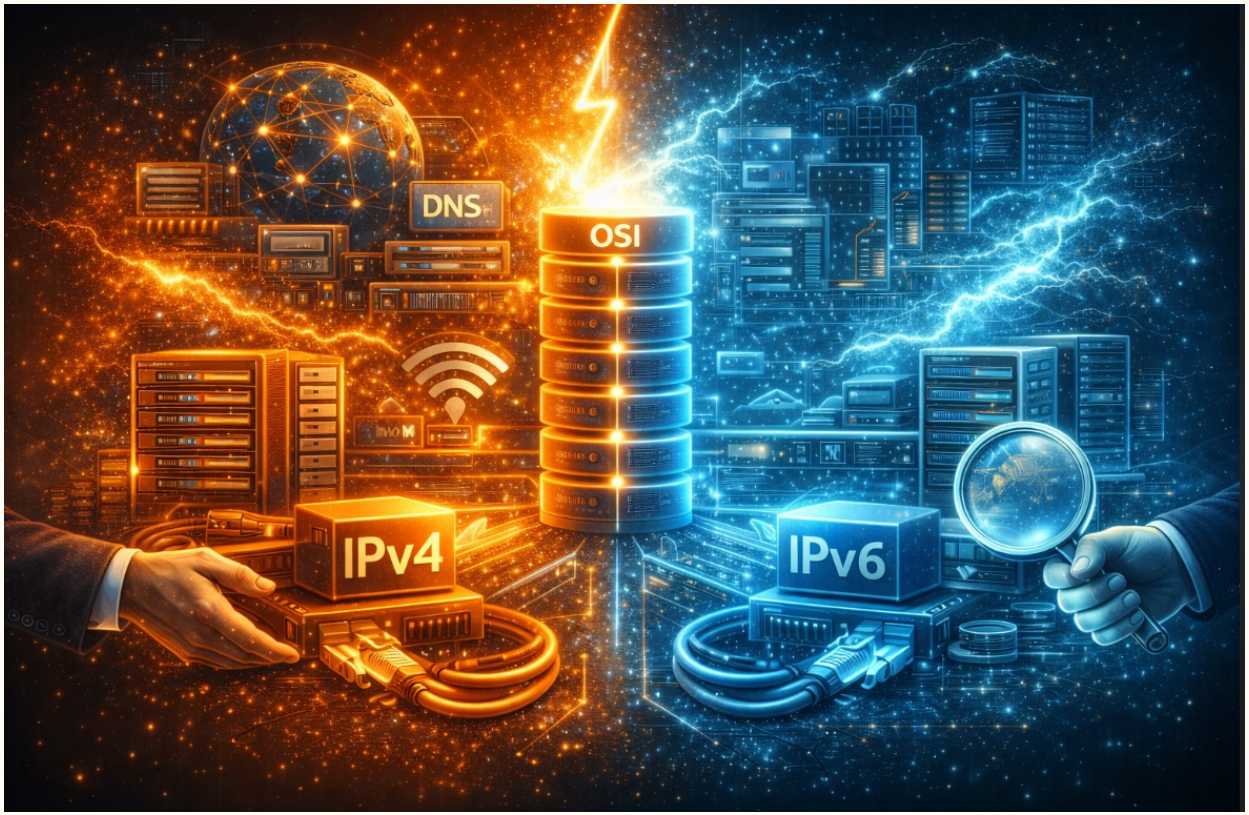
Netzwerke

OSI • LAN • WLAN • Gebäudeverkabelung • DHCP • DNS • IPv4/IPv6 • Fehlersuche

Netzwerk-Basics: Was ist das Ziel?



Das Netzwerk verbindet

Ein Netzwerk ermöglicht es Geräten, miteinander zu kommunizieren, Daten auszutauschen und zentrale Dienste bereitzustellen – ob Internet, Fileserver, Drucker oder VoIP-Telefonie.

Kernbegriffe: Paket/Frame, Adresse (MAC/IP), Port, Protokoll

Prüfungstipp: „Netzwerk geht nicht" ist nie die Ursache – immer eingrenzen: Kabel? IP? DNS? Gateway? Merksatz: Erst Layer finden, dann fixen.

