network Computing ist ein Protokoll, das es ermöglicht, sich per Fernzugriff mit einem entfernten Computer zu verbinden und die Benutzeroberfläche des Computers anzuzeigen oder zu steuern. Es ist ähnlich wie RDP, aber in der Regel plattformübergreifend und erfordert keine spezielle Software auf dem entfernten Computer.

Protokolle zur Fernwartung

RDP	VNC	SSH
• Remote Desktop Protocol • Microsoft spezifisch	• Virtual Network Computing • Platformunabhängig nutzbar	• Secure Shell • Lokal entfernte Kommandozeile verfügbar machen

Ethernet 1/2

- Familie von Netzwerktechniken
- IEEE-Norm 802.2
- Schichten 1 und 2 im OSI-Modell
- Vorwiegend in lokalen Netzwerken (LAN) zur kabelgebundenen Datenübertragung
- Verbinden großer Netzwerke (WAN)
- Vielzahl an Standards, für die das Institute of Electrical and Electronics Engineers (IEEE) verantwortlich ist

- Ethernet-Standard-Varianten über Glasfaser haben eine Link-Reichweite von bis zu 80 km, proprietäre auch mehr

Ethernet 2/2

Übertragungsraten

- Derzeit
  - 1, 10, 100 Megabit/s (Fast-Ethernet)
  - 1000 Megabit/s (Gigabit-Ethernet)
  - 2,5, 5, 10, 25, 40, 50, 100, 200 und 400 Gigabit/s
- 800 Gigabit/s und 1,6 Terabit/s werden entwickelt

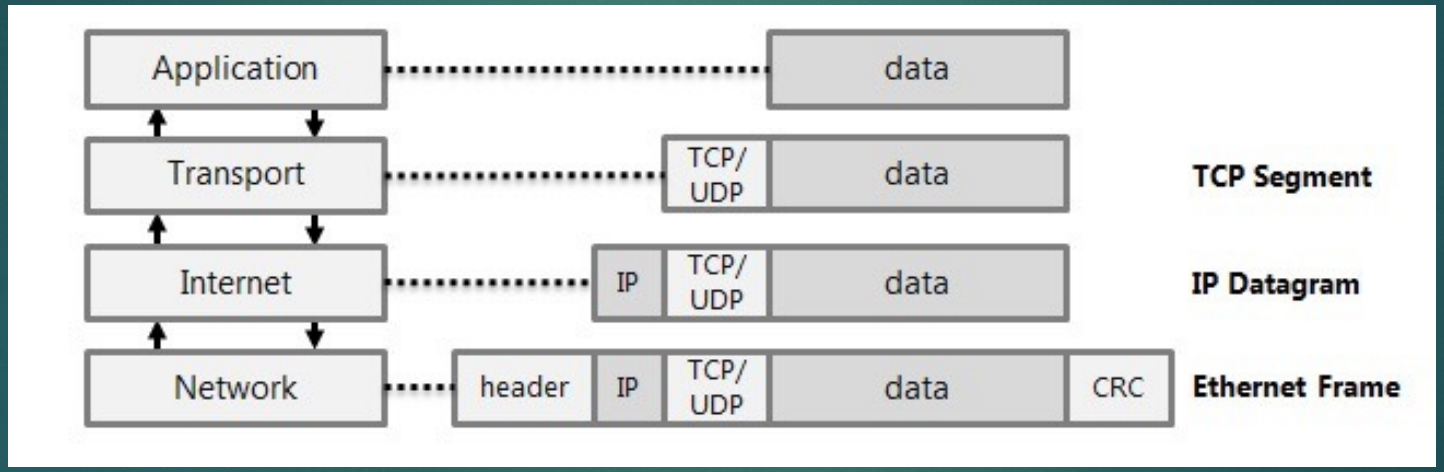
Ethernet Standards (Auswahl)

Standard	Datenrate	Kabeltyp	Max. Kabellänge	Anwendungen	Fazit
10BASE-T	10 Mbit/s	Twisted Pair (Cat3, Cat5)	100 m	Ältere Netzwerke, einfache Anwendungen	Geringe Bandbreite, veraltet
100BASE-TX	100 Mbit/s	Twisted Pair (Cat5, Cat5e)	100 m	Lokale Netzwerke, Standard in Büros	Für moderne Anwendungen oft zu langsam
1000BASE-T	1 Gbit/s	Twisted Pair (Cat5e, Cat6)	100 m	Moderne Netzwerke, anspruchsvolle Anwendungen	Hohe Bandbreite, weitverbreitet
2.5GBASE-T	2,5 Gbit/s	Twisted Pair (Cat5e, Cat6)	100 m	Neuere Netzwerke, Anwendungen mit mittlerem Bandbreitenbedarf	Höhere Bandbreite als Gigabit-Ethernet, kostengünstiger als 10-Gigabit-Ethernet

Quelle

Standard	Datenrate	Kabeltyp	Max. Kabellänge	Anwendungen	Fazit
5GBASE-T	5 Gbit/s	Twisted Pair (Cat5e, Cat6)	100 m	Neuere Netzwerke, Anwendungen mit höherem Bandbreitenbedarf	Noch höhere Bandbreite als 2,5-Gigabit-Ethernet, kostengünstiger als 10-Gigabit-Ethernet
10GBASE-T	10 Gbit/s	Twisted Pair (Cat6a, Cat7)	100 m	Unternehmensnetzwerke, Rechenzentren	Sehr hohe Bandbreite, gut geeignet für anspruchsvolle Anwendungen
25GBASE-T	25 Gbit/s	Twisted Pair (Cat6a, Cat7) bzw. Glasfaser	100 m bzw. >100 m	Rechenzentren, Cloud-Umgebungen	Sehr hohe Bandbreite, ideal für Serververbindungen
40GBASE-T	40 Gbit/s	Twisted Pair (Cat7) bzw. Glasfaser	100 m bzw. >100 m	Rechenzentren, Core-Netzwerke	Extrem hohe Bandbreite, ideal für anspruchsvolle Anwendungen
100GBASE-T	100 Gbit/s	Glasfaser	>100 m	Große Rechenzentren, Internet-Provider	Enorme Bandbreite, ideal für höchste Anforderungen

Ethernet und TCP



Quelle

TCP

Transmission Control Protocol

- Netzwerkprotokoll, das definiert, auf welche Art und Weise Daten zwischen Netzwerkkomponenten ausgetauscht werden
- Teil der Internetprotokollfamilie (TCP/IP-Protokollfamilie)
- Schicht 4 im OSI-Modell

- Eigenschaften:
  - zuverlässig
  - verbindungsorientiert
  - paketvermittelnd

UDP

User Datagram Protocol

verbindungsloses Netzwerkprotokoll, welches die schnelle und effiziente Übertragung von Datenpaketen zwischen Anwendungen, insbesondere in zeitkritischen Umgebungen, ermöglicht

- Teil der Internetprotokollfamilie (TCP/IP-Protokollfamilie)
- Schicht 4 im OSI-Modell

- Eigenschaften:
  - schnell und effizient
  - verbindungslos
  - weniger zuverlässig

Echtzeitkommunikation

- Datenübertragung, bei der Informationen **zeitkritisch und mit minimaler Verzögerung** ankommen müssen
- Beispiele: VoIP, Videochats oder industrieller Steuerung
- **Priorisierung** von Echtzeitdaten im Netzwerk, z. B. durch **Low-Latency-Switches** und **dedizierte Bandbreite**

Umgang mit Fehlern & Paketverlust

Maßnahme	Funktion
Forward Error Correction (FEC)	Fehlerbehebung durch zusätzliche Datenpakete
Redundanz (z. B. bei Streams)	Paketverlust kann durch doppelte Pakete ausgeglichen werden
NACK-Handling (bei RTP)	Empfänger signalisiert fehlende Pakete
Pufferung / Jitter-Buffer	Kurzzeitige Speicherung zum Ausgleich von Schwankungen

FibreChannel

- Netzwerkprotokoll und eine Transporttechnologie, die für den schnellen und sicheren Datentransfer zwischen Servern und Speichersystemen (SANs) entwickelt wurde
- Es wird primär in Rechenzentren eingesetzt, um Blockdaten extrem schnell und ausfallsicher zu übertragen – unabhängig vom normalen LAN

- Eigenschaften:
  - Hohe Geschwindigkeit
  - Deterministische Latenz
  - Separate Infrastruktur
  - Skalierbar & stabil
  - Hochverfügbar

Merkmal	Beschreibung
Geschwindigkeit	Typisch 8, 16, 32 oder 64 Gbit/s pro Port
Verbindungstyp	Punkt-zu-Punkt, Switched Fabric, Arbitrated Loop
Topologie	Meist Switched Fabric mit FC-Switches
Transportart	Blockbasiert (wie SATA oder SCSI), nicht dateibasiert
Physikalisch	Glasfaser oder Kupfer (obwohl „Fibre“ drinsteht)
Zuverlässigkeit	Sehr hoch, mit Fehlerkorrektur und garantierter Zustellung
Verwendung	SANs, Datenbanken, virtuelle Infrastrukturen, Backups

Ethernet versus FibreChannel

Kriterium	Fibre Channel (FC)	Ethernet
Zweck	Hochleistungszugriff auf Storage (Blockbasiert)	Allgemeine Datenkommunikation (Web, E-Mail, File, etc.)
Typische Verwendung	SANs in Rechenzentren	LANs, Intranets, WAN-Verbindungen
Transportiert…	Speicherblöcke (SCSI, NVMe)	Dateien, Pakete, Streams (TCP/IP, UDP)
Architektur	Eigene dedizierte Infrastruktur (HBA, FC-Switches)	Standard-Netzwerkinfrastruktur (NIC, Ethernet-Switches)
Datenrate	1–128 Gbit/s (typisch 8, 16, 32, 64 Gbit/s)	10 Mbit/s – 400 Gbit/s (Ethernet-Standards)
Latenz / Jitter	Sehr gering, deterministisch	Variabel, abhängig vom Netzwerkverkehr
Fehlertoleranz	Integriert (z. B. Buffer Credit, Flow Control)	Nicht immer garantiert, hängt vom Protokoll ab
Kosten	Hoch (Spezialhardware, FC-Switches, HBAs)	Günstiger, breite Verfügbarkeit
Komplexität	Hoch (WWNs, Zoning, Fabric Management)	Einfacher, weit verbreitet
Skalierbarkeit	Hoch, aber auf Storage ausgerichtet	Sehr hoch, flexibel einsetzbar
Physikalische Medien	Glasfaser (FC), Kupfer selten	Kupfer (Twisted Pair), Glasfaser (z. B. 10GBase-SR)
Sicherheit	Trennung durch dediziertes Netz	Muss durch VLANs, ACLs, Firewalls abgesichert werden
Protokolle	FCP (Fibre Channel Protocol, trägt z. B. SCSI)	TCP/IP, HTTP, FTP, DNS etc.

HTTPS 1/2

Hypertext Transfer Protocol Secure

- sichere Variante des HTTP-Protokolls, mit dem Webseiten im Internet übertragen werden
- verwendet Verschlüsselung (TLS/SSL), um die Kommunikation zwischen Client (z. B. Browser) und Server abzusichern
- Ziel: Schutz vor Mitlesen, Manipulation und Identitätsdiebstahl

HTTPS 2/2

Wie funktioniert HTTPS?