OSI-Modell: Die 7 Schichten

Das OSI-Modell ist ein Denkmodell, nicht 1:1 Realität – aber perfekt fürs strukturierte Troubleshooting in der Prüfung und Praxis.

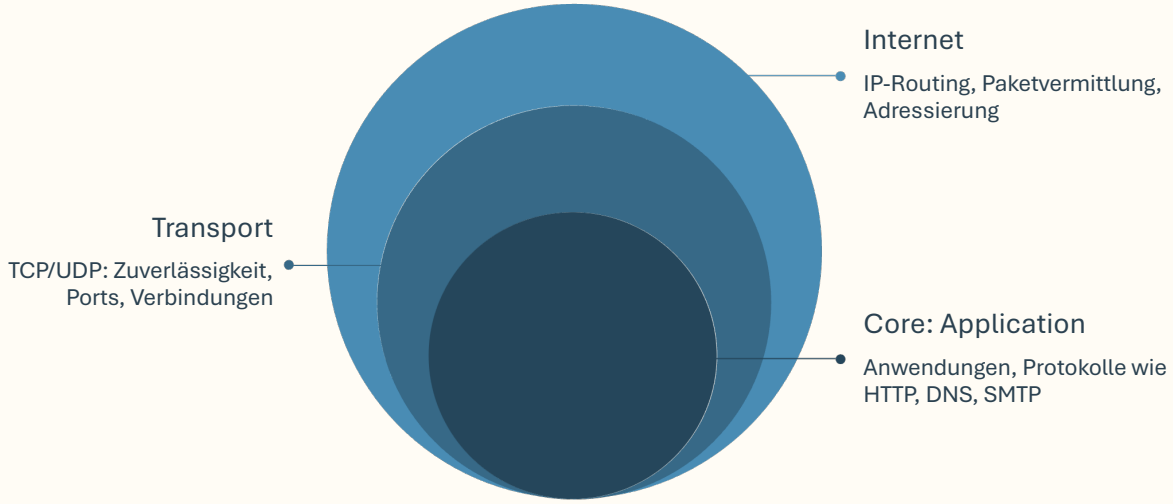
OSI-Modell: Merkhilfe für die Prüfung

Layer 1	Layer 2	Layer 3
Signal/Kabel	MAC-Adresse	IP-Adresse

Layer 4	Layer 7
Ports	Anwendung

> Mini-Merker: 1=Signal, 2=MAC, 3=IP, 4=Ports, 7=App

TCP/IP-Modell: Die Praxisbrücke



Warum TCP/IP wichtig ist

Das TCP/IP-Modell gruppiert die OSI-Schichten anders: Link (≈ OSI 1–2), Internet (≈ OSI 3), Transport (≈ OSI 4), Application (≈ OSI 5–7).

Tools und Fehlersuche in der Praxis denken oft in TCP/IP-Kategorien. Beide Modelle beschreiben dieselbe Idee mit unterschiedlicher Gruppierung.

Merksatz: OSI = Lernen/Diagnose, TCP/IP = Alltag

LAN-Grundlagen: Switch, Router, VLAN

Switch (Layer 2)

Leitet Frames nach MAC-Adresse weiter und baut eine MAC-Tabelle auf. Arbeitet innerhalb eines Netzwerksegments.

Router (Layer 3)

Verbindet verschiedene Netze miteinander, routet nach IP-Adresse. Fungiert als Default Gateway ins Internet.

VLAN

Logische Trennung im selben Switch – trennt Broadcast-Domänen und erhöht Sicherheit ohne zusätzliche Hardware.

Prüfungsfalle: „Switch verteilt Internet" ist falsch – Internet braucht Routing über Gateway!

MAC vs IP: Der kritische Unterschied

Prüfungsrelevant

Die Unterscheidung zwischen MAC- und IP-Adresse ist eine häufige Prüfungsfalle. Beide arbeiten auf unterschiedlichen Layern!

Merksatz: MAC im Raum, IP zwischen Gebäuden.

MAC-Adresse

Hardwareadresse, funktioniert lokal im LAN (Layer 2). Wird vom Switch verwendet.

IP-Adresse

Logische Adresse, routingfähig über Netze hinweg (Layer 3). Wird vom Router verwendet.

ARP (IPv4)

Ermittelt die MAC-Adresse zur IP-Adresse im lokalen Netzwerksegment.

Strukturierte Gebäudeverkabelung

Die drei Hauptbereiche

- **Campus/Backbone:** Verbindung zwischen Gebäuden
- **Vertikal:** Verkabelung zwischen Etagen im Gebäude
- **Horizontal:** Von der Etage zur Netzwerkdose am Arbeitsplatz

Passive Komponenten

Patchpanel, Netzwerkdose, Patchkabel, fest verlegte Leitungen

Aktive Komponenten

Switch, Router, Access Point

Gebäudeverkabelung: Typische Prüfungsfalle

01

Switch im Serverraum

Aktive Komponente, Ausgangspunkt der horizontalen Verkabelung

02

Patchpanel

Passive Komponente, Übergangspunkt zur festen Installation

03

Gebäudekabel (fest verlegt)

Starres Kabel in der Wand/Decke, nicht flexibel

04

Netzwerkdose

Passive Komponente am Arbeitsplatz

05

Patchkabel zum PC

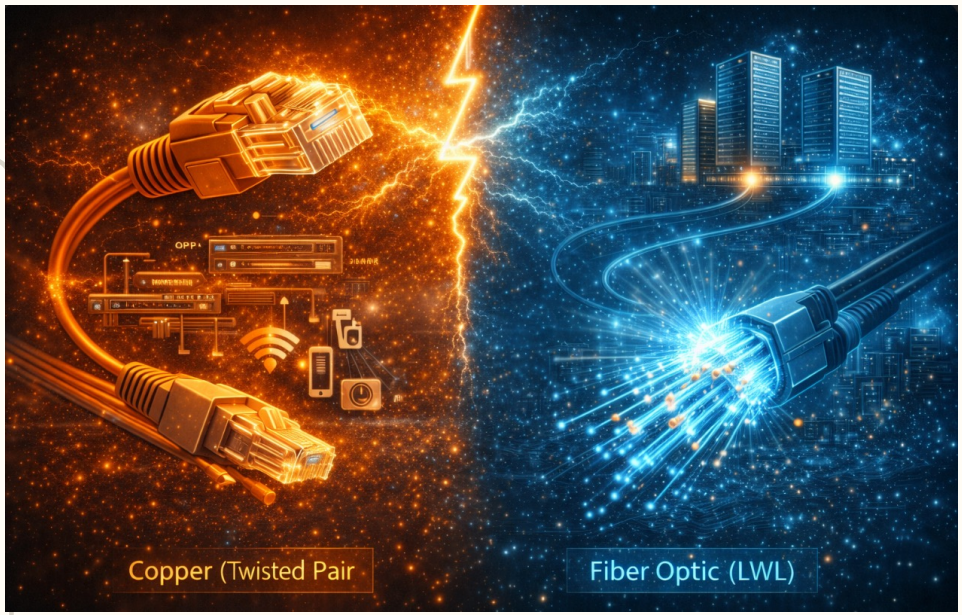
Flexibles Kabel für Endgerät

Wichtig: Patchkabel ≠ Gebäudekabel! Gebäudekabel ist fest verlegt (starr), Patchkabel ist flexibel.

Kupfer vs Glasfaser: Wann was?

Kupfer (Twisted Pair)

Günstig, einfach zu installieren, typisch bis 1–10 Gbit/s je nach Kategorie. Standard für Arbeitsplatzverkabelung. **PoE-fähig:** Stromversorgung über LAN-Kabel für Access Points, VoIP-Telefone, Kameras.



Glasfaser (LWL)

Große Distanzen möglich, EMV-robust gegen Störungen, hohe Bandbreite. Ideal für Backbone-Verkabelung und Etagen-Uplinks zwischen Gebäuden oder Stockwerken.

Lange Strecken + elektromagnetische Störungen → Glasfaser ist o
die saubere Lösung. Beispiel: Etagen-Uplink → LWL, Arbeitsplatz →

WLAN-Grundlagen: Funk ist kein Kabel

Shared Medium verstehen

WLAN ist ein geteiltes Medium – alle Geräte teilen sich die verfügbare Airtime. Deshalb ist sorgfältige Planung wichtiger als bei Kabel-LAN.