- **Verbindungsaufbau:**
  - Der Browser (Client) stellt eine Verbindung zum Webserver her – ähnlich wie bei HTTP.
  - Es wird **statt Port 80 der Port 443** verwendet.
- **TLS/SSL-Handshake:**
  - Der Server sendet sein **digitales Zertifikat** (z. B. von Let's Encrypt, DigiCert).
  - Der Client prüft, ob das Zertifikat gültig und vertrauenswürdig ist.
  - Danach wird ein **sicherer Schlüssel** (Session Key) ausgetauscht – meist mit RSA oder Diffie-Hellman.
- **Verschlüsselte Kommunikation:**
  - Alle Daten (Login, Formulare, Cookies usw.) werden **verschlüsselt übertragen**.
  - Dritte können den Datenverkehr nicht mitlesen oder verändern.

SSL und TLS

Secure Sockets Layer und Transport Layer Security

- Kryptoprotokolle, die eine sichere Verbindung zwischen zwei Systemen (z. B. Browser ↔ Webserver) ermöglichen
- Aufgaben:
  - Daten verschlüsseln (Vertraulichkeit)
  - Integrität garantieren (keine Manipulation möglich)
  - Identität des Kommunikationspartners prüfen (Authentizität)

- **Heute ist TLS 1.2 oder 1.3 Standard. SSL sollte nicht mehr verwendet werden.**

TLS Handshake

Client Hello
→ Der Browser sendet:

- TLS-Version,
- unterstützte Verschlüsselungsmethoden,
- Zufallswert

Server Hello
→ Der Server antwortet mit:

- Zertifikat (z. B. von Let's Encrypt),
- gewählter Verschlüsselung,
- eigenem Zufallswert

Zertifikatsprüfung
→ Der Client prüft die **Echtheit** des Zertifikats anhand der **CA (Certificate Authority)**

Schlüsselaustausch
→ Gemeinsamer Sitzungsschlüssel wird ausgehandelt (z. B. via Diffie-Hellman)

Handshake abgeschlossen
→ Ab jetzt erfolgt **alle Kommunikation verschlüsselt**

Mail-Protokolle

Protokoll	Zweck	Port (TLS)	Server-Speicherung	Synchro-nisation	Typ	Geeignet für…	Vorteile	Nachteile
SMTP	Versand	587	–	–	Push	Alle Mail-Server	Weltweit verbreitet, einfach, unterstützt Authentifizierung	Keine Verschlüsselung ohne TLS, kein Abruf
POP3	Abruf, Löschung	995	❌ (nur lokal)	❌	Pull	Einzel-PCs, Offline-Zugriff	Einfach, schnell, wenig Bandbreite, offline nutzbar	Keine Synchronisation, Gefahr von Datenverlust
IMAP	Abruf, Verwaltung	993	✅	✅	Pull	Mobile Geräte, moderne Mail-Clients	Modern, synchronisiert Geräte, Mails bleiben auf Server	Höherer Serverplatzbedarf, abhängig von Online-Zugang

POP3

Post Office Protocol v3

Eigenschaft	Beschreibung
Zweck	Abruf von E-Mails vom Server (einfach)
Typ	Pull
Port (Standard)	110 (unverschlüsselt), 995 (verschlüsselt)
Arbeitsweise	E-Mails werden vom Server gelöscht nach Abruf (standardmäßig)
Speicherung	Lokal auf dem Client
Synchronisierung	Keine (für mobile Geräte ungeeignet)

SMTP

Simple Mail Transfer Protocol

Eigenschaft	Beschreibung
Zweck	Versand von E-Mails
Typ	Push (vom Client/Server zum Empfänger)
Port (Standard)	25, 587 (TLS), 465 (SSL, veraltet)
Richtung	Vom E-Mail-Client oder -Server zum Zielserver
Authentifizierung	Ja (ab Port 587 üblich)
Sicherheit	TLS (STARTTLS oder SMTPS) empfohlen

SMTP schickt E-Mails **weg** – es ist kein Abrufprotokoll

IMAP

Internet Message Access Protocol

Eigenschaft	Beschreibung
Zweck	Abruf & Verwaltung von E-Mails auf dem Server
Typ	Pull
Port (Standard)	143 (STARTTLS), 993 (SSL)
Arbeitsweise	Mails bleiben auf dem Server, synchronisiert
Synchronisierung	Ja, ideal für mehrere Geräte
Speicherbedarf	Serverseitig

LDAP

- Ermöglicht den Zugriff auf Daten, die in einem hierarchischen Verzeichnis gespeichert sind, z. B. Benutzerkonten, Gruppen, Kennwörter und Berechtigungen
- Zentralisierung und Standardisierung von Authentifizierung und Autorisierung von Benutzern über verschiedene Anwendungen und Systeme hinweg

- Eigenschaften:
  - Flexibel
  - skalierbar
  - mit vielen Plattformen und Tools kompatibel

- TLS zusätzlich zur Verschlüsselung erforderlich
- Basiert auf einem Single-Sign-On-Mechanismus (SSO), was bedeutet, dass
  - Einmalige Eingabe der Anmeldeinformationen
  - kompromittierter Berechtigungsnachweis gibt Zugriff auf mehrere Ressourcen

SNMP

Simple Network Management Protocol

- Netzwerkprotokoll zur Überwachung und Steuerung von Netzwerkgeräten
- ermöglicht zentralen Management-Systemen (z. B. Monitoring-Tools) den Zugriff auf Statusinformationen von Geräten wie: Switches, Router, Firewalls, Server, Drucker, USVs

Ziel und Nutzen

- Netzwerkgeräte überwachen, Fehler erkennen und automatisiert reagieren
- Abfragen von Statuswerten (z. B. CPU-Auslastung, Temperatur, Uptime)
- Setzen von Konfigurationsparametern (nur bei v3 empfohlen)
- Alarmmeldungen (Traps) bei Störungen oder Ereignissen

WLAN Standards

1997 BIS HEUTE: WLAN-STANDARDS IM VERGLEICH

Standard	Gängige Bezeichnung	Erstveröffentlichung	Frequenzbereich	Max. Tempo je Antennenstream
IEEE 802.11	–	1997	2,4 Gigahertz	2 Mbps
IEEE 802.11b	WLAN-b	1999	2,4 Gigahertz	44 Mbps
IEEE 802.11a	WLAN-a	1999	5 Gigahertz	108 Mbps
IEEE 802.11g	WLAN-g	2003	2,4 Gigahertz	108 Mbps
IEEE 802.11n	WLAN-n/Wifi 4	2009	2,4 und 5 Gigahertz	150 Mbps
IEEE 802.11ad	WLAN-ad	2012	60 Gigahertz	4600 Mbps
IEEE 802.11ac	WLAN-ac/Wifi 5	2013	5 Gigahertz	866 Mbps
IEEE 802.11ax	WLAN-ax/Wifi 6	2019	2,4 und 5 Gigahertz	1201 Mbps
IEEE 802.11ax	Wifi 6E	2020	2,4 sowie 5 und 6 Gigahertz	1201 Mbps
IEEE 802.11be	WLAN-be/Wifi 7	seit 11/2023	2,4 sowie 5 und 6 Gigahertz	2900 Mbps

Quelle

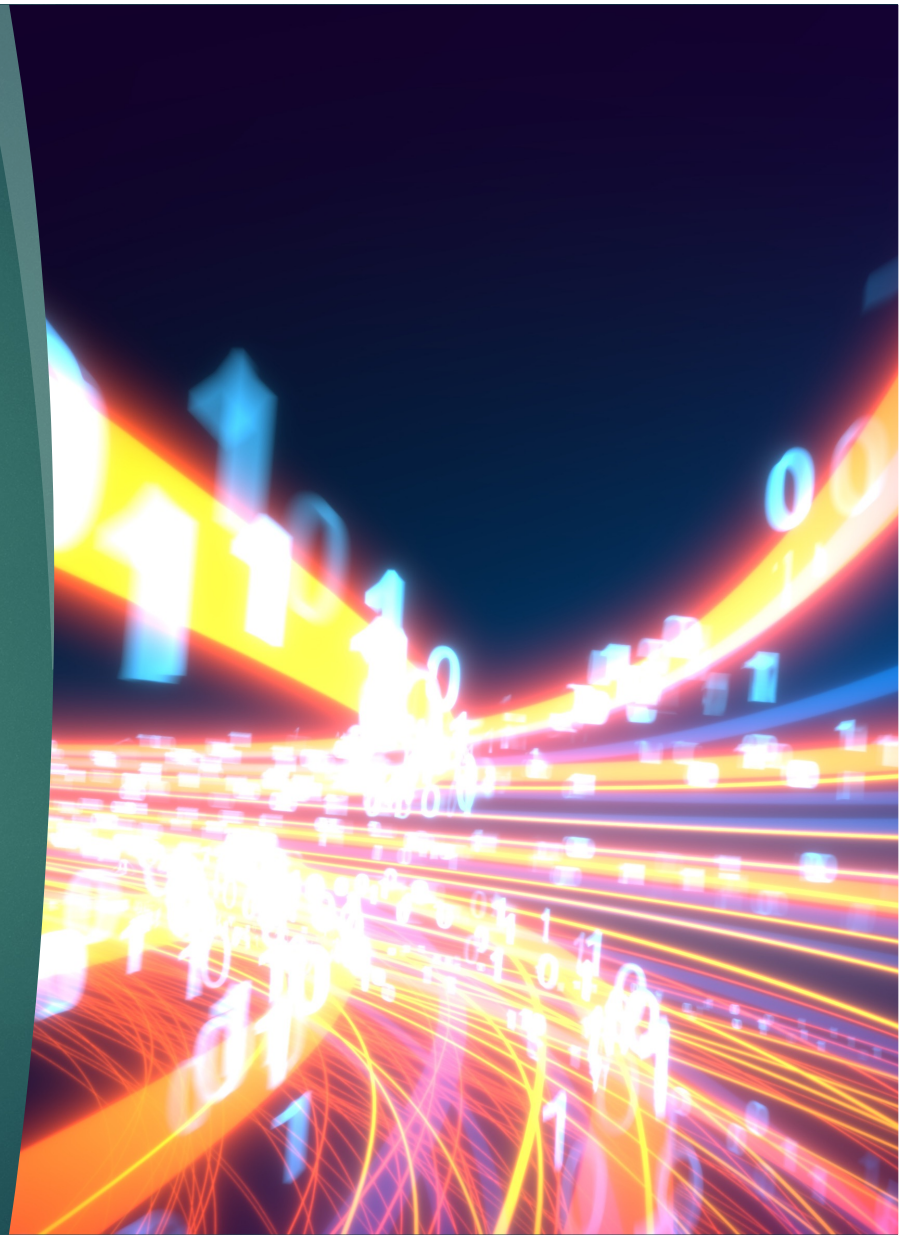
Bluetooth

- drahtloser Funkstandard zur Verbindung von Geräten über kurze Distanzen, bei geringem Energieverbrauch und niedriger Komplexität