Frequenzbänder im Vergleich

- **2,4 GHz:** Größere Reichweite, aber anfälliger für Störungen
- **5 GHz:** Höhere Geschwindigkeit, kürzere Reichweite
- **6 GHz:** Neuere Geräte, je nach Umgebung verfügbar

Der Access Point fungiert als Bridge ins kabelgebundene LAN.

Prüfungsfalle: „WLAN langsam = Internet langsam" – oft ist es ein Funkproblem (Signal/Channel/Airtime), nicht die Internetleitung!

WLAN-Sicherheit & Standards

Verschlüsselung

WPA2/WPA3: aktueller Standard für sichere Verbindungen. **WEP:** veraltet und unsicher – nicht mehr verwenden!

Authentifizierung

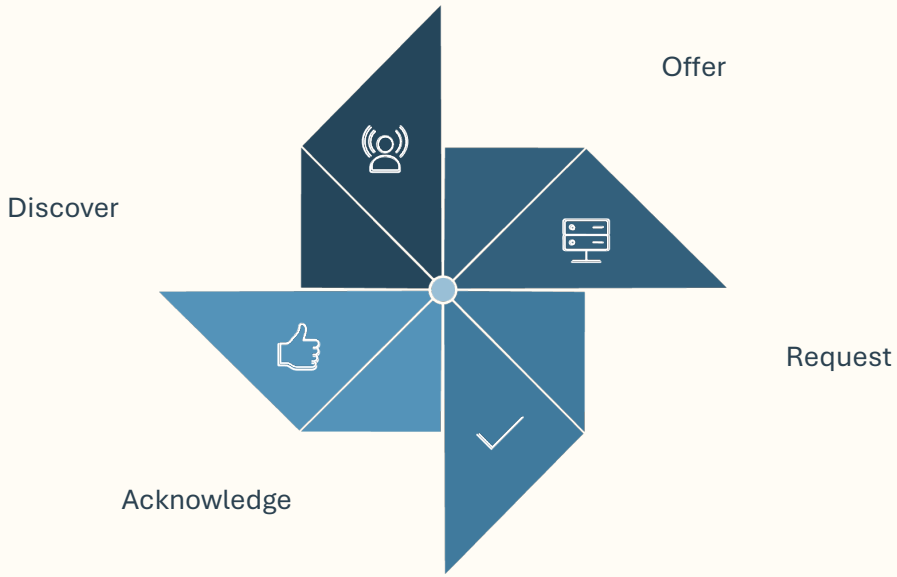
PSK (Pre-Shared Key): einfache Passphrase für kleine Umgebungen. **Enterprise (802.1X/RADIUS):** zentrale Authentifizierung für größere Netzwerke.

Gäste-WLAN

Immer getrennt vom internen Netz (via VLAN/Netzsegment). Gäste erhalten keinen Zugriff auf interne Ressourcen.

Mythos: „Versteckte SSID = sicher" ist falsch. Sicherheit kommt von WPA2/3 + Authentifizierung + Netzwerksegmentieru

DHCP: Automatische IP-Konfiguration



Was vergibt DHCP?

DHCP (Dynamic Host Configuration Protocol) vergibt automatisch IP-Adresse, Subnetzmaske, Default Gateway, DNS-Server und weitere Parameter an Clients.

DORA-Ablauf

1. **Discover:** Client sucht DHCP-Server
2. **Offer:** Server bietet IP-Konfiguration an
3. **Request:** Client fordert angebotene IP an
4. **Acknowledge:** Server bestätigt Vergabe

Lease: zeitlich begrenzte Vergabe. Reservierung möglich (feste IP für bestimmte MAC-Adresse).

DHCP: Typische Fehlerbilder

1

Kein DHCP Offer

DHCP-Server down, Client im falschen VLAN, DHCP-Relay/Snooping fehlt. **Symptom:** IP 169.254.x.x (APIPA)

2

Falsche Konfiguration

Falscher DHCP-Scope aktiv: Gateway oder DNS-Server falsch konfiguriert. Adresspool erschöpft.

3

IP-Konflikte

Doppelte statische IP im DHCP-Bereich vergeben. Statische IPs immer außerhalb des DHCP-Pools planen!

> Mini-Regel: DHCP-Pool sauber halten + Reservierungen für Sondergeräte (Server, Drucker) nutzen.

DNS: Das Telefonbuch des Internets

DNS (Domain Name System) löst lesbare Namen in IP-Adressen auf – z. B. www.example.com → 93.184.216.34

A-Record (IPv4)

Ordnet einem Hostnamen eine IPv4-Adresse zu

AAAA-Record (IPv6)

Ordnet einem Hostnamen eine IPv6-Adresse zu

CNAME

Alias für einen anderen Namen

MX-Record

Definiert Mail-Server für eine Domain

TXT-Record

Speichert Textinformationen (z. B. SPF, DKIM)

Caching & TTL: DNS-Antworten werden gecacht, um Anfragen zu beschleunigen. Die TTL (Time to Live) bestimmt, wie lange ein Eintrag gültig bleibt.

DNS-Ablauf: Rekursive Auflösung

So funktioniert DNS

1. Client fragt lokalen Resolver (meist Router, Server oder Provider-DNS)
2. Resolver fragt rekursiv weiter bis zum autoritativen Nameserver
3. Ergebnis wird mit TTL gecacht

Prüfungsfalle: Falscher DNS-Server im DHCP = komplette Namensauflösung funktioniert nicht!

Test: `nslookup` oder `dig` zeigt, welcher Server antwortet.

Merksatz: Erst IP testen (ping), dann Namen testen (nslookup).

DNS-Fehlersuche: Typisches Muster

Ping auf IP-Adresse funktioniert

Beispiel: `ping 8.8.8.8` erfolgreich → Netzwerk und Routing funktionieren

Ping auf Namen schlägt fehl

Beispiel: `ping www.google.com` schlägt fehl → DNS-Problem!

DNS-Server prüfen

Mit `ipconfig /all` (Windows) oder `cat /etc/resolv.conf` (Linux) DNS-Server-Einträge prüfen

Namensauflösung testen

`nslookup www.google.com` zeigt, ob und welcher DNS-Server antwortet

> „Internet geht nicht" ist oft DNS – IP-Ping geht, Name nicht!

IPv4: Aufbau & Adressierung

IPv4-Grundlagen

IPv4-Adressen bestehen aus 32 Bit, dargestellt als vier Dezimalzahlen: z. B. `192.168.1.10`

Subnetzmaske/CIDR: /24 = 255.255.255.0 – trennt Netz- vom Host-Anteil der Adresse.

Default Gateway: Der Router, der ins nächste Netz oder Internet führt.

Private IPv4-Bereiche

- `10.0.0.0/8` – großer Bereich
- `172.16.0.0/12` – mittlerer Bereich
- `192.168.0.0/16` – häufigster Heimnetz-Bereich

> **Prüfungsfalle:** IP passt, aber Gateway falsch → lokal geht, Internet nicht!