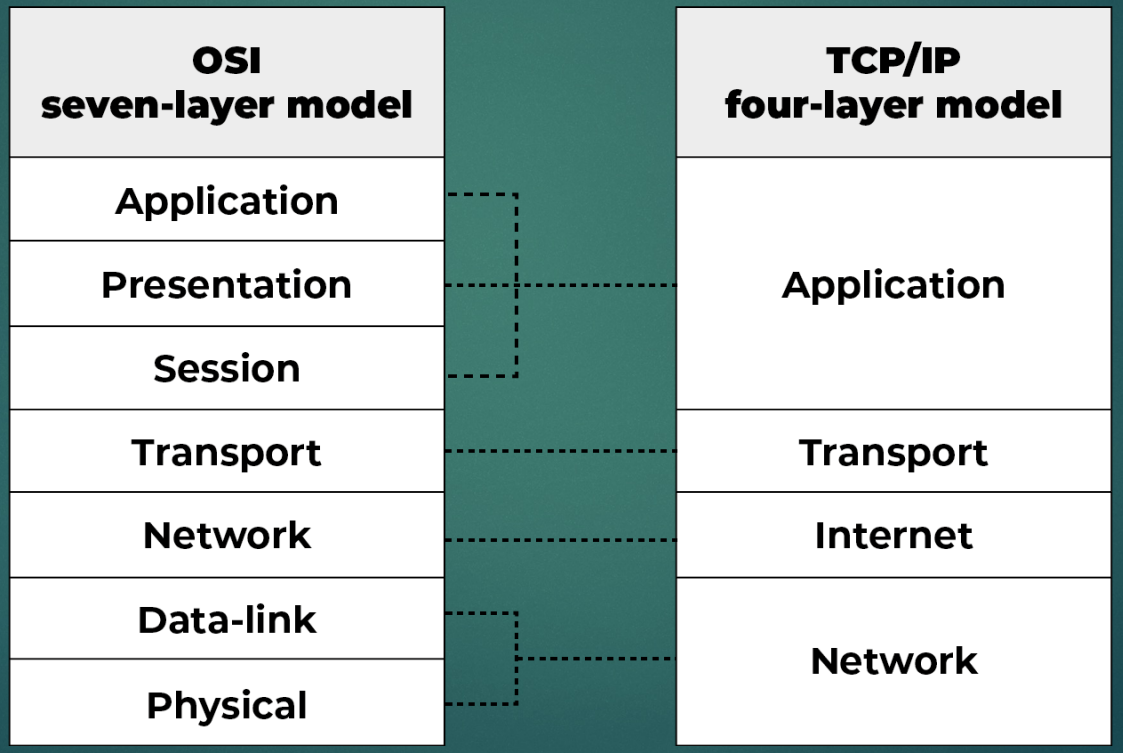
Art	Beschreibung	Beispiele
Bluetooth Classic	Für Audio, Datenübertragungen, längere Sessions	Kopfhörer, Lautsprecher, Freisprechanlagen, Tastatur, Maus
Bluetooth LE	Low Energy – ideal für Sensoren, Smartwatches, IoT (kurze, seltene Datenpakete)	Temperaturfühler, Smartwatch
Bluetooth Mesh	Netzwerkstruktur für IoT-Umgebungen – Geräte fungieren als Weiterleiter	Lichtsteuerung, Rollädenstuerung, Vernetzung medizinischer, industrieller oder landwirtschaftlicher Geräte

03 IP

- OSI vs. TCP/IP
- MAC vs. IP
- IPv4 vs. IPv6
- IPsec
- Öffentliche vs. Private
- IPv4-Klassen
- IPv4 Private Netze
- IPv6-Komponenten
- IPv6-Schreibweise
- IPv6-Sonderadressen
- APIPA vs. SLAAC
- Spezielle Adresstypen
- Begriffsklärungen
- DHCP-Lease
- DNS/Namensauflösung
- Routing
- QoS



OSI vs. TCP/IP 1/2



Quelle

OSI vs. TCP/IP 2/2

Nummer	OSI-Schicht	Englischer Name	TCP/IP-Modell	Verschickte Einheiten	Protokollbeispiele	Kopplungselemente
7	Anwendung	Application	Anwendung	Daten Daten Daten	HTTP, FTP, SMTP, DNS, Telnet	Gateway, Proxy, Layer-4-7-Switch – –
6	Darstellung	Presentation	wie oben	wie oben	wie oben	wie oben
5	Sitzung	Session	wie oben	wie oben	wie oben	wie oben
4	Transport	Transport	Transport	TCP: Segmente UDP: Datagramme	TCP, UDP	wie oben
3	Vermittlung-/Paket	Network	Internet	Pakete	IP, ICMP, IPsec	Router
2	Sicherung	Data Link	Netzzugriff	Frames	Ethernet,WLAN, MAC	Switch, Bridge, Access Point
1	Bitübertragung	Physical	wie oben	Bits	Token Ring	Kabel, Hub, Repeater

MAC vs. IP

MAC-Adressen

(auch als Hardware-Adressen bezeichnet)

48-Bit-Adressen

Eindeutig jedem Netzwerkgerät (z.B. Computer, Router, Switch) zugewiesen

Adressieren und Übertragung von Datenpaketen auf Schicht 2 (Sicherungsschicht) des OSI-Modells innerhalb eines lokalen Netzwerks (z.B. LAN)

Nur innerhalb eines lokalen Netzwerks verwendet

Vergabe durch Hersteller eines Gerätes

IP-Adressen

(Internet Protocol-Adressen)

32-Bit-Adressen (IPv4) oder 128-Bit-Adressen (IPv6)

Eindeutige Zuweisung zu jedem Gerät innerhalb eines Netzwerks

Adressieren und Übertragung von Datenpakete auf Schicht 3 (Netzwerkschicht) des OSI-Modells innerhalb eines Netzwerks

Verwendung, um Daten über das Internet zu übertragen

IPv4 vs. IPv6

IPv4

- 32-Bit-Adresse
- Unterstützt ursprünglich keine End-to-End-Verschlüsselung
- End-zu-End Verschlüsselung nachträglich mit IPsec standardisiert

IPv6

- 128-Bit-Adressen
- Unterstützt End-to-End-Verschlüsselung (IPsec)

- **Vorteile zu IPv4**
  - Mehr Geräte und Dienste anschließbar
  - Schlankerer Header
- **Nachteile zu IPv4**
  - Länger und komplexer
  - Schwieriger für menschliche Lesbarkeit und Fehlerbehebung

IPsec

- Sicherheitsprotokoll, das IP-Pakete auf Netzwerkschicht (Layer 3) verschlüsselt und absichert
- Gewährleistet Vertraulichkeit, Integrität und Authentizität beim Datenaustausch
- Schützt gesamten IP-Verkehr (im Vergleich zu TLS)

Ziel	Wirkung
Verschlüsselung	Dritte können IP-Daten nicht mitlesen
Authentifizierung	Absender kann verifiziert werden
Integritätsprüfung	Schutz vor Manipulation
Tunneling	Aufbau sicherer Verbindungen über unsichere Netzwerke (z. B. Internet)

Öffentliche vs. private

Öffentliche IP-Adressen

- IP-Adressen, die vom Internet Service Provider (ISP) einer Person oder Organisation zugewiesen werden und für die Kommunikation mit anderen Geräten im Internet verwendet werden
- Eindeutig und öffentlich zugänglich
- Von jedem Gerät im Internet erreichbar

Private IP-Adressen

- In privaten Netzwerken verwendet
- Nicht für die Kommunikation mit dem Internet bestimmt
- Können in jedem Netzwerk verwendet werden
- Sind nicht eindeutig

IPv4-Klassen

Netzwerk-Klasse	Adressbereich der Netzadressen	Erstes Oktett	Maximale Host-Adressen	Einsatzzweck
Klasse A (Oktett 1=Netz)	1.0.0.0 bis 127.0.0.0	0*** ****	16. 777. 214	Sehr große Netzwerke (z. B. Länder)
Klasse B (Oktett 1+2=Netz)	128.0.0.0 bis 191.255.0.0	10** ****	65.534	Mittlere Netzwerke (z. B. Unternehmen)
Klasse C (Oktett 1,2+3=Netz)	192.0.0.0 bis 223.255.255.0	110* ****	254	Kleine Netzwerke
Klasse D (speziell)	224.0.0.0 bis 239.255.255.255	1110 ****	Nicht verfügbar	Multicast-Gruppen
Klasse E (speziell)	240.0.0.0 bis 255.255.255.255	1111 ****	Nicht Verfügbar	Experimentelle Adressen

IPv4 Private Netze

Privates Klasse-A-Netzwerk	10.0.0.0 mit der Subnetzmaske 255.0.0.0 = ein Klasse-A-Netz
Privates Klasse-B-Netzwerk	172.16.0.0 (bis 172.31.255.255) mit der Subnetzmaske 255.240.0.0 = 16 Klasse-B-Netze
Privates Klasse-C-Netzwerk	192.168.0.0 (bis 192.168.255.255) mit der Subnetzmaske 255.255.0.0 = 255 Klasse-C-Netze

IPv6-Komponenten

Standortpräfix

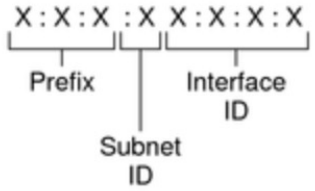
- 48 Bit auf der linken Seite (häufig auch 56 Bit)
- Auch andere Längen möglich, je nach benötigter Anzahl an Hosts
- Beschreibt die öffentliche Topologie

Subnetz-ID

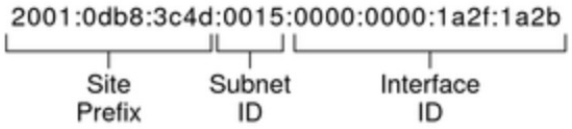
- 16-Bit (häufig auch 8 Bit)
- Dem eigenen Standort zugewiesen
- Beschreibt die private Topologie
  - bzw. Standorttopologie

Schnittstellen-ID

- 64 Bit auf der rechten Seite
- Auch als Token bezeichnet
- Oft Automatisch anhand der MAC-Adresse der Schnittstelle erstellt



Example:



Quelle

IPv6 - Schreibweise

Jeweils 2 Bytes werden zu einem 4-stelligen Block hexadezimaler Werte zusammengefasst, die durch einen Doppelpunkt getrennt sind

- Beispiel: 2001:0db8:85a3:08d3:1319:8a2e:0005:7344

Führende Nullen eines Blockes dürfen weggelassen werden

- Beispiel: 2001:db8:85a3:8d3:1319:8a2e:5:7344

Ein „Null-Block“ wird als „0 geschrieben“

Mehrere „Nuller-Blöcke“ können durch zwei Doppelpunkte (::) ersetzt werden

- Beispiel:
  - Aus: 2001:0db8:0000:0000:0000:0000:1428:57ab
  - Wird: 2001:db8::1428:57ab.

IPv6-Adressen mit Sonderfunktionen

:: oder ::0

- undefinierte IPv6 Adresse – entspricht der IPv4-Adresse 0.0.0.0

::1

- lokales Interface – entspricht der IPv4-Adresse 127.0.0.1 (Loopbackadresse)

0:0:0:0:0:ffff::

- „IPv4 mapped“ IPv6-Adressen. Die letzten 32 Bit enthalten die IPv4-Adressen. Auf diese Weise können geeignete Router zwischen IPv4 und IPv6 konvertieren und beide Welten miteinander verbinden.

weitere Sonder-Adressen: siehe „Spezielle Adresstypen“

APIPA und SLAAC

APIPA (Automatic Private IP Addressing)

- Ermöglicht in einem DHCP Netzwerk eine IPv4-Adresse aus dem Bereich 169.254.0.1 bis 169.254.255.254 automatisch zu beziehen, wenn kein DHCP-Server verfügbar ist
- Gerät wählt die nächste freie Adresse im Netzwerk von 169.254.0.1 bis 169.254.255.254 automatisch an
- Standardmäßig eingeschalten

SLAAC (Stateless Address Autoconfiguration)

- Ermöglicht, dass Computer automatisch eine IPv6-Adresse beziehen, wenn kein DHCP-Server verfügbar ist
- Verwendetes Präfix: fe80::
- Nutzt die Router Advertisement (RA) -Nachrichten, die von Routern im Netzwerk gesendet werden, um die notwendigen Informationen zu erhalten, um eine eindeutige IPv6-Adresse zu generieren
- Vor allem in kleineren Netzwerken und IoT-Umgebungen nützlich, die keinen DHCP-Server verwenden möchten

Spezielle Adresstypen

Link Local Addresses

- Spezielle Art von IP-Adressen, die nur innerhalb eines lokalen Netzwerks automatisch vergeben werden (per APIPA/SLAAC) und nicht routbar sind

Unique Local Addresses (ULA)

- Spezielle Art von IPv6-Adressen, die nur innerhalb eines privaten Netzwerks verwendet werden und nicht routbar sind
- Präfix: fc00::
- Dazu gedacht, eine Alternative zu den privaten IPv4-Adressen zu sein, i.d.R dennoch global eindeutig

Multicast

- Technik, bei der ein Datenpaket von einem Sender an mehrere Empfänger gleichzeitig gesendet wird
- IPv4-Adressbereich: 224.0.0.0/4
- Präfix IPv6: ff00::

Global Unicast

- Art von IP-Adressen, die für die globale Internetverbindung verwendet werden
- weltweit eindeutig
- Von Internet Service Providern (ISPs) zugewiesen
- IPv6: Präfix ist standardmäßig auf 48 Bit festgelegt

Begriffklärung

Subnetting

- Verfahren, bei dem ein großes Netzwerk in kleinere Unternetze unterteilt wird
- Ermöglicht die Erhöhung der Netzwerkeffizienz durch Reduktion der Anzahl der Geräte, die in einem Netzwerk zugelassen sind

Netzwerkmaske

- 32-Bit-Folge, die verwendet wird, um die Netzwerk- und Host-Teile einer IP-Adresse voneinander zu trennen
- Gibt an, welche Bits der IP-Adresse zum Netzwerk gehören und welche zum Host

CIDR (Classless Inter-Domain Routing)

- Methode zur Darstellung von IP-Adressen und Netzwerkmasken
- Ermöglicht flexiblere Netzwerkgröße und Maximierung der Anzahl an IP-Adressen
- Die ersten Bits (entsprechend der Länge des Präfixes) werden als Netzwerk-ID verwendet, die restlichen Bits als Host-ID

Broadcast

- Netzwerkbegriff, der sich auf die Übertragung von Daten an alle Geräte in einem Netzwerk bezieht
- Broadcast-Paket wird an alle Geräte im Netzwerk gesendet, anstatt nur an ein bestimmtes Gerät
- Werden verwendet, um wichtige Informationen wie die Zuweisung von IP-Adressen über DHCP oder die Suche nach Netzwerkdiensten zu verbreitet

DHCP-Lease

Discover:

- Der DHCP-Client sendet eine Broadcast-Nachricht im Netzwerk aus, um DHCP-Server zu suchen.

Offer:

- Der DHCP-Server, der die Broadcast-Nachricht empfängt, sendet ein Angebot an den Client mit der Information über die nächste verfügbare IP-Adresse, die Subnetzmaske, der Ip-Adresse des DHCP-Servers und die Lease-Zeit.

Request:

- Der DHCP-Client sendet eine Meldung an den/die DHCP-Server, in der er die ausgewählte IP-Adresse bestätigt. (Bei mehreren DHCP-Servern sucht sich der Client eine IP-Adresse heraus)

Acknowledge:

- Der DHCP-Server sendet eine Bestätigung an den Client, in der er die zugewiesene IP-Adresse und weitere Informationen wie Gateway-Adresse und DNS-Server bestätigt.

Namensauflösung

- Prozess, bei dem ein Hostname in eine IP-Adresse umgewandelt wird

DNS (Domain Name System)	Hosts-Datei
• Protokoll, das es ermöglicht, Domainnamen in IP-Adressen aufzulösen • Verwendet eine Hierarchie von Servern, die Einträge enthalten, die die Zuordnung von Namen zu IP-Adressen darstellen • Client kann eine Anfrage an einen DNS-Server senden, der die Anfrage an einen anderen Server weiterleitet, bis die gewünschte IP-Adresse gefunden wird	• Lokale Textdatei, die auf jedem Computer gefunden werden kann und die Zuordnung von Namen zu IP-Adressen enthält • Vorteil: schnell und einfach

Beispiele für DNS-Einträge

A-Einträge sind Einträge, die einen DNS-Namen mit einer IP-Adresse verknüpfen

AAAA-Einträge sind ähnlich wie A-Einträge, nur für IPv6-Adressen

NS-Einträge (Name Server-Einträge) enthalten Informationen über die DNS-Server, die für eine bestimmte Domain verantwortlich sind

PTR-Einträge (Pointer-Einträge) ermöglichen eine „umgekehrte“ Namensauflösung, also um aus einer IP-Adresse den Hostnamen zu machen

MX-Einträge (Mail Exchange-Einträge) enthalten Informationen darüber, welcher Mailserver für eine Domain zuständig ist. Der MX-Eintrag verweist auf einen A-Eintrag

SOA-Einträge (Start of Authority) enthalten Informationen über den primären DNS-Server, den Verantwortlichen der Domain und die Aktualisierungszeiten

CNAME-Einträge (Canonical Name) enthalten eine Weiterleitung von einem Alias-Domainnamen zu einem echten Domainnamen

Routing

- Prozess, bei dem Datenpakete in einem Netzwerk von einem Quell- zu einem Zielrechner weitergeleitet werden, unter der Verwendung von Routingtabellen
- Routingtabellen
  - Enthalten Informationen darüber, welche Wege die Datenpakete nehmen sollen, um ihr Ziel zu erreichen
  - Enthält Zielnetzwerke und die nächste Hop-Adresse (das nächste Gerät, an das das Datenpaket weitergeleitet werden soll)
  - Statisches Routing: Routingtabellen manuell von einem Netzwerkadministrator konfiguriert, bleiben während des Betriebs unverändert
  - Dynamisches Routing: Routingtabellen automatisch von einem Router erstellt und aktualisiert, indem dieser Routinginformationen von anderen Routern im Netzwerk erhält

Wenn ein Router ein Datenpaket erhält, sucht er in seiner Routingtabelle nach dem Zielnetzwerk und leitet das Paket dann an die nächste Hop-Adresse weiter. Auf diese Weise wird das Datenpaket schrittweise von Router zu Router durch das Netzwerk gesendet, bis es das Ziel erreicht hat.

Dynamisches Routing - Protokolle

RIPv2

- Routing Information Protocol
- Distance-Vector-Protokoll
- Maximale Distanz: 14 Router
- Unterstützt Load Balancing

OSPF

- Open Shortest Path First
- Link-State-Protokoll
- Geringe Konvergenszeit
- Routen-Berechnung auch anhand von Geschwindigkeit und Zuverlässigkeit einer Verbindung
- Unterstützt Load Balancing

Quality of Service

- Ermöglicht, die Leistung und die Verfügbarkeit von Netzwerkdiensten zu steuern und zu gewährleisten
- Geschäftskritische Anwendungen wie VoIP und SIP bekommen eine höhere Priorität und damit eine höhere Leistung und Verfügbarkeit

VoIP (Voice over IP)

- Durchführung von Sprachtelefonie über das Internet oder andere IP-basierte Netzwerke
- Nutzt die QoS-Funktionen, um die Qualität der Sprachübertragung zu gewährleisten, insbesondere die Latenzzeit und die Paketverlustrate

SIP (Session Initiation Protocol)

- Protokoll zum Initiieren, Ändern sowie Beenden von VoIP-Sessions
- Ermöglicht die Steuerung von Anrufen, die Übertragung von Medien (z.B. Sprache, Video) und die Übertragung von Daten während einer VoIP-Session

Übung
IPv6-Schreibweise

IPv6 ausgeschrieben	IPv6 Kurzschreibweise
fe80:00aa:0016:b001:0151:23f3:005a:0613	
	fe80:127:0:33:5:200:0:1b2c
2001:0000:0000:0000:f121:2134:a001:1513	
	ff31:1200::2034:1424
	fe82::ff:1:2
0000:0000:0000:ffff:0192:0168:0001:0152	
fe80:0000:0000:0001:0000:0000:0010:1000	
	fe80::55:e:169
	::ffff:192.168.1.172
	::1

Lösung
IPv6-Schreibweise

IPv6 ausgeschrieben	IPv6 Kurzschreibweise
fe80:00aa:0016:b001:0151:23f3:005a:0613	**fe80:aa:16:b001:151:23f3:5a:613**
fe80:0127:0000:0033:0005:0200:0000:1b2c	fe80:127:0:33:5:200:0:1b2c
2001:0000:0000:0000:f121:2134:a001:1513	**2001::f121:2134:a001:1513**
ff31:1200:0000:0000:0000:0000:2034:1424	ff31:1200::2034:1424
fe82:0000:0000:0000:0000:00ff:0001:0002	fe82::ff:1:2
0000:0000:0000:ffff:0192:0168:0001:0152	**::ffff:192:168:1:152**
fe80:0000:0000:0001:0000:0000:0010:1000	**fe80::1:0:0:10:1000**
fe80:0000:0000:0000:0000:0055:000e:0169	fe80::55:e:169
0000:0000:0000:ffff:0192:0168:0001:0172	::ffff:192.168.1.172
0000:0000:0000:0000:0000:0000:0000:0001	::1

06 Übertragungsmedien

- Primäre, sekundäre und tertiäre Verkabelung
- Übertragungsmodi
- LWL
- Twisted-Pair-Kabel
- DIN EN 50173-1
- EM-Verträglichkeit

Primäre, sekundäre und tertiäre Verkabelung

- **strukturieren Gebäudeverkabelung** (nach DIN EN 50173, ISO/IEC 11801)

Ebene	Beschreibung	Bereich / Reichweite	Typisches Medium
Primär	Verbindet **zentrale Hauptverteiler** mit **Gebäudeverteilern** auf einem **Campus**	• Gebäude zu Gebäude • **Lange Strecken** (oft > 100 m)	Meist Glasfaser (LWL)
Sekundär	Verbindet **Gebäudeverteiler** mit **Etagenverteilern** (über **Steigschächte**)	• **Gebäudeinterne Verkabelung** (vertikal) • Längen meist zwischen 50 und 90 m	Glasfaser oder geschirmte Kupferleitungen
Tertiär	Verbindet die **Etagenverteiler** mit den **Arbeitsplatz-Anschlussdosen**	• **Horizontale Verkabelung** (auf einer Etage) • Maximal **90 m Kabellänge** (plus max. 10 m Patchkabel → 100 m Regel)	Kupfer (Twisted Pair)

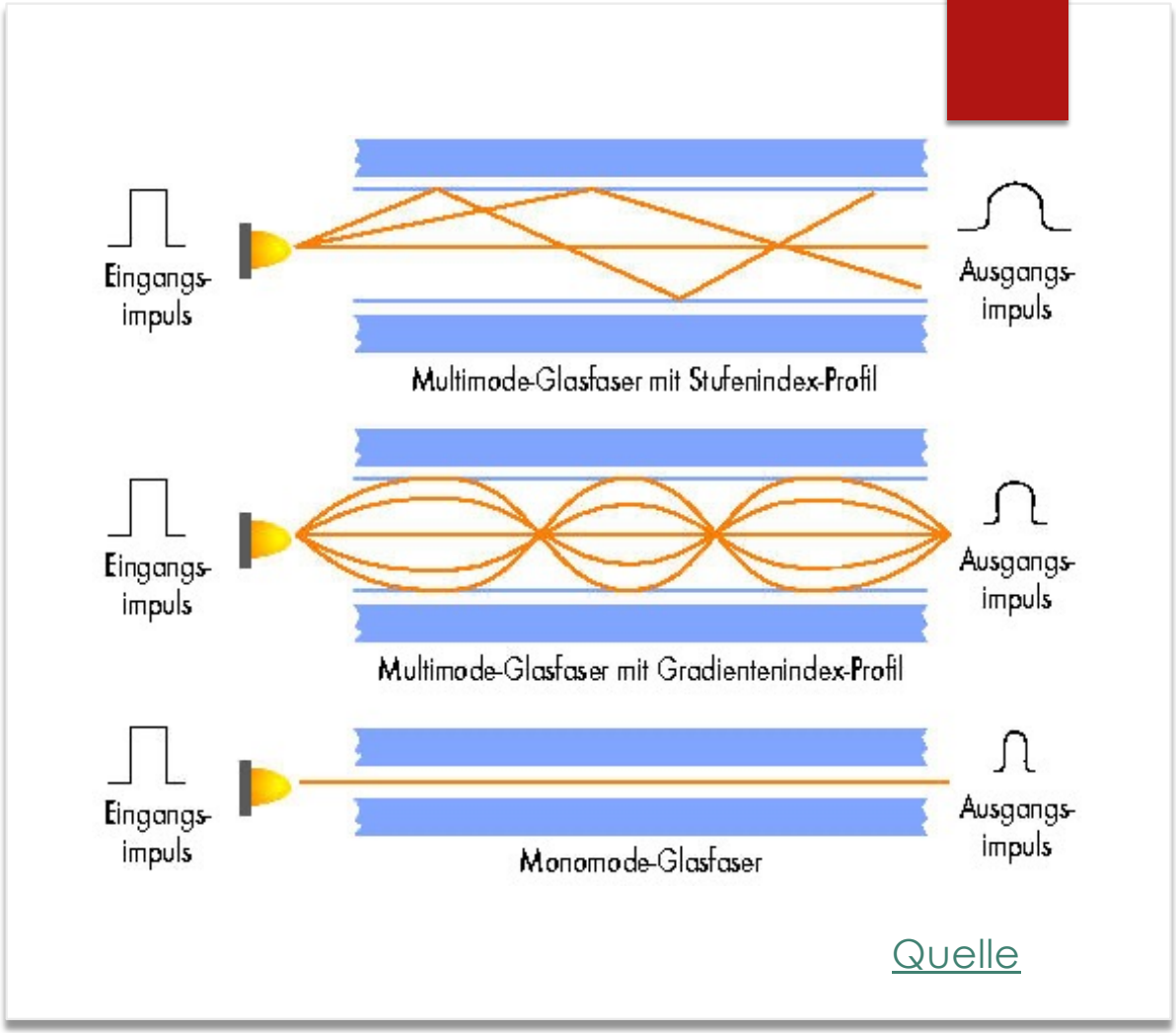
Übertragungsmodi

Modus	Eigenschaften	Richtung der Kommunikation	Gleichzeitig-keit	Beispiel
Simplex	• Kein Rückkanal • Sehr einfache Technik	• Einseitig • nur in eine Richtung	❌	• Fernsehübertragung • Pager
Halbduplex	• Nur eine Seite sendet zur gleichen Zeit • Steuerung der Sendezeit ist nötig	• Beidseitig • aber abwechselnd	❌	• Walkie-Talkie • CB-Funk
Vollduplex	• Zwei separate Kanäle oder Frequenzen • Sehr effiziente Kommunikation	• Beidseitig • gleichzeitig möglich	✅	• Telefonie • Ethernet ab 100 Mbit/s

LWL 1/2

Lichtwellenleiter

- Kabel aus einem lichtleitenden Stoff wie Glas oder spezielle Kunststoffe, die Licht per Totalreflexion leiten
- Bekanntester LWL: Glasfaser



Quelle

LWL 2/2

Multimode-Faser (Stufenindex-Faser)

- relativ großen Durchmesser (> 100 µm), mehrere Moden möglich
- stärkere Dämpfung und kleinere Bandbreite (< 100 MHz·km)
- Auf Grund unterschiedlicher Laufzeiten der verschiedenen Moden tritt eine erhebliche Impulsverbreiterung auf
- Typische Anwendung: Kurze Strecken (< 300 m), heute in der Datenkommunikation nicht mehr verbreitet

Multimode-Faser (Gradientenindex-Faser)

- Änderung des Brechungsindexes vom Kern zum Mantel hin, dadurch „Wellenbewegung“ der Moden
- geringe Laufzeitdifferenzen, geringe Impulsverbreiterung und geringe Dämpfung
- Bandbreite: < 1 GHz·km
- Typische Anwendung: für Lokale Netzwerke (< 500 m).

Single-Mode-Faser

- Kern und Mantel haben unterschiedliche Brechungsindizes
- Durchmesser ist sehr gering (< 9 µm), nur eine Mode möglich
- sehr geringe Dämpfung und große Bandbreite (> 10 GHz·km), keine Impulsverbreiterung
- Typische Anwendung: für Übertragung über große Entfernungen

Twisted-Pair-Kabel 1/4

- paarweise verdrillten Kupferadern zur Reduzierung elektromagnetischer Störungen
- Verdrillung der Adernpaare minimiert Übersprechen und externe Störeinflüsse

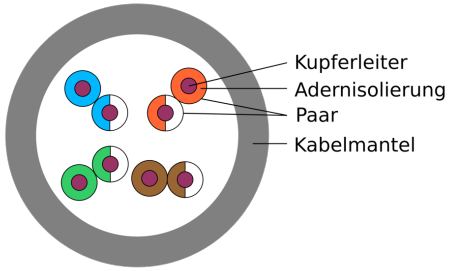
Quelle

Twisted-Pair-Kabel 2/4

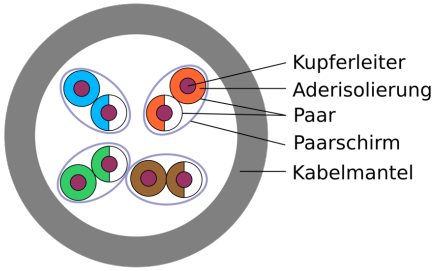
Schirmungstypen Bsp.:

- UTP: Ungeschirmt
- STP: Einzelschirmung jedes Paares
- S/UTP: Geflechtschirm um alle Paare
- S/FTP: Einzelschirmung jedes Paares plus Gesamtschirm

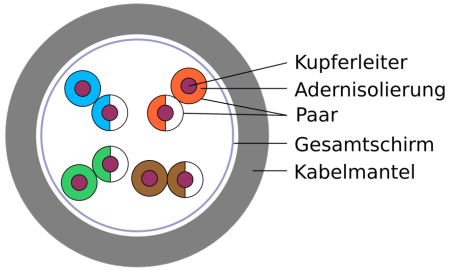
UTP



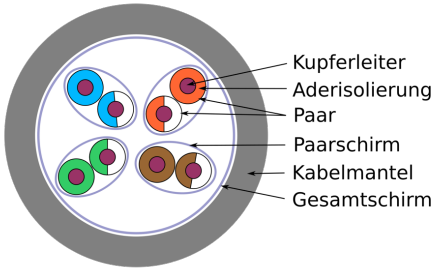
STP



S/UTP



S/FTP



Quelle

Twisted-Pair-Kabel 3/4

- X/YTP
  - X -> Außenverschirmung
  - Y -> Innenverschirmung
  - TP -> Twisted-Pair
  - S -> Geflecht
  - F -> Folie

Industry acronyms	ISO/IEC 11801 name	Cable shielding	Pair shielding
UTP	U/UTP	none	none
STP, ScTP, PiMF	U/FTP	none	foil
FTP, STP, ScTP	F/UTP	foil	none
STP, ScTP	S/UTP	braiding	none
SFTP, S-FTP, STP	SF/UTP	braiding, foil	none
FFTP	F/FTP	foil	foil
SSTP, SFTP, STP PiMF	S/FTP	braiding	foil
SSTP, SFTP	SF/FTP	braiding, foil	foil

Quelle

Kabel-typ	Max. Frequenz	Max. Datenrate	Max. Kabel-länge	Schirmung	Einsatzbereich / Eigenschaften
Cat5e	bis 100 MHz	bis 1 Gbit/s	100 m	UTP (ungeschirmt)	Für einfache Heimnetzwerke; anfällig für Störungen; geeignet für Umgebungen mit geringen Interferenzen
Cat6	bis 250 MHz	bis 1 Gbit/s		UTP oder STP	Reduziertes Übersprechen; bessere Performance als Cat5e; flexibler Einsatzbereich
Cat6a	bis 500 MHz	bis 10 Gbit/s (10GBASE-T)		meist STP	Verbesserte Abschirmung; zuverlässige Übertragung; für anspruchsvollere Netzwerkumgebungen
Cat7	bis 600 MHz	bis 10 Gbit/s (10GBASE-T)		STP (Einzelschirmung je Adernpaar)	Hohe Qualität bei Kupferkabeln; ideal für Rechenzentren und sicherheitskritische Anwendungen
Cat8	bis 2000 MHz	bis 40 Gbit/s (40GBASE-T)	30 m	S/FTP	Rechenzentren und professionellen Umgebungen, in denen hohe Bandbreiten und Geschwindigkeiten erforderlich sind

DIN EN 50173-1

- zentrale **europäische Norm** für die **strukturierte IT-Verkabelung in Kommunikationsnetzen**
- Festlegung **allgemeiner Anforderungen**, die für **alle Arten von Gebäuden und Anwendungen** gelten
- Grundlage für Planung, Installation und Betrieb von Netzwerken, wie z. B.:
  - Büronetzwerke
  - Rechenzentren
  - Industrieanlagen
  - Wohngebäude

Inhalt & Schwerpunkte der DIN EN 50173-1 1/2

- Allgemeine Anforderungen an Verkabelungsinfrastruktur
  - Modularer Aufbau der Verkabelung (Primär-, Sekundär-, Tertiärverkabelung)
  - Trennung zwischen passiver und aktiver Technik
  - Unabhängigkeit von spezifischen Anwendungen (z. B. VoIP, Ethernet, ISDN)
- Struktur der Verkabelung
  - Definition der Verkabelungsebenen (Campus, Gebäude, Etage)
  - Benennung und Anforderungen an:
    - Hauptverteiler (BD = Building Distributor)
    - Etagenverteiler (FD = Floor Distributor)
    - Anschlussdosen (TO = Telecommunications Outlet)
- Leistungsanforderungen
  - Kategorieeinteilung der Kupferkabel (z. B. Cat. 6A, Cat. 7A)
  - Klasseneinteilung der Übertragungsstrecken (z. B. Klasse EA, Klasse F)
  - Anforderungen an Dämpfung, NEXT, PSANEXT etc.

Inhalt & Schwerpunkte der DIN EN 50173-1 2/2

- Medientypen & Schnittstellen
  - Kupfer (symmetrisch, Twisted Pair)
  - Lichtwellenleiter (Multimode/Singlemode)
  - Steckertypen: RJ45, LC, SC, GG45, TERA etc.
- Sicherheits- und EMV-Anforderungen
  - Anforderungen an Schirmung, Erdung, Kabeltrennung (z. B. Strom vs. Daten)
  - Brandschutz und Installationszonen
- Zukunftssicherheit / Lebensdauer
  - Planung für neue Technologien (z. B. 25GBASE-T, 40GBASE-SR4)
  - Mindestlebensdauer der Verkabelung: mind. 10 Jahre

EM-Verträglichkeit

Elektromagnetische Verträglichkeit

- Fähigkeit eines elektrischen oder elektronischen Geräts, elektromagnetische Störungen nicht zu verursachen – und gleichzeitig selbst gegen solche Störungen unempfindlich zu sein

Aspekt	Bedeutung
Störfestigkeit	Das Gerät kann Störungen von außen vertragen, ohne Fehlfunktion
Störaussendung	Das Gerät verursacht keine (oder nur zulässige) elektromagnetischen Störungen
Funktion in EM-Umgebung	Auch im Umfeld anderer elektrischer Geräte bleibt das System funktionsfähig

Maßnahmen zur Verbesserung der EMV

Maßnahme	Erklärung	Beispiel
Schirmung (Shielding)	Kabel oder Gehäuse mit leitfähigem Material schützen	CAT.6A/CAT.7-Kabel mit Schirmung (F/UTP, S/FTP)
Verdrillung von Adern	reduziert Magnetfelder	Twisted Pair
Filterung	EMV-Filter verhindern das Einkoppeln oder Aussenden von Störungen	Netzfilter, Signalfilter in Schaltungen
Erdung / Potentialausgleich	Ableitung von Störströmen zur Erde	Erdung von Patchpanels, Racks, Kabeltrassen
Leitungsführung & Abstand	Trennung von Strom- und Datenleitungen	Trennung von Netzwerkkabeln und Stromleitungen
Normkonforme Kabellängen	Reduziert Resonanzeffekte	

05 Netzwerkdokumentation

- Überblick
- Inhalt
- Beispiel eines Netzplans
- Dokumentationen verständlich, strukturiert und inklusiv gestalten

Netzwerkdokumentation

- Essenzieller Bestandteil in der IT-Infrastruktur
- Präzise Erfassung und Speicherung aller relevanten Informationen über ein Netzwerk, einschließlich der Hardware, Software, und Benutzerkonfigurationen
- Ermöglicht effiziente Verwaltung eines Netzwerkes und Planung zukünftiger Erweiterungen

Inhalt 1/2

Einleitung:

- Überblick über das Netzwerk, Ziele der Dokumentation und Verantwortlichkeiten

Netzwerkübersicht:

- Detaillierte Beschreibung der Netzwerkarchitektur, inklusive Topologie-Diagramme

Geräte und Hardware:

- Dokumentation aller Netzwerkgeräte, einschließlich Router, Switches, Firewalls und Server, mit spezifischen Konfigurationsinformationen

IP-Adressierung:

- Auflistung aller IP-Adressen im Netzwerk, inklusive Subnetze und DHCP-Bereich

Verbindungen und Kabel:

- Detaillierte Aufzeichnungen über physische Verbindungen, Patch-Panels und Kabelwege

Inhalt 2/2

Sicherheit:

- Sicherheitsrichtlinien, Zugangskontrollen und Maßnahmen zur Netzwerksicherheit

Wartungsplan:

- Regelmäßige Wartungsaktivitäten und Ansprechpartner für verschiedene Netzwerkbereiche

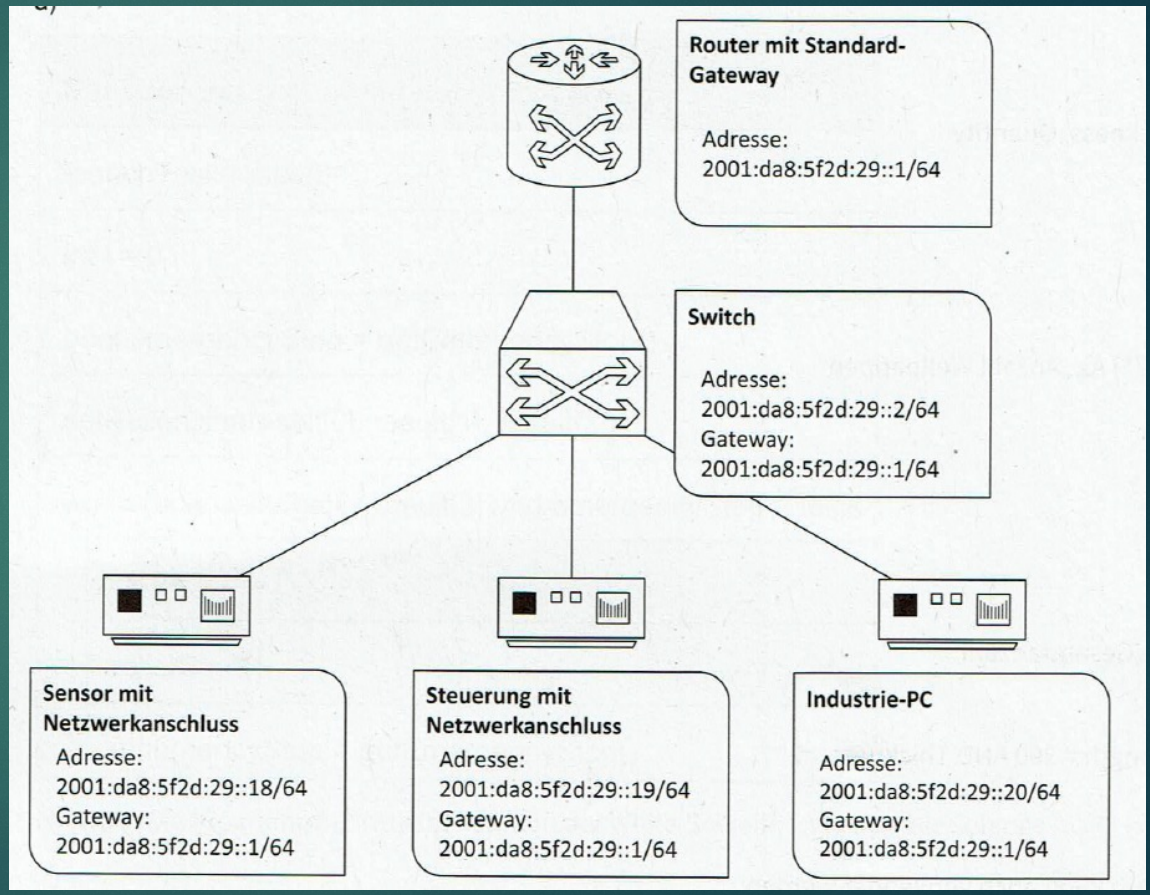
Notfallwiederherstellung:

- Pläne und Prozeduren für die Wiederherstellung des Netzwerks im Katastrophenfall

Versionshistorie:

- Änderungsverlauf und Versionenkontrolle, um eine Übersicht über alle vorgenommenen Änderungen zu behalten

Beispiel eines Netzplans



Dokumentationen verständlich, strukturiert und inklusiv gestalten 1/2

Zielgruppengerecht

Kriterium	Umsetzung in der Praxis
Zielgruppe analysieren	Wer liest die Doku? → Endanwender, Admins, Azubis, Fachkräfte, Management?
Fachbegriffe erklären	Nur verwenden, wenn notwendig – ggf. mit Glossar/Tooltip
Sprachniveau anpassen	Verständlich, aktiv, kurz – z. B. B1/B2 statt akademisches C2
Struktur & Gliederung	Klare Abschnitte, Überschriften, nummerierte Schritte
Praxisnähe sicherstellen	Beispiele, Screenshots, realitätsnahe Anwendungsfälle
Vermeidung von „IT-Sprech“	z. B. statt „inkrementelles Backup“ → „nur neue oder geänderte Dateien sichern“
Formatwahl berücksichtigen	Unterschiedliche Zielgruppen bevorzugen z. B. PDF, Video, Web, Ausdruck

Dokumentationen verständlich, strukturiert und inklusiv gestalten 2/2

Barrierefreiheit

Maßnahme	Erklärung / Tools
Einfache Sprache	Kurze Sätze, keine doppelten Verneinungen, klare Sprache
Textalternativen für Bilder	Alt-Texte bei Grafiken, z. B. in Word, PDF, HTML
Hoher Farbkontrast	z. B. schwarzer Text auf weißem Hintergrund (WCAG-konform)
Barrierefreie Dateiformate	PDF/UA, HTML5 mit semantischen Tags, kein reines Bild-PDF
Tabellen strukturiert gestalten	Kopfzeilen deklarieren, Zellen beschriften
Navigation ermöglichen	Inhaltsverzeichnis, Hyperlinks, Kapitelüberschriften als echte Formatvorlagen nutzen
Kompatibilität mit Screenreadern	PDF- und Word-Dateien testen mit z. B. NVDA, JAWS, VoiceOver

06 Netzwerkkonfiguration

- Siehe Zusatzdokument

07 Barcode, QR-Code, RFID-Chip

- Barcode
- QR-Code
- RFID-Chip

Barcode

Vorteile:	Nachteile:
• Technologie seit Jahrzehnten bewährt • Lassen sich leicht erstellen (am PC oder per Etikettensoftware) • Preisgünstig in der Herstellung • Lesegeräte sind weit verbreitet • Flexibel einsetzbar – von kleinen Verpackungen bis hin zu Lagerregal-Reihen	• Sichtkontakt muss vorhanden sein • Pulkerfassung ist nicht möglich • Funktionsprobleme bei Verschmutzungen und Beschädigungen • Kein Diebstahlschutz implementierbar

QR-Code

Vorteile:	Nachteile:
• Technologie ist etabliert • Mehr Informationen als bei normalen Barcodes einfügbar • Einfache Anfertigung am PC mithilfe eines QR-Codefonts in Word, einer Etikettensoftware oder eines Web-Dienstes • Hohe Verbreitung geeigneter Lesegeräte (unter anderem Smartphones) • Flexibler Einsatz auf beliebig großen Flächen	• Sichtkontakt erforderlich • Keine Pulkerfassung möglich • Empfindlich gegenüber Verschmutzungen und Beschädigungen • Kein Diebstahlschutz für Produkte möglich

RFID-Chip

Vorteile:

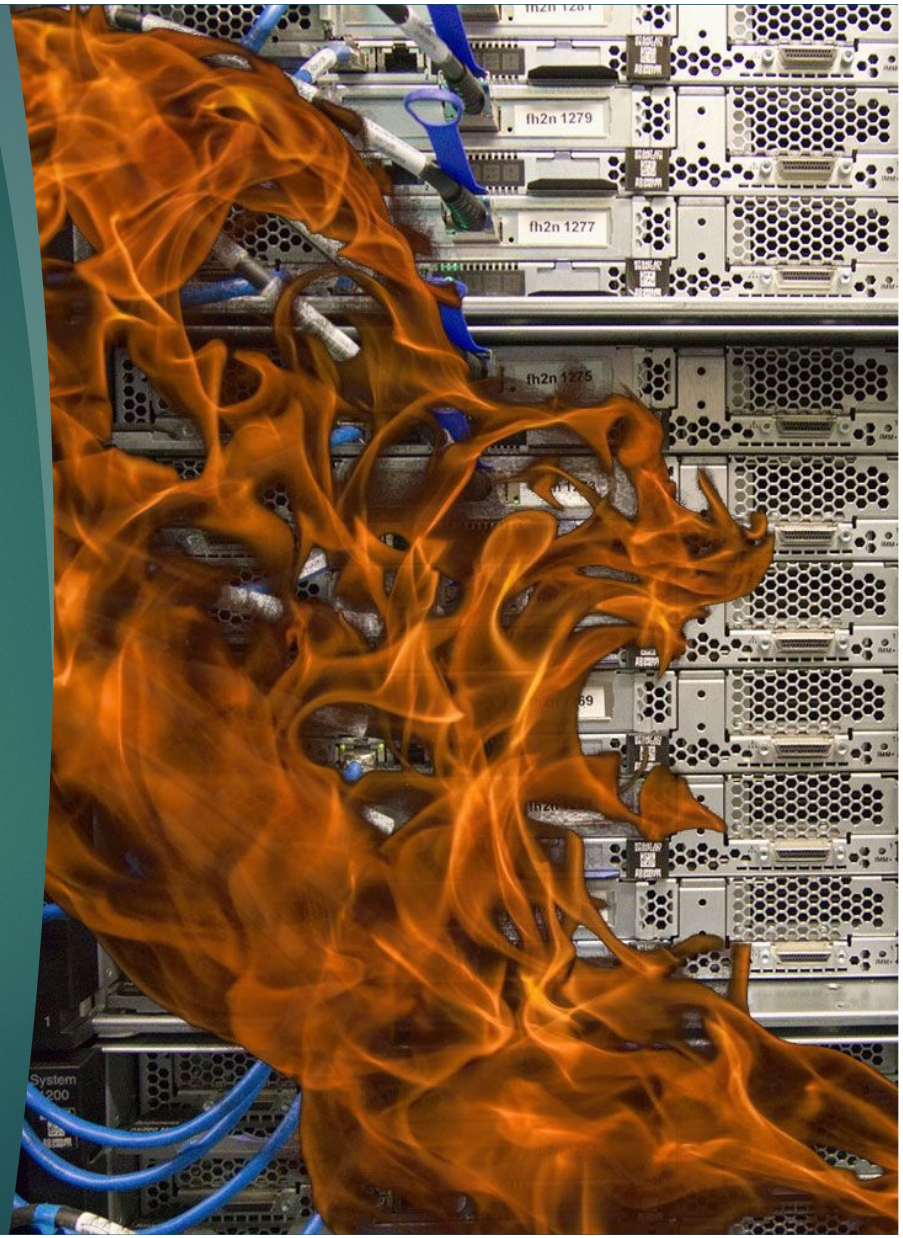
- Kein Sichtkontakt zwischen Sender und Empfänger vonnöten – daher so gut wie unsichtbar zu befestigen
- Praktisch hundertprozentige Ersterkennungsrate
- Schneller Datenaustausch
- Große Distanzen zwischen Transponder und Lesegerät möglich
- Unempfindlich gegen Verschmutzungen, kleinere Beschädigungen und viele andere Umwelteinflüsse
- Präzisere Datenerfassung als bei Barcodes möglich
- Erfassung ist durchgängig in Echtzeit durchführbar

Nachteile:

- Kostenintensiver und komplexer als QR- oder Barcode-Lösungen
- Je nach RFID-Typ empfindlich bei Metallen und Flüssigkeiten

08 Störungen

- Begriffsklärung: Verfügbarkeit
- Ausfallwahrscheinlichkeiten
- MTBF
- Redundanzmodelle
- Verfügbarkeit erhöhen
- Präventive Wartung und Störungsvermeidung
- Störungsbeseitigung
- Monitoring
- Disaster Recovery
- ANR
- S.M.A.R.T.



Begriffsklärung: Verfügbarkeit

Availability

- Anteil der Zeit, in der ein System oder Dienst **funktionsfähig** ist – gemessen am gesamten Betrachtungszeitraum
  - **MTBF (Mean Time Between Failures)** = durchschnittliche Zeit zwischen zwei Ausfällen
  - **MTTR (Mean Time To Repair)** = durchschnittliche Reparaturdauer

$$\text{Verfügbarkeit} = \frac{\text{MTBF}}{\text{MTBF} + \text{MTTR}}$$

Verfügbarkeit in Praxiswerten

Verfügbarkeit	Max. Ausfallzeit pro Jahr	Beschreibung
90 %	≈ 36 Tage	Einfach verfügbar
99 %	≈ 3,65 Tage	Standardserver
99,9 %	≈ 8,8 Stunden	Gut, aber nicht kritisch
99,99 %	≈ 52 Minuten	Hochverfügbar (HA)
99,999 %	≈ 5 Minuten	Mission Critical

Ausfallwahrscheinlichkeiten

- Einzelkomponenten (z. B. Server, Switch, USV)
  - Jedes Gerät hat eine eigene **Ausfallrate** oder **MTBF** (z. B. laut Hersteller)
  - Wahrscheinlichkeiten lassen sich aus Erfahrungswerten, Datenblättern oder Monitoring ableiten
- Serienschaltung von Komponenten **(Abhängigkeit)**
  - Wenn alle Komponenten **nacheinander** geschaltet sind:

$$\text{Gesamtverfügbarkeit} = V_1 \times V_2 \times \ldots \times V_n$$

- Parallelschaltung (Redundanz) **(Fehlertoleranz)**
  - Wenn Systeme **parallel/redundant** geschaltet sind (z. B. Cluster):

$$\text{Ausfallwahrscheinlichkeit}_{\text{redundant}} = P(A) \times P(B) \Rightarrow V = 1 - P_{\text{gesamt}}$$

MTBF

Mean Time Between Failures

- statistische Kenngröße, die angibt, **wie lange ein technisches System durchschnittlich fehlerfrei funktioniert**, bevor es ausfällt

$$\text{MTBF} = \frac{\text{Gesamte Betriebszeit}}{\text{Anzahl der Ausfälle}}$$

- **Wofür wird MTBF verwendet?**
  - **Bewertung der Zuverlässigkeit** von Geräten
  - Grundlage zur Planung der **Verfügbarkeits- und Redundanzkonzepte**
  - Entscheidungshilfe beim **Hardwarekauf**

⚠ **Wichtig:**

- MTBF ist ein **statistischer Mittelwert**, kein Versprechen. Ein Gerät mit hoher MTBF kann trotzdem frühzeitig ausfallen.
- MTBF berücksichtigt **nur Betriebszeit vor Ausfall**, **nicht die Reparaturdauer**.
- Die Reparaturdauer wird durch **MTTR (Mean Time to Repair)** gemessen

Redundanzmodelle

Modell	Bedeutung	Beschreibung	Beispiel
N	Kein Backup	Ein System trägt die komplette Last	Ein einzelner Server ohne Backup
N+1	Ein zusätzliches System	Eine Komponente mehr als notwendig	3 aktive Server, 1 als Standby
N+2	Zwei zusätzliche Systeme	Zwei unabhängige Ausfälle tolerierbar	4 aktive Server, 2 Standby
2N	Vollständige Verdopplung	Alles doppelt vorhanden	Zwei identische Rechenzentren
2N+1	Vollständige Verdopplung + 1	Noch eine Reserve zusätzlich zur 2N	Zwei aktive Cluster + 1 Hot-Standby

Verfügbarkeit erhöhen

- Redundanzen
  - RAID, Cluster
- Monitoring & Wartung
  - Alerting-Systeme, Predicitve Maintenance
- Virtualisierung & Cloud-Technologien
  - Cloud Load Balancing, Disaster Recovery
- Netzwerk- und Stromsicherheit
  - USV, Notstromaggregate, VLANs, Segmentierung
- Organisatorische und vertragliche Maßnahmen
  - SLAs, Notfallpläne, Schulungen, Dokumentationen
- Am Besten: Kombination mehrerer Maßnahmen

Präventive Wartung und Störungsvermeidung 1/2

Anmerkung:
Predictive Maintenance
= Präventive Wartung

Kategorie	Maßnahme	Wirkung / Ziel
Hardware-Wartung	Austausch von Lüftern, Festplatten, Netzteilen nach Lebensdauer	Vermeidung von Ausfällen durch Verschleiß
	Temperaturüberwachung (Sensoren, SNMP)	Schutz vor Überhitzung, gezielte Kühlungsmaßnahmen
	Staubentfernung und Reinigung in Serverräumen	Reduziert thermische Probleme
	Batterietests bei USVs	Sicherstellung unterbrechungsfreier Stromversorgung
Softwarepflege	Regelmäßige Sicherheits- und Systemupdates	Schließen von Sicherheitslücken
	Patchmanagement mit Testumgebung	Minimiert Update-Risiken
	Firmware-Updates von Switches, Router etc.	Vermeidet Inkompatibilitäten und Abstürze
Monitoring & Frühwarnung	Implementierung von Monitoring-Tools (z. B. Zabbix, Nagios)	Frühzeitiges Erkennen von Fehlerzuständen
	Schwellenwertüberwachung (CPU, RAM, Netzlast)	Reagieren, bevor es kritisch wird
	Logfile-Analyse automatisieren	Detektion von Mustern oder Fehlverhalten

Präventive Wartung und Störungsvermeidung 2/2

Und	Maßnahme	Wirkung / Ziel
Datensicherung & Tests	Regelmäßige Backup-Tests (Restore-Probe)	Sicherstellung der Wiederherstellbarkeit
	Notfallübungen (z. B. Stromausfall simulieren)	Reaktionszeit & Abläufe verbessern
Infrastrukturpflege	Klimatisierung (z. B. Serverraumkühlung)	Vermeidet Hardwareausfälle durch Hitze
	Prüfung von Stromkreisen & Lastverteilung	Absicherung gegen Überlast oder Brandgefahr
Prozesse & Organisation	Wartungspläne erstellen und dokumentieren	Vermeidet Vergessen und Unregelmäßigkeiten
	Schulungen für Admins & Techniker	Reduziert menschliche Fehler
	Zugriffs- und Rechtekontrollen regelmäßig prüfen	Vermeidet Fehlkonfigurationen und Missbrauch

Störungsbeseitigung

Neustart betroffener Dienste	Kabelverbindungen prüfen/tauschen
Systemneustart (Reboot)	Switch- oder Router-Port wechseln
Failover auf redundante Systeme	Verbindungsmonitoring aktivieren
Rückspielen eines Backups	Lastverteilung (Load Balancing) anpassen
DNS-Cache leeren	Zeitgleiches Herunterfahren bei Überhitzung
Treiber neu installieren	Remote Management verwenden
Schnittstellen neu starten	System in abgesicherten Modus starten
Benutzer trennen oder sperren	Recovery-Konsole verwenden
Firewall-Regeln anpassen / temporär deaktivieren	Temporär auf Cloud-Ressourcen umschalten
Temporärer Rollback eines Updates	Zugriffsrechte überprüfen / korrigieren

Monitoring

- Ziele:
  - Fehler frühzeitig erkennen
  - Leistung analysieren
  - Ausfälle vermeiden

Monitoringdaten

- Nur relevante, aussagekräftige Metriken erfassen – keine Datenflut, aber auch keine blinden Flecken
- **Herausforderung:**
  - Zu viele Daten = **Überwachung wird unübersichtlich**
  - Zu wenige Daten = **kritische Probleme werden übersehen**
  - **Abhängigkeiten** müssen verstanden werden (z. B. RAM-Spitzen durch Backup-Prozesse)

Typische Monitoringdaten

Kategorie	Beispiele
Systemressourcen	CPU-Auslastung, RAM, Festplattenfüllstand
Netzwerk	Bandbreite, Paketverlust, Schnittstellenstatus
Dienste	Erreichbarkeit von Webservern, Datenbanken etc.
Sicherheit	Login-Versuche, Firewall-Status, Virensignaturen
Hardware	Lüfterstatus, Temperaturen, S.M.A.R.T.-Werte
Applikationen	Datenbankantwortzeit, Queue-Längen, Fehlercodes

Monitoringdaten - Schwellwerte

- **Ziel**:
  - Automatisches Erkennen, wann ein Wert **auffällig oder kritisch** ist – ohne Fehlalarme oder Ignorieren echter Probleme
- **Herausforderung:**
  - Falsch gesetzte Schwellen → **False Positives / False Negatives**
  - Systeme verhalten sich **nicht immer linear** (z. B. kurzer CPU-Peak ≠ Problem)
  - Schwellwerte müssen **regelmäßig überprüft und angepasst** werden
  - Unterschiedliche Systeme/Hersteller haben **abweichende Normalwerte**

Typische Schwellwerte

Typ	Beispiel
Fixe Grenzwerte	CPU > 85 % → Warnung
Trendbasierte Werte	„Mehr als doppelt so viele Anfragen wie im Durchschnitt“
Zeitabhängig	Backuplast nachts erlaubt, tagsüber nicht
Kombinationswerte	Hohe CPU + viele Prozesse = kritisch

Disaster Recovery 1/2

Notfallkonzept

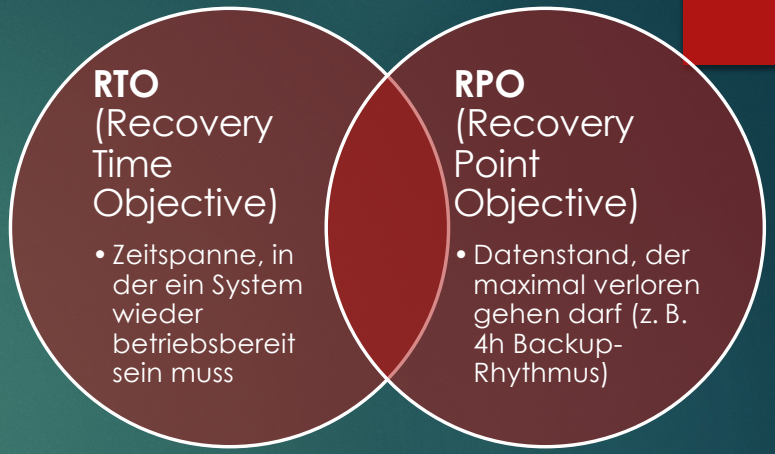
- zentraler Bestandteil der IT-Sicherheit und Betriebsbereitschaft
- beschreibt Maßnahmen, Pläne und Strategien, um im Falle schwerwiegender Störungen den IT-Betrieb schnellstmöglich wiederherzustellen

Ziele

- Minimierung von Ausfallzeiten
- Vermeidung von Datenverlust
- Sicherstellung der Geschäftskontinuität
- Einhaltung gesetzlicher/regulatorischer Anforderungen
- Transparente Verantwortlichkeiten und Abläufe im Krisenfall

Disaster Recovery 2/2

2 zentrale Kennzahlen:



Bestandteil	Beschreibung
Risikoanalyse	Identifikation möglicher Schadensszenarien (z. B. Stromausfall, Ransomware)
Kritikalitätsbewertung	Welche Systeme sind für den Betrieb unverzichtbar?
Wiederanlaufpläne	Schritt-für-Schritt-Anleitungen zur Systemwiederherstellung
RTO / RPO	Zielvorgaben für Wiederanlaufzeit (RTO) und maximal tolerierten Datenverlust (RPO)
Backup-Strategien	Wo, wie oft und wie lange werden Daten gesichert?
Ausweichsysteme	Hot-, Warm- oder Cold-Standby-Systeme
Kommunikationspläne	Wer wird wann wie informiert?
Test- & Trainingsmaßnahmen	Regelmäßige Simulationen, um Ernstfall zu üben

ANR

Automatic Network Reconfiguration

- Mechanismen in Hochverfübarkeits-Netzwerken, bei denen das System automatisch auf Veränderungen reagiert, z. B. bei:
  - **Ausfällen** von Netzwerkkomponenten (Switch, Leitung, Knoten)
  - **Verbindungsänderungen** (z. B. bei mobilen Clients)
  - **Topologieänderungen** (z. B. durch Erweiterung oder Umbau)

Vorteile:

- Erhöhte Verfügbarkeit
- Verbesserte Leistung
- Reduzierter Administrationsaufwand
- Skalierbarkeit

ANR Beispiele

- **Netzwerk-Switches:**
  - Switch-Ausfall -> Pfad wird automatisch neu berechnet, um die beste Route zu finden
- **Cloud-Umgebungen:**
  - dynamisch erstellte und gelöschte VMs erhalten und nutzen ihre Netzwerkkonfiguration automatisch
- **Verteilnetze:**
  - optimierte Netzwerktopologie zur Reduktion von Verlusten, Ausgleich von Lasten sowie Verbesserung der Spannungsqualität (in Stromnetzen)

ANR Technologien

- **DHCP (Dynamic Host Configuration Protocol):**
  - Automatische Zuweisung von IP-Adressen und anderen Netzwerkkonfigurationen
- **IMDS (Instance Metadata Service):**
  - Abruf von Metadaten einschließlich Netzwerkkonfigurationen für VMs in Cloud-Umgebungen
- **Routing-Protokolle:**
  - Zur Ermittlung der besten Pfade für Pakete
  - OSPF, BGP
- **Software Defined Networking (SDN):**
  - zentrale Steuerung und Konfiguration des Netzwerks

S.M.A.R.T. 1/2

- standardisiertes Diagnoseverfahren, das in Speicherlaufwerken integriert ist, um frühzeitig Fehler oder Ausfälle zu erkennen und den Zustand der Laufwerke zu überwachen
- Wichtige Rolle in der Netzwerktechnik , z. B. bei:
  - Servern mit Festplatten
  - NAS-Systemen
  - Storage-Systemen im Rechenzentrum
  - Backup-Servern

S.M.A.R.T. überwacht zahlreiche Sensorwerte und Zustandsparameter, z. B.:

Parameter	Bedeutung
Power-On Hours	Betriebsstunden
Reallocated Sectors	Ersetzte defekte Sektoren
Pending Sectors	Noch nicht zugewiesene (unsichere) Sektoren
Temperatur	Laufwerkstemperatur
Read Error Rate	Fehler bei Lesevorgängen
Spin-Up Time	Zeit, bis die Platte drehbereit ist

S.M.A.R.T. 2/2

S – *Self*

- Festplatte bzw. SSD **überwacht sich selbst**

M – *Monitoring*

- **überwacht laufend** verschiedene Betriebswerte wie Temperatur, Fehler, Betriebszeit usw.

A – *Analysis*

- gesammelten Werte werden **analysiert**, um mögliche Ausfälle frühzeitig zu erkennen

R – *And Reporting*

- Laufwerk kann **Warnmeldungen ausgeben** oder seinen Zustand an ein Monitoring-System **melden**

T – *Technology*

- **Technologie**, die in der Firmware von Laufwerken integriert ist

09 Wichtige Serverarten

- Mailserver
- Webserver
- Groupwareserver
- Datenbankserver
- Proxyserver

Mailserver

- **Aufgabe:**
  - Verwaltung von E-Mails
  - Annahme, Versand, Weiterleitung und Speicherung von Nachrichten
- **Typische Dienste/Protokolle:**
  - SMTP
  - IMAP, POP3
  - Webmail-Zugriff via HTTPS
- **Einsatz:**
  - Unternehmenskommunikation
  - Private Mailprovider

Webserver

- **Aufgabe:**
  - Bereitstellung von Webinhalten (HTML, CSS, JS, PHP etc.)
  - Hosting von Webseiten, APIs, Webanwendungen
- **Typische Dienste/Protokolle:**
  - HTTP, HTTPS
  - WebSockets, CGI, PHP-FPM
- **Einsatz:**
  - Websites, Webshops, Kundenportale

Groupwareserver

- **Aufgabe:**
  - Zentrale Zusammenarbeit im Team (E-Mails, Kalender, Kontakte, Aufgaben)
  - Kombiniert oft Funktionen von Mailserver, Kalender, Chat, Dokumentenablage
- **Typische Dienste/Protokolle:**
  - CalDAV, CardDAV
  - IMAP/SMTP
  - Webinterface
- **Einsatz:**
  - Organisationen, Unternehmen, Bildungseinrichtungen
  - z. B. Microsoft Exchange, Zimbra, Kopano

Datenbankserver

- **Aufgabe:**
  - Verwaltung strukturierter Daten in Datenbanken
  - Bereitstellung von Abfragen (SQL), Speicherung, Indizierung, Transaktionen
- **Typische Dienste/Protokolle:**
  - SQL (MySQL, PostgreSQL, MSSQL, Oracle SQL)
  - JDBC, ODBC, REST-APIs
- **Einsatz:**
  - Backends für Websites, ERP-Systeme, Anwendungen

Proxyserver

- **Aufgabe:**
  - Vermittlung zwischen Client und Zielserver
  - Zugriffskontrolle, Caching, Anonymisierung, Inhaltsfilterung
- **Typische Dienste/Protokolle:**
  - HTTP(S), FTP, SOCKS, DNS
- **Einsatz:**
  - Firmennetzwerke (Webfilter)
  - Performanceverbesserung durch Caching
  - Datenschutz (Anonymisierung)