Subnetting: Die Basics für AP1

/24 Netz

256 Adressen (0–255), davon nutzbar 254 Hosts (1–254). Netzwerkadresse = .0, Broadcast = .255

Größere Netze

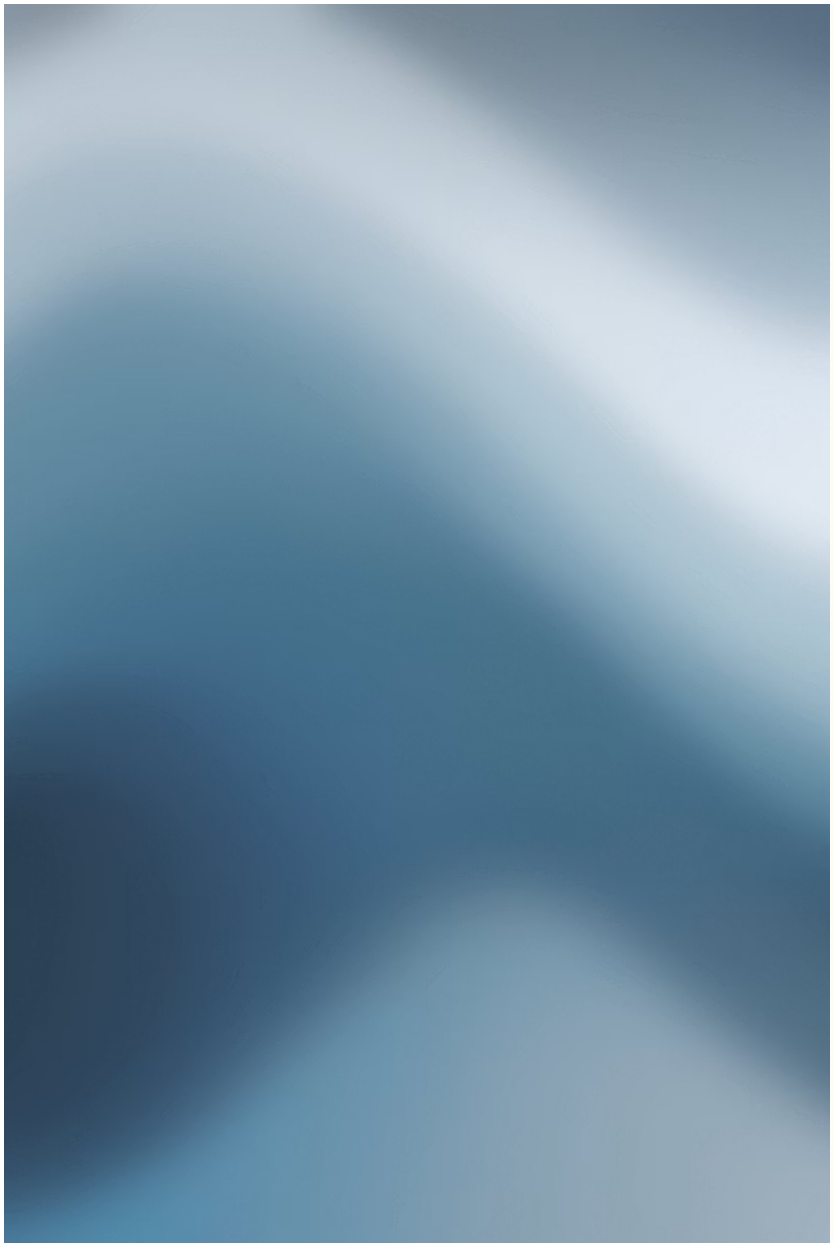
/23 = 512 Adressen, /22 = 1024 Adressen – mehr Hosts pro Netz

Kleinere Netze

/25 = 128 Adressen, /26 = 64 Adressen – weniger Hosts, mehr Subnetze

Häufigster Fehler: Host in falschem Netz → erreicht Gateway nicht!

> Beispiel: `192.168.1.10/24` und `192.168.2.10/24` sind NICHT im selben Netz und können nicht direkt kommunizieren.



NAT: IPv4-Adressübersetzung

Was ist NAT?

NAT (Network Address Translation) übersetzt private IP-Adressen in eine öffentliche IP – typischerweise am Router ins Internet.

Warum NAT?

IPv4-Adressknappheit: Viele Geräte teilen sich eine öffentliche IP

Trennung intern/extern: Interne Struktur bleibt verborgen

Sicherheitsaspekt

NAT ist KEIN Sicherheitsfeature per se – Sicherheit kommt durch Firewall-Regeln!

Portfreigaben: Nur wenn nötig, mit klaren Regeln und Monitoring einrichten.

IPv6: Die Zukunft ist da

Adressformat

128 Bit, hexadezimal: z. B. 2001:db8::1. Deutlich mehr Adressen als IPv4.

/64 Standard

Im LAN ist /64 Standard (Interface-ID). Link-local: fe80::/10 – immer vorhanden, nur lokal.

Adressvergabe

SLAAC: Router Advertisements zur automatischen Konfiguration.
DHCPv6: Alternative oder Ergänzung zu SLAAC.

Prüfungsfalle: