OSI-SCHICHTENMODELL IM ÜBERBLICK

OSI-REFERENZMODELL (7 SCHICHTEN)

7. ANWENDUNGSSCHICHT (APPLICATION)



- Bietet Netzwerkschnittstellen und Protokolle für Anwendersoftware und Nutzerinteraktionen.
- Web & Dateitransfer: HTTP, HTTPS, FTP, TFTP.
- Kommunikation & Namensauflösung: DNS, DHCP, SMTP, IMAP, POP3, SSH.
- PDU: Daten (Data / Message).

4. TRANSPORTSCHICHT (TRANSPORT)



- Stellt die Ende-zu-Ende-Kommunikation zwischen Prozessen auf Quell- und Zielsystemen bereit und regelt Zuverlässigkeit sowie Durchsatz.
- TCP: Verbindungsorientiert, garantiert Zustellung, Flusskontrolle, Segmentierung mit ACK.
- UDP: Verbindungslos, minimaler Overhead, keine Verlustüberwachung, echtzeitfähig.
- Adressierung & PDU: Portnummern zur Prozessuzordnung. PDU: Segment (TCP) / Datagramm (UDP).

8. KAPSELUNG UND INTERAKTIONSPRINZIPIEN



- Veranschaulicht den Weg von Anwendungsdaten durch den Netzwerkstapel und die Transformation der Protokolldateneinheiten.
- Senderichtung (Kapselung): Anwendungsdaten erhalten sukzessive TCP/UDP-Header, IP-Header und Ethernet-Frame-Header/Trailer.
- Empfangsrichtung (Entkapselung): Frame wird auf Layer 2 geprüft, IP-Header auf Layer 3 ausgewertet, Port auf Layer 4 zugestellt.
- Vergleich TCP/IP-Modell: Schichten 5-7 entsprechen der TCP/IP-Anwendungsschicht; Schichten 1-2 dem Netzzugang.

3. VERMITTLUNGSSCHICHT (NETWORK)



- Übernimmt die logische Netzadressierung, Paketweiterleitung sowie Pfadbestimmung (Routing) über heterogene Netzwerkgrenzen hinweg.
- Protokolle: IPv4, IPv6, ICMP, Routing-Protokolle (OSPF, BGP).
- Aufgabe: Bestimmung des optimalen Pfades anhand Routing-Tabellen und Metriken.
- Hardware & PDU: Router, Layer-3-Switches. PDU: Paket (Packet).

6. DARSTELLUNGSSCHICHT (PRESENTATION)



- Transformiert Rohdaten in syntaktisch standardisierte Formate und übernimmt Kodierungs- sowie Verschlüsselungsaufgaben.
- Aufgaben: Datenkonvertierung (z. B. ASCII, UTF-8, ASN.1), Datenkompression.
- Sicherheit: Kryptografische Verschlüsselung (historische Zuordnung von TLS/SSL).
- PDU: Daten (Data).

5. SITZUNGSSCHICHT (SESSION)



- Steuert, synchronisiert und beendet logische Sitzungen zwischen Anwendungen auf unterschiedlichen Endsystemen.
- Aufgaben: Dialogsteuerung (Halbduplex/ Vollduplex), Setzen von Synchronisationspunkten (Checkpoints).
- Protokolle & Schnittstellen: RPC, NetBIOS, Sockets (Sitzungsaspekte).
- PDU: Daten (Data).

1. BITÜBERTRAGUNGSSCHICHT (PHYSICAL LAYER)



- Überträgt unstrukturierte Rohbitströme über ein physikalisches Medium mittels elektrischer, optischer oder elektromagnetischer Signale.
- Protokolle & Standards: Ethernet (100BASE-TX, 1000BASE-T), DSL, EIA-232.
- Hardware-Komponenten: Kabel (Kupfer, Glasfaser), Repeater, passive Hubs, Transceiver.
- PDU: Bit.

2. SICHERUNGSSCHICHT (DATA LINK LAYER)



- Gewährleistet eine verlässliche und fehlerfreie Direktverbindung benachbarter Knoten innerhalb eines physischen Netzsegments.
- Aufteilung: Untertelilt in LLC (Logical Link Control) und MAC (Media Access Control).
- Adressierung & Protokolle: MAC-Adressen (48 Bit), Ethernet (IEEE 802.3), WLAN (IEEE 802.11), ARP.
- Hardware & PDU: Layer-2-Switches, Bridges. PDU: Frame (Rahmen).

8. KAPSELUNG UND INTERAKTIONSPRINZIPIEN

1. Datenursprung (L7-L5)	→	2. Segmentierung (L4)	→	3. Paketierung & Routing (L3)	→	4. Rahmung & Adressierung (L2)	→	5. Signalisierung (L1)
Anwendung formuliert Nutzdaten, kodiert Formate und eröffnet logische Sitzung.		Transportschicht unterteilt Datenstrom in Segmente und vergibt Quell- sowie Zielports.		Vermittlungsschicht ergänzt logische IP-Adressen und bestimmt nächsten Hop im Netzwerk.		Sicherungsschicht verpackt Paket in Frame mit MAC-Adressen und zyklischer Redundanzprüfung (CRC).		Bitübertragungsschicht wandelt Bits in elektrische Signale, Lichtpulse oder Funkwellen um.

Eigene Diagnose-Notiz: Welcher Layer verursacht das aktuelle Verbindungsproblem?

Auf welcher Schicht tritt ein Übertragungsfehler typischerweise auf?

1. **Keine Signalverbindung oder Link-LED aus**
   → Kabel, Stecker und physische Ports (Layer 1) kontrollieren.
2. **Link aktiv, aber keine ARP-Antwort oder Duplex-Mismatch**
   → MAC-Adressierung, VLAN-Konfiguration und Switchports (Layer 2) analysieren.
3. **Ping auf Standard-Gateway schlägt fehl**
   → IP-Konfiguration, Subnetzmaske und Routing-Tabelle (Layer 3) prüfen.
4. **Ping erfolgreich, aber Port-Verbindung abgewiesen (Connection Refused)**
   → Dienststatus, Portfreigaben und Host-Firewall (Layer 4) verifizieren.

TCP/IP-Modell vs. OSI-Modell

Vergleich von 7 OSI-Schichten mit 4 TCP/IP-Schichten

1. HISTORISCHE ENTSTEHUNG

Die beiden Modelle entstanden aus grundlegend verschiedenen Ingenieursphilosophien zwischen staatlicher Standardisierung und militärischer Forschung.



- OSI: Entwickelt ab Ende der 1970er-Jahre durch ISO und ITU-T als formaler, allumfassender Weltstandard.
- TCP/IP: Entstanden in den 1970er-Jahren im Auftrag der DARPA für robuste Paketvermittlung im ARPANET.
- Prinzip: OSI definierte zuerst Standards vor der Implementierung; TCP/IP folgte dem Ansatz von "Rough Consensus and Running Code".

2. ANWENDUNGSEBENE

Die oberste Ebene stellt Schnittstellen für Netzwerkanwendungen bereit. TCP/IP bündelt drei funktionale Schichten des OSI-Modells in einer gemeinsamen Anwendungsschicht.



- OSI 7 (Anwendung): Direkte Anwendungsinteraktion (z. B. HTTP, FTP, SMTP, DNS).
- OSI 6 (Darstellung): Datenformate, Zeichenkodierung, Kompression und Verschlüsselung (TLS/SSL).
- OSI 5 (Sitzung): Sitzungsaufbau, -verwaltung und Synchronisation von Dialogen.
- TCP/IP 4 (Anwendung): Deckt alle Aufgaben der Schichten 5 bis 7 direkt im Anwendungsprozess ab.

3. TRANSPORTSCHICHT

Die oberste Ebene stellt Schnittstellen für Netzwerkanwendungen bereit. die logische Ende-zu-Ende-Verbindung Schichten auf OSI-Modells in einer Quell- und Zielhost.



- Adressierung: Nutzung von Port-Nummern zur Unterscheidung gleichzeitiger Verbindungen (Sockets).
- Verbindungsorientiert (TCP): Zuverlässiger Bytestrom, Bestätigungen, Flusssteuerung und Retransmissions.
- Verbindungslos (UDP): Schlanker, unbestätigter Datagramm-Versand ohne Flusskontrolle für Echtzeitdienste.
- Segmentierung: Aufteillung großer Anwendungsdatenströme in handhabbare Segmente.

4. VERMITTLUNGSSCHICHT

Die logische Weiterleitung über heterogene Teilnetzgrenzen hinweg (Hop-by-Hop-Routing) findet auf dieser Schicht statt.



- OSI 3: Vermittlungsschicht (Network Layer) mit logischer Adressierung und Wegewahl.
- TCP/IP 2: Internetschicht mit dem zentralen Internet Protocol (IPv4 und IPv6).
- Hilfsprotokolle: ICMP für Kontroll- und Fehlermeldungen sowie ARP zur Auflösung logischer in physische Adressen.
- Forwarding: Router wetren IP-Header aus, um Weiterleitungsentschiedungen anhand von Routingtabellen zu treffen.

5. NETZZUGANG & BITÜBERTRAGUNG

Die physische Kopplung und Übertragung unstrukturierter Bitströme über physische Medien.



- OSI 2: Sicherungsschicht (Data Link) für knotenbezogene Rahmenerstellung (Framing) und MAC-Adressierung.
- OSI 1: Bitübertragungsschicht (Physical) für Kabel, Stecker, Spannungspegel und Funkwellen.
- TCP/IP 1: Netzzugangsschicht (Network Access / Link Layer) vereint Sicherung und Signalübertragung.
- Standards: Ethernet (IEEE 802.3), Wi-Fi (IEEE 802.11) und Point-to-Point-Protokolle (PPP).

6. PDU-MAPPING & DATENKAPSELUNG

Jede Schicht fügt den Nutzdaten (Payload) beim Sender eigene Steuerinformationen (Header/Trailer) hinzu (Kapselung) und entfernt diese beim Empfänger (Entkapselung).

- Anwendungsebene: Protokolldaten / Nachricht (Application Data).
- Transportschicht: Segment (TCP) oder Datagramm (UDP) mit Port-Headern.
- Vermittlungsschicht: Paket mit Quell- und Ziel-IP-Adressen.
- Sicherungsschicht: Rahmen (Frame) mit MAC-Adressen und Frame Check Sequence (FCS).
- Bitübertragungsschicht: Bitstrom (Bits) über das physikalische Übertragungsmedium.





7. ARCHITEKTURVERGLEICH

Sytukturierte Gegenüberstellung der Kernunterschiede für Netzwerktechnik und Fehlerdiagnose.

- Schichtenanzahl: 7 Schichten (OSI) gegenüber 4 Schichten (TCP/IP).
- Standardisierung: OSI wurde als hersteller-neutraler ISO-Standard entworfen; TCP/IP als IETF-RFCs.
- Kopplung: OSI trennt Protokolle strikt von Schichten; TCP/IP ist direkt um IP und TCP aufgebaut.
- Verbreitung: TCP/IP beherrscht weltweite Produktivumgebungen; OSI dominiert Ausbildungs- und Diagnosetermonologie.



8. SCHNELLDIAGNOSE

Systematischer Prüfablauf zur Lokalisierung von Netzwerkfehlern entlang der Modellgrenzen.



- Kein Link-Signal oder keine Kabelverbindung (Schicht 1/Link) → Kabel, Transceiver, Port-LEDs und physische Schnittstellen auf Schicht 1 prüfen.
- Link vorhanden, aber keine lokale LAN-Kommunikation (Schicht 2) → VLAN-Zuordnung, Switchport-Status und ARP-Tabelle auf Schicht 2 prüfen.
- Lokales Netz erreichbar, aber Ziel-IP antwortet nicht (Schicht 3) → IP-Konfiguration, Subnetzmaske, Standard-Gateway und Routingtabellen analysieren.
- IP erreichbar via ICMP-Ping, aber Dienst reagiert nicht (Schicht 4) → Ziel-Port auf Schicht 4 via Portscan/Telnet testen sowie Firewall-Regeln prüfen.
- Port offen, aber Übertragung schlägt fehl (Schicht 7) → Anwendungskonfiguration, SSL/TLS-Zertifikate und HTTP-Statuscodes auf Schicht 7 untersuchen.

MINDMAP: PHYSISCHE VS. LOGISCHE NETZWERK-TOPOLOGIEN

1. STERN-TOPOLOGIE (STAR)



Alle Endgeräte sind über Punkt-zu-Punkt-Verbindungen an einen zentralen Knoten (Switch oder Hub) angebunden. Der Standardaufbau moderner kabelgebundener lokaler Netzwerke (Ethernet LAN).

- **Vorteile:** Hohe Ausfallsicherheit bei Kabelbruch einzelner Stationen, einfache Fehlersuche und Skalierbarkeit.
- **Nachteile:** Single Point of Failure am zentralen Switch; erhöhter Verkabelungsaufwand.
- **Signalfluss:** Punkt-zu-Punkt zur Zentrale, Weiterleitung per Frame-Switching.

2. BUS-TOPOLOGIE (BUS)



Alle Stationen teilen sich ein einziges durchgehendes Übertragungsmedium (Hauptstrang). An den beiden Kabelenden verhindern Abschlusswiderstände (Terminatoren) störende Signalreflexionen.

- **Vorteile:** Geringer Kabelbedarf, einfache Installation bei kleinen Netzwerken.
- **Nachteile:** Kollisionsdomäne für alle Stationen, Kabelbruch legt das Gesamtsystem lahm, schwierige Lokalisierung von Störungen.
- **Einsatzgebiet:** Historisches Koaxial-Ethernet (10BASE2/5), moderne industrielle Feldbusse (CAN).

3. RING-TOPOLOGIE (RING)



Jeder Netzwerkknoten ist genau mit zwei Nachbarn verbunden, sodass ein geschlossener Kreis entsteht. Signale wandern gerichtet von Station zu Station, die jeweils als Repeater dient.

- **Vorteile:** Kein zentraler Vermittlungsknoten nötig, deterministische Zugriffszeiten (z. B. via Token-Passing).
- **Nachteile:** Unterbrechung an einer Stelle trennt den Ring (sofern kein redundanter Doppelring wie bei FDDI/SONET vorliegt).
- **Praxis:** Physisch oft über Ringleitungsverteiler (MAU) realisiert – physischer Stern, logischer Ring.

4. VERMASCHTES NETZ (MESH)



Knoten sind mit mehreren (Teilvermaschung) oder allen anderen Knoten (Vollvermaschung) direkt verbunden. Bietet maximale Redundanz und alternative Pfade bei Ausfällen.

- **Vollvermaschung:** Formel n*(n-1)/2 Leitungen bei n Knoten; extremer Port- und Kabelaufwand.
- **Teilvermaschung: Gezielte Redundanz** zwischen Kernsystemen (z. B. Routing-Backbones im WAN und Internet).
- **Vorteile:** Höchste Verfügbarkeit, dynamische Wegewahl bei Verbindungsausfall.

5. BAUM-TOPOLOGIE (TREE)



Hierarchische Struktur, ausgehend von einer zentralen Wurzelkomponente (Root), die sich über Verteilungsschichten (Distribution) zu Endgeräten (Access) auffächert.

- Typischer Einsatz: Großflächige Unternehmen mit Core-, Distribution- und Access-Switches.
- **Vorteile:** Exzellente Skalierbarkeit, strukturierte Gliederung nach Abteilungen/Segmenten.
- **Risiko:** Fällt ein übergeordneter Verteilknoten aus, verliert der gesamte darunterliegende Tellbaum den Netzzugang.

6. HYBRIDE TOPOLOGIE



Kombination aus zwei oder mehr grundlegenden Topologieformen zur Ausnutzung jeweiliger Stärken in unterschiedlichen Netzbereichen.

- **Ptern-Bus-Hybrid:** Einzelne Arbeitsgruppen im Sternmuster an Hubs/Switches, die über einen Bus-Backbone gekoppelt sind.
- **Stern-Ring-Hybrid:** Sternförmige Verbindung zur zentralen Medienzugriffseinheit bei ringförmigem Token-Umlauf.
- **Nutzen:** Flexible Anpassung an bauliche Gegebenheiten und Budgets in Bestandsgebäuden.

7. TOPOLOGIE-ENTSCHEIDUNGSLOGIK & PRÜFUNG



Systematischer Leitfaden zur Auswahl der geeigneten Netzwerkstruktur anhand von Ausfallsicherheitsanforderungen, Kosten und Redundanzzielen.

- **Schritt 1:** Kritikalität der Verfügbarkeit definieren (Toleranz für Single Point of Failure).
- **Schritt 2:** Physisches Leitungsbudget und Switch-Port-Kapazitäten ermitteln.
- **Schritt 3:** Geometrische Ausdehnung und Skalierungsbedarf über die nächsten 3-5 Jahre festlegen.

PRAXIS-CHECK

Verwechseln Sie bei Netzwerkanalysen nicht das Schaltschema im Rack mit dem Datenpfad: Ein Switch-Netzwerk ist physisch ein Stern, logisch werden Frames jedoch anhand von MAC-Tabellen zielgerichtet weitergeleitet.

SIGNALFLUSS VS. LEITUNGSFÜHRUNG



WELCHE NETZWERKTOPOLOGIE ERFÜLLT IHRE PRIMÄRE PROJEKTANFORDERUNG AM BESTEN?

Maximale Hochverfügbarkeit und Nulltoleranz für Verbindungsabbrüche im Core/Backbone	Standard-Büroumgebung mit einfacher Wartung, modularer Erweiterbarkeit und moderatem Budget	Großes Campus-Netzwerk über mehrere Stockwerke oder Gebäude mit hierarchischer Administration	Industrielle Sensorstrecke mit minimaler Verkabelung entlang einer linearen Produktionslinie
Wählen Sie ein vermaschtes Netz (Mesh) mit redundanten Pfaden und dynamischem Routing.	Setzen Sie auf eine Stern-Topologie (Star) mit zentralen managed Switches.	Implementieren Sie eine strukturierte Baum-Topologie (Core-Distribution-Access).	Nutzen Sie eine Bus-Topologie mit korrekter Terminierung oder einen industriellen Redundanz-Ring.

8. SCHNELLE ÜBERSICHT & MERKSÄTZE



Die wichtigsten Merksätze zur Differenzierung und Einordnung von Netzwerktopologien für Diagnose und Entwurf.

- **Physisch ungleich Logisch:** Die Kabelverlegung (Kupfer/Glasfaser) legt nicht zwingend den Datenpfad fest.
- **Stern ist Standard:** Nahezu jedes moderne Ethernet-Büronetzwerk ist physisch als Stern aufgebaut.
- **Mesh bietet Redundanz:** Vollvermaschung ist im LAN meist unwirtschaftlich, im Internet-Backbone jedoch elementar.
- **Baum ermöglicht Skalierung:** Standard für hierarchische Segmentierung und VLAN-Strukturen.
- **Terminierung beachten:** Offene Bus-Enden erzeugen Signalreflexionen und Störungen im gesamtem Segment.

Eigene Netzanalyse:

Physische Topologie im Projekt: _____

Logische Topologie & Übertragungsmedium: _____

Identifizierte Single Points of Failure & Redundanzmaßnahmen:

_____

_____

NETZWERKKATEGORIEN NACH AUSDEHNUNG

(PAN, LAN, MAN, WAN, GAN)

1. PAN – PERSONAL AREA NETWORK



- Das Personal Area Network verbindet persönliche Endgeräte im unmittelbaren Nahbereich eines Nutzers. Typische Reichweiten liegen unter 10 Metern.
- Medien & Standards: Bluetooth (IEEE 802.15.1), BLE, ZigBee, NFC, USB.
- Latenz & Raten: Niedrige Bandbreiten (oft < 24 Mbit/s), Latenz 5 bis 50 ms.
- Administration: Vollständig privat durch den Endanwender kontrolliert.

2. LAN & WLAN – LOCAL AREA NETWORK



- Das LAN deckt räumlich begrenzte Umgebungen wie Büros, Wohnungen oder Serverräume ab. Es bietet höchste Datenraten bei minimaler Latenz.
- Medien & Standards: Ethernet (IEEE 802.3, Kupfer Cat6a/Glasfaser) und Wi-Fi (IEEE 802.11ax/be).
- Latenz & Raten: 1 Gbit/s bis 100 Gbit/s; Latenzen im Bereich < 1 ms.
- Administration: Zentral durch lokale Netzwerkadministratoren ohne Drittanbieter-Carrier.

5. GAN & INTERNET



- Das weltumspannende Netz, aggregiert [illegible] über globale Unterseekabel und Satellitenverbindungen.
- Medien & Standards: Interkontinentale Seekabel, BGP (Border Gateway Protocol, RFC 4271), Satellitenetze (LEO/GEO).
- Latenz & Raten: Weltweite Paketlaufzeiten von 50 bis 250+ ms; aggregierter Terabit-Durchsatz.
- Administration: Dezentral; Koordination von Nummern und Routing über IANA/RIRs und globale Peering-Abkommen.

3. MAN – METROPOLITAN AREA NETWORK



- Ein MAN verbindet mehrere Standorte innerhalb einer Stadt oder Metropolregion, typischerweise bis zu einem Radius von circa 50 Kilometern.
- Medien & Standards: Metro-Ethernet, Dark Fiber, DWDM, Richtfunk.
- Latenz & Raten: 10 Gbit/s bis 400 Gbit/s; Latenz ca. 1 bis 5 ms.
- Administration: Konsortien, Stadtnetz-betreiber oder Telekommunikationsanbieter.

4. WAN – WIDE AREA NETWORK



- Ein WAN erstreckt sich über Regionen, Länder oder Kontinente und verbindet voneinander entfernte Unternehmens-standorte oder Rechenzentren.
- Medien & Standards: MPLS, SD-WAN, Standleitungen, Glasfasertrassen, Satellitenstrecken.
- Latenz & Raten: Bandbreiten bedarfs-orientiert (100 Mbit/s bis 100 Gbit/s); Latenz 10 bis 80 ms.
- Administration: Mehrmandanten-Betrieb durch Internet Service Provider (ISPs) und Carrier.

6. ADMINISTRATIONS- & SICHERHEITSGRENZEN



- Jeder Übergang zwischen den Netz-dimensionen definiert Sicherheits- und Vertrauensgrenzen, an denen Paketfilterung, Adressübersetzung und Verschlüsselung greifen.
- Demilitarisierte Zone (DMZ): Isoliert öffentlich erreichbare Dienste vom internen LAN.
- Border Gateway: Übergabepunkt zu externen ISPs via BGP und Firewall-Inspektion.
- Verschlüsselung: VPN-Tunnelung (IPsec, WireGuard) bei Transit über ungesicherte WAN/GAN-Pfade.

7. ENTSCHEIDUNGSLOGIK ZUR NETZWERKLASSIFIKATION

Nutzen Sie diesen Leitfaden zur schnellen Bestimmung der passenden Netzwerkkategorie bei Architekturentschiedungen.

Welche geografische Distanz und Trägerschaft liegt für die geplante Verbindung vor?

Distanz < 10 Meter, Anbindung von Nahbereichs-sensoren oder Peripherie	PAN
Distanz innerhalb eines Gebäudes/Geländes (< 1 km), vollständiges privates Eigentum	LAN/WLAN
Distanz bis ca. 50 km über Stadtgebiet, Anbindung externer Standorte	MAN
Überregionale oder kontinentale Distanz, Routing über Drittanbieter-Netze	WAN/GAN

8. VERGLEICH & CHECKLISTE



Prüfen Sie vor jeder Netzwerkplanung die technischen Parameter und dokumentieren Sie die Zonengrenzen.

- Latenzerwartung: Sub-ms (LAN) vs. mittlere ms (MAN/WAN) vs. hohe ms (GAN).
- Fehlertoleranz: Redundante Uplinks und dynamisches Routing (OSPF/BGP) ab MAN/WAN zwingend einplanen.
- Zuständigkeit: Klare SLA-Abgrenzungen an den Übergabepunkten (Demarcation Point) definieren.

ARBEITSSCHRITTE

1. **Schritt 1: Dimension bestimmen**
   Geografische Ausdehnung erfassen und ermitteln, ob öffentlicher Raum oder Trägerwege durchquert werden.
2. **Schritt 2: Medium und Protokolle wählen**
   Passende Layer-1- und Layer-2-Standards selektieren (z. B. Cat6a/Glasfaser im LAN vs. Carrier-MPLS im WAN).
3. **Schritt 3: Übergangspunkte absichern**
   Firewalls, Adressübersetzung (NAT) und End-to-End-Verschlüsselung für alle WAN/GAN-Verbindungen.

ARBEITSSCHEID

1. **Schritt 1: Dimension bestimmen**
   Geografische Ausdehnung erfassen und ermitteln, ob öffentlicher Raum oder Trägerwege durchquert werden.
2. **Schritt 2: Medium und Protokolle wählen**
   Passende Layer-1- und Layer-2-Standards selektieren (z. B. Cat6a/Glasfaser im LAN vs. Carrier-MPLS im WAN).
3. **Schritt 3: Übergangspunkte absichern**
   Firewalls, Adressübersetzung (NAT) und End-to-End-Verschlüsselung für alle WAN/GAN-Verbindungen konfigurieren.

PLANUNGSFELD

Geplantes Netzwerkszenario & Zielstandorte:

Zugeordnete Netzwerkkategorie (PAN/LAN/MAN/WAN/GAN):

Definierte Demarcation Points & Carrier-Schnittstellen:

PRAKTISCHER MERKSATZ



Die physikalische Distanz diktiert das Übertragungsmedium und die Latenz; der Betreiberstatus bestimmt die Sicherheits- und Routing-Verantwortung.

KUPFERBASIERTE MEDIEN: TWISTED PAIR & KOAXIALKABEL

1. GRUNDLAGEN DER KUPFERMEDIEN

Elektrische Signalübertragung über metallische Leiter bildet das physische Fundament lokaler Datennetze.



- **Signalübertragung:** Bitmuster werden als Spannungswechsel über Kupferadern übertragen.
- **Verdrillungseffekt:** Gegensinnige Verdrillung neutralisiert symmetrische elektromagnetische Störfelder.
- **Dämpfung & Reichweite:** Ohmscher Widerstand und Kapazität begrenzen Standard-Verlegekabel auf 100 m Gesamtlänge.

2. TWISTED-PAIR-KATEGORIEN

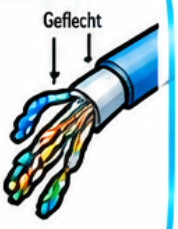
Spezifikationen definieren Bandbreite, Schirmungsanforderungen und maximale Datenraten von Cat5e bis Cat8.



- **Cat 5e:** Bis zu 100 MHz Bandbreite, Standard für Gigabit-Ethernet (1000BASE-T bis 100 m).
- **Cat 6 / 6A:** Cat 6 bis 250 MHz (10 Gbit/s bis 55 m); Cat 6A bis 500 MHz (10 Gbit/s über volle 100 m).
- **Cat 7 / 7A:** Bis 600 bzw. 1000 MHz mit zwingender Einzelschirmschicht; nutzt GG45- oder TERA-Steckverbinder.
- **Cat 8 (8.1 / 8.2):** Bis 2000 MHz für Rechenzentren mit 25/40 Gbit/s über maximal 30 m Linklänge.

3. SCHIRMUNGSCODES NACH ISO/IEC 11801

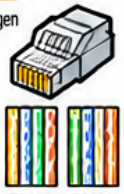
Die Nomenklatur XX/TTP beschreibt den mechanischen Aufbau gegen Nebensprechen und Einstrahlung.



- **U/UTP:** Ungeschirmte Adernpaare in ungeschirmtem Außenmantel, flexibel, anfällig für Alien Crosstalk.
- **F/UTP:** Gesamtschirmt aus Folie um ungeschirmte Adernpaare; Basisschutz gegen hochfrequente Störungen.
- **U/FTP:** Jedes Adernpaar einzeln mit Folie umhüllt, kein gemeinsamer Gesamtschirm; minimiert internes NEXT.
- **S/FTP:** Gesamtschirm aus Kupfergeflecht kombiniert mit 25lerten Adernpaaren; Standard im Profibereich.

4. STECKVERBINDER & BELEGUNG

Physische Schnitttstellen und standardisierte Farbcodierungen nach TIA/EIA gewählleisten Kompatiblität.



- **RJ45-Stecker (8P8C):** Universeller Modularkontakt für Twisted-Pair-Kabel in LAN-Strukturen.
- **Farbkodierung:** T568A und T568B legen die Pinbelegung der vier verdrillten Aderpaare verbindlich fest.
- **Straight-Through vs. Crossover:** Direkte Endgeräteverbindung erforderte früher Crossover; heute löst dies Auto-MDI-X.

5. KOAXIALKABEL-AUFBAU & STANDARDS

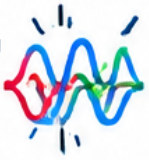
Koaxialleitungen führen Signale über einen zentrierten Innenleiter, umgeben von Dielektrikum und Schirmung.



- **Schichtaufbau:** Innenleiter (Seele), Isolator/Dielektrikum, leitende Schirmung und isolierender Schutzmantel.
- **Historische Ethernet-Standards:** 10BASE2 (Thinnet, 50 Ohm, RG-58, max. 185 m) und 10BASE5 (Thicknet, max. 500 m).
- **Abschlusswiderstand:** Bus-Topologien erfordern an beiden Kabelenden zwingend 50-Ohm-Terminatoren gegen Signalreflexionen.
- **Moderne Nutzung:** DOCSIS-Breitbandnetze über RG-6 Koaxialkabel (75 Ohm Wellenwiderstand) bis zum Kabelmodem.

6. STÖREFFEKTE & SIGNALQUALITÄT

Physikalische Phänomene beeinträchtigen Übertragungsgeschwindigkeit und Signalintegrität auf Kupferstrecken.



- **NEXT & FEXT:** Nah- und Fernnebensprechen durch kapazitive Kopplung benachbarter Adernpaare.
- **Alien Crosstalk:** Störende elektromagnetische Einkopplung zwischen getrennten, parallel verlegten Kabeln.
- **Skineffekt:** Mit steigender Signalfrequenz verlagert sich der Stromfluss an die Leiteroberfläche.

7. AUSWAHL- & ENTSCHEIDUNGSMATRIX

Leitfaden zur Auswwäl des optimalen Kupferübertragungsmediums für verschiedene Einsatzszenarien.

Welches Kupferübertragungsmedium erfordert die geplante Netzwerkumgebung?

Büroarbeitsplatz / Standard-LAN bis 1 Gbit/s und Strecken bis 90 m	Zukunftssichere Gebäudeverkabelung bis 10 Gbit/s bei hoher Störbelastung
Verlegung von Cat 6 U/UTP oder F/UTP mit Standard-RJ45-Dosen; kosteneffizient und montagefreundlich.	Einsatz von Cat 6A oder Cat 7 S/FTP mit durchgehender Erdung und geschirmten RJ45/GG45-Modulen.
Rechenzentrum-Verbindung zwischen Server-Racks mit 25/40 Gbit/s unter 30 m	Breitband-Internetanschluss via Kabel-TV-Netzwerk (DOCSIS)
Installation von Cat 8 S/FTP-Kabeln oder vorkonfektionierten Direct-Attach-Kupferkabeln (DAC).	Nutzung von 75-Ohm-Koaxialleitungen (RG-6/RG-59) mit F-Steckverbindern bis zum Übergabepunkt.

8. PRAXISCHECK & MESSWERTE

Wesentliche Kontrollschritte bei der Zertifizierung und dem Testen neu installierter Kupferstrecken.



- **Permanent Link Test:** Mestechnische Prüfung der Verlegestrecke ohne Patchkabel (maximal 90 Meter zulässig).
- **Channel Link Test:** Gesamtmessung inklusive beidseitiger Patchkabel (maximal 100 Meter Gesamllänge).
- **Durchgang & Pinbelegung:** Wiremap-Test erkennt Dreher, Kurzschlüsse, offene Adern und vertauschte Paare (Split Pairs).
- **Dämpfungs- und NEXT-Grenzwerte:** Automatisierter Protokollabgleich gegen die Spezifikationskurven der jeweiligen Kategorie.

⚠ Praxis-Hinweis zur Erdung

Geschirmte Kabel (FTP/STP) müssen beidseitig fachgerecht auf das Potenzialausgleichssystem aufgelegt werden. Fehlerfafte Schirmerdung erzeugt Erdschleifen, die Signalstörungen verschlimmern statt dämpfen.

Schritt 1:
Mechanischen Biegeradius prüfen

Sicherstellen, dass der hersteller-definierte Mindestbiegeradius (typisch 4-facher Außendurchmesser) nicht unterschritten wird.

Schritt 2:
Schirmung und Adern auflegen

Adernpaare maximal 13 mm vor dem Auflegewerkzeug entdrillen, um Nahnebensprechen (NEXT) an der Kontaktstelle zu minimieren.

Schritt 3:
Zerttifizierungsmessung durchführen

Feldprüfgerät auf die gewählte Norm (z. B. Cat 6A Channel) einstellen und Wiremap, Rückflussdämpfung sowie Laufzeitdifferenz protokollieren.

Geprüfte Strecke / Link-ID	Installierte Kabelkategorie & Schirmungstyp	Gemessene Streckenlänge & NEXT-Status

LICHTWELLENLEITER: SINGLEMODE VS. MULTIMODE



1. GRUNDPRINZIP DER LICHTWELLENLEITER

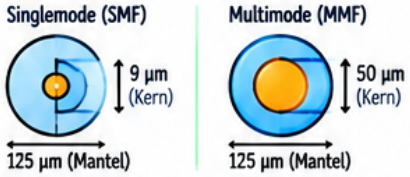
Lichtwellenleiter (LWL) übertragen Daten als modulierte Lichtsignale durch optische Glas- oder Kunststofffasern. Durch Totalreflexion an der Grenze zwischen Kern und Mantel wird der Lichtstrahl verlustarm über weite Distanzen geführt.

- Optische Übertragung: Immun gegen elektromagnetische Störfelder (EMI/RFI)
- Aufbau: Innerer Kern (Core) zur Signalführung, umgeben vom Mantelglas (Cladding)
- Brechungsindex: Kern besitzt höheren Brechungsindex als das umgebende Cladding
- Einsatzbereich: LAN-Backbones, Rechenzentren und kontinentale Weitverkehrsnetze

Schutz vor Potenzialverschleppung
Da LWL rein optisch arbeiten, entsteht keine galvanische Verbindung zwischen Gebäuden – Erdschleifen und Blitzschlagübertragungen über das Datenkabel sind physikalisch ausgeschlossen.

2. KERN- UND MANTELDURCHMESSER

Die geometrische Dimensionierung bestimmt direkt die physikalischen Ausbreitungsmodi des Lichts. Der standardisierte Außendurchmesser des Claddings beträgt einheitlich 125 µm.



- Singlemode (SMF): Sehr kleiner Kerndurchmesser von typischerweise 9 µm (z. B. 9/125 µm)
- Multimode (MMF): Großer Kerndurchmesser von meist 50 µm (OM2-OM5) oder 62,5 µm (OM1)
- Cladding (Mantel): Identisch bei 125 µm für beide Fasertypen zwecks Steckmechanik
- Primärbeschichtung (Coating): 250 µm Schutzschicht aus Acrylat gegen mechanische Schäden

3. LICHTQUELLEN: LED, VCSEL UND LASER

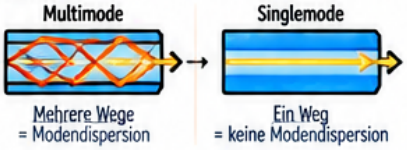
Unterschiedliche Fasertypen verlangen abgestimmte optische Sender hinsichtlich Spektralbreite, Leistung und Kohärenz.



- LED: Günstig, breites Spektrum, nur für historische Multimode-Kabel (OM1/OM2 bis 100 Mbit/s)
- VCSEL (850 nm): Oberflächenemittierender Halbleiterlaser für moderne Multimode-Netze (OM3/OM4/OM5)
- Fabry-Pérot- / DFB-Laser (1310/1550 nm): Extrem schmalbandige Laser für Singlemode-Verbindungen
- Leistungsaufnahme & Kosten: Laser-Transceiver sind kostspieliger als Multimode-Optiken

4. MODENDISPERSION UND DÄMPFUNG

Signalverzerrungen begrenzen die maximale Reichweite und Bandbreite von Glasfaserkabeln je nach Fasertyp drastisch.



- Modendispersion: Lichtstrahlen legen im breiten Multimode-Kern unterschiedliche Wege und Zeiten zurück
- Pulsverbreiterung: Bei Multimode führt Modendispersion zum Ineinanderlaufen aufeinanderfolgender Lichtpulse
- Singlemode-Vorteil: Keine Modendispersion, da nur eine einzige Grundmode transversal propagiert
- Chromatische Dispersion: Wellenlängenabhängige Laufzeitunterschiede bei SMF erst ab vielen Kilometern relevant

Achtung bei Modenmischung
Niemals Singlemode- und Multimode-Fasern direkt zusammenstecken. Die Kerndurchmesser-Diskrepanz (9 µm zu 50 µm) erzeugt immense Koppelverluste von über 10–20 dB.

5. STECKERTYPEN IM NETZWERKEINSATZ

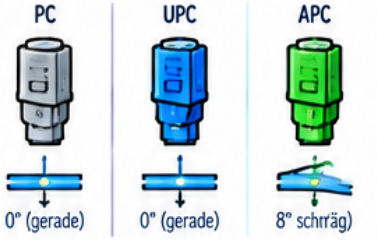
Optische Steckverbinder fixieren die Faserkerne hochpräzise zueinander. Sie unterscheiden sich in Formfaktor und Packungsdichte.



- LC (Lucent Connector): Kompakter SFF-Stecker mit Push-Pull-Klinke, De-facto-Standard in Switches
- SC (Subscriber Connector): Robuster rechteckiger Raststecker, klassisch in Gebäudeanschlüssen
- ST (Straight Tip): Runder Bajonettverschluss, vor allem in älteren Industrieinstallationen
- MPO/MTP (Multi-Fiber Push-On): Mehrfaserstecker (12 oder 24 Fasern) für 40G/100G/400G-Trunks

6. POLIERUNGSARTEN: PC, UPC UND APC

Der Stirnflächenschliff des Steckers bestimmt die optische Rückflussdämpfung (Return Loss) und schützt Transceiver vor Reflexionen.



- PC (Physical Contact): Leicht balliger Schliff, typische Rückflussdämpfung ca. -30 dB bis -40 dB.
- UPC (Ultra Physical Contact): Feiner auspoliert, blaues Steckergehäuse, Dämpfung ca. -50 dB bis -55 dB
- APC (Angled Physical Contact): 8-Grad-Schrägschliff, grünes Steckergehäuse, Rückflussdämpfung > -60 dB
- Kompatibilität: Niemals UPC (blau) direkt mit APC (grün) koppeln – Gefahr von Faserbruch.

7. PRAXISVERGLEICH: SMF VS. MMF

Gegenüberstellung der Kernkriterien zur Auswahl der richtigen Übertragungstechnologie im Unternehmensnetzwerk.



	SMF (Gelber Kabelmantel)	MMF (Türkis/Erika-Violett)
Reichweite	10 km bis über 80 km ohne Repeater (ITU-T G.652)	Bis zu 300-550 m bei 10 Gbit/s (OM3/OM4)
Kabelkosten	oft günstiger oder gleichwertig	ähnlich
Gesamtkosten	SMF-Optiken (SFP+/QSFP) sind teurer	MMF dominiert Inhouse-Strecken bis 300 m

8. ENTSCHEIDUNGSMATRIX: VERKABELUNGSSTRATEGIE

Strukturierte Entscheidungshilfe zur Wahl der passenden LWL-Technologie im Planungsprozess.

- Inhouse / RZ-Rack-to-Rack: Multimode OM4 mit LC oder MPO für günstige Transceiver
- Campus-Backbone / WAN: Singlemode OS2 mit LC-APC/UPC für zukunftssichere Reichweiten

Welche Distanz und Umgebung soll überbrückt werden?

Strecke unter 300 Meter (Innerhalb RZ oder Etagenverteiler)	Strecke über 300 Meter, Gebäudeübergang oder WAN-Anbindung
Multimode (OM3/OM4) mit 850 nm VCSEL-Transceivern und LC-Duplex oder MPO-Steckern einsetzen.	Singlemode (OS2) mit 1310/1550 nm DFB-Lasern einsetzen, um Modendispersion kompletzu vermeiden.

ETHERNET-STANDARDS (IEEE 802.3)

1. GRUNDLAGEN & IEEE 802.3 ARCHITEKTUR



Ethernet definiert standardisierte Protokolle und Spezifikationen für kabelgebundene LAN-Netzwerke auf Schicht 1 (Physical) und Schicht 2 (Data Link) des OSI-Modells.

- Ursprünglicher Standard: CSMA/CD als Medienzugriffsverfahren (Trägerprüfung und Kollisionserkennung).
- Moderne Ethernet-Netze: Punkt-zu-Punkt-Verbindungen mit Vollduplex (Switches eliminieren Kollisionen).
- Framing: Standard-Ethernet-II-Frame (Präambel, SFD, Ziel-MAC, Quell-MAC, EtherType, Nutzlast 46-1500 Bytes, FCS/CRC).
- Reichweitenlimitierung für Kupferkabel (Twisted Pair): Physikalische Obergrenze standardmäßig 100 Meter.

2. FAST ETHERNET (100 MBIT/S)



Der 1995 verabschiedete Standard IEEE 802.3u steigerte die Datenrate von 10 Mbit/s auf 100 Mbit/s.

- 100BASE-TX: Verwendet 2 Adernpaare von Cat-5 UTP/STP, Leitungscodierung 4B5B über MLT-3.
- 100BASE-FX: Glasfaser-Variante (Multimode) mit 1300 nm Wellenlänge für Distanzen bis 2 km.
- Maximale Kupfersegmentlänge: Strikt auf 100 Meter pro Streckenabschnitt limitiert.
- Etablierung der Auto-Negotiation: Automatische Abstimmung von Geschwindigkeit und Duplex-Modus.

3. GIGABIT ETHERNET (1 GBIT/S)



Mit IEEE 802.3z (Glasfaser) und IEEE 802.3ab (Kupfer) wurde der Gigabit-Durchsatz im Unternehmensumfeld zum Standard.

- 1000BASE-T: Übertragung über alle 4 Adernpaare von Cat-5e/Cat-6 mit PAM-5-Codierung und Echo-Kompensation.
- 1000BASE-SX: Multimode-Glasfaser (850 nm) für Gebäude-Backbones bis zu 550 m.
- 1000BASE-LX: Singlemode-Glasfaser (1310 nm) für Campusnetze mit Reichweiten bis zu 5 km.
- Vollduplex-Betrieb: Durch paralleles Senden und Empfangen wird theoretisch 1 Gbit/s in beide Richtungen erzielt.

4. 10-GIGABIT ETHERNET (10G)



IEEE 802.3ae und IEEE 802.3an definieren 10 Gbit/s für Rechenzentren, Aggregation Layer und Core-Netze.

- 10GBASE-T: Kupferverbindung bis 100 m erfordert mindestens Cat-6A (Cat-6 nur bis max. 55 m eingeschränkt nutzbar).
- 10GBASE-SR: Kurzstrecken-Multimode (850 nm) über OM3/OM4 bis 300 m bzw. 400 m.
- 10GBASE-LR: Langstrecken-Singlemode (1310 nm) für Reichweiten bis zu 10 km.
- Reiner Vollduplex-Betrieb: CSMA/CD wird in 10G-Spezifikationen nicht mehr unterstützt.

5. HIGH-SPEED ETHERNET: 40G & 100G



Eingeführt durch IEEE 802.3ba, adressieren 40G und 100G den exponentiell wachsenden Bandbreitenbedarf moderner Fabrics.

- Multi-Lane-Architektur: Bündelung paralleler Kanäle (4x10G für 40GBASE-SR4 bzw. 4x25G für 40GBASE-SR4 bzw. 4x25G für 100GBASE-SR4).
- QSFP-Transceiver: QSFP+ (40G) und QSFP28 (100G) mit MPO/MTP-Mehrfasersteckern.
- 100GBASE-LR4: WDM-Multiplexing von 4 optischen Wellenlängen über ein einzelnes Singlemode-Faserpaar bis 10 km.
- Einsatzbereich: Rechenzentrums-Spine-Leaf-Topologien und Internet Exchange Points.

6. ULTRA-HIGH-SPEED ETHERNET: 400G & AUSBLICK



IEEE 802.3bs standardisiert 200G und 400G für Cloud-Hyperscaler, KI-Cluster und Telekommunikations-Backbones.

- Modulationsverfahren: Wechsel von NRZ zu PAM4 (4 Amplitudenstufen zur Verdopplung der Bitrate pro Baud).
- Transceiver-Formfaktoren: QSFP-DD (Double Density) und OSFP ermöglichen dichte Portbelegungen.
- 400GBASE-DR4 / FR4: 500 m über parallele Singlemode-Fasern oder 2 km via optisches Multiplex Distanzen.
- Zukunftsentwicklung: IEEE 802.3df und 802.3dj treiben 800G und 1,6 Tbit/s für Hochleistungsrechenzentren voran.

7. KABELMEDIEN & STECKVERINDER IM VERGLEICH



Die Wahl des physischen Mediums bestimmt Signalqualität, Dämpfung, Störfedrigkeit und maximale Übertragungsdistanz.

- Twisted Pair (RJ45): Cat-5e (1G), Cat-6 (1G/10G bis 55m), Cat-6A (10G bis 100m) mit Schirmungsarten wie U/UTP, S/FTP.
- Multimode-Glasfaser (OM3/OM4/OM5): Größerer Kerndurchmesser (50 µm), kostengünstige VCSEL-Laser, für Gebäude-Infrastruktur.
- Singlemode-Swimfaaser (OS2): Kleiner Kerndurchmesser (9 µm), Laserdioden, minimale Dämpfung für weite Distanzen.
- Direct Attach Copper (DAC): Passive/aktive Kupfer-Twinax-Kabel für extrem latenzarme Rack-Verkabelungen (1-7 m).

8. ZUSAMMENFASSUNG & PRAXIS-SELEKTOR



Strukturierte Übersicht zur Dimensionierung von Ethernet-Leitungen nach Bandbreite, Latenz und Infrastruktur.

- Endgeräte (Office / IoT): 1000BASE-T über Cat-6 bietet optimales Kosten-Nutzen-Verhältnis.
- Server-Anbindung (Virtualisierung): 10GBASE-T oder 10G SFP+ DAC/SR für geringe Latenz und ausreichenden Durchsatz.
- Switch-to-Switch-Backbone: Mindestens 40G/100G über MPO-Multimode oder Singlemode-Faser.
- Sicherheitsaspekt: Segmentierung (VLAN nach 802.1Q) und MACsec (802.1AE) für kryptographischen Schutz auf Layer 2.

Praxis-Hinweis zur Verkabelung
Für Neuinstallationen im Büroumfeld empfiehlt sich standardmäßig Cat-6A oder Cat-7 mit RJ45/GG45, um zukunftssicher 10 Gbit/s ohne Leitungstausch zu gewährleisten.

Welcher Ethernet-Standard passt zu Ihrer Infrastruktur-Anforderung?



Arbeitsplatzrechner oder Drucker im lokalen Büronetz
→ 1000BASE-T über bestehende Cat-5e/Cat-6 Verkabelung mit RJ45-Ports nutzen.



Verbindung zwischen Switches im gleichen Server-Rack (Distanzen unter 5m)
→ 10G SFP+ Direct Attach Copper (DAC) oder 25G/40G DAC-Kabel zur Kostensenkung und Latenzminimierung einsetzen.



Verbindung zwischen zwei separaten Gebäudekomplexen (> 500 m Distanz)
→ 1000BASE-LX oder 10GBASE-LR über OS2-Singlemode-Glasfaser verlegen, um Potenzialunterschiede und Signaldämpfung zu beherrschen.

ETHERNET-FRAME-AUFBAU & MAC-ADRESSIERUNG

1. PREAMBLE & SFD

- 7 Bytes Präambel (10101010 ...)
- + 1 Byte SFD (10101011).
- Taktsynchronisation der Netzwerkschnittstelle.
- Startet die Adressfelder.



2. ZIEL-MAC

- 6 Bytes (48 Bit) an Byte 8 bis 13.
- Unicast oder Broadcast.
- Liefert an passenden Port (CAM-Table).



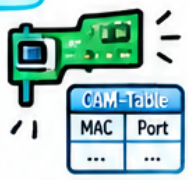
8. STEUERBITS (I/G & U/L)

- I/G-Bit (Bit 0): Unicast oder Multicast.
- U/L-Bit (Bit 1): Global oder lokal.
- MAC-Randomisierung & Spoofing setzen oft U/L = 1.



3. QUELL-MAC

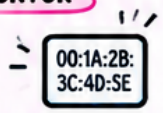
- 6 Bytes (48 Bit) direkt nach Ziel-MAC.
- Switch-Learning.
- Immer Unicast (Bit 0 = 0).



ETHERNET L2 FRAME

7. 48-BIT MAC-STRUKTUR

- 3 Bytes OUI (Hersteller).
- 3 Bytes NIC (Geräte-ID).
- Hex: 00:1A:2B:3C:4D:5E.





4. ETHERTYPE / LÄNGE

- 0x0800 (IPv4).
- 0x0806 (ARP).
- >1500 = EtherType.
- ≤1500 = Längenfeld.



6. FCS (CRC-32)

- 4 Bytes (32 Bit).
- Polynomdivision (CRC-32).
- Fehlerhafte Frames werden verworfen.



5. PAYLOAD & PADDING

- 46–1500 Bytes (Standard-MTU).
- Mind. 64 Bytes Frame.
- Padding bei kleinen Paketen.



Ethernet-Frame-Struktur & MAC-Adressierung

Auf der Sicherungsschicht (OSI-Schicht 2) werden Daten für die Übertragung im lokalen Netzwerk in standardisierte Einheiten gekapselt: die Ethernet-Frames. Ein Frame stellt sicher, dass Netzwerkkarten physische Bitströme synchronisieren, Start- und Endpunkte erkennen sowie Absender und Empfänger anhand ihrer physischen MAC-Adressen fehlerfrei zuordnen können.

- **Schicht-2-Kapselung:** Verbindet die Bitübertragung mit logischer Adressierung im LAN.
- **Ethernet II vs. IEEE 802.3:** Unterscheidung über das EtherType- oder Längenfeld bei Schwellenwert 1500 (0x05DC).
- **Eindeutige Hardware-Identifikation:** 48-Bit-MAC-Adressen steuern das Switching innerhalb derselben Broadcast-Domäne.

Unterscheidung EtherType und Länge

Werte ab 1536 (0x0600) identifizieren das gekapselte Protokoll der Vermittlungsschicht (Ethernet II).

Werte bis 1500 (0x05DC) geben die Frame-Länge nach IEEE 802.3 an.

Praxis-Prüfpfad: Frame- und MAC-Analyse

Verwenden Sie diesen strukturierten Entscheidungsbaum bei der Netzwerkanalyse im Sniffer (z. B. Wireshark), um Frames Schicht für Schicht präzise zuzuordnen.

Welcher Wert steht im Feld an Byte-Position 12-13 (nach den MAC-Adressen)?

- **Wert ist größer oder gliech 0x0600** (>= 1536) → **Ethernet-II-Frame**
  Lesen Sie den EtherType aus: 0x0800 (IPv4), 0x0806 (ARP), 0x86DD (IPv6) und übergeben Sie die Nutzdaten direkt an das zugehörige Schicht-3-Protokoll.
- **Wert ist kleiner oder gleich 0x05DC** (<= 1500) → **IEEE-802.3-Frame**
  Mit Längenangabe. Die Nutzlast beginnt typischerweise mit einem LLC-Header (z. B. DSAP/SSAP), um das Zielprotokoll zu bestimmen.

Praktischer Frame-Analyse-Leitfaden

Folgen Sie dieser schrittweisen Anleitung, um empfangene Ethernet-Pakete in der Praxis zu prüfen und Fehler im Schicht-2-Verkehr strukturiert zu isolieren.

1. **Ziel- und Quell-MAC extrahieren**
   Prüfen Sie die ersten 12 Bytes des Frames.
   Prüfen Sie das I/G-Bit des ersten Bytes:
   Unicast (Bit 0 = 0) oder Multicast/Broadcast (Bit 0 = 1)?
2. **Herstellerherkunft über OUI ermitteln**
   Gleichen Sie die ersten 3 Bytes der Quell-MAC mit der IEEE-OUI-Datenbank ab, um den Hersteller zu verifizieren.
3. **Protokoll-Demultiplexing via EtherType**
   Lesen Sie das EtherType-Feld aus, um IPv4 (0x0800), ARP (0x0806) oder IPv6 (0x86DD) zu erkennen.
4. **Mindestlänge & Integritätsprüfung validieren**
   Stellen Sie sicher, dass der Frame mind. 64 Bytes lang ist (ggf. Padding prüfen) und der 4-Byte-FCS der CRC-32 entspricht.

Labor-Arbeitsblatt: Frame- & MAC-Inspektion

Tragen Sie bei Ihrer nächsten Wireshark-Analyse die Frame-Parameter eines ausgewählten Netzwerkpakets ein:

Ziel-MAC-Adresse (Hexadezimal, 6 Bytes): _____

Quell-MAC-Adresse & ermittelter OUI-Hersteller: _____

EtherType-Wert (Hexadezimal) & decodiertes L3-Protokoll: _____

Payload-Länge (Bytes) und festgestellte Padding-Größe: _____

FCS / CRC-Status (Gültig / Prüfsummenfehler): _____

KOLLISIONS- UND BROADCASTDOMÄNEN

1. DEFINITION KOLLISIONSDOMÄNE

Ein Netzwerkabschnitt, in dem simultane Übertragungen von zwei oder mehr Stationen zu elektrischen Signalüberlagerungen und damit zu Datenverlust führen.



- Relevanz bei Halbduplex: Geteilte Medien (Shared Media) wie Koaxialkabel oder Hubs.
- Erkennung: CSMA/CD auf Ethernet-Ebene.
- Auswirkung: Hohe Kollisionsraten → Re-Transmissions, Latenzanstieg, Durchsatzabfall.

2. DEFINITION BROADCASTDOMÄNE

Die Gesamtheit aller Netzwerkteilnehmer, die ein Layer-2-Broadcast-Paket (Zieladresse FF:FF:FF:FF:FF:FF) empfangen und verarbeiten müssen.



- Typische Broadcasts: ARP-Anfragen und DHCP-Discover-Nachrichten.
- Verarbeitung: Jedes Endgerät analysiert den Frame bis Layer 3 im Protokollstapel.
- Risiko: Zu große Domänen erzeugen CPU-Last und begünstigen Broadcast-Stürme.

3. HUB (LAYER 1)

Ein Hub arbeitet als reiner elektrischer Signalverstärker (Repeater) und verfügt über keinerlei MAC-Adresslogik.



- 1 Kollisionsdomäne: Alle Ports teilen denselben physikalischen Übertragungskanal.
- 1 Broadcastdomäne: Signale werden blind an alle Ports geflutet.
- Modernes Urteil: In produktiven Netzwerken obsolet, da wenige Clients den Bus blockieren.

4. SWITCH (LAYER 2)

Ein Switch leitet Frames anhand der Quell- und Ziel-MAC-Adressen über eine interne Switching-Tabelle gezielt weiter.



- N Kollisionsdomänen: Jeder Port ist eine eigene, isolierte Kollisionsdomäne.
- Vollduplex-Betrieb: Kollisionen technisch ausgeschlossen (getrennter Sende-/Empfangspfad).
- 1 Broadcastdomäne: Broadcasts werden weiterhin auf alle Ports im selben VLAN geflutet.

5. ROUTER (LAYER 3)

Ein Router arbeitet auf Schicht 3 (IP) und verbindet unterschiedliche Subnetze. Er leitet Pakete gezielt basierend auf Routing-Tabellen weiter.



- Trennung von Broadcasts: Router terminieren Layer-2-Broadcasts standardmäßig.
- N Broadcastdomänen: Jede Schnittstelle definiert eine eigene Broadcastdomäne.
- Sichsuheitsgrenze: Ermöglicht Zugriffskontrollen mittels ACLs und Firewall-Regeln.

6. VLANS (802.1Q)

Virtual Local Area Networks (VLANs nach IEEE 802.1Q) unterteilen einen physischen Layer-2-Switch in mehrere unabhängige logische Segmente.



- Broadcast-Isolation: Ports in unterschiedlichen VLANs gehören verschiedenen Broadcastdomänen an.
- Inter-VLAN-Routing: Erfordert eine Routing-Instanz (Router oder L3-Switch).
- Ressourceneffizienz: Spart physische Verkabelung für Abteilungen oder Mandanten.

7. DIREKTER KOMPONENTENVERGLEICH

Die exakte Zuordnung von Geräten zu ihren Domänengrenzen entscheidet über Netzwerkdurchsatz und Stabilität.

- Hub (8 Ports): 1 Kollisionsdomäne | 1 Broadcastdomäne
- Switch (24 Ports, unkoofiguriert): 24 Kollisionsdomänen | 1 Broadcastdomäne
- Switch (24 Ports, aufgeteilt in 3 VLANs): 24 Kollisionsdomänen | 3 Broadcastdomänen
- Router (4 geroutete Schnittstellen): 4 Kollisionsdomänen | 4 Broadcastdomänen

Welche Netzwerkanforderung soll erfüllt werden?

Kollisionen auf dem Kabelsegment eliminieren und Bandbreite pro Gerät garantieren.

- Einsatz eines Layer-2-Switches mit Vollduplex-Verbindung pro Endgerät (Mikrosegmentierung).

Ausbreitung von ARP-/DHCP-Broadcasts begrenzen oder Subnetze voneinander isolieren.

- Netzwerk in VLANs unterteilen und Kopplung über einen Router bzw. Layer-3-Switch vornehmen.

8. ZUSAMMENFASSUNG & BEST PRACTICES

Wichtige Faustregeln für die tägliche Netzwerkarchitektur und Systemadministration.



- Faustregel Kollision: Geteilte Medien erfordern CSMA/CD; dedizierte Switch-Ports im Vollduplex lösen Kollisionen vollständig auf.
- Faustregel Broadcast: Ein IP-Subnetz entspricht im Standardfall genau einer Layer-2-Broadcastdomäne.
- Best Practice Segmentierung: Max. 200–500 aktive Hosts pro Broadcastdomäne.

Praxis-Tipp: Fehlerbild Broadcast-Sturm

Entstehen Switching-Schleifen ohne STP, kreisen Broadcasts endlos in der Broadcastdomäne. Das führt binnen Sekunden zum Totalausfall der Netzwerkleistung.

Vorgehen im Störungsfall

1. Schritt 1: Topologie erfassen
   Alle Hubs, Switches, VLANs und Router-Schnittstellen identifizieren.
2. Schritt 2: Kollisionsdomänen zählen
   Jeden Switch-Port als eigene Domäne. Alle am Hub = 1 Domäne.
3. Schritt 3: Broadcastdomänen bestimmen
   Layer-2-Pfade bis zur nächsten Router-Schnittstelle oder VLAN-Grenze.

SWITCHING-PRINZIPIEN & CAM

1. WAS IST EIN L2-SWITCH?

Ein Layer-2-Switch verbindet Netzwerkgeräte innerhalb desselben lokalen Netzwerks (LAN) auf der Sicherungsschicht des OSI-Modells.



- Arbeitet auf Schicht 2 (Data Link Layer) anhand von MAC-Adressen
- Trennt Kollisionsdomänen pro Switch-Port für volle Bandbreite
- Erhält im Standardbetrieb eine gemeinsame Broadcast-Domäne

2. DIE MAC-TABELLE (CAM)

Die Content Addressable Memory (CAM) Tabelle ordnet erlernte physische Hardware-Adressen festen Switch-Ports zu.

MAC	PORT	VLAN
00:11:22:33:44:55	3	10
AA:BB:CC:DD:EE:FF	7	20
11:22:33:44:55:66	5	10

- Dynamische Bindung: MAC-Adresse zu physischem Port und VLAN
- Ermöglicht zielgerichtete Zustellung statt Broadcast-Flutung
- Hardware-beschleunigtes Lookup über spezialisierte CAM-Bausteine

3. DER LERNPROZESS (LEARNING)

Eingehende Ethernet-Frames werden sofort analysiert, um die Topologie im laufenden Betrieb dynamisch zu erfassen.



- Auslesen der Quell-MAC-Adresse (Source MAC) im Frame-Header
- Ermtagen der Quell-MAC zusammen mit der Portnummer in die CAM
- Bestehende bahträge werden mit aktuellem Zeitstempel aktualisiert

4. FORWARDING & FILTERING

Sobald die Ziel-MAC in der CAM-Tabelle bekannt ist, wird der Frame selektiv und isoliert zugestellt.



- Forwarding: Frame verlässt ausschließlich den zugeordneten Ziel-Port
- Filtering: Frame wird auf allen anderen Switch-Ports blockiert
- Kollisionsfreie Vollduplex-Übertragung zwischen Endgeräten

5. FLOODING (UNBEKANNTE ZIELE)

Ist die Ziel-MAC-Adresse nicht in der CAM-Tabelle verzeichnnt oder handelt es sich um Broadcasts, flutet der Switch.



- Unknown Unicast: Frame geht an alle Ports außer den Eingangs-Port
- Aroadcasts (FF:FF:FF:FF:FF:FF) und Multicasts werden geflutet
- Antwortet das Zielgerät, lernt der Switch dessen Port umgehend

7. STORE-AND-FORWARD VS. CUT-THROUGH

Switches nutzen unterschiedliche interne Verfahren zur Paketprüfung vor der eigentlichen Weiterleitung.



- Store-and-Forward: Liest gesamten Frame, prüft FCS-Prüfsumme, verwirft Fehler
- Cut-Through: Leitet direkt nach dem Lesen der ersten 6 Ziel-Bytes weiter
- Fragment-Free: Liest die ersten 64 Bytes (Mindestgröße), filtert Runts

8. ENTSCHEIDUNGSLOGIK & DIAGONSE

Kompakter Leitfaden zur Überprüfung der Switch-Weiterleitung bei der praktischen Fehlerbehebung.

1. Quell-MAC analysieren und Port eintragen (Learning)
2. Ziel-MAC prüfen: Bekannt (Forwarding) vs. Unbekannt (Flooding)
3. Switch-Tabelle prüfen: 'show mac address-table' (Cisco/Standard)

Sicherheitshinweis: CAM-Table-Overflow

Angreifer können gefälschte MAC-Adressen massenhaft einspeisen (MAC Flooding). Läuft der CAM-Speicher voll, verhält sich der Switch wie ein Hub (Fail-Open) und leitet allen Datenverkehr an alle Ports weiter.

1. **Frame-Empfang & Source-Lookup**
   Der Switch nimmt den Ethernet-Frame an Port X entgegen und liest Quell-MAC. Falls neu oder veraltet, wird Port X aktualisiert.
2. **Destination-Lookup & Weiterleitung**
   Switch prüft Destination-MAC: Bei Treffer gezieltes Unicast-Forwarding, bei Unbekannt/Broadcast Flooding über alle aktiven Ports außer Port X.

Geprüfter Switch-Port / Ziel-MAC

Ergebnis show mac address-table / Status

Ist die Ziel-MAC-Adresse des ankommenden Frames in der CAM-Tabelle eingetragen?

Ja
(Eintrag vorhanden)
Frame wird gezielt über den assoziierten Port weitergeleitet (Forwarding) und an allen anderen Ports blockiert (Filtering).

Nein
(Unbekannte Unicast-MAC oder Broadcast)
Frame wird als Unbekannter Unicast an sämtliche aktiven Ports desselben VLANs geflutet (Flooding), ausgenommen der Eingangs-Port.

ARP & PROXY-ARP MINDMAP

1. FUNKTION & BEDEUTUNG

Das Address Resolution Protocol (ARP) schlägt die Brücke zwischen logischer Vermittlungsschicht (IPv4) und physischer Netzzugangsschicht (Ethernet). Ohne ARP kann ein IP-Paket im lokalen Netz keinem physischen Netzwerkadapter zugestellt werden.

- Löst 32-Bit-IPv4-Adressen in 48-Bit-MAC-Adressen (Hardware-Adressen) auf.
- Arbeitet direkt auf Layer 2 über Ethernet-Frames mit dem EtherType-Feld 0x0806.
- Notwendig für die Kommunikation zwischen Hosts im selben IP-Subnetz.
- IPV6 erstezt diesen Mechanismus vollständig durch das Neighbor Discovery Protocol (NDP).

2. DER ARP-REQUEST

Kennt ein Quell-Host die MAC-Adresse des Ziels nicht, initiiert er eine Suchanfrage an das gesamte lokale Netzwerksegment.



- Versand als Ethernet-Broadcast an die Ziel-MAC FF:FF:FF:FF:FF:FF.
- Alle Netzwerkgeräte im Layer-2-Segment empfangen und analysieren den Frame.
- Inhaltliche Kernfrage des Pakets: "Wer hat die IP-Adresse X? Bitte antworte an IP Y!".
- Opcode 1 im ARP-Header identifiziert das Paket als Anfrage (Request).

3. DER ARP-REPLY

Nur das Zielgerät mit der gesuchten IPv4-Adresse beantwortet die ARP-Anfrage. Alle anderen Hosts verwerfen den Request.



- Antwort erfolgt direkt als Unicast an die konkrete Quell-MAC-Adresse des Senders.
- Opcode 2 im ARP-Header deklariert die Nachricht als gültige Antwort.
- Enthält die verbindliche Zuordnung der abgefragten Ziel-IP zur eigenen MAC-Adresse.
- Quell-Host aktualisiert sofort seine interne ARP-Tabelle mit den erhaltenen Daten.

4. ARP-CACHE-MANAGEMENT

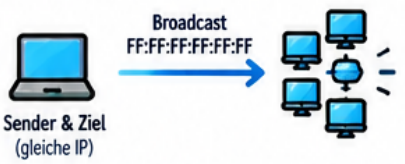
Um Broadcast-Überlastungen im lokalen Segment zu verhindern, werden gelernte Zuordnungen temporär im lokalen Arbeitsspeicher zwischengespeichert.



- Dynamische Einträge besitzen ein Timeout (je nach OS meist zwischen 60 Sekunden und 20 Minuten).
- Veraltete oder inaktive Zuordnungen werden nach Ablauf der Frist automatisch verworfen.
- Manuelle statische Einträge sind dauerhaft, erfordern aber administrative Pflege.
- Verhindert repetitive Broadcasts für aufeinanderfolgende Datenpakete desselben Ziels.

5. GRATUITOUS ARP

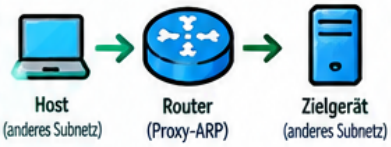
Ein Host sendet unaufgefordert einen ARP-Request für seine eigene zugewiesene IPv4-Adresse an das Netzwerk.



- Erkennung von IP-Adresskonflikten (Duplicate Address Detection): Antwortet ein Host, liegt ein Konflikt vor.
- Aktualisierung fremder ARP-Caches bei Austausch einer Netzwerkschnittstelle oder Failover.
- Wichtiger Mechanismus für High-Availability-Cluster zur Übernahme virtueller IP-Adressen.
- Sender-IP und Target-IP sind im Paket-Payload identisch gesetzt.

6. PROXY-ARP-PRINZIP

Ein Router oder Gateway beantwortet ARP-Anfragen stellvertretend für ein Gerät, das in einem anderen Subnetz oder Segment liegt.



- Ermöglicht Hosts ohne Standard-Gateway-Konfiguration das Erreichen entfernter Netze.
- Router liefert bei Übereinstimmung der Route seine eigene Router-MAC-Adresse zurück.
- Sender glaubt fälschlicherweise, das Zielgerät befinde sich im selben lokalen Segment.
- Erhöht die Auslastung und Komplexität und birgt bei Fehlkonfigurationen Risiken für Routing-Schleiden.

7. PRAKTISCHE ANWENDUNG & DIAGNOSE

Mit nativen Betriebssystem-Befehlen lässt sich der ARP-Cache einsehen, leeren und zur Fehlerbebebung bei Adresskonflikten heranziehen.

Sicherheitshinweis: ARP-Spoofing

Da ARP standardmäßig unauthentifiziert ist, können gefälschte ARP-Replies gesendet werden, um Datenverkehr über einen Angreifer umzuleiten (Man-in-the-Middle). Schutz bieten Dynamic ARP Inspection (DAI) auf Switches oder statische Einträge.

1 ARP-Tabelle anzeigen

Windows / Linux / macOS: Führen Sie 'arp -a' im Terminal aus (unter modernen Linux-Systemen alternativ 'ip neigh show'), um alle gecachten IP-MAC-Paare anzuzeigen.

2 Cache bereinigen

Windows: 'arp -d *' in einer Administrator-PowerShell ausführen. Linux: 'sudo ip neigh flush all' oder 'sudo arp -d <IPv*'. macOS: 'sudo arp -a -d'.

3 Auflösung überprüfen

Pingen Sie die Ziel-IP an und prüfen Sie anschließend erneut mit 'arp -a', ob die MAC-Adresse dynamisch gelernt wurde.

8. ZUSAMMENFASSUNG & MERKSÄTZE

Die Kernfakten des Address Resolution Protocols kompakt zusammengefasst für die Netzwerkpraxis:

- ARP operiert auf Layer 2 und verbindet IP-Adressen mit Ethernet-MAC-Adressen.
- **Anfrage = Broadcast** (alle hören mit). **Antwort = Unicast** (nur der Anfragende empfängt).
- Einträge im ARP-Cache sind flüchtig und verfallen automatisch nach einem Timeout.
- Gratuitous ARP meldet Adresswechsel und prüft auf IP-Kollisionen.
- Proxy-ARP lässt Router als Stellvertreter für entfernte Hosts antworten.

ARP & PROXY-ARP



VLAN-Grundlagen nach IEEE 802.1Q

1. Definition & Broadcast-Domänen



Ein VLAN bildet eine eigenständige Broadcast-Domäne. Broadcast-Frames wie ARP-Anfragen verbleiben strikt innerhalb des jeweiligen VLANs und belasten keine fremden Segmente.

- Jedes VLAN entspricht logisch einem isolierten physischen Switch
- Eindämmung von ARP- und DHCP-Broadcast-Stürmen
- Verbindung zwischen VLANs erfordert Routing auf Schicht 3

2. Das 802.1Q-Tag-Format (4 Bytes)



Der IEEE 802.1Q-Standard fügt ein 4-Byte-Feld direkt nach der Quell-MAC-Adresse in den Standard-Ethernet-Frame ein. Dieses Tag gliedert sich in TPID und TCI.

- TPID (Tag Protocol Identifier, 16 Bit): Fester Wert 0x8100
- TCI (Tag Control Information): Umfasst PCP, DEI und VID
- Gesamtlänge des Tags: Exakt 32 Bit bzw. 4 Oktette

3. TCI-Felder: PCP, DEI und VID



Innerhalb der Tag Control Information steuern drei Teilfelder die Priorisierung, Verwerfbarkeit und logische Netzzugehörigkeit des Frames.

- PCP (Priority Code Point, 3 Bit): 8 Prioritätsstufen für QoS nach IEEE 802.1p
- DEI (Drop Eligible Indicator, 1 Bit): Markierung für Frame-Verwerfung bei Überlastung
- VID (VLAN Identifier, 12 Bit): Kennung des logischen Netzes (Werte 0 bis 4095; 1–4094 nutzbar)

8. Konfigurations-Workflow & Verifikation



Schrittweises Vorgehen zur sauberen VLAN-Segmentierung auf Standard-Switches.

1. **VLANs in der Switch-Datenbank anlegen**
   VLAN-ID definieren und sprechenden Namen vergeben (z. B. VLAN 10 "Management", VLAN 20 "Clients).
2. **Access-Ports konfigurieren**
   Switch-Ports den Ziel-VLANs zuweisen und den Modus fest auf Access setten.
3. **Trunk-Verbindungen einrichten**
   Switch-to-Switch-Verbindungen als Trunk deklarieren, Native VLAN anpassen und erlaubte VLANs einschränken.
4. **Funktion & Isolation verifizieren**
   VLAN-Tabelle prüfen (z. B. `show vlan brief`) und Erreichbarkeit via Ping innerhalb sowie zwischen VLANs testen.

IEEE 802.1Q VLAN Grundlagen



4. Access-Ports (Untagged)



Access-Ports verbinden Endgeräte wie PCs, Drucker oder Server, die in der Regel keine 802.1Q-Tags verarbeiten können.

- Port ist fest genau einem einzigen VLAN zugewiesen
- Switch entfernt das Tag beim Senden an das Endgerät
- Switch fügt das VLAN-Tag beim Empfang ungetaggter Frames intern hinzu

6. Native VLAN & Sicherheitsrisiken



Das Native VLAN verarbeitet Frames auf einem Trunk-Port ohne 802.1Q-Tag. Es dient der Abwärtskompatibilität, birgt jedoch Risiken wie VLAN-Hopping.

- Ungetaggte Frames auf dem Trunk werden dem Native VLAN zugewiesen
- Standard-Einstellung ist herstellerabhängig meist VLAN 1
- Best Practice: Native VLAN auf ungenutzte ID ändern (z. B. VLAN 999) und explizit taggen

Sicherheitshinweis: VLAN-Hopping
Vermeiden Sie die Standard-ID VLAN 1 auf Trunks. Ein Angreifer kann durch Double-Tagging Frames in fremde Netze einschleusen, wenn das Native VLAN auf beiden Trunk-Enden ungetaggt bleibt.

5. Trunk-Ports (Tagged Links)



Trunk-Ports transportieren Frames mehrerer VLANs über eine gemeinsame physische Leitung, beispielsweise zwischen zwei Switches oder zum Router.

- Frames tragen das 4-Byte-VLAN-Tag zur eindeutigen Zuordnung
- Ermöglicht standortübergreifende VLAN-Ausdehnung über Switche hinweg
- VLAN-Filterung (VLAN Trimming) beschränkt zulässige IDs

7. Inter-VLAN-Routing



Da Switches Frames strikt innerhalb ihres VLANs isolieren, ist zur Kommunikation zwischen unterschiedlichen VLANs Layer-3-Routing erforderlich.

- **Router-on-a-Stick:** Physischer Trunk zum Router mit logischen Subinterfaces
- **Layer-3-Switch (Multilayer-Switch):** Routing über interne SVIs (Switch Virtual Interfaces)
- Zugriffskontrolle via Layer-3-Access-Control-Lists (ACLs) oder Firewall-Regeln

VLAN-Port-Entscheidungsmatrix

Entscheidungsbaum zur korrekten Port-Zuweisung und Betriebsart bei der Netzwerksegmentierung.



Geplante VLAN-ID / Subnetz-Bereich

_____

Zugehörige Switch-Port-Nummer & Endgerät-Typ

_____

Welcher Gerätetyp wird an den Switch-Port angeschlossen?

Endgerät ohne 802.1Q-Unterstützung (PC, Drucker, Client-Kamera)	Konfiguriere den Port als statischen Access-Port mit fester VLAN-ID. Tags vor Weiterleitung strikt strippen.
Netzwerkkomponente (Switch, Router, Hypervisor mit virtuellen Switches)	Konfiguriere den Port als 802.1Q-Trunk. Definiere ein dediziertes Native VLAN und beschränke die Allowed-VLAN-Liste.

INTER-VLAN-ROUTING: ROAS & L3-SWITCHES

1. GRUNDPRINZIP INTER-VLAN-ROUTING

Virtual Local Area Networks (VLANs) trennen Ethernet-Netzwerke auf Layer 2 in isolierte Broadcast-Domänen. Da Endgeräte aus unterschiedlichen VLANs nicht direkt über Layer-2-Frames kommunizieren können, erfordert jeder Datenfluss zwischen verschiedenen VLANs eine Vermittlung auf Vermittlungsschicht (Layer 3). Inter-VLAN-Routing übernimmt diese logische Verbindung und setzt Sicherheitsrichtlinien sowie Filterregeln zwischen den Subnetzen durch.

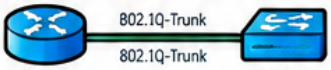
- VLANs isolieren Broadcast-Domänen auf Layer 2 für Mandantentrennung und Netzhygiene.
- Kommunikation über VLAN-Grenzen hinweg erfordert zwingend Routing auf Layer 3.
- Jedes logische VLAN bildet ein eigenes IP-Subnetz.
- Typische Architekturen: Dedizierter Router oder Multilayer-Switch (Layer 3 Switch).

ARCHITEKTUR-MERKSATZ

Ohne Layer-3-Routing bleiben VLANs vollständig isoliert. Der Standard-Gateway-Eintrag am Host zeigt stets auf das Layer-3-Interface seines jeweiligen VLANs.

2. ROUTER-ON-A-STICK (ROAS) ARCHITEKTUR

Router-on-a-Stick nutzt ein einziges physisches Trunk-Kabel zwischen einem Layer-2-Switch und einem physischen Router-Interface. Auf dem Router wird das physische Interface in mehrere logische Subinterfaces unterteilt, Jedes Subinterface wird einem spezifischen VLAN zugewiesen und terminiert das entrspechende IP-Subnetz über



Router (mit Subinterfaces) — Switch (Layer 2)

- **Physische Topologie:** Ein einzelner 802.1Q-Trunk-Port verbindet Switch und Router.
- **Logische Struktur:** Auftellung eines physischen Interfaces (z. B. g0/0) in Subinterfaces (z. B. g0/0.10).
- **Kapselung:** Jedes Subinterface entpackt und verpackt VLAN-Tags über "encapsulation dottq <VLAN-ID>".
- **Gateway-Rolle:** Jedes Subinterface erhält die IP-Adresse des Standard-Gateways für sein VLAN.

HARDWARE-VORAUSSETZUNG

Das physische Router-Interface muss administrativ aktiviert sein (no shutdown), wahrend die IP-Adressen ausschließlich den Subinterfaces zugewiesen werden.

3. ROAS SCHRITT-FÜR-SCHRITT KONFIGURATION

Zur praktischen Umsetzung von Router-on-a-Stick sind koordinierte Schritte auf Switch und Router notwendig. Diese Prozedur richtet einen 802.1Q-Trunk und konfiguriert die korrespondierenden Subinterfaces am Router.

1. **Switch-Trunk einrichten**
   Den Uplink-Port zum Router als 802.1Q-Trunk definieren (*switchport mode trunk*) und die benötigten VLANs über die Trunk-Allowed-Liste freigeben.
2. **Physisches Router-Interface aktivieren**
   Hauptinterface auf dem Router öffnen (interface g0/0), keine IP-Adresse vergeben und mit "no shutdown" in den aktiven Betriebsmodus versetzen.
3. **Subinterfaces anlegen und 802.1Q binden**
   Subinterface exstellen (interface g0/0.10), VLAN-Tagging zweisen (encapsulation dottq 10) und die Subnetz-Gateway-IP konfigurieren (ip address 192.168.10.1 255.255.255.0).
4. **Zweites Subinterface konfigurieren**
   Weiteres Subinterface für das Ziel-VLAN erzeugen (interface g0/0.20), Tag binden (encapsulation dottq 20) Verbunden ("C") aufscheinen, und Ping-Tests zwischen den VLANs durchführen.

4. SWITCHED VIRTUAL INTERFACES (SVI) AUF LAYER-3-SWITCHES

Moderne Unternehmensnetze nutzen Multilayer-Switches mit Switched Virtual Interfaces (SVIs). Ein SVI ist ein virtuelles Layer-3-Interface innerhalb des Switches, das direkt an ein Layer-2-VLAN gekoppelt ist. Die Paketvermittlung zwischen VLANs erfolgt intern über hardwarebeschleunigte ASICs mit Leitungsgeschwindigkeit.

- **Hardware-Routing:** Vermittlung im Switching-Chip (ASIC) ohne externe Kabelumwege.
- **Drahtlose Bandbreite:** Beseitigt den Single-Cable-Flaschenhals externer Router.
- **SVI-Definition:** Logisches Interface pro VLAN (z. B. "interface vlan 10") fungiert als lokales Gateway.
- **Aktivierung:** Globaler Befehl "**ip routing**" schaltet die Layer-3-Engine des Switches scharf.

KRITISCHER AKTIVIERUNGSBEFEHL

Auf vielen L3-Switches ist IPv4-Routing standardmäßig deaktiviert. Ohne "ip routing" im globalen Konfigurationsmodus leitet der Switch Pakete zwischen SVIs nicht weiter.

5. SVI EINRICHTUNG UND ROUTED PORTS

Die Einrichtung von Layer-3-Switches umfasst das Erstellen der VLANs, das Hochfahren der zugehörigen SVIs und bei Bedarf das Konfigurieren geroteter Uplink-Ports zu Core-Routern.

1. **Globales Routing aktivieren**
   In den Konfigurationsmodus wechseln und "ip routing" ausführen, um die interne Forwarding-Tabelle für Layer-3-Pakete ön initialisieren.
2. **VLANs in der Switch-Datenbank anlegen**
   Layer-2-VLANs instanziieren (vlan 10, vlan 20) und mit Namen versehen; ein SVI kann nur aktiv werden, wenn das Basis-VLAN existiert.
3. **SVI für VLANs konfigurieren**
   SVI aufufen (interface vlan 10), Gateway-IP zuweisen (192.168.10.1 255.255.255.0) und Interface mit "no shutdown" aktivieren.
4. **Routed Ports für Uplinks einrichten (optional)**
   Einen physischen Switchport mittels "no switchport" in einen reinen Layer-3-Port wandeln und eine Point-to-Point-IP für Upstream-Routing vergeben.

6. ARCHITEKTURVERGLEICH: ROAS VS. L3-SWITCH

Die Wahl zwischen Router-on-a-Stick und Multilayer-Switching hängt von Durchsattanforderungen, Budget, Skalierungszielen und Sicherheitsarchitektur ab. Folgende Kriterien grenzen beide Verfahren praxisnah ab.

- **Durchsatz:** ROAS teilt sich die Bandbreite eines Uplinks (Flaschenhals); L3-Switch routet im Backplane-Takt mit mehreren Gigabit/Terabit pro Sekunde.
- **Latenz:** ROAS refordert Frame-Austritt und Re-Entry über dieselbe Leitung; L3-Switch vermitellt intern im Nanosekundenbereich.
- **Sicherheitsfunktionen:** Externe Router bieten oft tiefere Stateful-Firewall- und VPN-Funktionen; L3-Switches fokussieren primär auf Stateless ACLs.
- **Kostenaufwand:** ROAS ist ideal für kleine Zweigstellen oder Labore; L3-Switches sind Standard im Enterprise-Campus- und Datacenter-Design.

7. FEHLERSUCHE UND DIAGNOSE-WORKFLOW

Inter-VLAN-Probleme resultieren meist aus fehlerhaften Tags, fehlenden Gateways oder inaktiven Interfaces. Nutzen Sie diesen systematischen Diagnosepfad beide Verfahren Behebung. ab.

- **VLAN-Status:** Prüfen, ob das VLAN aktiv ist und mindestens ein Port im Zustand 'up' ist (show vlan brief).
- **Trunk-Tags:** Verifizeiren, ob die VLAN-IDs auf dem Trunk erlaubt sind (show interfaces trunk).
- **Subinterface-Encapsulation:** Sicherstellen, dass die VLAN-ID im Encapsulation-Befehl mit dem Switchport übereinstimmt.
- **Host-IP-Konfiguration:** Kontrollieren, ob IP-Adresse, Subnetzmaske und Standard-Gateway am Client exakt zum SVI bzw. Subinterface passen.

ARCHITEKTUR-MERKSATZ

Ohne Layer-3-Routing bleiben VLANs vollständig isoliert. Der Standard-Gateway-Eintrag am Host zeigt stets auf das Layer-3-Interface seines jeweiligen VLANs weiss.

7. REHITEKTURVERGLEICS ROAS VS. L3-SWITCH

Inter-VLAN-Probleme resulter-on-meist aus fehlmyrter-Switching Tags, fehlenden Gateways oder inaktiven Interfaces. Nutzen Sie diesen systematischen Diagnosepfad zur schnellen Behehung. ab.

- **VLAN-Status:** Prüfen, ob das VLAN aktiv ist und mindestens ein Port im Zustand 'up' ist (show vlan brief).
- **Trunk-Tags:** Verifizeieen, ob die VLAN-IDs auf dem Trunk erlaubt sind (show interfaces trunk).
- **Subinterface-Encapsulation:** Sicherstellen, dass die VLAN-ID im Encapsulation-Befehl mit dem Switchport übereinstimmt.
- **Host-IP-Konfiguration:** Kontrollieren, ob IP-Adresse, Subnetzmaske und Standard-Gateway am Client exakt zum SVI bzw. Subinterface passen.

HÄUFIGE STOLPERFALLE

Ein SVI bleibt im Status 'Line protocol down', wenn kein einziger physischer Port im jeweiligen VLAN aktiv (Up/Up) oder als Trunk mit diesem VLAN aktiv geschaltet ist.

8. DESIGN-ENTSCHEIDUNGSBAUM & PLANUNGSPROTOKOLL

Nutzen Sie diesen Entscheidungsbaum zur Wahl des passenden Routing-Verfahrens für ein neues Netzwerksegment sowie das Arbeitsblatt für Ihre konkrete IP- und VLAN-Planung.

VLAN-ID & Name (z. B. VLAN 10 - Verwaltung):	
Geplantes IP-Subnetz & CIDR (z. B. 192.168.10.0/24):	
Gateway-Adresse für SVI / Subinterface (z. B. 192.168.10.1):	
Routing-Methode (Router-on-a-Stick / L3-Switch SVI):	
Sicherheits-ACLs oder Filterregeln am Gateway.	

Welche primären Anforderungen hat das geplante Inter-VLAN-Routing-Szenario?

- Hoher interner Datendurchsatz (> 1 Gbit/s), minimale Latenz, Enterprise-Campus → **Einsatz eines L3-Switches** mit Switched Virtual Interfaces (SVIs) und ASIC-basiertem Wire-Speed-Routing.
- Geringes Budget, Labornetzwerk, niedriger Durchsatz oder Bedarf an tiefer Stateful-Inspektion → **Router-on-a-Stick (ROAS)** mit 802.1Q-Trunk und Subinterfaces auf einem Standard-Router.

SPANNING TREE PROTOCOL (STP, RSTP, MSTP)

1. GRUNDPRINZIP & SCHLEIFENPROBLEM



Auf Layer 2 existiert kein TTL-Feld wie im IP-Header. Zirkulieren Broadcast-, Multicast- oder unbekannte Unicast-Frames in redundanten Switch-Topologien, entsteht ohne Vorkehrungen ein zerstörerischer Broadcast-Sturm.

- Endlose Frame-Duplizierung überlastet Bandbreite und Switch-CPUs.
- MAC-Address-Flapping überschreibt fortlaufend die Forwarding-Tabellen.
- STP löst das Problem: Logische Blockierung redundanter Pfade bei physischer Redundanz.

L2 vs. L3
IP-Pakete verwerfen sich nach Ablauf des TTL-Zählers selbst. Ethernet-Frames besitzen keinen TTL-Mechanismus und kreisen unbegrenzt weiter.

2. STP-WAHLVERFAHREN (ROOT BRIDGE)



Alle Switches tauschen BPDUs (Bridge Protocol Data Units) aus, um die zentrale Kontrollinstanz (Root Bridge) im Subnetz zu ermitteln.

- Kriterium 1: Niedrigste Bridge Priority (Standardwert: 32768, konfigurierbar in 4096er-Schritten).
- Kriterium 2 (Tie-Breaker): Niedrigste Basis-MAC-Adresse des Switches.
- Alle aktiven Ports der gewählten Root Bridge erhalten immer den Status Designated Port (Forwarding).

3. PORT-ROLLEN & TOPOLOGIE-BERECHNUNG



Jeder Non-Root Switch bestimmt anhand der Pfadkosten (Path Cost) zur Root Bridge genau einen aktiven Upstream-Port.

- Root Port (RP): Port mit den geringsten kumulierten Pfadkosten zur Root Bridge pro Non-Root Switch.
- Designated Port (DP): Pro Link der Port, der den günstigsten Pfad zur Root Bridge bereitstellt (weiterleitend).
- Non-Designated / Alternate Port: Blockiert normalen Datenverkehr, verhindert aktiv die Schleifenbildung.

4. KLASSISCHES STP (IEEE 802.1D)



Der ursprüngliche Standard vermeidet Loops zuverlässig, benötigt jedoch lange Konvergenzzeiten bei Topologieänderungen.

- Zustände: Blocking -> Listening (15s) -> Learning (15s) -> Forwarding.
- Typische Konvergenzzeit: 30 bis 50 Sekunden bis zur Wiederherstellung des Verkehrs.
- Nicht mehr zeitgemäß für moderne, echtzeitkritische Unternehmensnetzwerke.

5. RAPID STP (IEEE 802.1W)

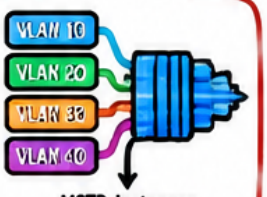


RSTP beschleunigt die Konvergenz drastisch auf wenige Millisekunden durch ein aktives Handshake-Verfahren.

- Vereinfachte Zustände: Discarding, Learning, Forwarding.
- Proposal/Agreement-Handshake synchronisiert Switch-Verbindungen unmittelbar ohne feste Timer.
- Edge Ports (Endgeräte-Ports mit PortFast) wechseln sofort in Forwarding ohne Topologie-Benachrichtigung.

Praxis-Tipp
Konfiguriere Access-Ports zu PCs und Druckern immer als Edge Ports / PortFast, um unnötige Topologie-Neuberechnungen zu verhindern.

6. MULTIPLE STP (IEEE 802.1S)



Während PVST+ eine STP-Instanz pro VLAN betreibt und Switch-Ressourcen bindet, gruppiert MSTP mehrere VLANs in Instanzen.

- VLAN-to-Instance-Mapping: Hunderte VLANs werden wenigen MST-Instanzen zugewiesen.
- Ermöglicht echtes L2-Load-Balancing über alternative redundante Uplinks.
- Dramatische Reduktion von Switch-CPU-Last und BPDU-Traffic in großen Netzen.

7. SECURITY & SCHUTZMECHANISMEN



Böswillige oder fehlkonfigurierte Switches können die Root-Rolle an sich reißen und Traffic umleiten oder lahmlegen.

- BPDU Guard: Deaktiviert Edge-Ports sofort (Error-Disabled), falls eine unautorisierte BPDU empfangen wird.
- Root Guard: Verhindert, dass fremde Switches auf bestimmten Ports zur Root Bridge gewählt werden.
- Loop Guard: Schützt vor unidirektionalen Link-Fehlern, wenn BPDUs unerwartet ausbleiben.

Sicherheits-Notiz
BPDU Guard auf allen Benutter-Ports aktivieren, um versehentlich angeschlossene Fremd-Switches abzuwehren.

8. ENTSCHEIDUNGSLEITFADEN STP-PROTOKOLL

Wähle das passende Spanning-Tree-Protokoll passend zur Netzwerkgröße und Hardware-Ausstattung:

- Kleine homogene Netze: RSTP / Rapid-PVST+ für minimale Komplexitäit.
- Große VLAN-Strukturen: MSTP zur Einsparung von Systemressourcen.

Welche STP-Variante sollte im Netzwerk primär implementiert werden?

Heterogene Multi-Vendor-Umgebung mit vielen VLANs (> 50)	Reines Cisco- oder Standard-Netzwerk mit moderater VLAN-Zahl (< 30)	Legacy-Umgebung mit alter Hardware und IEEE 802.1D
Implementiere MSTP (IEEE 802.1s) mit definierten Instanz-Gruppen für optimales Uplink-Load-Balancing.	Nutze Rapid-PVST+ oder RSTP (IEEE 802.1w) für Sub-Sekunden-Konvergenz bei minimalem Konfigurationsaufwand.	Modernisiere auf RSTP/MSTP; konfiguriere bis dahin Loop Guard und BPDU Guard an allen Access-Ports.

LINK AGGREGATION (LACP)

IEEE 802.3ad / 802.1ax

1. DEFINITION & KERNKONZEPT



Link Aggregation fasst mehrere physische Ethernet-Verbindungen zwischen zwei Netzwerkgeräten zu einer einzigen logischen Verbindung zusammen (oft als Port-Channel oder EtherChannel bezeichnet). Dies erhöht den aggregierten Durchsatz und schafft automatische Redundanz ohne Routing-Mehraufwand.

- Erhöhung der Gesamtbandbreite ohne kostspielige Schnittstellen-Upgrades.
- Ausfallsicherheit: Fällt ein physisches Kabel aus, verbleibt der Link im Betrieb.
- Verhindert Schleiten auf Schicht 2 in Kombination mit Spanning-Tree-Mechanismen.

2. STANDARDS & PROTOKOLLE



Für die Aushandlung stehen standardisierte sowie herstellerspezifische Verfahren zur Verfügung. IEEE 802.3ad wurde später in den Standard IEEE 802.1ax überführt und definiert LACP als herstellerübergreifendes Referenzprotokoll.

- IEEE 802.3ad / IEEE 802.1ax: Offener Industriestandard LACP.
- PAgP (Port Aggregation Protocol): Proprietärer Vorläufer von Cisco.
- Statischer Trunk: Manuelle Bündelung ohne Kontrollprotokoll (Mode: On).

3. LACP-MODI & AUSHANDLUNG



LACP tauscht Link Aggregation Control Protocol Data Units (LACPDUs) aus. Zwei Hauptmodi bestimmen das dynamische Aushandlungsverhalten zwischen zwei Switch-Ports.

- Active Mode: Sendet aktiv LACPDUs und initiiert die Kanabildung.
- Passive Mode: Wartet auf eintreffende LACPDUs und antwortet nur.
- Kompatibilität: Mindestens ein Endpunkt muss im Modus 'Active' konfiguriert sein.

PRAXIS-REGEL FÜR MODUSWAHL

Eine Verbindung zwischen zwei passiven Ports ('Passive' zu 'Passive') baut niemals einen aktiven Aggregations-Trunk auf.

4. LASTVERTEILUNG (LOAD-BALANCING)



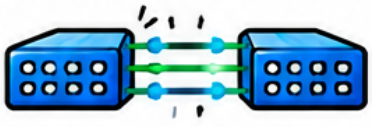
Der Datenverkehr wird nicht auf Bitebene über Leitungen verteilt, sondern pro Datenstrom (Flow) über Hash-Funktionen auf einzelne Links zugewiesen. Dies verhindert Out-of-Order-Pakete.

- Source-/Destination-MAC: Hash-Berechnung anhand von L2-Adressen.
- Source-/Destination-IP: Verteilung basierend auf IPv4- oder IPv6-Adressen.
- L4-Port-Hashing: Berücksichtigt TCP/UDP-Ports für feinere Lastverteilung.

5. FAILOVER-VERHALTEN & REDUNDANZ

Kommt es zu einer Leitungsunterbrechung oder einem Ausfall eines Ports, greift die automatische Fehlererkennung von LACP ohne Spanning-Tree-Neuberechnung für den gesamten Trunk.

- Source-/Destination Weiterbetrieb: Überlebechung Links tragen den restlichen Verkehr.
- LACP-Timer: Fast Periodic (1s Intervall, 3s Timeout) vs. Slow (30s Intervall, 90s Timeout).
- Kein STP-Flapping: Der logische Trunk-Port bleibt dauerhaft im Status 'Forwarding'.



6. VORAUSSETZUNGEN & SCHNITTSTELLENPARAMETER

Für einen fehlerfreien Zusammenschluss müssen alle gebündelten physikalischen Schnittstellen strikt identisch parametriert sein.

- Gleiche Bandbreite und Duplexmodus (z. B. 1 Gbit/s Full Duplex).
- Einheitliche VLAN-Konfiguration (Native VLAN und erlaubte Trunk-VLANs).
- Identische MTU-Größe auf allen Member-Ports des Trunks.



7. FEHLERBEHEBUNG & DIAGNOSE



Strukturierter Prüfpfad bei der Inbetriebnahme und Analyse inaktiver Port-Channels.

- Statusprüfung: 'show etherchannel' bzw. 'show lacp neighbor'.
- Port-Suspension: Überprüfung auf Duplex-, Speed- oder MTU-Abweichungen.
- Kabel- und Transceiver-Fehler auf Schicht 1 ausschließen.

SCHRITT FÜR SCHRITT

1. **Port-Status abfragen**
   Mit Management-Befehlen prüfen, ob der logische Channel als 'Up' markiert ist und welche Member-Ports teilnehmen.
2. **LACPDU-Austausch verifizieren**
   Sicherstellen, dass beidseitig Steuerframes empfangen werden und mindestens eine Seite auf 'Active' geschaltet ist.
3. **VLAN- und MTU-Konformität abgleichen**
   Fehlkonfigurationen bei Trunk-Zulassungen oder Frame-Größen korrigieren, um Port-Suspensions aufzuheben.

8. KURZÜBERBLICK & BEST PRACTICES



Zusammenfassung essenzieller Merkmale für den professionellen Netzwerkeinsatz.

- LACP (802.3ad/802.1ax) stets statischen Bündelungen vorziehen.
- L4-Hashing wählen, wenn viele parallele Verbindungen dieselben IPs nutzen.
- Trunk-Ausfallzeiten durch Fast-LACP-Timer minimieren.

Verwendeter Hash-Aligorithmus (L2/L3/L4) _____

LACP-Timer-Einstellung (Fast oder Slow) _____

Notizen zur Schnittstellenbelegung _____

IPv4-HEADER PROTOKOLLSTRUKTUR



1. GRUNDSTRUKTUR & BASISFELDER

Der IPv4-Header steuert die Vermittlung von Datenpaketen auf Vermittlungsebene (Schicht 3) und besitzt eine Standardlänge von 20 Bytes ohne optionale Zusatzfelder.

- **Version (4 Bit):** Definiert das Protokoll (stets Binärwert 0100 für IPv4).
- **IHL / Internet Header Length (4 Bit):** Gibt Header-Länge in 32-Bit-Wörtern an (Minimum 5 = 20 Bytes).
- **DSCP & ECN (8 Bit):** Bestimmt Dienstgüte (QoS-Priorisierung) und Benachrichtigung bei Netzwerküberlastung.
- **Total Length (16 Bit):** Gesamtlänge des Pakets (Header plus Payload) in Bytes (maximal 65.535 Bytes).

Header-Länge berechnen
Multipliziere den IHL-Wert stets mit 4: Ein IHL-Wert von 5 entspricht exakt 20 Bytes Standardheader.

2. FRAGMENTIERUNG & REASSEMBLY

Wenn ein Paket die Maximum Transmission Unit (MTU) eines Zwischennetzes überschreitet, teilt der Router das Paket auf und nutzt drei Header-Felder zum Wiederzusammensetzen.

- **Identification (16 Bit):** Eindeutige Kennung aller Fragmente eines ursprünglichen Datagramms.
- **Flags (3 Bit):** Bit 0 reserviert (0), Bit 1 DF (Don't Fragment), Bit 2 MF (More Fragments).
- **Fragment Offset (13 Bit):** Position der Nutzdaten im unfragmentierten Paket, gemessen in 8-Byte-Blöcken.
- **Reassembly:** Der Zielhost setzt das Gesamtpaket erst anhand übereinstimmender ID und Offsets zusammen.



3. KONTROLL- & PRÜFFELDER

Zur Vermeidung von Endlosschleifen und zur Gewährleistung intakter Adressierungsdaten werden Steuerwerte pro Zwischenstation aktualisiert.

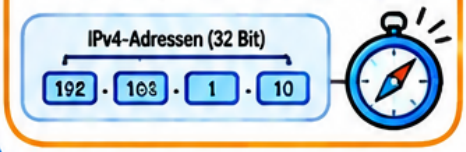
- **Time to Live / TTL (8 Bit):** Hop-Zähler; wird von jedem Router um 1 dekrementiert (Verwurf bei 0 mit ICMP Time Exceeded).
- **Protocol (8 Bit):** Weist Payload dem Zielprotokoll der Transportschicht zu (z. B. 0x06 = TCP, 0x11 = UDP, 0x01 = ICMP).
- **Header Checksum (16 Bit):** Einerkomplement-Prüfsumme ausschließlich über die Header-Felder.
- **Hop-by-Hop Aktualisierung:** Da die TTL sinkt, muss jeder Router die Prüfsumme zwingend neu berechnen.

Sicherheitshinweis zu TTL
Manipulationen oder ungewöhnliche TTL-Sprünge dienen Netzwerk-Scannern zum OS-Fingerprinting und Routing-Tracing.

4. ADRESSIERUNG & OPTIONEN

Die Ziel- und Quellangaben bilden das Fundament für weltweites Routing über autonome Systeme hinweg.

- **Source IP Address (32 Bit):** IPv4-Adresse des ursprünglichen Absenders.
- **Destination IP Address (32 Bit):** IPv4-Adresse des anvisierten Zielsystems.
- **Options & Padding (variabel):** Optionale Felder für Tests oder Source Routing; Padding füllt auf ein 32-Bit-Vielfaches auf.
- **Feste Position:** Quell- und Zieladresse liegen immer an Byte-Offset 12 bis 19 des Headers.



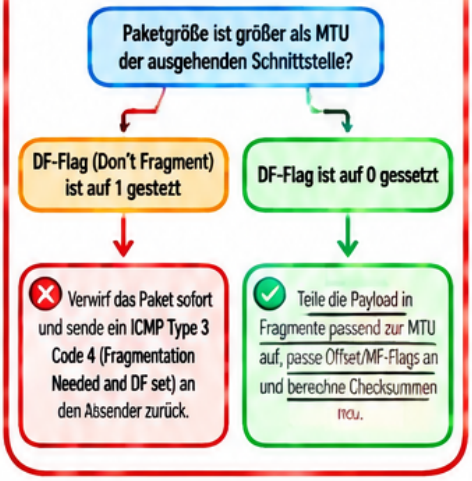
5. SCHRITT-FÜR-SCHRITT PAKETANALYSE

Gehe systematisch vor, um einen IPv4-Header im Hexadezimal-Dump manuell oder in Wireshark zu analysieren.

1. **Byte 0 prüfen** (Version & IHL)
   Überprüfe das erste Byte: Der Wert 0x45 zeigt Version 4 und IHL 5 (20 Bytes Header) an.
2. **Gesamtlänge auslesen** (Byte 2-3)
   Lies den 16-Bit-Wert von Total Length aus, um Header- und Nutzdatenumfang zu trennen.
3. **Fragmentierungs-Flags prüfen** (Byte 6)
   Prüfe Bit 1 (DF): Ist es gesetzt (Wert 0x40), darf kein Router das Paket unterteilen.
4. **TTL & Protokoll ermitteln** (Byte 8-9)
   Byte 8 liefert die verbleibende Hop-Zahl; Byte 9 bestimmt den Transport-Parser (TCP: 6, UDP: 17).
5. **Absender und Empfänger isolieren** (Byte 12-19)
   Wandle die beiden jeweils 4 Byte langen Abschnitte in dezimale Punktnotation zur Identifikation um.

6. ENTSCHEIDUNGSWEGWEISER: ROUTER-VERHALTEN

Wie reagiert ein Router, wenn ein ankommendes IPv4-Paket die Schnittstellen-MTU überschreitet?



7. PRAXIS-ARBEITSBLATT: HEADER-DEKODIERUNG

Trage hier deine ermittelten Werte aus einem Trace-Ausschnitt für eine eigene Laboranalyse ein.

Hex-Dump Byte 0-3 (Version, IHL, DSCP, Total Length):

Gefundene Quell- und Ziel-IP (Dotted Decimal):

Transportprotokoll & Port-Zuordnung:

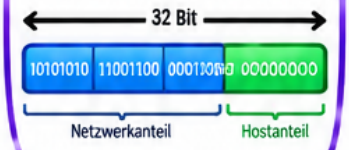
8. ZUSAMMENFASSUNG & MERKREGEL

Der IPv4-Header ist modular aufgebaut und bildet die Grundlage des weltweiten Routings.

- **Feste Basis:** Standard-Header ist exakt 20 Bytes lang.
- **Hop-Limit:** TTL verhindert permanente Routing-Schleifen.
- **Integrität:** Checksumme schützt nur den Header, nicht die Payload.
- **Adressen:** 32 Bit Quell- und 32 Bit Zieladresse sind unveränderlich im Core geroutet.

Prüfungsfokus
Merke die Standard-Protokollnummern für Byte 9: 1 = ICMP, 6 = TCP, 17 = UDP.

IPV4: KLASSEN VS. CIDR



1. GRUNDLAGEN DER IPV4-ADRESSIERUNG



Eine IPv4-Adresse besteht aus exakt 32 Bit, gliedert in vier Oktette à 8 Bit, getrennt durch Punkte (Dotted-Decimal-Notation, z. B. 192.168.1.1). Jede IP-Adresse teilt sich zwingend in zwei logische Bereiche: den Netzwerkanteil zur Identifikation des Subnetzes und den Hostanteil zur Identifikation des einzelnen Endgeräts.

- 32-Bit-Gesamtlänge entspricht einem mathematischen Adressraum von 2^32 (ca. 4,29 Milliarden Adressen).
- **Netzwerkanteil:** Bestimmt den Routing-Pfad im globalen und lokalen Netz.
- **Hostanteil:** Adressiert Schnittstellen konkreter Endgeräte innerhalb des Zielnetzes.
- Grenze zwischen Netz- und Hostanteil wird erst durch die Subnetzmaske bzw. den Präfix definiert.

Kernprinzip der Adressteilung
Ohne zugehörige Subnetzmaske oder Präfixlänge ist eine IPv4-Adresse nicht routingfähig, da Router Anfang und Ende des Zielnetzwerks nicht ermitteln können.

2. HISTORISCHE KLASSENNETZE (CLASSFUL)



Im ursprünglichen Classful-Modell (RFC 791) war die Grenze zwischen Netzwerk- und Hostanteil fest durch die führenden Bits der Adresse vorgegeben. Es gab keine flexiblen Masken; Router erkannten die Netzgröße strikt anhand der ersten Bits im ersten Oktett.

- **Klasse A** (0.0.0.0 bis 127.255.255.255): Erstes Bit '0', Standardmaske /8 (255.0.0.0). 126 Netze mit je 16.777.214 nutzbaren Hosts.
- **Klasse B** (128.0.0.0 bis 191.255.255.255): Erste Bits '10', Standardmaske /16 (255.255.0.0). 16.384 Netze mit je 65.534 Hosts.
- **Klasse C** (192.0.0.0 bis 223.255.255.255): Erste Bits '110', Standardmaske /24 (255.255.255.0). ca. 2,09 Mio. Netze mit je 254 Hosts.
- **Klasse D** (224.0.0.0/4 für Multicast) & **Klasse E** (240.0.0.0/4 für experimentelle Zwecke reserviert).

4. CIDR & PRÄFIXNOTATION (RFC 4632)



Classless Inter-Domain Routing (CIDR) hob 1993 die festen Klassengrenzen vollständig auf. Die Subnetzmaske wird nun flexibel als Schrägstrich gefolgt von der Anzahl der fortlaufenden Netzwerk-Bits dargestellt (CIDR-Präfix /n).

- **Freie Bitgrenzen:** Ein Präfix kann jeden ganzzahligen Wert von /0 bis /32 annehmen.
- Präfix /24 entspricht 255.255.255.0 (24 gesetzte Netzwerk-Bits, 8 Host-Bits).
- Präfix /27 entspricht 255.255.255.224 (27 Netzwerk-Bits, 5 Host-Bits -> 32 Adressen, 30 Hosts).
- Präfix /30 (4 Adressen, 2 Hosts) dient ideal für Punkt-zu-Punkt-Verbindungen zwischen zwei Routern.

5. ROUTE AGGREGATION & SUPERNETTING



Ein zentraler Vorteil von CIDR ist das Aggregieren mehrerer zusammenhängender Teilnetze zu einer einzigen zusammenfassenden Routing-Ankündigung (Supernetting).

- **Entlastung der Backbone-Router:** Tausende Netzrouten werden zu wenigen summarischen Präfixen zusammengefasst.
- **Beispiel:** Vier /24-Netze (192.168.0.0/24 bis 192.168.3.0/24) werden zusammengefasst als 192.168.0.0/22.
- **Voraussetzung für Supernetting:** Die Netze müssen bitweise zusammenhängend und an derselben Bitgrenze ausgerichtet sein.
- **BGP-Effizienz:** Verhindert Speicherüberläufe und Rechenlasten in den globalen Internet-Routern.

6. SCHRITT-FÜR-SCHRITT: CIDR-SUBSTRUKTUREN BERECCHNEN

Pnhand der CIDR-Präfixlänge:



- Freie Bit. Fost Bits ermitelen kann
- Rskrite B (128.0.0.0 bis Adressen im Block berechneri.
- Abzrift Sun Netzbare Horl Broadcastmon.
- Rikste 4 : (26 bis 22.0.0.0 bis 22 (26 bebinc.ziff. bagbarer Hentes).

Präfix /30 (4 Adressen, 2 Hosts) dient ideal für

Beispiel: /26

6. SCHRITT-FÜR-SCHRITT: CIDR-SUBSTRUKTUREN BERECHNEN



Praktischer Leitfaden zur Bestimmung von Subnetz-Parametern anhand der CIDR-Präfixlänge:

- **Schritt 1:** Host-Bits ermitteln (h = 32 - Präfixlänge n).
- **Schritt 2:** Gesamtzahl der Adressen im Block berechnen (2^h).
- **Schritt 3:** Nutzbare Host-Adressen bestimmen (2^h - 2; Abzug von Netzadresse und Broadcast).
- **Schritt 4:** Subnetzmaske im betroffenen Oktett ermitteln (256 - Blockgröße).

Beispiel: /26

1	2	3	4
Host-Bits identifizieren	**Blockgröße berechnen**	**Nutzbare Schnittstellen festlegen**	**Subnetzmaske bilden**
32 - 26 = 6 Host-Bits.	2^6 = 64 Adressen pro Subnetz.	64 - 2 = 62 konfigurierbare Host-Adressen.	255.255.255.192

7. PRAXISVERGLEICH: KLASSEN VS. CIDR BEISPIEL



Gegenüberstellung einer realen Netzzuweisung für eine Niederlassung mit genau 50 Hosts:

- **Klassisches Modell:** Zuweisung eines vollen Klasse-C-Netzes (/24 mit 254 Hosts). **Adressverschwendung: 204 Adressen** (ca. 80 % ungenutzt).
- **CIDR-Modell:** Zuweisung eines maßgeschneiderten /26-Netzes (62 nutzbare Hosts). **Adressverschwendung:** Lediglich 12 ungenutzte Adressen.
- **Sicherheitsgewinn:** Kleinere Broadcast-Domänen und minimierte Angriffsflächen für ARP-Spoofing und unautorisierte Geräte.

CIDR-Auswahlentscheidung
Wählen Sie stets die kleinste Zweierpotenz, die den Hostbedarf plus Netzadresse und Broadcast-Adresse vollständig deckt.

Welche CIDR-Präfixlänge eignet sich für die Anforderung?

Genau 2 nutzbare Router-Schnittstellen (Transfernetz)	Wähle /30 (4 Adressen: Netzadresse, 2 Host-IPs, Broadcast).
Zwischen 3 und 14 Endgeräte	Wähle /28 (16 Adressen: 14 nutzbare Hosts).
Zwischen 15 und 30 Endgeräte	Wähle /27 (32 Adressen: 30 nutzbare Hosts).
Swischen 31 und 62 Endgeräte	Wähle /26 (64 Adressen: 62 nutzbare Hosts).

8. ZUSAMMENFASSUNG & MERKSÄTZE

Wesentliche Erkenntnisse für Prüfung und Praxisnetzwerke:

- Klassennetze (A, B, C) sind historisch überholt; heutiges IPv4-Routing basiert ausschließlich auf CIDR.
- CIDR trennt Netz- und Hostanteil an beliebigen Bitpositionen (RFC 4632).
- Die CIDR-Notation /n nennt die genaue Anzahl führender Netzwerk-Einsen in der 32-Bit-Maske.
- Supernetting (Route Aggregation) schützt globale Routingtabellen vor Überlastung.
- Netzadresse (alle Host-Bits 0) und Directed Broadcast (alle Host-Bits 1) dürfen keinen Endgeräten zugewiesen werden.



Ermittelte Netzadresse (z. B. 192.168.10.0/26):

Berechnete Broadcast-Adresse:

Verfügbarer Host-Bereich (Erste bis letzte nutzbare IP):

PRIVATE IPv4-ADRESSEN & SPEZIALBEREICHE

Private IPv4-Adressen sind nicht im öffentlichen Internet routbar und bilden die Basis für sichere Netzwerksegmente.

1. 10.0.0.0/8 ENTERPRISE CLASS



- Großkonzerne und komplexe Campusnetze.
- 16.777.216 Adressen.
- Ideal für große Netzwerke.

2. 172.16.0.0/12 MID-SIZE SUBNETS



- Firmen- und Laborumgebungen.
- 1.048.576 Adressen (16 × /16-Präfixe).
- Flexibel und skalierbar.

3. 192.168.0.0/16 HOME & SOHO



- Heimanwender und Zweigstellen.
- 65.536 Adressen (256 Subnetze /24).
- Standard für kleine Netzwerke.

4. NAT & GATEWAY TRANSLATION



- Private IPs ins Internet.
- Source-NAT (SNAT/Masquerading).
- Am Gateway bzw. Firewall.

5. 127.0.0.0/8 LOOPBACK



- Interne Kommunikation.
- Standard: 127.0.0.1.
- Verlässt den Rechner nicht.

6. 169.254.0.0/16 APIPA LINK-LOCAL



- Automatische Selbstkonfiguration.
- Kein DHCP-Server erreichbar.
- Nur im selben Switch-Segment.

Sicherheitsaspekt RFC 1918
Pakete mit privaten Quell- oder Zieladressen werden von Internet-Core-Routern verworfen (Drop). Dies bietet einen Basis-Schutz, ersetzt jedoch keine zustandsbehaftete Firewall.

7. RFC 6598 CGNAT 100.64.0.0/10



- Internetdienstanbieter.
- Adressraum für Carrier-Grade NAT.
- Mehrere Kunden hinter einer öffentlichen IP.

8. ROUTING DROP RULE & FILTER



- Private IPs werden von Internet-Core-Routern verworfen.
- Schutz vor unerwünschtem Routingverkehr.
- Firewall-Regeln zusätzlich nutzen.

1. ZWECK UND SCHUTZFUNKTION PRIVATER IP-BEREICHE

Private IPv4-Adressen nach RFC 1918 sind globale IP-Bereiche, die in lokalen Netzwerken beliebig oft wiederverwendet werden können, da sie im öffentlichen Internet nicht geroutet werden. Sie bilden das Fundament moderner Netzwerksegmentierung und schonen den knappen IPv4-Adressraum.

- Keine direkte Erreichbarkeit aus dem weltweiten Internet ohne Vermittlungsinstanz.
- Schutz vor direkten Scans und unerwünschtem einfallendem Routingverkehr.
- Kommunikation ins Internet erfordert Network Address Translation (NAT) am Gateway.

Sicherheitsaspekt RFC 1918
Pakete mit privaten Quell- oder Zieladressen werden von Internet-Core-Routern verworfen (Drop). Dies bietet einen Basis-Schutz, erstazt jedoch keine zustandsbehaftete Firewall.

2. KLASSIFIKATION DER DREI RFC-1918-BLÖCKE

RFC 1918 definiert exakt drei Adressbereiche für private Netzwerke, die sich in Größe und typischem Einsatzgebiet unterscheiden:

- 10.0.0.0/8 (10.0.0.0 – 10.255.255.255): 16.777.216 Adressen, ideal für Großkonzerne und komplexe Campusnetze.
- 172.16.0.0/12 (172.16.0.0 – 172.31.255.255): 1.048.576 Adressen in 16 zusammenhängenden /16-Präfixen, häufig in Firmen- und Laborumgebungen.
- 192.168.0.0/16 (192.168.0.0 – 192.168.255.255): 65.536 Adressen in 256 Subnetzen (/24), Standard für Heimanwender und Zweigstellen.

3. SPEZIELLE IPv4-SONDERBEREICHE

Neben RFC 1918 existieren weitere reservierte Sonderadressen mit systemkritischen Steuerfunktionen, die ebenfalls nicht für das globale Internet-Routing freigegeben sind:

- **Loopback** (127.0.0.0/8): Interne Kommunikation auf demselben Host (Localhost, Standard: 127.0.0.1).
- **APIPA / Link-Local** (169.254.0.0/16): Automatische Selbstkonfiguration bei Ausfall des DHCP-Servers.
- **Carrier-Grade NAT** (100.64.0.0/10): Adressraum für Internetdienstanbieter nach RFC 6598.
- **Multicast** (224.0.0.0/4): Adressblock für Gruppenkommunikation (Klasse D).

APIPA-Verhalten erkennsen
Erhält ein Client eine IP aus 169.254.x.x, konnte der Host keinen DHCP-Server erreichen. Er kann nur mit Systemen im selben physischen Switch-Segment sprechen.

4. PRAKTISCHER WORKFLOW: IP-KLASSIFIKATION UND ROUTING-CHECK

Folgen Sie dieser Anleitung, wenn Sie im Terminal oder in Firewall-Logs eine IP-Adresse verifizieren müssen:

1. Erstes Oktett analysieren
   Prüfen Sie das erste Oktett: Beginnt die Adresse mit 10, 127, 169, 172 oder 192??
2. Subnetzgrenze gegen RFC-Definition prüfen
   Liegt die Adresse in 10.0.0.0/8, 172.16.0.0/12 oder 192.168.0.0/16? Bei 172.x muss das zweite Oktett zwischen 16 und 31 liegen.
3. Sonderfunktionen ausschließen
   Prüfen Sie auf Loopback (127.0.0.1) oder APIPA (169.254.x.x). Diese Pakete dürfen den Host bzw. das lokale Kabelsegment niemals verlassen.
4. Routing- und NAT-Regel validieren
   Soll das Paket ins Internet gelangen, verifizieren Sie, ob das Border-Gateway Source-NAT (SNAT/Masquerading) mit einer öffentlichen IP ausführt.

Welcher Adresskategorie ist die vorliegende IP zuzuordnen?

Adresse beginnt mit 10., 172.16-31. oder 192.168.	RFC 1918 Privatnetz: Intern routbar. Gateway benötigt NAT für Internetzugriff.
Adresse beginnt mit 169.254.	APIPA Link-Local: Lokale Notkonfiguration; DHCP-Server-Erreichkarkeit und Switch-Port prüfen.
Adresse beginnt mit 127.	Loopback-Schnittstelle: Lokaler Host, verlässt den Rechner nicht.
Reine Übereinstimmung mit Sonderbereichen	Öffentliche IP-Adresse: Global im Internet routbar.

5. LABOR-ARBEITSBLATT: NETZWERK-DOKUMENTATION

Erfassen Sie hier die lokalen Subnetze und Sonderadressen Ihrer Laborumgebung:

Zugeordnetes RFC 1918 Subnetz (z. B. 192.168.10.0/24)

Standard-Gateway / NAT-Router IP

DHCP-Vergabebereich (Pool von – bis)

Lokale Loopback-Dienste (Port & Dienst)

SUBNETTING & BIT-MASKEN

1. WAS IST SUB-NETTING?



Subnetting unterteilt einen größen IPv4-Adressbereich in kleinere, logisch isolierte Teilnetze (Subnetze). Dies optimiert die Adressnutzung, verkleinert Broadcast-Domänen und strukturiert Netze nach Standorten oder Abteilungen.

- **Ziel:** Gezielte Segmentierung und effiziente Zuweisung knapper IPv4-Ressourcen.
- **Sicherheit:** Trennt Netzzonen und ermöglicht differenzierte Firewall-Regeln.
- **Performance:** Begrenzt Broadcast-Traffic strikt auf das lokale Segment.

2. DIE BIT-STRUKTUR DER SUBNETZMASKE

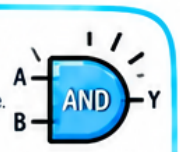


Eine IPv4-Adresse umfasst exakt 32 Bit (4 Oktette). Die Subnetzmaske weist jedem Bit eine feste Funktion zu: Eine ununterbrochene Kette aus Einsen (1) definiert den Netzteil, gefolgt von einer Kette aus Nullen (0) für den Hostteil.

- **Beispiel /24:** 11111111.11111111.11111111.00000000 = 255.255.255.0
- **Beispiel /26:** 11111111.11111111.11111111.11000000 = 255.255.255.192
- **Host-Kapasität:** Bestimmt durch n Nullen im Hostbereich via 2^n Adressen.



3. BITWEISES UND (LOGISCHES ANDING)



Router bestimmen das Zielnetz durch bitweise AND-Verknüpfung von IP-Adresse und Subnetzmaske. Ein Bit im Ergebnis ist nur dann 1, wenn beide Ausgangsbits 1 sind.

- **Bahrheitstabelle:** 1 AND 1 = 1; alle anderen Bitkombinationen ergeben 0.
- **Funktion:** Maskiert alle variablen Host-Bits aus und liefert die eindeutige Netzadresse.
- **Routing:** Ermöglicht dem Router den schnellen Lookup in der Forwarding-Tabelle.



Rechenregel ANDing
IP-Bit (1) AND Masken-Bit (1) = 1.
Sobald ein Masken-Bit 0 ist, wird das Ergebnis im Hostteil zwingend zu 0 gesetzt.

4. SCHRITT-FÜR-SCHRITT BERECHNUNG



Standardisierter Algorithmus zur manuellen Ermittlung aller relevanten Kenndaten eines Subnetzes bei gegebener Host-IP und CIDR-Maske.

1. **Schritt 1: Host-Bits ermitteln**
   Ziehe das CIDR-Präfix von 32 ab: n = 32 − Präfix (z. B. bei /26: 32 − 26 = 6 Host-Bits).
2. **Schritt 2: Blockgröße berechnen**
   Potenziere zur Basis 2: Gesamtzahl der Adressen = 2^n (z. B. 2^6 = 64 Adressen pro Subnetz).
   (z. B. 2^6 = 64 Adressen
3. **Schritt 3: Netz- & Broadcastadresse bestimmen**
   Netzadresse: Alle Host-Bits auf 0. Broadcastadresse: Alle Host-Bits auf 1 (oder Netzadresse +
   Alle Host-Bits esgesamtzose = Blockgröße - 1).
4. **Schritt 4: Nutzbare Host-Range festlegen**
   Erste nutzbare IP = Netzadresse + 1.
   Letzte nutzbare IP = Broadcastadresse − 1.

5. KONKRETES PRAXISBEISPIEL: 192.168.10.77 /26



Detaillierte Zerlegung einer IP-Adresse im /26-Präfix zur Veranschaulichung der mathematischen Transformation.

- **Gegeben:** IP 192.168.10.77 mit Subnetzmaske 255.255.255.192 (/26).
- **Viertes Oktett binär:** IP = 01001101 (77). Maske = 11000000 (192).
- **Ergebnis ANDing:** 01000000 = 64 (Netzadresse: 192.168.10.64).
- **Broadcast-Adresse:** 64 + 64 − 1 = 127 (192.168.10.127).
- **Nutzbare Hosts:** 192.168.10.65 bis 192.168.10.126 (insgesamt 62 Endgeräte).

IP	01001101
Maske	11000000
AND = 64	01000000

6. DIE ZWEI RESERVIERTEN SONDER-ADRESSEN



In jedem Subnetz sind exakt zwei Adressen reserviert und dürfen keinem Host (PC, Server, Drucker) statisch oder per DHCP zugewiesen werden.

- **Netzadresse** (Host-Bits alle 0): Repräsentiert das Subnetz seblst im Routing.
- **Broadcastadresse** (Host-Bits alle 1): Adressiert alle Knoten gleichzeitig im lokalen Netzsegment.
- **Formel nutzbare Hosts:** $2^n - 2$ (wobei n der Anzahl der Host-Bits entspricht).



Achtung bei Planungen
Vergiss beim Dimensionieren niemals das Abziehen der 2 Adressen. Ein /30 bietet genau 4 Adressen, wovon exakt 2 für Hosts nutzbar sind (ideal für Router-Point-to-Point-Links).

7. CIDR-PRÄFIX-SCHNELLREFERENZ

Kompakte Orientierungstabelle für gängige Subnetze im letzten Oktett (/24 bis /30) zur schnellen Auslegung.

Präfix	Maske (letztes Oktett)	Blockgröße	Nutzbare Hosts
/24	.0	256	254
/25	.128	128	126
/26	.192	64	62
/27	.224	32	30
/28	.240	16	14
/29	.248	8	6
/30	.252	4	2 (Punkt-zu-Punkt)



8. ENTSCHEIDUNG & PRAXIS-WORKBENCH



Nutze den Entscheidungsbaum zur Bestimmung der Maske und trage die Berechnungswerte direkt in die Arbeitszeilen ein.

Gegebene Ziel-IP und CIDR-Präfix: _____

Subnetzmaske (Dezimal & 4. Oktett Binär): _____

Netz-ID und Broadcast-Adresse: _____

Gültige Host-Range (Erste bis letzte IP): _____

Welche Netzmaske deckt den Hostbedarf bei minimalem Adressverlust?

- Bedarf <= 2 Hosts (z. B. Router-Link) → Wähle /30 (255.255.255.252). 4 Adressen insgesamt, 2 nutzbar.
- Bedarf 3 bis 14 Hosts → Wähle /28 (255.255.255.240). 16 Adressen insgesamt, 14 nutzbar.
- Bedarf 15 bis 62 Hosts → Wähle /26 (255.255.255.192). 64 Adressen insgesamt, 62 nutzbar.
- Bedarf 63 bis 126 Hosts → Wähle /25 (255.255.255.128). 128 Adressen insgesamt, 126 nutzb

VARIABLE LENGTH SUBNET MASKING (VLSM)

Effiziente Adressraumoptimierung nach exaktem Hostbedarf

1. DEFINITION & KERNKONZEPT

Variable Length Subnet Masking (VLSM) ermöglicht die Unterteilung eines IP-Netzwerkbereichs in Subnetze mit unterschiedlichen Präfixlängen (Subnetzmasken). Im Gegensatz zum starren Classful- oder FLSM-Subnetting (Fixed Length Subnet Masking) wird der Adressraum an den realen Host-Bedarf angepasst.

- Vermeidung massiver Verschwendung von Host-Adressen in IPv4-Netzen.
- Hierarchisches Aufteilen größerer Blöcke in kleinere Teilnetze.
- Zwingende Voraussetzung: Classless-Routing-Protokolle (z. B. OSPF, EIGRP, BGP, RIPv2).

2. FLSM VS. VLSM IM VERGLEICH



Gleiche Maske für alle Subnetze

Unterschiedliche Masken pro Segment

- FLSM: Einheitliche Blockgröße führt bei Punkt-zu-Punkt-Links (2 Hosts) zu bis zu 95 % Adressverlust.
- VLSM: Punkt-zu-Punkt-Links erhalten präzise /30- oder /31-Netze, während Serverfarmen /24 erhalten.
- Optimale Ausnutzung privater (RFC 1918) und knapper öffentlicher IPv4-Adressräume.

3. DIE FORMEL ZUR HOST-BERECHNUNG

Jedes Subnetz reserviert zwei Adressen: die Netzadresse (alle Host-Bits 0) und die Broadcast-Adresse (alle Host-Bits 1).

- Formel für nutzbare Hosts: 2^h - 2 >= erforderliche Hosts (h = Anzahl Host-Bits).
- Präfixlänge: 32 - h = CIDR-Präfix (z. B. 32 - 6 = /26 für 62 nutzbare Hosts).
- Blockgröße (Schrittweite im letzten Oktett): 2^h bzw. 256 minus Subnetzmaskenwert.

Subnetz-Berechnung beachten

Die zwei reservierten Adressen (Netz-ID und Broadcast) dürfen niemals Endgeräten zugewiesen werden. Bei /30 (4 Adressen) bleiben genau 2 nutzbare IP-Adressen übrig.

4. SCHRITTWEISE VLSM-PLANUNG

Zur Vermeidung von Überlappungen müssen Teilnetze stets absteigend nach Hostbedarf sortiert und adressiert werden.

1. **Schritt 1: Bedarfsanalyse und Sortierung**
   Listen Sie alle benötigten Subnetze auf und sortieren Sie diese zwingend in absteigender Reihenfolge nach der Anzahl benötigter nutzbarer Host-Adressen.
2. **Schritt 2: Blockgröße und Maske ermitteln**
   Bestimmen Sie für jedes Subnetz die kleinste Zweierpotenz, die (Bedarf + 2) abdeckt, und errechnen Sie das zugehörige Präfix (/xx).
3. **Schritt 3: Fortlaufende Adressvergabe**
   Weisen Sie dem größten Subnetz die Basisadresse zu. Das nächste Subnetz beginnt exakt an der nächsten Blockgrenze (Netzadresse + Blockgröße).
4. **Schritt 4: Router-Links am Ende adressieren**
   Weisen Sie Punkt-zu-Punkt-Verbindungen zwischen Routern kleine /30-Blöcke (4 IPs, 2 Hosts) aus den verbliebenden Abschnitten zu.

5. BERECHNUNGSBEISPIEL: Ausgangsnetz 192.168.10.0/24

Aufteilung eines /24-Netzes für eine Firmenzentrale mit unterschiedlichen Segmenten:

- Segment A (50 Hosts):
  Benötigt 2^6 = 64 Adressen -> 192.168.10.0/26
  (Nutzbar: .1 bis .62, Broadcast: .63).
- Segment B (25 Hosts):
  Benötigt 2^5 = 32 Adressen -> 192.168.10.64/27
  (Nutzbar: .65 bis .94, Broadcast: .95).
- Segment C (12 Hosts):
  Benötigt 2^4 = 16 Adressen -> 192.168.10.96/28
  (Nutzbar: .97 bis .110, Broadcast: .111).
- WAN-Link (2 Hosts):
  Benötigt 2^2 = 4 Adressen -> 192.168.10.112/30
  (Nutzbar: .113 bis .114, Broadcast: .115).

6. TYPISCHE FEHLER & ÜBERLAPPUNGEN VERMEIDEN

Die häufigsten Stolperfallen bei der praktischen Umsetzung von VLSM in Unternehmensnetzen:

- Falsche Reihenfolge: Wer kleine Subnetze vor größen plant, zerschneidet Adressblöcke und erzeugt ungenutzte Lücken.
- Ungültige Startadresse: Jedes Subnetz muss an einer ganzzahligen Vielfachen seiner Blockgröße beginnen.
- Verwendung veralteter Routing-Protokolle: RIPv1 überträgt keine Subnetzmasken und kann VLSM nicht routen.

Achtung bei Routen-Zusammenfassung

Unüberelgte VLSM-Strukturen erschweren die Routen-Aggregation (Supernetting). Planen Sie zusammenfassbare Hierarchien pro Standort ein.

7. ENTSCHEIDUNGSLOGIK FÜR DAS SUBNETZ-DESIGN

Ermitteln Sie die passende Maske anhand des konkreten Segments:

Welche Art von Netzwerksegment muss adressiert werden?

Punkt-zu-Punkt-Verbindung zwischen zwei Routern	Standard-Client- oder Server-VLAN mit 10 bis 250 Endgeräten	Große Campus-Netzwerke oder WLAN-Gastnetze (> 245 Geräte)
Verwenden Sie /30 (2 nutzbare Adressen) oder RFC 3021 /31 (falls Router Punkt-zu-Punkt ohne Broadcast unterstützen).	Ermitteln Sie die nächste Zweierpotenz (2^h - 2 >= Bedarf) und wählen Sie das Präfix zwischen /28 (14 Hosts) und /24 (254 Hosts).	Präfixe unter /24 wählen (/23 für bis zu 510 Hosts, /22 für bis zu 1022 Hosts) und Routing-Aggregation berücksichtigen.

8. VLSM-PLANUNGSPROTOKOLL & ARBEITSBLATT

Verwenden Sie dieses Formular zur praktischen Berechnung und Dokumentation eines neuen Adressbereichs.

Segmentname / Standort:

Benötigte nutzbare Host-Adressen:

Zugeordnete CIDR-Präfixlänge & Subnetzmaske (z. B. /27 - 255.255.255.224):

Netzwerk-ID / Startadresse:

Nutzbarer Host-Bereich (Erste IP bis Letzte IP):

Broadcast-Adresse:

CIDR & SUPERNETTING: ADRESSAGGREGATION

1. KLASSENBASIERTE GRENZEN VS. CIDR



Frühe IPv4-Netze waren starr in Klassen unterteilt (Klasse A mit /8, B mit /16, C mit /24). Dies führte zu enormer Adressverschwendung und drohender Erschöpfung des IPv4-Adressraums. CIDR (Classless Inter-Domain Routing, RFC 1519) hob diese starren Klassengrenzen auf und erlaubt beliebige Präfixlängen.

- Klassenbasiert: Klasse C bot lediglich 254 Hosts, Klasse B direkt 65.534 Hosts ohne praxistaugliche Zwischenstufen.
- CIDR-Prinzip: Beliebige Bitlängen für den Netzwerkteil (/8 bis /32) ermöglichen bedarfsgerechte Adresszuteilung.
- Effizienzgewinn: Vermeidet die Zuweisung überdimensionierter Adressblöcke an Organisationen.

GRUNDREGEL
CIDR trennt Netz- und Hostanteil bitgenau über die Präfixlänge, völlig unabhängig von der ersten IP-Ziffer.

2. CIDR-NOTATION UND PRÄFIXLÄNGEN (/8 BIS /32)



Die CIDR-Notation kennzeichnet ein Netzwerk durch die IP-Basisadresse, gefolgt von einem Schrägstrich und der Anzahl gesetzter Netzwerkbits im Präfix. Je kürzer das Präfix, desto größer ist der verfügbare Hostbereich im Subnetz.

- /8 entspricht 255.0.0.0 (16.777.214 nutzbare Hosts)
- /16 entspricht 255.255.0.0 (65.334 nutzbare Hosts)
- /24 entspricht 255.255.255.0 (254 nutzbare Hosts)
- /30 entspricht 255.255.255.252 (2 nutzbare Hosts für Point-to-Point-Links)
- /32 entspricht 255.255.255.255 (Host-Route, Einzeladresse)

3. SUPERNETTING: PRINZIP UND MECHANIK



Supernetting fasst mehrere zusammenhängende kleinere Netze (z. B. mehrere /24-Netze) durch Verkürzen der gemeinsamen Präfixmaske zu einem übergeordneten Supernetz zusammen. Die Router-Hardware gleicht dabei nur noch die gemeinsamen führenden Bits ab.

- **Bedingung 1:** Die zusammenzufassenden Subnetze müssen binär lückenlos aneinandergrenesen (kontiguierlich).
- **Bedingung 2:** Die Anzahl der Netze muss eine Zweierpotenz sein (2, 4, 8, 16...).
- **Bedingung 3:** Die erste IP-Adresse des Blocks muss sich ganzzahlig durch die Gesamtzahl der Hostadressen teilen lassen.

SUPERNETTING-VORAUSSETZUNG
Ungleiche oder getrennte Netzblöcke können nicht sauber in einem einzigen Präfix ohne Nebenwirkungen gebündelt werden.

4. ROUTE SUMMARIZATION IN BACKBONE-NETZEN



Durch Routenkonsolidierung (Route Summarization) kündigt ein Edge-Router gegenüber Upstream-Providern und dem Internet-Backbone nur ein einziges aggregiertes Präfix an, anstatt dutzende Einzelsubnetze separat zu propagieren.

- **Beispiel:** Vier /24-Netze (192.168.0.0/24 bis 192.168.3.0/24) teilen 22 gemeinsame Bits.
- **Zusammenfassung:** Die vier Netze werden als 192.168.0.0/22 angekündigt.
- **Topologie-Vorteil:** Interne Netzschwankungen (Flapping Links) verbleiben lokal und triggern keine globalen BGP-Updates.

5. REDUKTION VON ROUTINGTABELLENGRÖßEN

Ohne Aggregation müssten globale Router Millionen spezifischer Routen im extrem schnellen TCAM-Speicher verwalten. CIDR und Route Summarization verhindern die Überlastung des BGP-Routingtisches der Internet-Core-Router.

- **TCAM-Entlastung:** Drastische Verringerung des Speicherbedarfs auf Core- und Edge-Routern.
- **CPU-Schonung:** Schnellere Routing-Entscheidungen durch kürzere Tabellendurchläufe.
- **Stabilität:** Lokale Flaps erreichen dank Aggregation nicht den weltweiten DFZ (Default-Free Zone).



6. ZUWEISUNGSHIERARCHIE: IANA UND RIRs

Öffnulliche IP-Adressräume und CIDR-Blöcke werden streng hierarchisch zugeteilt. Dies gewährleistet, dass Provider große Blöcke erhalten, die geographisch und strukturell konsolidiert geroutet werden können.

- **IANA:** Verwaltet den globalen IP-Adressraum auf oberster Ebene.
- **RIRs (Regional Internet Registries):** Z. B. RIPE NCC (Europa), ARIN (Nordamerika), APNIC (Asien-Pazifik).
- **ISPs und Endkunden:** Erhalten aggregierbare CIDR-Blöcke (z. B. /20 oder /19) zur internen Verteilung.



7. SCHRITT-FÜR-SCHRITT: AGGREGATION MANUELL BERECHNEN



Folgen Sie diesem Ablauf, um mehrere zusammenhängende Teilnetze zu einer fehlerfreien Supernetting-Route zusammenzufassen.

1. **Subnetze binär notieren**
   Schreiben Sie die Oktette der Ausgangsnetze in Binärform auf, insbesondre das Oktett, in dem sich die Adressen unterscheiden.
2. **Gemeinsame Präfix-Bits ermittlen**
   Zählen Sie von links nach rechts, wie viele Bits in allen Netzadressen exakt identisch sind.
3. **Neue Präfixlänge bestimmen**
   Die Anzahl der übereinstimmenden Bits ergibt den neuen CIDR-Präfixwert (z. B. 22 dientische Bits = /22).
4. **Supernetz-Adresse und Maske festlegen**
   Setzen Sie alle restlichen Host-Bits auf 0. Die resultierende Adresse mit der neuen Bitlänge bildet das konsolidierte Supernetz.

8. LONGEST PREFIX MATCH & ROUTING-ENTSCHEIDUNG



Enthält die Routingtabelle sowohl aggregierte Routen als auch spezifische Subnetze, entscheidet das Prinzip des Longest Prefix Match über den Paketpfad.

- **Spezifität gewinnt:** Ein Router wählt stets die Route mit dem längsten passenden Präfix (höchste Bitanzahl).
- **Beispiel:** Ziel 192.168.1.50 passt auf 192.168.0.0/22 und 192.168.1.0/24. Der Router wählt zwingend /24.

PRAXIS-TIPP
Mithilfe von Longest Prefix Match können gezielte Ausnahme-Routen trotz übergeordneter Aggregation definiert werden.

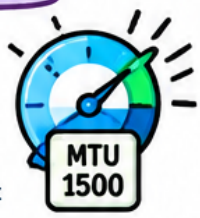
Eigene Subnetze für Zusammenfassung (z. B. 10.0.4.0/24 bis 10.0.7.0/24):

Ermitteltes konsolidiertes Supernetz (Basisadresse / Präfix):

IPv4-FRAGMENTIERUNG & PMTUD

1. GRUNDLAGEN DER MTU

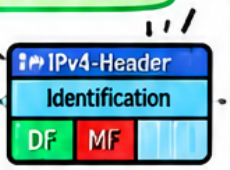
Die Maximum Transmission Unit (MTU) definiert die maximale Nutzdaten- bzw. Paketgröße (inklusive IP-Header), die auf einer Schicht-2-Verbindung ohne Aufteilung übertragen werden kann. Standard-Ethernet nutzt eine MTU von 1500 Bytes. Überschreitet ein IPv4-Paket die MTU des ausgehenden Interfaces, muss es fragmentiert oder verworfen werden.



- Ethernet-Standard: 1500 Bytes maximale IP-Paketgröße
- Kürzere MTU durch Tunnelprotokolle (z. B. PPPoE: 1492 Bytes, GRE, IPsec)
- Minimale IPv4-Standard-MTU: 576 Bytes gemäß RFC 791

2. IP-HEADER: IDENTIFICATION & FLAGS

Für die Fragmentierung reserviert der IPv4-Header drei essenzielle Steuerfelder: das Identification-Feld zur Zuordnung und zwei Kontroll-Flags, die das Verhalten von Routern und Endsystemen steuern.



- Identification (16 Bit): Eindeutige ID aller zusammengehörigen Fragmente eines Originalpakets
- DF-Flag (Don't Fragment): Bit 1 im Flag-Feld. Verbietet Routern die Fragmentierung; bei MTU-Überschreitung wird verworfen
- MF-Flag (More Fragments): Bit 2 im Flag-Feld. Steht auf 1 für alle Fragmente außer dem letzten (MF = 0)

3. FRAGMENT OFFSET BERECHHUNG

Das Fragment-Offset-Feld (13 Bit) gibt die Position der fragmentierten Nutzdaten bezogen auf das Ursprungspaket in 8-Byte-Blöcken (64-Bit-Schritten) an. Die Nutzdatenlänge jedes Zwischenfragments muss daher stets ein Vielfaches von 8 Bytes betragen.



- Erstes Fragment: Offset = 0, MF = 1 (enthält Original-Transport-Header, z. B. TCP/UDP)
- Folgende Fragmente: Offset = (bisherige kumulierte Datenbytes) / 8, MF = 1
- Letztes Fragment: Offset = (Gesamtdaten vor Fragment) / 8, MF = 0

4. REASSEMBLY AM EMPFÄNGER

Router auf dem Transportweg setzen Fragmente nicht wieder zusammen. Das Reassembly erfolgt aus Performance- und Routing-Gründen ausschließlich am finalen Zielhost anhand von Absender-IP, Ziel-IP, Protokollnummer und Identification-ID.



- Pufferung im Arbeitsspeicher des Empfängers bis zum Eintreffen aller Fragmente
- Reassembly-Timer (Standard: 30–60 s): Läuft er ab, werden alle Teilpakete verworfen
- Paketverlust-Multiplikator: Geht ein einziges Fragment verloren, schlägt das gesamte Reassembly fehl

5. FUNKTIONSWEISE VON PMTUD

Path MTU Discovery (RFC 1191) ermittelt dynamisch die kleinste MTU entlang des gesamten Übertragungspfades, um routerseitige Fragmentierung vollständig zu vermeiden.



- Der Sender setzt bei allen ausgehenden Paketen das DF-Bit (Don't Fragment = 1)
- Ein Zwischenrouter mit zu kleiner MTU verwirft das Paket
- Router sendet Fehlermeldung: ICMP Type 3, Code 4 (Fragmentation Needed and DF set)
- Paket enthält die Next-Hop MTU; Sender passt seine Paketgröße entsprechend an

6. BLACK-HOLE-ROUTER & FEHLERBILD

Blockieren Firewalls oder fehlerhafte Middleboxen ICMP-Nachrichten unbedacht, entsteht ein sogenanntes Path MTU Black Hole. Verbindungen initiieren erfolgreich, frieren aber bei größeren Datentransfers plötzlich ein.



- TCP-Handshake funktioniert (SYN/ACK sind klein und unterbieten MTU)
- Nutzdatenübertragung (z. B. TLS-Zertifikate, Webseiten) blockiert dauerhaft
- Ursache: ICMP Type 3 Code 4 wird gefiltert, Sender erhält keine MTU-Rückmeldung

Praxis-Symptom
Verbindung bleibt nach TLS Client Hello oder HTTP-GET hängen: Typisches Anzeichen für ein PMTUD Black Hole.

7. TROUBLESHOOTING & LÖSUNGEN

Zur Diagnose und Behebung von MTU- und PMTUD-Problemen stehen standardisierte Befehle und Router-Konfigurationen zur Verfügung.



- Ping-Test mit DF-Bit (Windows): ping -f -l 1472 <Ziel-IP>
- Ping-Test mit DF-Bit (Linux): ping -M do -s 1472 <Ziel-IP>
- TCP MSS Clamping: Router modificiert MSS im SYN-Paket (MSS = MTU - 40 Bytes)
- ICMP-Filterrichtlinien korrigieren: Type 3 Code 4 an Edge-Firewalls explizit erlauben

8. ZUSAMMENFASSUNG & BEST PRACTICES

Moderne IP-Netzwerke weiden Router-Fragmentierung aus Gründen der Latenz, CPU-Last und Sicherheit (wie z B. Fragmentierungs-Angriffe und Firewall-Bypass). In IPv6 wurde die Router-Fragmentierung vollständig abgeschafft.



- Fragmentierung vermeiden: DF=1 als Standard in modernen Stacks
- MSS Clamping an VPN- und PPPoE-Gateways aktivieren
- ICMP Type 3 Code 4 niemals ungeprüft global blockieren

ICMPv4 – Diagnose- und Kontrollprotokoll

ICMPv4 (Internet Control Message Protocol)

1. Grundlagen & Protokollzweck



Das Internet Control Message Protocol Version 4 (ICMPv4) ist ein integraler Bestandteil der TCP/IP-Internet-Schicht (OSI-Schicht 3). Es übermittelt Diagnose-, Steuer- und Fehlermeldungen für das IP-Routing.

- Protokoll-ID 1 im IPv4-Header direkt gekapselt
- Keine eigene Port-Adressierung (im Unterschied zu TCP/UDP)
- Dient nicht dem Datentransport für Endanwendungen
- Essentiell für die Stabilität des Vermittlungsnetzes

2. Echo Request & Reply (Ping)



Ping dient der Überprüfung der bidirektionalen Erreichbarkeit und Latenz zwischen zwei Netzknoten durch den standardisierten Echo-Austausch.

- Echo Request (Typ 8, Code 0) fragt Antwort an
- Echo Reply (Typ 0, Code 0) bestätigt Erreichbarkeit
- Payload enthält Sequenznummer und Zeitstempel
- Ermöglicht RTT-Messung (Round Trip Time)

3. Destination Unreachable



Wird erzeugt, wenn ein IP-Paket vom Router oder Host nicht zugestellt werden kann. Enthält präzise Unterursachen im 8-Bit-Code-Feld.

- ICMP Typ 3 signalisiert Nichterreichbarkeit
- Code 0: Netz unerreichbar (Routing-Tabelle fehlt Pfad)
- Code 1: Host unerreichbar (ARP-Auflösung scheitert)
- Code 3: Port unerreichbar (kein Dienst lauscht bei UDP)
- Code 4: Fragmentierung nötig, aber DF-Bit gesetzt (Path MTU)

4. Time Exceeded & Traceroute



Der Hop-by-Hop-Mechanismus verhindert Endlosschleifen im Routing und dient der Pfadanalyse über das Time-To-Live (TTL)-Feld.

- ICMP Typ 11 Code 0: TTL im Transit auf 0 dekrementiert
- Verhindert deuarhaftes Zirkulieren von Paketen
- Traceroute sendet Pakete mit aufsteigender TTL (1, 2, 3...)
- Jeder Zwischenrouter generiert beim Verwerfen Typ 11
- ICMP Typ 11 Code 1: Fragment Reassembly Time Exceeded

5. Redirect & Router Discovery



Mechanismen zur dynamischen Weg-Optimierung und Erkennung von Default-Gateways im lokalen Netzsegment.

- ICMP Redirect (Typ 5): Informiert Host über besseren First-Hop-Router
- Router Solicitation (Typ 10): Host sucht aktive Gateways
- Router Advertisement (Typ 9): Router verkünden Existenz und Priorität
- Redirects gelten nur für dasselbe Subnetz und sind oft deaktiviert

6. Sicherheitsrisiken & Angriffe



Aufgrund mangelnder Authentifizierung in Standard-ICMPv4 können Kontrollpakete für Angriffe und Spionage missbraucht werden.

- ICMP-Tunneling: Datenexfiltration über die Nutzlast von Ping-Paketen
- Smurf-Angriff: DDoS mittels gefälschter Quell-IP an Broadcast-Adressen
- ICMP Redirect Spoofing: Man-in-the-Middle durch gefälschte Routen
- Reconnaissance: Netzwerk-Scanning zur Topologie- und OS-Erkennung

Sicherheitshinweis
ICMP-Nachrichten enthalten zur Fehlerzuordnung die ersten 64 Bit der ursprünglichen Payload. Angreifer können dies zum Abfangen sensibler Header-Informationen nutzen.

7. Filterregeln & Härtung



Ein vollständiges Blockieren von ICMP bricht Standards und Diagnosetools. Daher muss selektives Filtering implementiert werden.

- Echo Request (Typ 8) an Perimeter-Firewalls rate-limiten oder drosseln
- Destination Unreachable (Typ 3, Code 4) zwingend für Path MTU Discovery erlauben
- Time Exceeded (Typ 11) für Monitoring zulassen
- ICMP Redirects (Typ 5) host- und routerseitig vollständig deaktivieren
- Broadcast-Ping-Verarbeitung am Host via Kernel-Parameter sperren

8. Diagnose-Arbeitsablauf



Strukturierter Ablauf zur Fehleranalyse und Netzwerkdiagnose mit Standard-ICMP-Befehlen.

1. Schritt 1: Lokalen Stack prüfen
   ping 127.0.0.1.
2. Schritt 2: Standard-Gateway anpingen
   Router-IP des lokalen Subnetzes.
3. Schritt 3: Externe IP adressieren
   ping 8.8.8.8.
4. Schritt 4: Pfadanalyse durchführen
   traceroute (Linux) oder tracert (Windows).

Network Address Translation (NAT): SNAT, DNAT und PAT

1. GRUNDPRINZIP & IPv4-KNAPPHEIT



NAT vermittelt zwischen privaten IP-Bereichen (RFC 1918) und dem öffentlichen Internet, um den begrenzten IPv4-Adressraum effizient zu nutzen.

- Private Bereiche: 10.0.0.0/8, 172.16.0.0/12 und 192.168.0.0/16 werden im WAN nicht geroutet.
- Der Router ersetzt Adressinformationen im IP-Header beim Passieren der Netzwerkgrenze.
- Spart weltweite Adressen ein und trennt interne Netztopologien von externen Beobachtern ab.

2. STATISCHES & DYNAMISCHES NAT



Klassische NAT-Methoden übersetzen Adressen auf Layer-3-Ebene ohne Berücksichtigung von Transport-Ports.

- Statisches NAT (1:1): Weist einer festen internen IP genau eine öffentliche IP dauerhaft zu.
- Dynamisches NAT (M:N): Schöpft aus einem Pool öffentlicher IPs für mehrere interne Hosts.
- Einschränkung: Bei Adresspool-Erschöpfung können keine neuen Verbindungen initiiert werden.

3. PAT / NAPT (PORT ADDRESS TRANSLATION)



PAT bzw. Masquerading erlaubt hunderten internen Clients das simultane Surfen über eine einzige offizielle IPv4-Adresse.

- Überladung (Overload): Nutzt TCP/UDP-Portnummern (Layer 4) zur Unterscheidung von Kommunikationsffüssen.
- Mapt interne Source-Sockets (IP + Quellport) auf externe Ephemeral-Ports des Gateways.
- Standardverfahren in sämtlichen Heim- und KMU-Internetroutern.

4. SNAT VS. DNAT & PORT-FORWARDING



Die Richtung des Verbindungsaufbaus bestimmt, ob Quell- oder Zieladressen manipuliert werden müssen.

- SNAT (Source NAT): Modifiziert beim ausgehenden Verkehr die Absender-IP in die Gateway-IP.
- DNAT (Destination NAT): Übersetzt eingehende Ziel-IPs/Ports zur Serververöffentlichung.
- Port-Forwarding: Leitet externe Zielports gezielt an dedizierte Server im internen LAN weiter.

5. NAT-SESSION-TABELLEN & STATE-TRACKING



Der Router führt eine Zustandstabelle (State Table) im RAM, um eintreffende Rückpakete dem korrekten internen Sender zuzuordnen.

- Eintragsstruktur: [Protokoll, Quell-IP, Quellport, Gateway-Port, Ziel-IP, Zielport].
- Dynamisches Lifecycle-Management: TCP-Verbindungen enden bei FIN/RST, UDP nach Idle-Timeout.
- Rechenaufwand: Erfordert fortlaufende Neuberechnung der IP- und TCP/UDP-Checksummen.

Stateful Tracking

UDP ist verbindungslos; NAT-Router simulieren Sitzungen über softwarebasierte Inaktivitäts-Timer.

6. NAT-TRAVERSAL & PROTOKOLL-HÜRDEN



Protokolle, die IP-Adressen in der Nutzlast (Payload) übertragen oder Header verschlüsseln, scheitern oft an herkömmlichen NAT-Routern.

- SIP & FTP: Benötigen Application Layer Gateways (ALG) oder STUN/TURN, um Payloads zu patchen.
- IPsec AH/ESP: AH schlägt durch geänderte IP-Header fehl; ESP untzt NAT-Traversal (UDP-Port 4500).
- End-to-End-Verletzung: NAT bricht das ursprüngliche Internet-Architekturprinzip direkter Host-Erreichbarkeit.

Kritischer Hinweis

NAT ist kein Ersatz für eine vollwertige Firewall, auch wenn unaufgeforderter eingehender Verkehr geblockt wird.

7. CARRIER-GRADE NAT (CGNAT) & DUAL-STACK



Aufgrund des weltweiten IPv4-Mangels schalten Internet-Service-Provider zusätzliches NAT auf Netzbetreiberebene.

- Double-NAT: Kundenrouter erhält keine öffentliche IPv4, sondern eine Adresse aus 100.64.0.0/10.
- Auswirkungen: Eingehendes Port-Forwarding beim Endkunden schlägt ohne IPv6 oder IPv4-Tunnel fehl.
- Lösungsansatz: Einführung von Dual-Stack (echtes IPv6 + IPv4) oder NPTv6 zur Bereinigung.

8. ZUSAMMENFASSUNG & NAT-TYP-ENTSCHEIDUNG



Praxisleitfaden zur Auswahl des richtigen Übersetzungsverfahrens für Netzwerkadministratoren.

- Mehrere Clients ins Web teilen: Port Address Translation (PAT/Overload) einsetzen.
- Dienst im WAN bereitstellen: Destination NAT (DNAT/Port-Forwarding) einrichten.
- Feste Partnerschaft/Zertifikate: Statisches 1:1 NAT mit exklusiver IP nutzen.

Welche Kommunikationsrichtung und Dienstart liegt vor?

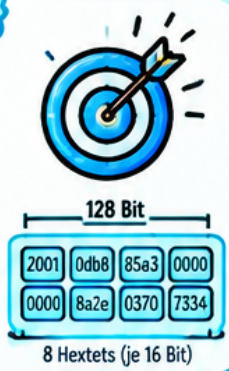
- Interner Client greift auf externen Webdienst zu → PAT / SNAT verwenden (Source IP wird zur WAN-IP, Quellport wird umgesetat).
- Externer Client greift auf internen Webserver zu → DNAT / Port-Forwarding konfigurieren (WAN-Zielport wird auf interne LAN-IP gemoppt).



IPv6-Architektur & 128-Bit-Adressaufbau

1. 128-Bit-Adressraum & Hexadezimale Notation

- IPv6 ersetzt die 32-Bit-Adressen von IPv4 durch einen 128 Bit langen Adressraum, der in 8 Blöcke (Hextets) zu je 16 Bit unterteilt wird. Jeder Block wird als vierstellige Hexadezimalzahl dargestellt und durch Doppelpunkte getrennt.
- 128 Bit Gesamtlänge ermöglichen 2^128 (ca. 3,4 × 10^38) eindeutige Adressen.
- Format: 8 Hextets durch Doppelpunkte separiert (z. B. 2001:0db8:85a3:0000:0000:8a2e:0370:7334).
- Hexadezimalziffern von 0 bis f (Groß- und Kleinschreibung ist technisch identisch, RFC 5952 empfeihlt Kleinbuchstaben).



2. Kürzungsregeln (RFC 5952)

- Um lange IPv6-Adressen übersichtlich darzustellen, definieren die Standards verbindliche Regeln zur Zeichenkompression führender Nullen und aufeinanderfolgender Null-Blöcke.
- Regel 1 (Führende Nullen): Innerhalb eines 16-Bit-Blocks dürfen führende Nullen weggelassen werden (:0db8: wird zu :db8:; :0000: wird zu :0:).
- Regel 2 (Doppel-Doppelpunkt "::"): Eine zusammenhängende Folge von Blöcken mit ausschließlich Nullen darf einmalig durch "::" ersetzt werden.
- Stritte Einschränkung: "::" darf exakt einmal pro Adresse vorkommen, da die genaue Hextet-Anzahl sonst mathematisch unbestimmt ist.

Vorher:
2001:0db8:0000:0000:0000:8a2e:0370:7334

Nachher:
2001:db8::8a2e:370:7334

3. Adressaufteilung: Präfix vs. IID

- Eine reguläre IPv6-Unicast-Adresse teilt sich standardmäßig in zwei gleich große Hälften von jeweils 64 Bit auf: das Routing-Präfix und den Interface Identifier.
- Erste 64 Bit (Netzwerk- & Subnetz-Präfix): Beinhaltet globales Routing-Präfix und die vom Administrator vergebene Subnet-ID.
- Letzte 64 Bit (Interface Identifier, IID): Identifiziert die Netzwerkschnittstelle (Host-Antell) eindeutig innerhalb des Subnetzes.

Standard-Subnetzmaske im LAN ist grundsätzlich /64, um zustandslose Autokonfiguration (SLAAC) zu garantieren.



4. EUI-64-Format & Datenschutzrisiko

- Das klassische modifizierte EUI-64-Verfahren erzeugt den 64-Bit-Interface-Identifier automatisch direkt aus der physikalischen 48-Bit-MAC-Adresse der Netzwerkkarte.
- Verfahren: Die 48-Bit-MAC-Adresse wird halbiert, in der Mitte wird der Hex-Wert 0xfffe eingefügt.
- Universal/Local-Bit: Das 7. Bit des ersten Oktetts (U/L-Bit) wird invertiert (0x02 XOR).
- Privatsphären-Problem: Da die Hardware-MAC unveränderlich in der IP sichtbar bleibt, ist der Client über Netzwerkgrenzen hinweg eindeutig trackbar.

48-Bit-MAC
00:1A:2B:3C:4D:5E

EUI-64 (64 Bit)
02:1A:2B:FF:FE:3C:4D:5E

5. RFC 7217 & Privacy Extensions

- Moderne Betriebssysteme verrichten im Endgerätebereich auf EUI-64 und uutzen kryptografische Pseudozufallswerte zum Schutz der Identität im Internet.
- RFC 7217 (Stable Privacy Addresses): Erzeugt einen IID per kryptografischem Hash aus Präfix, Interface-ID und geheimem Schlösseel – stabil im selben LAN, aber untreschendlich in fremden Netzen.
- Privacy Extensions (RFC 4941): Generiert zusätzllich temporäre, regelmäßig wechselnde IPv6-Adressen für ausgehende Webverbindungen.
- Vorteil: Unterbindet geräteübergreifendes Tracking, ohne das lokale SLAAC-Routing zu behindern.

6. Wegfall von Broadcasts & Multicast-Architektur

- IPv6 eliminiert das Konzept des ungerichteten Broadcast-Traffiss vullständig, um unbeteiligte Netzwerkhosts vor unnötiger Interrupt- und Prozessorlast zu schützen.
- Kein Broadcast: Netzwerkanfragen fluten nicht mehr alle Stationen im Layer-2-Segment.
- Multicast-Präfix ff00::/8: Gezielte Ansprache von Host-Gruppen (z. B. ff02::1 für alle Knoten, ff02::2 für alle Router im Link).
- Anycast: Mehrere Schnittstellen teilen sich dieselbe Adresse; Router leiten Datenpakete stets zum topologisch nächstgelegenen Ziel.

7. Neighbor Discovery Protocol

- Anstelle des broadcastbasierten ARP-Protokolls aus IPv4 nntzt IPv6 das Neighbor Discovery Protocol (NDP), basierend auf ICMPv6-Multicast.
- Router Solicitation (RS) & Router Advertisement (RA): Clients entdecken automatisch Gateway-Router und Netzwerkpräfixe.
- Neighbor Solicitation (NS) & Neighbor Advertisement (NA): Löst IPv6-Adressen in Link-Layer-MAC-Adressen auf (Ersatz für ARP).
- Duplicate Address Detection (DAD): Prüft vor Aktivierung einer Adresse per Multicast, ob diese im Subnetz bereits existiert.

8. Adressberechnung & Praxis

Schritt-für-Schritt-Prüfung zur korrekten Kompression und Identifikation von IPv6-Adressen im praktischen Netzwerkbetrieb.

Praxis-Regel für Doppelpunkte
Wenn beim Entpacken einer komprimierten IPv6-Adresse unklar ist, wie viele Nullen fehlen: Zähle vorhandene Hextets. Es müssen am Ende genau 8 Blöcke à 16 Bit stehen.

Schritt 1: Führende Nullen eliminieren
Prüfe jeden 16-Bit-Block einzeln und streiche linksstehende Nullen (z. B. 0042 → 42, 0000 → 0).

Schritt 2: Längste Nullfolge komprimieren
Identifiziere die längste zusammenhängende Kette von Null-Blöcken und ersetze diese durch "::". Bei Gleichstand die linke Kette wählen.

Schritt 3: Präfix und IID trennen
Setze den Trennstrich bei /64 (nach dem vierten Hextet): Die ersten 64 Bit steuern das Routing, die letzten 64 Bit bilden den IID.

Übungsadresse: 2001:0db8:0000:0000:0008:0800:200c:417a komprimieren

Ermittelte Subnetz-Präfix-Hälfte (/64)

Ermittelter 64-Bit Interface Identifier (IID)

Welche Adress-Konfigurationsmethode soll im LAN gewählt werden?

Zustandslose automatische Konfiguration mit Datenschutz erwünscht
→ Verwende SLAAC (/64-Präfix) in Kombination mit RFC 7217 oder Privacy Extensions (RFC 4941).

Feste Serverdienste mit exakter zentraler IP- und DNS-Zuweisung
→ Verwende statische Zuweisung mit manueller IID oder Stateful DHCPv6 zur Protokollierung.

IPv6 ADRESSTYPEN & SCOPES

1. LINK-LOCAL (FE80::/10)



Link-Local-Adressen dienen der direkten Kommunikation innerhalb desselben physischen oder virtuellen Netzwerkschnittstellen-Segments (Link).

- Präfix: Immer fe80::/10 (standardmäßig fe80::/64 konfiguriert).
- Wird auf jedem IPv6-fähigen Interface automatisch erzeugt (SLAAC oder EUI-64).
- **Nicht routingfähig:** Router verwerfen Pakete mit **Link-Local-Zieladressen** an Schnittstellengrenzen.
- **Unverzichtbar für Protokolle wie Neigbbor Discovery Protoocl (NDP) und Routing-Peering (z. B. OSPFv3).**

Zone Index beachten
Da dieselbe Link-Local-Adresse auf mehreren physischen Interfaces existieren kann, verlangt das Betriebssystem oft einen Zonen-Identifier (z. B. fe80::1%eth0 bzw. fe80::1%1).

2. UNIQUE LOCAL (FC00::/7 / FD00::/8)



Unique Local IPv6 Unicast Addresses (ULA) entsprechen funktional den privaten IPv4-Adressbereichen nach RFC 1918.

- Adressbereich: fc00::/7; in der Praxis wird das L-Bit auf 1 gesetzt, was zu fd00::/8 führt.
- Routbar innerhalb einer Organisation, eines Rechenzentrums oder über VPN-Strecken.
- Keine Weiterleitung im öffentlichen Internet; Schutz vor unabsichtlicher externer Erreichbarkeit.
- Globale Eindeutigkeit durch 40-Bit-Pseudozufalls-Präfix minimiert Adresskollisionen bei Firmenfusionen.

3. GLOBAL UNICAST (2000::/3)



Global Unicast Addresses (GUA) sind weltweit eindeutige, öffentlich im globalen Internet geroutete Adressen.

- Präfix: 2000::/3 (umfasst alle Adressen von 2000:: bis 2fff:ffff::...).
- Hierarchischer Aufbau: Global Routing Prefix (z. B. /48), Subnet-ID (16 Bit) und Interface-ID (64 Bit).
- Jedes Subnetz erhält regulär ein /64-Präfix für standardkonforme Host-Autokonfiguration.
- Macht Network Address Translation (NAT) für schiere Adressknappheit überflüssig.

4. LOOPBACK & UNSPECIFIED (::1 & ::)



Spezielle Unicast-Adressen zur Identifikation des lokalen Hosts und für Initialisierungszustände.

- **Loopback (::1/128):** Entspricht 127.0.0.1 in IPv4; Adressierung interner Dienste auf demselben Host.
- **Unspecified (::/128):** Alle 128 Bits auf null; zeigt das Fehlen einer gültigen IP-Adresse an.
- Einsatz von ::/128 als Quelladresse während Duplicate Address Detection (DAD) und DHCPv6-Anfragen.
- Kein Paket mit Ziel ::/128 darf jemals auf ein Netzwerksegment gesendet werden.

5. MULTICAST-STRUKTUR (FF00::/8)



IPv6 ersetzt Broadcasts vollständig durch Multicast. Pakete gehen gezielt an abonnierte Empfängergruppen.

- Präfix: ff00::/8 (erste 8 Bits fest auf 11111111 gesetzt).
- Format: 8 Bit Präfix, 4 Bit Flags (Transient/Well-known), 4 Bit Scope-ID, 112 Bit Gruppen-ID.
- ff02::1 (Link-Local All-Nodes): Erreicht alle IPv6-Geräte
- ff02::2 (Link-Local All-Routers): Erreicht alle Router auf dem jeweiligen Link.

Multicast Scopes (4-Bit Feld)
1: Interface-Local | 2: Link-Local | 5: Site-Local | 8: Organization-Local | E: Global.

5. PRAXCAST-ANALYSE & IDENTIFIKATION



Anycast teilt diesselbe Unicast-Adresse mehreren Schnittstellen zu. Routingprotokolle lenken Anfragen zum nächstgelegenen Ziel.

- Syntaktisch nicht von regulären Global Unicast- oder ULA-Adressen zu unterscheiden.
- One-to-Nearest-Kommunikation: Paket gelangt zum topologisch kürzesten Netzknoten.
- Standardanwendung: Hochverfügbarkeit und Latenzminimierung für DNS-Wurzelserver und CDNs.
- Subnet-Router-Anycast: Jedes Subnetz besitzt eine reservierte Anycast-Adresse (Interface-ID komplett 0).

6. ANYCAST-ADRESSIERUNG



Anycast teilt dieselbe Unicast-Adresse mehreren Schnittstellen zu. Routingprotokolle lenken Anfragen zum nächstgelegenen Ziel.

- Syntaktisch nicht von regulären Global Unicast- oder ULA-Adressen zu unterscheiden.
- Unbedingt Test-Konfigurationen bei Firewall-Regeln zum topologisch kürzesten Netzknoten.
- Interface-ID Validierung: Hochverfügbarkeit und Security Extensions (RFC DNS) die most ofts präet CDNs.
- Sicherheits- und Routingfilter Interfale ti-Local am Sonder-reseter ingress und egress blockiert enforcement for).

7. PRAXIS-ANALYSE & IDENTIFIKATION



Vierstufiger Leitfaden zur schnellen Bestimmung des Adresstyps und Gültigkeitsbereichs in Mitschninten und Konfigurationen.

- Ermöglicht verlässliche Identifikation bei Paketanalysen mit Wireshark oder tcpdump.
- Verhindert Fehlkonfigurationen bei Firewall-Regeln und Interface-Zuweisungen.

8. ZUSAMMENFASSUNG & SCOPE-ENTSCHEIDUNG

Entscheidungslogik zur Auswahl des korrekten IPv6-Adresstyps für Netzwerkdienste und Schnittstellen.

- GUA für öffentliche Internet-Dienste ohne NAT-Zwangsmechanismus.
- ULA für interne Infrastrukturen, Testumgebungen und isolierte Netze.
- Link-Local für Netzwerkinfrastruktur-Peering und lokale Konnektivität.

Welcher Gültigkeitsbereich (Scope) wird für die Verbindung benötigt?

1. **Ausschließlich lokale Verbindung im selben LAN / Subnetz**
   → fe80::/10 (Link-Local) verwenden; keine Router-Konfiguration oder öffentliches Präfix erforderlich.
2. **Unternehmensweit routbar, aber strikt vom Internet isoliert**
   → fd00::/8 (Unique Local Address) konfigurieren mit zufällig generiertem 40-Bit Global-ID-Block.
3. **Weltweite Erreichbarkeit und direkte Kommunikation im Internet**
   → 2000::/3 (Global Unicast) mit vom ISP zugewiesenem Präfix (z. B. /48 oder /56) implementieren.
4. **Gleichzeitige Benachrichtigung einer Knotengruppe auf dem Link**
   → ff02::/16 Multicast-Adresse ansprechen (z. B. ff02::1 für alle Knoten, ff02::2 für alle Router).

IPv6-Header & Extension Headers

40 Bytes Festlänge + Modulare Kettung

1. Basis-Header-Architektur

Im Gegensatz zum variablen IPv4-Header besitzt der IPv6-Basis-Header eine feste Länge von genau 40 Bytes (320 Bit). Durch den Verzicht auf Prüfsummen und variable Optionen auf Router-Ebene wird das Weiterleiten hardwarebeschleunigt.



- Feste Struktur eliminiert Header-Length-Felder (IHL)
- Keine Hop-by-Hop-Prüfsumme zur Reduktion von Routing-Latenzen
- Klare 64-Bit-Ausrichtung für Hochleistungs-Switching

Design-Vorteil
Zwischenrouter müssen bei IPv6 standardmäßig keine Prüfsummen neu berechnen oder Optionen parsen, was den Durchsatz massiv steigert.

2. Felder 1–4: Version, Traffic Class, Flow Label, Payload Length

Die ersten 64 Bit des Headers organisieren Versionierung, Dienstgüte und Längenangaben für die Nutzdaten.



- Version (4 Bit): Konstante Bitfolge 0110 für IPv6
- Traffic Class (8 Bit): Entspricht IPv4-TOS/DiffServ für QoS und Priorisierung
- Flow Label (20 Bit): Kennzeichnet zusammenhängende Paketflüsse für Echtzeitrouting
- Payload Length (16 Bit): Länge aller nachfolgenden Bytes (Extension Headers plus Nutzlast, max. 65.535 Bytes)

3. Felder 5–8: Next Header, Hop Limit, Adressfelder

Die verbleibenden Felder definieren den Protokolltyp des Folgeheaders, die Lebensdauer und die beiden Adressbereiche.

- Next Header (8 Bit): Spezifiziert den nächsten Extension Header oder das Transportprotokoll (z. B. TCP=6, UDP=17)
- Hop Limit (8 Bit): Zähler für maximale Router-Übergänge (ersetzt IPv4-TTL; Dekrement pro Hop)
- Source Address (128 Bit / 16 Bytes): Eindeutige Absenderadresse
- Destination Address (128 Bit / 16 Bytes): Finale oder Zwischenzieladresse



4. Verkettungsprinzip (Extension Header Chaining)

Optionale Parameter werden bei IPv6 nicht im Basis-Header eingebettet, sondern als eigenständige Kettenelemente zwischen dem Basis-Header und dem Transport-Header eingefügt.

- Kettenglied-Logik: Jeder Header enthält ein 'Next Header'-Feld, das auf das darauffolgende Element verweist
- Verarbeitungsreihenfolge: Zwischenrouter ignorieren alle Extension Headers außer Hop-by-Hop
- Ende der Kette: Der letzte Extension Header verweist auf das Payload-Protokoll (z. B. TCP/UDP/ICMPv6)



Verkettungsregel
Hop-by-Hop Options muss, falls vorhanden, zwingend direkt auf den Basis-Header folgen (Wert 0 im Next-Header-Feld des Basis-Headers).

5. Übersicht gängiger Extension Headers



Die IANA definiert feste Protokollnummern für standardisierte Extension Headers, die nach empfohlener Reihenfolge angeordnet werden.

- Hop-by-Hop Options (Wert 0): Spezielle Anweisungen für jeden Router auf dem Pfad (z. B. Jumbogramme)
- Routing Header (Wert 43): Erzwingt das Passieren bestimmter Knotenpunkte (Source Routing)
- Fragment Header (Wert 44): Ermöglicht Fragmentierung ausschließlich durch den sendenden Host (End-to-End)
- Encapsulating Security Payload (ESP, Wert 50): IPSec-Verschlüsselung und Integritätsschutz
- Authentication Header (AH, Wert 51): IPSec-Authentifizierung und Integritätsprüfung
- Destination Options (Wert 60): Zusätzliche Optionen ausschließlich für den Endempfänger

6. Analyseablauf einer IPv6-Header-Kette



Systematischer Prüfprozess zur Dekodierung eines IPv6-Pakets in einem Netzwerkanalysator.

1. **Basis-Header extrahieren**
   Lese die ersten 40 Bytes ein, validiere Version 6, Adresslängen und notiere das erste Next-Header-Feld.
2. **Folgeheader identifizieren**
   Prüfe den Next-Header-Wert: Ist es ein bekannter Extension Header (z. B. 0, 43, 44, 50, 51, 60) oder ein Transportprotokoll (6, 17)?
3. **Extension-Header-Kette traversieren**
   Lese die Header-Länge des aktuellen Extension Headers aus, springe zum nächsten Next-Header-Feld und wiederhole den Schritt.
4. **Transport-Payload übergeben**
   Sobald ein Transportprotokoll erreicht wird, übergebe das nachfolgende Byte-Segment an den TCP/UDP-Stack.

7. Entscheidungsbaum: Fragmentierung & Filterung



Kriterien zur Handhabung von Extension Headers in Router- und Firewall-Konfigurationen.

Welche Header-Eigenschaft trifft auf das eingehende IPv6-Paket zu?

Hop-by-Hop Header ist vorhanden	Fragment Header erkannt	Unbekannter Extension-Header-Typ
Jeder Zwischenrouter verarbeitet die Optionen in Software/Hardware; unzulässige Optionen verwerfen das Paket.	Zwischenrouter fragmentieren niemals selbst. Nur Zielhost rekonstruiert Segmente anhand des Identification-Feldes.	Router leiten regulär weiter, sofern keine Sicherheitsrichtlinie unbekannte Kettentypen blockiert.

8. Praxis-Dokumentation: Paket-Inspektion

Protokollvorlage zur manuellen Analyse von IPv6-Verbindungen und Header-Ketten im Laborbetrieb.

- Vollständige Erfassung der Kette zur Erkennung von Evasion-Techniken
- Dokumentation von MTU- und Fragmentierungs-auffälligkeiten



Absender- und Ziel-IPv6-Adresse

Verkettungsreihenfolge (z. B. IPv6 → HBH → Frag → TCP)

Payload Length und beobachtete MTU

Besondere Header-Flags oder Anomalien

NEIGHBOR DISCOVERY PROTOCOL (NDP) IN IPv6

1. WAS IST NDP?



Das Neighbor Discovery Protocol (NDP) ersetzt im IPv6-Netzwerk das veraltete IPv4-ARP sowie ICMPv4-Router-Funktionen. Es arbeitet vollständig auf Basis von ICMPv6-Nachrichten und regelt die direkte Kommunikation im lokalen Verbindungssegment (Link-Local).

- **Keine Broadcasts:** Arbeitet gezielt mit Link-Local Multicast statt störender Rundrufe.
- **Protokollbasis:** Basiert auf spezifischen ICMPv6-Pakettypen (Typen 133 bis 137).
- **Kernfunktionen:** Adressauflösung, Router-Erkennung und Erkennung doppelter Adressen.

2. ROUTER SOLICITATION (RS)



Sobald ein IPv6-Host eine Verbindung zu einer Netzschnittstelle herstellt, sendet er eine Router Solicitation (ICMPv6 Typ 133), um aktive Gateways im Segment ohne Wartezeit abzufragen.

- **Zieladresse:** Multicast an 'Alle Router' (ff02::2).
- **Zweck:** Fordert Router auf, unverzüglich ihre Konfigurationsparameter mitzuteilen.
- **Absender:** Link-Local-Adresse (fe80::/10) des anfragenden Schnittstellen-Ports.

3. ROUTER ADVERTISEMENT (RA)



Router antworten auf RS-Nachrichten oder senden periodisch unaufgefordert Router Advertisements (ICMPv6 Typ 134) an die Multicast-Gruppe 'Alle Knoten' (ff02::1).

- **Netzwerkpräfixe:** Übermittelt IPv6-Präfixe für SLAAC (zustandslose Autokonfiguration).
- **Routing-Parameter:** Definiert Hop-Limits, MTU-Größe und Router-Lebensdauer.
- **Konfigurations-Flags:** Das M-Flag (Managed) und das O-Flag (Other) steuern DHCPv6 und zusätzliche Dienste wie DNS.

4. NEIGHBOR SOLICITATION (NS)



Neighbor Solicitation (ICMPv6 Typ 135) dient der Auflösung einer Ziel-IPv6-Adresse in die zugehörige MAC-Adresse (Layer 2) sowie zur Prüfung der Erreichbarkeit benachbarter Knoten.

- **Ersatz für ARP-Request:** Keine Netzwerkflutung per Broadcast mehr.
- **Zieladresse:** Verwendet die spezifische Solicited-Node-Multicast-Adresse des Zielhosts.
- **Payload:** Enthält die Link-Layer-Adresse (MAC) des anfragenden Quellknotens.

5. NEIGHBOR ADVERTISEMENT (NA)



Das Neighbor Advertisement (ICMPv6 Typ 136) ist die dierkte Antwort auf eine NS-Anfrage oder dient als spontane Statusaktualisierung über eine geänderte Link-Layer-Adresse.

- **Antwortmodus:** Unicast-Antwort an den Abfragenden oder Multicast bei unaufgeforderten Updates.
- **Flag-Bits:** R-Flag (Router), S-Flag (Solicited/angefordert), O-Flag (Override/Überschreiben bestehender Caches).
- **Neighbor Cache:** Aktaulisiert die Zuordnungstabelle der Hosts im Subnetz.

6. DUPLICATE ADDRESS DETECTION (DAD)



Vor der aktiven Nutzung einer neuen Unicast-Adresse prüft jeder IPv6-Knoten zwingend mittels DAD, ob diese Adresse bereits im Segment vergeben ist.

- **Tentative State:** Adresse bleibt vorläufig inaktiv und verarbeitet noch keinen normalen Datenverkehr.
- **Testablauf:** Knoten sendet NS für die eigene Adresse mit unspezifizierter Quell-IP (::).
- **Kollisionserkennung:** Trifft ein NA ein, gilt die Adresse als belegt und wird deaktiviert.

Sicherheitshinweis: NDP-Snooping

Da NDP im Standard unverschlüsselt und unauthentifiziert arbeitet, können manipulierte RA/NA-Pakete zu Man-in-the-Middle-Angriffen führen. In Campus-Netzen schützen RA-Guard und First-Hop-Security-Mechanismen auf Switch-Ebene.

7. SOLICITED-NODE MULTICAST



Statt Anfragen an alle Stationen zu senden, berechnet IPv6 für jede Schnittstelle eine deterministische Solicited-Node-Multicast-Adresse.

- **Präfix:** Fester Adressbereich ff02::1:ff00:0/104.
- **Adressbildung:** Die untersten 24 Bit (6 Hex-Stellen) der Unicast-IPv6-Adresse werden an das Präfix angehängt.
- **Hardwarefilter:** Switch und Netzwerkkarte filtern Pakete auf Ethernet-Ebene heraus, unbeteiligte CPUs werden nicht unterbrochen.

8. ZUSAMMENFASSUNG & ABLAUF



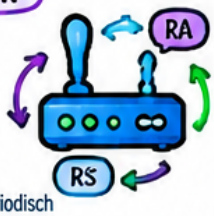
Der typische Initialisierungszyklus eines Hosts im IPv6-Segment folgt einer festen Abfolge von Selbstkonfiguration, Schutz vor Kollisionen und Einbindung des Gateways.

1. Link-Local-Generierung (fe80::/10).
2. DAD-Prüfung via Solicited-Node-Multicast.
3. RS-Meldung senden und RA vom Router verarbeiten.
4. NS/NA für die kontinuierliche Nachbarschafts- und MAC-Auflösung nutzen.

IPv6 Autokonfiguration

1. Grundprinzip der IPv6-Autokonfiguration

IPv6 bietet integrierte Mechanismen zur dynamischen Adresszuweisung ohne zwingende manuelle Eingabe. Hosts ermitteln ihr Subnetz-Präfix autonom über ICMPv6 Neighbor Discovery Router Advertisements.



- Router Solicitation (RS): Host sendet Multicast an alle Router (ff02::2)
- Router Advertisement (RA): Router antwortet periodisch oder auf Anfrage an alle Knoten (ff02::1)
- Keine Broadcasts: Vollständiger Verzicht auf IPv4-typische Broadcast-Stürme
- Dual-Stack fähig: Funktioniert parallell zu IPv4 oder in reinen IPv6-Umgebungen

2. SLAAC: Stateless Address Autoconfiguration

SLAAC erlaubt einem Host, seine IPv6-Adresse vollständig autonom ohne zentralen Adress-Server zu generieren. Das Netz-Präfix liefert der lokale Router.



- Präfix-Erhalt: 64-Bit-Netzwerkpräfix wird dem ICMPv6 RA entnommen
- Interface Identifier: 64-Bit-Hostanteil via EUI-64 (MAC-basiert) oder RFC 7217 (zufällig)
- Autonomie: Kein zentraler Zustandsspeicher auf dem Router oder Server nötig
- Privacy Extensions: Temporäre Adressen nach RFC 4941 schützen die Privatsphäre des Clients

3. RA-Flags: M-, O- und A-Flag Steuerung

Im Router Advertisement definieren spezifische 1-Bit-Schalter exakt, wie Clients Netzwerkadressen und Zusatzparameter konfigurieren müssen.



- A-Flag (Autonomous Flag): Bei 1 generiert der Host via SLAAC eine IPv6-Adresse aus dem Präfix
- M-Flag (Managed Address Configuration): Bei 1 ferdert der Host die IPv6-Adresse via Stateful DHCPv6 an
- O-Flag (Other Configuration): Bei 1 fragt der Host sonstige Parameter (DNS, NTP, SIP) via Stateless DHCPv6 an
- Priorität: M-Flag übersteuert bei Adressvergabe typischerweise die alleinige SLAAC-Konfiguration

Achtung bei Flag-Kombinationen

Ist A=1 und M=1 gesetzt, erstellen Clients häufig sowohl eine autonome SLAAC-Adresse als auch ein Lease via DHCPv6. Dies führt zu multiplen IPv6-Adressen auf demselben Interface.

4. Stateless DHCPv6

Kombination aus SLAAC für die IP-Adresse und einem schlanken DHCPv6-Server für systemweite Infrastrukturparameter.

- Flag-Konfiguration: A=1, M=0, O=1 im RA signalisiert
- Adressbezug: Adresserzeugung erfolgt ausschließlich über SLAAC durch den Client
- Optionsverteilung: DHCPv6 liefert rekursive DNS-Server (RDNSS), Suchdomänen und NTP-Server
- Skalierbarkeit: Der DHCPv6-Server speichert keine Leases oder Client-Zustände



5. Stateful DHCPv6 & IPAM

Klassisches Administrationsmodell analog zu IPv4 DHCP. Ein dedizierter Server steuert die exakte Adressvergabe und speichert jeden Lease.



- Flag-Konfiguration: A=0, M=1, O=beliebig (Zentralvergabe erzwungen)
- IPAM-Integration: Lückenlose Inventarisierung und zentrale Lease-Datenbank für Audits
- Zuweisungsarten: Vergabe fester Adressen (IA_NA) und Präfix-Delegation (IA_PD)
- Einschränkung: Standard-DHCPv6 liefert kein Standard-Gateway: dieses stammt immer aus dem RA

6. Duplicate Address Detection (DAD)

Obligatorische Sicherheitsprüfung: Jeder Host muss jede neu konfigurierte Unicast-Adresse vor deren Inbetriebnahme auf Eindeutigkeit im Link prüfen.



- Tentative-Status: Adresse darf noch keinen regulären Datenverkehr senden oder empfangen
- Neighbor Solicitation (NS): Host sendet Anfrage an die solicited-node Multicast-Adresse
- Neighbor Advertisement (NA): Trifft eine Antwort ein, liegt ein Adresskonflikt vor
- Konfliktfall: Das Interface deaktiviert die kollidierende IP und protokolliert einen Fehler

7. Entscheidungsmatrix: Verfahrensauswahl

Wählen Sie das optimale Autokonfigurationsverfahren basierend auf den regulatorischen und administrativen Anforderungen Ihres Netzes.

- Heim- und IoT-Netze: Reines SLAAC (ggf. mit RFC 8106 RDNSS im RA) für minimalen Verwaltungsaufwand
- Standard-Unternehmensnetz: Stateless DHCPv6 für autonome IP-Generierung bei konsistenter DNS-Infrastruktur
- Hochregulierte Enterprise-Netze: Stateful DHCPv6 zur revisionssicheren IPAM-Protokollierung
- Dual-Stack-Betrieb: Abstimmung mit verhandenen IPv4-DHCP-Reservierungen erforderlich

Welche Anforderungen stellt die Netzwerkumgebung an die IP-Adressvergabe?

Strikte Audit-Pflicht, feste Lease-Tabellen und zentrale IPAM-Kontrolle gefordert	Setze M=1, A=0 im RA; betreibe Stateful DHCPv6 für IA_NA-Zuweisungen.
Autonome Adressierung gewünscht, aber zentrale DNS- und Domänen-parameter nötig	Setze A=1, M=0, O=1 im RA; nutze SLAAC kombiniert mit Stateless DHCPv6.
Minimaler Infrastrukturaufwand ohne DHCP-Server (z. B. Gast-WLAN oder IoT)	Setze A=1, M=0, O=0 im RA; liefere DNS-Server direkt über RFC 8106 RDNSS-Optionen aus.

8. Best Practices

Ein konsistentes Design verhindert Konfigurationskonflikte auf Endgeräten und stellt die Erreichbarkeit sicher.



- Router Advertisements sind immer zwingend, da IPv6-Gateways nicht über DHCPv6 gelernt werden
- SLAAC erfordert strikt standardisierte /64-Subnetzmasken auf den Router-Interfaces
- Aktiviere RFC 4941 Privacy Extensions auf Endgeräten gegen Client-Tracking
- Dokumentiere Flag-Profile standardisiert je VLAN im Netzwerkkonzept

IPv6-MIGRATIONSMETHODEN



1. DUAL-STACK-BETRIEB

Beim Dual-Stack-Ansatz werden IPv4 und IPv6 nativ und parallel auf denselben Schnittstellen, Betriebssystemen und Routern ausgeführt.



- Gleichzeitige Zuweisung von IPv4- und IPv6-Adressen an denselben Host
- DNS entscheidet dynamisch: AAAA-Record für IPv6, A-Record für IPv4
- Automatische Bevorzugung von IPv6 durch moderne Betriebssysteme (Happy Eyeballs Standard RFC 8305)

2. TUNNELING: 6IN4 & STATISCHE TUNNEL

IPv6-Pakete werden unverändert als Nutzlast in standardkonforme IPv4-Pakete gekapselt, um reine IPv4-Netzsegmente zu durchqueren.



- Direkte IP-in-IP-Kapselung mit IPv4-Protokolltyp 41
- Erfordert beidseitig konfigurierte statische IPv4-Endpunkte
- Typischer Einsatz bei Tunnel-Brokern zur Anbindung früher IPv6-Inseln

3. TUNNELING: 6TO4 & AUTOMATISCHE ROUTER

Ein historisches automatisches Übergangsverfahren (RFC 3056), das das feste Präfix 2002::/16 mit der öffentlichen IPv4-Adresse verknüpft.



- Automatische Bildung des /48-Präfixes aus 2002:IPv4-Adresse::/48
- Benötigt Relais-Router im öffentlichen Internet (Anycast 192.88.99.1)
- Heute weitgehend obsolet wegen asymmetrischem Routing und Zuverlässigkeitsproblemen

4. GRE-TUNNEL & POINT-TO-POINT

Generic Routing Encapsulation kapselt beliebige Layer-3-Pakete in Routing-Tunneln zwischen zwei Netzwerkpunkten.



- Kapselung von IPv6-Verkehr innerhalb von GRE über IPv4 (Protokoll 47)
- Unterstützt die Übertragung von Multicast und dynamischen Routing-Protokollen wie OSPFv3
- Geringfügiger Overhead durch austäzliche Header (24 Byte GRE + IPv4)

5. TEREDO: NAT-TRAVERSAL

Ein Client-basierter Übergangsmechanismus (RFC 4380), der IPv6-Pakete in UDP/IPv4-Datagramme packt, um IPv4-NAT-Router zu überwinden.



- Standard-UDP-Zielport 3544 zur Umgehung von NAT-Einschränkungen
- Teredo-Server hilft bei der Adresserkennung, Teredo-Relay routet Pakete ins native IPv6-Netz
- Wegen Sicherheitsrisiken und Latenzen in modernen Unternehmensnetzen meist deaktiviert

6. DUALSETZUNG: NAT64 & DNS64

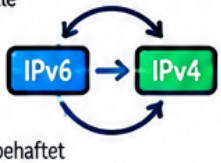
Breitband-Architektur für Internet Service Provider zur Einsparung von öffentlichen IPv4-Adressen bei Endkunden.



- BWA-Kunde (B4-Element) erhält nur eine native IPv6-Adresse und ein IPv6-Präfix
- Ausgehender IPv4-Verkehr wird im Heimrouter in IPv4 getunnelt (IPv4-in-IPv6)
- Schlüsseltechnologie für moderne IPv6-only-Mobilfunk- und Providernetze und

6. ÜBERSETZUNG: NAT64 & DNS64

Ermöglicht reinen IPv6-Endgeräten die bidirektionale Kommunikation mit Systemen, die ausschließlich über IPv4 erreichbar sind.



- DNS64 synthetisiert Pseudo-IPv6-Adressen (Präfix 64:ff9b::/96) aus IPv4 A-Records
- NAT64-Gateway übersetzt IPv6-Pakete zustandsbehaftet in IPv4-Pakete und umgekehrt
- Schlüsseltechnologie für moderne **IPv6-only-Mobilfunk-** und Providernetze

7. DUAL-STACK LITE (DS-LITE)

Breitband-Archietktur für Internet Service Provider zur Einsparung von öffentlichen IPv4-Adressen bei Endkunden.

- BWA-Kunde (B4-Element) erhält nur eine native IPv6-Adresse und ein IPv6-Präfix
- Ausgehender IPv4-Verkehr wird im Heimrouter in IPv6 getunnelt (IPv4-in-IPv6)
- Carrier-Grade NAT (AFTR-Gateway) beim Provider entpackt den Tunnel und übersetzt IPv4

8. TRANSITIONS-ENTSCHEIDUNGSLOGIK & PRÜFUNG

Strukturierte Kriterien zur Wahl des passenden Übergangsverfahrens im Netzwerkbetrieb.



- Dual-Stack wählen, wann immer öffentliche IPv4-Adressen und Router-Kapazitäten ausreichen
- NAT64/DNS64 für konsequente Neuausrichtung auf reine IPv6-Infrastrukturen
- Tunnelverfahren nur gezielt als Übergangskorridore zwischen getrennten Segmenten nutzen

DHCPv4 (Dynamic Host Configuration Protocol) – DORA, Timer & Security

1. DHCPv4 KERNFUNKTION & PORTS



Das Dynamic Host Configuration Protocol (DHCPv4) ermöglicht die automatisierte Zuweisung von Netzwerkparametern an Hosts innerhalb eines IPv4-Netzes. Es operiert im User Datagram Protocol (UDP) auf Anwendungsebene und verwendet dedizierte Portnummern: Clients senden Anfragen an Server-Port 67, während Server Antworten an Client-Port 68 zurücksenden.

- Server-Port: UDP 67 (Empfang von Client-Anfragen)
- Client-Port: UDP 68 (Empfang von Server-Antworten)
- Automatisierte Adressvergabe verhindert Adresskonflikte und minimiert manuellen Verwaltungsaufwand

2. DER DORA-ZYKLUS IM DETAIL



Die Initialkonfiguration eines Hosts ohne statische IP-Adresse erfolgt in vier sequenziellen Phasen: Discover, Offer, Request und Acknowledge.

DISCOVER → OFFER → REQUEST → ACK

1. **DHCPDISCOVER (Broadcast)**
   Der unkonfigurierte Client sendet einen Broadcast (Ziel-IP: 255.255.255.255, Quell-IP: 0.0.0.0) über UDP 67 ins lokale Netz, um erreichbare DHCP-Server zu lokalisieren.
2. **DHCPOFFER (Unicast oder Broadcast)**
   Verfügbare DHCP-Server reservieren eine freie IPv4-Adresse aus ihrem Pool und bieten diese zusammen mit Lease-Parametern an.
3. **DHCPREQUEST (Broadcast)**
   Der Client wählt eines der Angebote aus und signalisiert per Broadcast verbindlich die Annahme der angebotenen Lease an alle Server im Segment.
4. **DHCPACK (Bestätigung)**
   Der ausgewählte Server bestätigt die Lease endgültig mit DHCPACK. Erst nach Empfang dieses Pakets bindet der Client die Adresse an seine Schnittstelle.

3. WESENTLICHE DHCP-OPTIONEN



Über standardisierte Optionsfelder übermittelt der DHCP-Server essenzielle Konfigurationsdaten über die reine IPv4-Adresse hinaus an den anfragenden Host.

- Option 1: Subnetzmaske (definiert Netz- und Hostanteil des Segments)
- Option 3: Router / Standard-Gateway (Next-Hop für Datenverkehr außerhalb des Subnetzes)
- Option 6: Domain Name Server (DNS-Server-IPs zur Namensauflösung)
- Option 42: Network Time Protocol (NTP-Server zur Zeitsynchronisation)

DHCPv4 ARCHITEKTUR



4. LEASE-DAUER & ERNEUERUNGS-TIMER (T1 / T2)



Eine IP-Adresse wird nicht permanent, sondern temporär für die Dauer der Lease verliehen. Zwei interne Timer steuern die vorzeitige Erneuerung.

- **Lease-Zeitraum:** Gültigkeitsdauer der IP-Zuweisung im Netzwerk
- **T1-Timer (Renewal, ca. 50 % der Lease):** Client versucht per gezieltem Unicast an den vergebenden Server die Lease zu verlängern
- **T2-Timer** (Rebinding, ca. 87,5 % der Lease): Bleibt T1 erfolglos, sendet der Client Broadcasts an beliebige erreichbare DHCP-Server im Netz

5. DHCP-RELAY-AGENT & IP HELPER ADDRESS



Da Router standardmäßig Broadcasts (wie DHCPDISCOVER) verwerfen, können Clients in entfernten Subnetzen ohne lokalen DHCP-Server keine Adressen anfordern. Ein DHCP-Relay-Agent (konfiguriert via IP Helper Address auf dem Router oder Layer-3-Switch) fängt den lokalen Broadcast ab, kapselt ihn in ein geroutetes Unicast-Paket und leitet ihn direkt an den zentralen DHCP-Server weiter.

- Überwindung von Broadcast-Domänen über Routergrenzen hinweg
- Zentralisierte DHCP-Verwaltung für mehrere VLANs und Subnetze
- Einfügen des giaddr-Feldes (Gateway IP Address) zur korrekten Pool-Auswahl durch den Server

6. SICHERHEITSINSTRUMENT: DHCP-SNOOPING



DHCP-Snooping ist eine Layer-2-Sicherheitsfunktion auf Switches zum Schutz vor Rogue-DHCP-Servern und Adresserschöpfungsangriffen (DHCP Starvation).

- Klassifizierung von Switch-Ports in vertrauenswürdig (trusted) und unvertrauenswürdig (untrusted)
- Server-Antworten (DHCPOFFER, DHCPACK) werden auf unvertrauenswürdigen Ports sofort verworfen
- Erstellung einer dynamischen DHCP-Snooping-Binding-Database (Zuordnung von MAC, IP, Lease, VLAN und Switch-Port)
- Dient als verlässliche Datenrgrundlage für Dynamic ARP Inspection (DAI) und IP Source Guard

Sicherheitshinweis für Campus-Netze
Unberechtigte DHCP-Server in Kundenports können Man-in-the-Middle-Angriffe ermöglichen, indem sie kompromittierte Standard-Gateways und DNS-Server verteilen. DHCP-Snooping muss daher auf allen Access-Switches aktiviert sein.

7. FEHLERDIAGNOSE BEI DHCP-PROBLEMEN



Strukturierter Entscheidungsbaum zur Lokalisierung von Verbindungs- und Adressierungsfehlern im DHCP-Betrieb.

Welche IPv4-Adresse weist die Schnittstelle des Clients auf?

Adresse liegt im Bereich 169.254.0.0/16 (APIPA)	Adresse liegt im erwarteten Subnetz, aber kein Internetzugriff möglich	Adresse liegt in einem fremden, nicht autorisierten Subnetz
Client erhält keine DHCP-Antwort. Prüfe physische Verbindung, VLAN-Zuordnung, Port-Sicherheit und ob der DHCP-Relay-Agent bzw. Server erreichbar ist.	Prüfe die übergeebenen Optionen: Ist Option 3 (Default Gateway) erreichbar und Option 6 (DNS) funktionsfähig?	Verdacht auf Rogue-DHCP-Server. Aktiviere DHCP-Snooping auf dem Access-Switch und identifiziere den unberechtigten Quell-Port.

8. NETZWERK-AUDIT: DHCP-KONFIGURATIONSPROTOKOLL



Prüfformular zur Dokumentation von DHCP-Parametern und Sicherheitsvorkehrungen im betreuten Subnetz.

Geprüftes Subnetz / VLAN-ID: _____

Primäre & Sekundäre DHCP-Server-IPs: _____

Konfigurierte Lease-Dauer (T1 / T2 Zeiten): _____

Verifizierte DHCP-Optionen (Gateway, DNS, NTP): _____

_____

DHCP-Snooping Status (Trusted Ports / Unstrusted Ports): _____

_____

DOMAIN NAME SYSTEM (DNS): ARCHITEKTUR & NAMENSAUFLÖSUNG

1. WAS IST ES: ZWECK & HIERARCHIE



Das Domain Name System (DNS) übersetzt menschenlesbare Hostnamen in maschinenlesbare IP-Adressen. Die Namensstruktur ist streng hierachisch von der Wurzel bis zum Host aufgebaut.

- Root-Zone: Repräsentiert durch den Punkt am Ende eines FQDNs; weltweit verteiltes Netz redundanter Root-Server.
- Top-Level-Domains (TLD): Oberste Kategorieebenen wie generische (.com, .org) oder länderspezifische Kennungen (.de, .ch).
- Second-Level-Domain & Subdomains: Die eigentliche Inhaberdomain sowie davorliegende Dienst-Präfixe (z. B. www oder mail).

2. DIE SERVER-ROLLEN



Die DNS-Infrastruktur teilt die Aufgaben strikt zwischen anfragenden Vermittlern und verbindlichen Datenquellen auf.

- Rekursiver Resolver: Server des Providers oder Routers, der die vollständige Kette an Abfragen für den Client abarbeitet.
- Root-Nameserver: Verweisen den Resolver bei unbekannten Adressen gezielt an die zuständigen TLD-Server.
- Authoritative Nameserver: Halten die endgültige Zonendatei und liefern die verbindliche Antwort für eine Domain.

3. ABFRAGETYPEN: REKURSIV VS. ITERATIV



Bei der Auflösung interagieren Resolver und Nameserver über zwei grundlegende Abfragemuster.

- Rekursive Abfrage: Der Client fordert vom Resolver: 'Liefere mir die finale IP-Adresse oder einen definitiven Fehler.'
- Iterative Affrage: Der Resolver befragt Root- und TLD-Server; diese liefern jeweils nur Verweise auf den nächsten Nameserver.
- Lastverteilung: Das Zusammenspiel entlastet übergeordnete Server, da Resolver die schrittweise Navigation übernehmen.

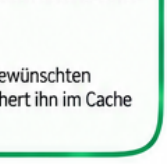
4. WORKFLOW DER NAMENSAUFLÖSUNG



Schrittfolge einer vollständigen Namensauflösung ohne vorherigen Cache-Treffer für eine Domain.

1. **Schritt 1: Client-Prüfung**
   Der Browser prüft den lokalen OS-Cache und fragt bei einem Fehlversuch den konfigurierten rekursiven Resolver an.
2. **Schritt 2: Root-Anfrage**
   Der Resolver kontaktiert einen Root-Server, welcher die IP-Referenz der zuständigen TLD-Nameserver zurückmeldet.
3. **Schritt 3: TLD-Verweis**
   Der Resolver fragt den TLD-Nameserver an und erhält als Antwort die Nameserver der gesuchten Second-Level-Domain.
4. **Schritt 4: Finale Antwort**
   Der autoritative Server liefert den gewünschten Resource Record; der Resolver speichert ihn im Cache und antwortet dem Client.

5. CACHING & TIME-TO-LIVE (TTL)



Caching verhindert die weltweite Überlastung der Infrastruktur durch das Zwischenspeichern von Datensätzen.

- Resolver- & OS-Cache: Bereits aufgelöste Einträge werden lokal gespeichert und unmittelbar beantwortet.
- TTL-Feld: Gibt in Sekunden vor, wie lange ein Record gültig bleibt, bevor er verworfen und neu angefragt werden muss.
- Kompromiss: Hohe TTL senkt die Netzwerklast; niedrige TTL erlaubt schnelle IP-Umzüge bei Wartungsarbeiten oder Migrationen.

6. NETZWERKPORT 53: UDP VS. TCP



DNS nutzt standardmäßig Port 53 auf der Transportschicht, wechselt das Übertragungsprotokoll jedoch nach Zweck.

- Port 53 UDP: Standard für reguläre Namensabfragen; bietet minimale Latenz ohne vorherigen Verbindungsaufbau.
- Paketgrößen-Limit: Klassische UDP-Antworten waren auf 512 Byte begrenzt (mittels EDNS0 erweiterbar).
- Port 53 TCP: Pflicht für Zonentransfers (AXFR/IXFR) zwischen Primary- und Secondary-Nameservern sowie bei abgeschnittenen UDP-Antworten.

Transportprotokoll-Entscheidung
Reicht die Paketgröße für eine vollständige UDP-Antwort nicht aus, setzt der Server das Truncated-Flag (TC-Bit). Der Resolver baut daraufhin sofort eine TCP-Verbindung über Port 53 auf.

7. GÄNGIGE RESOURCE RECORDS



Zonendateien organisieren Netzwerk- und Routingdaten in standardisierten Record-Formaten.

- A & AAAA: Verknüpfen Namen mit einer IPv4-Adresse (A, 32-Bit) bzw. IPv6-Adresse (AAAA, 128-Bit).
- CNAME: Definiert einen Alias-Namen, der auf einen anderen kanonischen Hostnamen weiterleitet.
- MX & NS: MX legt die zuständigen Mailserver fest; NS delegiert Zonen an autoritative Nameserver.
- TXT: Freitextfeld, essentiell für E-Mail-Authentifizierung (SPF, DKIM, DMARC) und Domainvalidierung.

8. FEHLERBEHEBUNG & DIAGNOSE-ENTSCHEIDUNG



Vorgehen bei Verbindungsabbrüchen oder inkonsistenten DNS-Antworten im laufenden Netzwerkbetrieb.

- NXDOMAIN vs. SERVFAIL: NXDOMAIN signalisiert eine nicht existierende Domain; SERVFAIL deutet auf Server- oder DNSSEC-Probleme hin.
- Lokaler Cache: Veraltete IP-Einträge erfordern ein Zurücksetzen des Betriebssystem-Caches vor weiteren Tests.

Welcher Diagnoseschritt greift bei Fehlschlagen der Namensauflösung?

Ping auf IP-Adresse erfolgreich, aber Hostname schlägt fehl	Resolver meldet SERVFAIL oder Timeout auf Port 53
Lokalen Resolver-Cache leeren (z. B. ipconfig /flushdns) und mit 'dig' oder 'nslookup' direkt den Upstream-DNS prüfen.	Prüfen, ob UDP- und TCP-Port 53 in der lokalen Firewall blockiert sind; Fallback auf alternativen Resolver testen.

DNS RESOURCE RECORDS & ZONENDATEIEN

1. GRUNDPRINZIP: ZONENDATEI & SOA

Eine DNS-Zonendatei ist eine strukturierte Textdatei auf einem Nameserver, die alle Zuordnungen und Parameter eines autoritativen Domainbereichs definiert. Jede gültige Zonendatei beginnt verbindlich mit einem Start-of-Authority-Eintrag (SOA).

- Definiert primäre Nameserver-Quelle und administrative Kontaktadresse (E-Mail mit Punkt statt @).
- Seriennummer (Serial): Format YYYYMMDDNN zur Steuerung von Zonentransfers (AXFR/IXFR) an sekundäre Server.
- Refresh-, Retry- und Expire-Intervalle in Sekunden für die sekundäre Synchronisation.
- Negative Caching TTL: Definiert die Zwischenspeicherdauer für NXDOMAIN-Antworten (nicht existierende Domains).

Wichtige SOA-Regel
Wird eine Zonendatei editiert, muss die Seriennummer (Serial) zwingend erhöht werden, da sekundäre Nameserver die Änderungen sonst ignorieren.

2. ADRESS-EINTRÄGE: A UND AAAA

Die elementaren Einträge für das Vorwärts-Lookup (Forward DNS) zur direkten Übersetzung von menschenlesbaren Hostnamen in routingfähige Netzwerkadressen.

- A-Record (IPv4): Mappt FQDN auf eine 32-Bit-Dezimaladresse (z. B. www.example.de. IN A 192.0.2.1).
- AAAA-Record (IPv6): Mappt FQDN auf eine 128-Bit-Hexadezimaladresse (z. B. 2001:db8::1).
- Dual-Stack: Gleichzeitige Bereitstellung beider Records unter demselben Hostnamen ermöglicht moderne IPv4/IPv6-Konnektivität.
- TTL (Time to Live): Steuert, wie viele Sekunden Resolver das Abfrageergebnis im Cache vorhalten dürfen.



3. ALIASING: CNAME UND ANWENDUNG

Der Canonical Name (CNAME) verweist einen Alias-Hostnamen auf einen bereits definierten kanonischen Hostnamen (Target FQDN).

- Zweck: Mehrere Dienste (z. B. blog.example.de und shop.example.de) transparent auf ein gemeinsames Ziel verweisen.
- Keine Kombination: Ein Alias mit CNAME-Record darf keine weiteren Resource Records (wie TXT oder MX) für denselben Namen besitzen.
- Apex-Einschränkung: Der Domain-Apex bzw. Zone-Root (@ / example.de) darf gemäß Standard RFC 1034 keinen CNAME tragen, da dort SOA- und NS-Records zwingend existieren müssen.
- Verkettung vermeiden: CNAME sollte idealerweise direkt auf einen A/AAAA-Host zeigen, um zusätzliche DNS-Lookups zu minimieren.



4. E-MAIL-ROUTING: MX-RECORDS

Mail Exchange (MX) Resource Records steuern die Zustellung von E-Mails via SMTP für die berteffende Domäne.

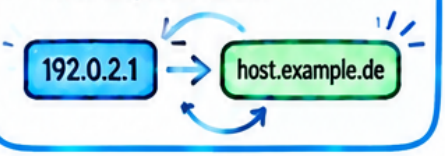
- Ziel-Typ: Ein MX-Record muss immer auf einen vollqualifizierten Hostnamen mit existierendem A- oder AAAA-Record verweisen, niemals direkt auf eine IP-Adresse.
- Prioritätswert (Pref): Numerischer Wert (z. B. 10, 20). Der sendende Mailserver wählt stets den erreichbaren Zielserver mit der niedrigsten Zahl.
- Redundanz: Primäre und sekundäre Mail-Gateways lassen sich über abgestufte Prioritätswerte konfigurieren.
- Falllacck: Existiert kein MX-Record, versuchen konforme MTAs ersatzweise die Zustellung an die IP-Adresse des A-Records der Domäne.



5. RÜCKWÄRTSAUFLÖSUNG: PTR-RECORDS

Der Pointer-Record (PTR) führt die inverse Auflösung durch: Er liefert den kanonischen Hostnamen zu einer gegebenen IP-Adresse (Reverse DNS / rdNS).

- IPv4-Reverse-Zone: Verwendet die hierarchische Pseudodomäne in-addr.arpa mit umgekehrter Byte-Reihenfolge (z. B. 1.2.0.192.in-addr.arpa).
- IPv6-Reverse-Zone: Verwendet ip6.arpa mit invertierten Halbbytes (Nibbles), getrennt durch Punkte.
- Anti-Spam-Prüfung: Empfangende Mailserver verifizieren oft Forward-Confirm Reverse DNS (FCrDNS), um verdächtige Einwahl-IPs ohne passenden PTR abzuweisen.
- Zonenzuständigkeit: Reverse-Zonen werden in der Regel vom jeweiligen IP-Netzbetreiber bzw. Internet Service Provider delegiert und verwaltet.



6. TEXT-DATEN & SICHERHEIT: TXT-RECORDS

TXT-Records enthalten beliebigen ASCII-Text und dienen heute primär der E-Mail-Authentifizierung und Inhabervalidierung.

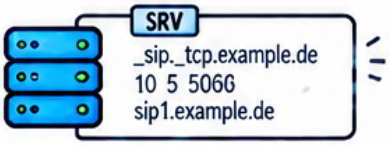
- SPF (Sender Policy Framework): Definiert im TXT-Record autorisierte IP-Adressen und Server, die E-Mails für die Domain versenden dürfen (z. B. v=spf1 mx -all).
- DKIM (DomainKeys Identified Mail): Publiziert kryptografische öffentliche Schlüssel (Public Keys) unter Selektor-Subdomains zur Signaturprüfung eingehender Mails.
- DMARC-Richtlinie: Konfiguriert unter _dmarc.exemple.de die Durchsstzung (Reject/Quarantine) und Berichterstattung bei SPF- oder DKIM-Fehlschlägen.
- Domain-Verifikation: Plattformen (Suchmaschinen, SaaS) nutzen TXT-Token zum Nachweis der Domain-Inhaberschaft.



7. SERVICE LOCATION: SRV-RECORDS

Service Records (SRV) ermöglichen das Auffinden von Netzwerkdiensten unter Angabe von Portnummer, Protokoll und Gewichtung ohne feste Portkonventionen.

- Aufbau: _Service._Proto.Name TTL IN SRV Priority Weight Port Target (z: B. _sip._tcp.example.de).
- Port-Flexeiblität: Dienste können auf unkonventionellen Ports laufen, ohne dass Clients diese manuell konfigurieren müssen.
- Priorität und Gewichtung: Priority legt die Server-Reihenfolge fest; Weight steuert die statistische Lastverteilung unter Servern gleicher Priorität.
- Typische Einsatzzwecke: Miccrosoft Active Direotory (LDAP/Kerberos-Auffindung), SIP/VoIP, XMPP und WebRTC-Infrastrukturen.



8. ZONENDELEGIERUNG: NS-RECORDS & GLUE

Name Server (NS) Records verankern die hierarchische Delegierung von DNS-Zonen an zuständige Nameserver im weltweiten DNS-Baum.

- Delegierung: Die übergeordnete Zone (z. B. .de) verweist via NS-Records auf die Nameserver der Subzone (z. B. ns1.example.de).
- Glue Records: Liegt der Nameserver innerhalb der delegierten Zone, muss die Elternzone zwingend vorberechnete A/AAAA-Records (Glue) ausliefern, um Zirkelbezüge zu verhindren.
- Redundanz: Mindestens zwei unabhängige Nameserver (primär/sekundär) auf physisch getrennten Netzwerken sind zwingender Standard.
- Autoritative Antworten: Resolver nutzen NS-Records, um die autoritative Quelle zur Beantwortung der Anfrage abzufragen.



DNS-RESOURCE-RECORDS – ENTSCHEIDUNGSBAUM & PRAXIS-CHECKLISTE

SCHNELL-DIAGNOSE: DNS-RECORD-AUSWAHL

Verwenden Sie diesen Entscheidungsbaum, um im operativen Netzwerkbetrieb sofort den korrekten Resource-Record-Typ für Ihre Konfigurationsaufgabe zu bestimmen.

Welche Art von Ziel oder Funktion soll für die Domain bzw. Ressource im DNS hinterlegt werden?

1. IP-ADRESSE

Hostname soll direkt auf eine IP-Adresse aufgelöst werden.



A-Record für IPv4 (32-Bit) oder AAAA-Record für IPv6 (128-Bit) einrichten. Niemals CNAME verwenden, falls Domain-Apex oder weitere Records vorliegen.

2. ALIAS / CNAME

Subdomain soll als reines Synonym/Alias auf einen anderen Hostnamen verweisen.



CNAME-Record verwenden. Sicherstellen, dass kein Domain-Apex betroffen ist und keine weiteren Records unter demselben Namen existieren.

3. E-MAIL-EMPFANG

Zuständigkeit für eingehenden E-Mail-Empfang definieren.



MX-Record konfigurieren, Prioritätswert angeben und auf den FQDN des Mailservers verweisen (nicht direkt auf IP).

4. REVERSE DNS

Zuordnung einer IP-Adresse zurück zu einem Hostnamen (Reverse DNS).



PTR-Record in der passenden in-addr.arpa- oder ip6.arpa-Zone beim zuständigen ISP/Netzbetreiber anlegen.

5. AUTHENTIFIZIERUNG

E-Mail-Authentifizierung (SPF/DKIM/DMARC) oder Domain-Nachweis.



TXT-Record mit der geforderten Konfigurationszeichenkette (z. B. SPF-Regelwerk oder DKIM-Schlüssel) hinterlegen.

6. SRV-DIENST

Spezifischer Dienst benötigt dynamische Angabe von Port und Protokoll.



SRV-Record mit Dienstkürzel, Protokoll, Priorität, Gewichtung und Zielport erstellen.

7. ZUSAMMENFASSUNG

Alle wichtigen Record-Typen auf einen Blick.



Die passende Record-Art sorgt für eine stabile, sichere und korrekte DNS-Konfiguration.

PRAXIS-CHECKLISTE: ZONEN-KONFIGURATION

Prüfpunkte vor der Freigabe oder Migration einer produktiven DNS-Zonendatei.

- [ ] **1 SOA-RECORD** ✓
  SOA-Serial gemäß Konvention (YYYYMMDDNN) erhöht und Kontaktadresse syntaktisch korrekt formatiert.
- [ ] **2 NS-SERVER** ✓
  Mindestens zwei geografisch und topologisch getrennte NS-Server konfiguriert und erreichbar.
- [ ] **3 GLUE-RECORDS** ✓
  Notwendige Glue-Records bei zoneninternen Nameservern in der übergeordneten Zone hinterlegt.
- [ ] **4 CNAME-KOLLISIONEN** ✓
  Keine CNAME-Kollisionen auf dem Domain-Apex und keine koexistierenden Einträge bei CNAME-Hosts.
- [ ] **5 MX-EINTRÄGE** ✓
  MX-Einträge verweisen ausnahmslos auf gültige A/AAAA-Records und nicht auf CNAMEs oder IPs.
- [ ] **6 SPF & DMARC** ✓
  SPF- und DMARC-TXT-Records validiert (keine doppelten SPF-Einträge pro Zone).
- [ ] **7 PTR-RECORDS** ✓
  PTR-Records stimmen exakt mit dem HELO/EHLO-Hostnamen der ausgehenden Mailserver überein.

DNSSEC & DNS-TRANSPORT

Sichere DNS-Auflösung durch kryptografische Signaturen und verschlüsselte Transportprotokolle.

1. KRYPTOGRAFISCHE RRs



DNSSEC erweitert Zonen um standardisierte Resource Records (RRs) zur Verifikation:

- **RRSIG:** Digitale Signatur über ein komplettes Resource Record Set (RRset) mit Gültigkeitszeitraum
- **DNSKEY:** Enthält den öffentlichen Schlüssel der Zone zur Prüfung der RRSIG-Signaturen
- **DS (Delegation Signer):** Hashwert des DNSKEY der Kindzone, hinterlegt in der übergeordneten Elternzone

2. ZSK UND KSK



Zur Trennung administrativer Aufgaben nutzt DNSSEC ein zweistufiges Schlüsselkonzept:

- **ZSK** (Zone Signing Key): Signiert die operativen RRsets der Zone, wird häufig und automatisiert rotiert
- **KSK** (Key Signing Key): Signiert ausschließlich das DNSKEY-RRset, interagiert mit der übergeordneten Zone
- Die Trennung minimiert den Koordinationsaufwand mit der übergeordneten Registry bei Schlüsselwechseln

3. CHAIN OF TRUST



Die lückenlose Validierungskette verbindet die DNS-Wurzel mit der angefragten Domäne:

- **Trust Anchor:** Bekannter öffentlicher KSK der DNS-Root-Zone ('.') im Resolver hinterlegt
- Root verweist per DS-Record auf den KSK der TLD (z. B. '.de')
- TLD verweist per DS-Record auf den KSK der Domäne (z. B. 'example.de')
- Ein Resolver verwirft die Antwort mit SERVFAIL, falls ein Kettenglied ungültig ist

4. NSEC & NSEC3



Authentifizierter Nachweis der Nichtexistenz (Authenticated Denial of Existence):

- **NSEC:** Zeigt lexikografisch auf den nächsten vorhandenen Eintrag; ermöglicht jedoch Zone-Walking
- **NSEC3:** Verhindert Zone-Walking durch kryptografische Hashes und optionales Salting der Domainnamen
- Beweist manipulationssicher, dass eine Domain oder ein RRset tatsächlich nicht existiert (NXDOMAIN).

5. DoT (DNS OVER TLS)



DNS-Transportverschlüsselung auf Protokollebene via RFC 7858:

- Verwendet dedizierten TCP-Port 853 für eine direkte TLS-Verschlüsselung der DNS-Nachrichten
- Einfache netzwerkseitige Erkennung und Filterung in Unternehmensumgebungen anhand des Ports
- Geringerer Protokoll-Overhead im Vergleich zu DoH, primär in Betriebssystemen und Routern implementiert

6. DoH (DNS OVER HTTPS)

Kapselung von DNS-Anfragen in Standard-Webverkehr via RFC 8484:

- Nutzt reguläre HTTP/2- oder HTTP/3-Verbindungen über den Standard-Port 443
- DNS-Abfragen sind im regulären Webdatenverkehr schwer von HTTPS-Zugriffen unterscheidbar
- Erschwert Zensur und MITM-Inspektion, schränkt jedoch auch lokale Sicherheitsfilter im LAN ein.



7. VALIDIERUNGSABLAUF

Schritte eines validierenden DNS-Resolvers beim Erhalt einer Antwort:

1. Resolver empfängt RRset samt RRSIG und den zugehörigen DNSKEY-Einträgen
2. RRSIG wird mit dem ZSK entschlüsselt und der mathematische Hash über das RRset geprüft
3. Der ZSK wird durch den KSK verifiziert, der ist geprüft a. bei vorgeschaltetem DS-Record der Elternzone geprüft
4. Umgehung lokaler DNS-Sperren auf Client-Ebene oder DNS over HTTPS (DoH) auf Port 443 im Browser oder Systemdienst konfigurieren.



8. ARCHITEKTUR-VERGLEICH



Entscheidungsmatrix zur Auswaal des passenden Sicherheitsverfahrens:

- **DNSSEC:** Zwingend erforderlich für fälschungssichere Auflösung (Integrität der Einträge)
- **DoT:** Ideal für netzwerkweite Verschlüsselung am Resolver/Gateway mit klaren Firewall-Regeln
- **DoH:** Ideal für roaming Endgeräte und Webbrowser in potenziell restriktiven Gastnetzen

Implementiert: DNSSEC-Validierung am lokalen Resolver aktiv (Status prüfen via dig +dnssec)

Implementiert: Verschlüsseiter Upstream-Transport konfiguriert (DoT Port 833 oder DoH Port 443)

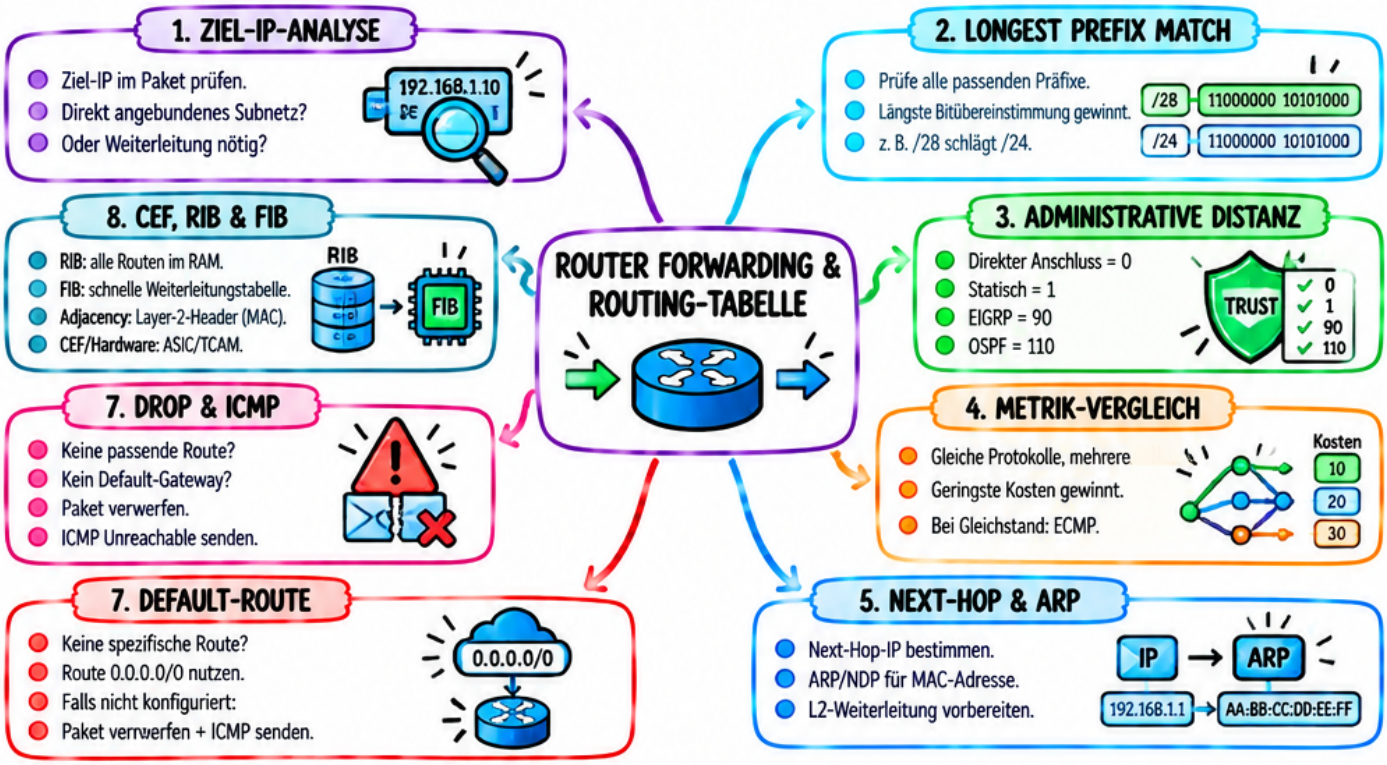
Notizen zur Konfiguration und Zertifikatsprüfung der Upstream-Resolver

Welches DNS-Sicherheitsverfahren soll primär implementiert werden?

Schutz vor gefälschten DNS-Antworten und Cache Poisoning erforderlich
DNSSEC-Validierung auf dem rekursiven Resolver aktivieren und DS-Records in der Domain-Registry pflegen.

Verschlüsselung im LAN/WAN mit klarer Netzwerk- und Port-Administration gewünscht
DNS over TLS (DoT) auf Port 853 zwischen Client/Gateway und vertrauenswürdigem Upstream-Resolver einrichten.

Umgehung lokaler DNS-Sperren auf Client-Ebene oder Roaming in Fremdnetzen
DNS over HTTPS (DoH) auf Port 443 im Browser oder Systemdienst konfigurieren.



Routing-Entscheidungsbaum & Kernprinzipien

Pakete auf Vermittlungsschichtebene werden anhand systematischer Kriterien durch den Router analysiert und an das passende Ausgangsinterface weitergeleitet.

1. **Ziel-IP-Prüfung:** Gehört die Zieladresse zum direkt angebundenen Subnetz oder erfordert sie Weiterleitung?
2. **Longest Prefix Match (LPM):** Die Route mit der spezifischsten Subnetzmaske (längste Bitübereinstimmung) gewinnt immer.
3. **Administrative Distanz (AD):** Bei Routen aus verschiedenen Quellen zum selben Zielnetz entscheidet der niedrigere Distanzwert (höhere Vertrauenswürdigkeit).
4. **Metrik-Vergleich:** Innerhalb desselben Routing-Protokolls gewinnt der Pfad mit den geringsten berechneten Kosten (Metrik).
5. **Next-Hop-Auflösung:** Bestimmung der IP des Folge-Routers und Ermittlung der zugehörigen L2-MAC-Adresse via ARP/NDP.
6. **Default Gateway:** Greift keine spezifische Route, wird der Datenverkehr über die Route 0.0.0.0/0 weitergereicht.
7. **Paket-Verwerfung (Drop):** Fehlt eine passende Route und ein Standard-Gateway, verwirft der Router das Paket und sendet ICMP Unreachable.
8. **Hardware-Beschleunigung:** Moderne Architekturen spiegeln Routing-Entscheidungen aus der RIB in die FIB und Adjacency-Tabellen (CEF).

Prüfregel für Pfadkollisionen

LFM schlägt stets die Administrative Distanz: Eine spezifischere Route (/26) gewinnt immer gegenüber einer allgemeineren Route (/24), selbst wenn letztere eine geringere AD bestizt.

Schritte der Weiterleitung

1. **Ingress & Dekapsulierung**
   L2-Frame-Header prüfen, FCS validieren und den L3-IPv4/IPv6-Header zur Auswertung der Zieladresse freigeben.
2. **LPM-Lookup & FIB-Abgleich**
   Prüfung der Routing-Tabelle bzw. FIB auf den längsten passenden Präfix zur Ziel-IP.
3. **TTL-Dekrementierung & L2-Rewrite**
   Time-to-Live um 1 verringern (Verwerfen bei TTL=0), Checksumme neu berechnen und Quell-/Ziel-MAC des nächsten Hops einsetzen.
4. **Egress-Übertragung**
   Weiterleitung des neu paketierten Rahmens über das ermittelte physische Ausgangsinterface.

Welche Route wird für das ankommende IP-Paket ausgewählt?

Präfixe unterscheidlich lang (z. B. /28 vs. /24)	Präfixe identisch, aber unterscheidliche Quellen (z. B. OSPF vs. EIGRP)	Präfixe und Routing-Protokoll identisch, Pfade parallel	Kein passender Eintrag in der Routing-Tabelle
Wähle die Route mit der längsten Bitmaske (Longest Prefix Match), unabhängig von Protokoll oder AD.	Wähle die Route mit der niedrigeren Administrativen Distanz (z. B. Connected=0, Static=1, EIGRP=90, OSPF=110).	Vergleiche Metrikwerte: Der Pfad mit niedrigeren Kosten siegt; bei Gleichstand greift Equal-Cost Multi-Path (ECMP).	Nutze Default-Route (0.0.0.0/0). Falls nicht konfiguriert: Paket verwerfen und ICMP Type 3 senden.

Routing-Architektur: RIB, FIB und Hardware-Forwarding

Zur Sicherstellung von Durchsatzraten im Terabit-Bereich trennen moderne Router strikt zwischen logischer Wegfindung (**Control Plane**) und tatsächlichem Paketversand (**Data Plane**).

- **Routing Information Base (RIB):** Steuerzentrale im RAM mit sämtlichen gelernten Routen aus allen Quellen und Routing-Protokollen.
- **Forwarding Information Base (FIB):** Auf Höchstgeschwindigkeit optimierte Abbild-Tabelle der besten Routen zur Vermeidung rekursiver Lookups.
- **Adjacency Table:** Speichert fertig vorbereitete Layer-2-Header-Informationen (MAC-Adressen) für direkte Next-Hop-Übertragungen.
- **Cisco Express Forwarding (CEF) / Hardware-Switching:** Ausführung der Forwarding-Entscheidung direkt in ASICs/TCAM ohne CPU-Unterbrechung.
- **Process Switching vs. Fast Switching:** Historische Verfahren, bei denen jedes oder das erste Paket über die System-CPU verarbeitet wurde.

Welche Route praktischen Fehlerdiagnose

Stimmt der Pfad in der Routing-Tabelle (RIB), aber Pakete gehen verloren, liegt häufig eine fehlerhafte Adjacency-Tabelle in der Hardware (ARP-Auflösung fehlgeschlagen) vor.

Routing-Architrating-Entscheidung & Metrik-Forwardise

Zur Sicherstellung von Durchsastraten im Terabit-Beerich trennen moderne Router strikt zwischen logischer Wegfindung (**Control Pallemic**.

- **Routing Information Base (RIB):** Steuerzentrale im RAM mit sämtlichen gelernten Routen aus allen Quellen und Routing-Protokollen.
- **Forwarding Information Base (FIB):** Auf Höchstgeschwindigkeit optimierte Abbild-Tabele der besten Routen zur Vermeidung oreiminsiwer Lookups.
- **Adjacency Table:** Speichert fertig vorbereitete Layer-2-Header-Informationen (MAC-Adressen) für direkte Next-Hop-Übertragungen.
- **Cisco Express Forwarding (CEF) / Hardware-Switching:** Ausführung der Forwarding-Entscheidung direkt in ASICs/TCAM ohne CPU-Unterbrechung.
- **Process Switching vs. Fast Switching:** Historische Verfahren, bei denen jedes oder das erste Paket über die System-CPU verarbeitet wurde.

Hinweis zur praktischen Fehlerdiagnose

Stimmt der Pfad in der Routing-Tabelle (RIB), aber Pakete gehen verloren, liegt häufig eine fehlerhafte Adjacency-Tabelle in der Hardware (ARP-Auflösung fehlgeschlagen) vor.

Arbeitsblatt: Forwarding-Entscheidung & Metrik-Analyse

Überprüfen Sie Ihr Verständnis der Routing-Logik. Ermittlen Sie für die Szenarien den jeweils gewinnenden Pfad anhand von LPM, AD und Metrik.

- Tragen Sie in die Zeilen ein, welche Route gewählt wird und welche Forwarding-Komponente angesprochen wird.
- Berücksichtigen Sie insbesendere Konflikte zwischen statischen Routen, OSPF und Default-Pfaden.

Fall 1: Ziel 192.168.1.45 mit Routen 192.168.1.0/24 (OSPF, AD 110) und 192.168.1.32/28 (Statisch, AD 1): Welcher Pfad gewinnt und warum?

Fall 2: Ziel 10.0.5.10 mit zwei /24-Routen aus OSPF (Metrik 20) und EIGRP (AD 90): Welcher Pfad wird in die Routing-Tabelle (RIB) übereonommen?

Fall 3: Unterscheidungsmerkmal RIB vs. FIB: Warum erfolgt der reale Datenfluss über die FIB statt der RIB?

Eigene Diagnose-Notiz: Verhalten des Routers bei TTL=1 vor der Schnittstellenausgabe:

STATISCHES ROUTING & DEFAULT ROUTES

Manuelle Pfadsteuerung für präzise und stabile Netzwerkkommunikation.

1. DEFINITION & SYNTAX

- Befehl (Cisco IOS): ip route <Zielnetz> <Maske> <Next-Hop/Interface>
- Next-Hop-Adressierung: rekursive Auflösung über Egress-Schnittstelle.
- Interface-Bindung: direkte Ausgangsschnittstelle (primär für P2P empfohlen).
- Administrative Distanz: Standard 1, manuell anpassbar.





2. GATEWAY OF LAST RESORT & DEFAULT ROUTE

- IPv4-Notation: 0.0.0.0/0 (Präfix 0.0.0.0 mit Maske 0.0.0.0).
- IPv6-Notation: ::/0 (alle Adressräume, Präfixlänge 0).
- Longest Prefix Match: niedrigste Spezifität (/0) und greift erst, wenn kein längerer Match vorliegt.



3. FLOATING STATIC ROUTES (AD-STEUERUNG)

- AD erhöhen (z. B. 10 oder 90 gegenüber Primärroute mit AD 1).
- Failover: Bei Link-Ausfall rückt die Floating Route in die Routingtabelle ein.
- Rückfall: Primärroute wieder verfügbar → Backup-Route wird verdrängt.



Achtung bei Ethernet-Verbindungen

Bei nur hinterlagertem Link bleibt die Egress-Schnittstelle aktiv (Up/Up). Ein einfacher AD-Fallback versagt hier ohne IP-SLA-Tracking.

4. IP-SLA-TRACKING

- SLA-Probe: regelmäßige Pings an Next-Hop oder Gegenstelle.
- Track-Objekt: überwacht den Status (Reachability ≠ Up/Down).
- Routenkopplung: Route ist an Track-Objekt gebunden; bei Down sofort entfernt.



5. NULL-ROUTING (NULL0)

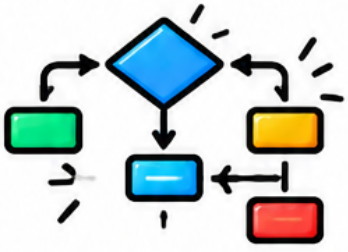
- Zweck: verhindert Routing-Schleifen bei Summarization.
- Sicherheit: dämpft DoS-Angriffe durch frühes Verwerfen.
- Ressourcenschutz: vermeidet unendliche ICMP-Redirects oder Bounce-Backs.



6. FORWARDING-ENTSCHEIDUNG

Hierarchische Auswertungslogik zur Bestimmung von Schnittstelle und Next-Hop.

1. Direkt verbundenes Zielnetzwerk: ARP-Lookup / Neighbor Discovery.
2. Longest Prefix Match: längste Subnetzmaske.
3. Gateway of Last Resort: 0.0.0.0/0 bzw. ::/0.
4. Drop & ICMP Unreachable: bei fehlendem Match.



7. KONFIGURATIONS-WORKFLOW & VALIDIERUNG

Strukturierter Ablauf zur fehlerfreien Implementierung und Verifikation.

- Konfigurationsfolge: Primärroute, SLA-Tracking, Floating Route, Null-Route.
- Validierungsbefehle: 'show ip route', 'ping', 'traceroute', 'show track'.

1. Primärroute und Next-Hop prüfen (AD 1).
2. IP-SLA-Tracking instanziieren (ICMP-Echo + Track-Objekt).
3. Floating Static Route anlegen (AD z. B. 200).
4. Failover-Test durchführen (Next-Hop isolieren, 'show ip route').



8. ROUTEN-DOKUMENTATION

Tragen Sie die Parameter Ihres Netzwerksegments ein, um Routen, Failovers und Tracking-Werte festzuhalten.



- Verhindert IP-Konflikte und Routing-Blackholes.
- Vorlage für Change-Management und Audit-Prozesse.

Ziel-Subnetz & CIDR-Maske (z. B. 10.50.0.0/16)

Primäre Next-Hop IP & Interface

Backup Next-Hop IP & Konfigurierte AD

IP-SLA Zieladresse & Ping-Intervall (Sekunden)

Aggregierte Null0-Route zur Schleifenvermeidung

DYNAMISCHE ROUTING-PROTOKOLLE

IGP vs. EGP, Distance Vector & Link State

1. AUTONOME SYSTEME (AS)

Das Internet besteht aus unabbängig verwalteten Netzbereichen unter einer einheitlichen Routing-Richtlinie.

- Jedes AS besitzt eine eindeutige autonome Systemnummer (ASN).
- Interne Netzstrukturen bleiben nach außen hin verborgen.
- Routing-Entscheidungen unterscheiden strikt zwischen intra-AS und inter-AS.



2. IGP – INTERIOR GATEWAY PROTOCOLS

Routing-Protokolle für den Nachrichtenaustausch innerhalb einer geschlossenen Organization.

- Ziel: Schnellstmögliche Konvergenz und optimale Pfadwahl.
- Geringer administrativer Overhead pro Ffadeintrag.
- Typische Vertreter: OSPF, IS-IS, RIP und EIGRP.



3. EGP – EXTERIOR GATEWAY PROTOCOLS

Protokolle zur Verbindung unterschiedlicher autonomer Systeme über das globale Internet.

- Skalierbarkeit über Millionen globaler Netzrouten.
- Steuerung durch vertragliche Richtlinien (Policy-based Routing).
- Heutiger weltweiter De-facto-Standard: BGP (Border Gateway Protocol).



8. MERKREGELN

Essenzielle Faustregeln für die Netzwerkarchitektur und Prüfungsvorbereitung.

- IGP routet im eigenen Haus (Topologie bekannt), EGP verbindet fremde Welten (Policy-basiert).
- Bellman-Ford: "Routing nach Hörensagen" – einfach, aber langsame Konvergenz.
- Dijkstra SPF: "Routing nach eigener Karte" – ausfallsicher und präzise.
- BGP nutzt AS_PATH als Schleifenschutz-attribut auf globaler Ebene.



Eigene Topologie: Verwendetes IGP und zugewiesene Area-Nummer

Eigene AS-Nummer (ASN) oder ISP-Upstream-Gateway

4. DISTANCE-VECTOR-ALGORITHMEN

Austausch vollständiger Routingtabellen nur mit direkt benachbarten Routern.

- Basiert auf dem Bellman-Ford-Algorithmus.
- Metrik: Meist Hop-Count (z. B. RIP, maximal 15 Hops).
- Problem: Anfällig für Routing-Schleifen (Count-to-Infinity).



5. LINK-STATE-ALGORITHMEN

Jeder Router kennt die vollständige Netzwerktopologie und berechnet Pfade autonom.

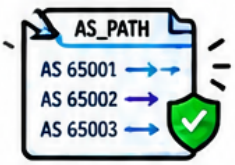
- Nutzt Dijkstras SPF-Algorithmus (Shortest Path First).
- Router senden Link-State Advertisements (LSA) per Flooding.
- Schnelle Konvergenz ohne Schleifen; benötigt mehr Speicher und CPU.



6. PATH-VECTOR-PRINZIP (BGP)

Erweiterung des Distanzvektor-Prinzips um den vollständigen AS-Pfadvektor.

- Erkennt Routing-Schleifen sofort durch wiederkehrende ASN im Pfad.
- Pfadwahl erfolgt nach konfigurierbaren BGP-Attributen und Policies.
- Unterteilt in eBGP (zwischen AS) und iBGP (innerhalb desselben AS).



7. PROTOKOLL-AUSWAHLMETHODIK

Vierstufiger Leitfaden zur Bestimmung des passenden dynamischen Routing-Verfahrens.

Administrative Distanz
Lernen Router eine Route über mebrere Protokolle, entscheidet die niedrigere Administrative Distanz (AD) über die Bevorzugung im Kernel.

1. **Einsatzbereich prüfen**
   Bestimmen, ob der Verkehr rein intern (IGP) oder zu externen Partnern/ISPs geroutet wird (EGP).
2. **Netzgröße & Latenzanforderungen analysieren**
   Bei komplexen Netzen Link-State wählen; bei simplen Muiti-Hop-Verbindungen reichen vereinfachte Verfahren.
3. **Metriken & Konvergenzzeiten definieren**
   OSPF nach Interface-Bandbreite konfigurieren oder BGP-Path-Attribute definieren.
4. **Schleifenprävention sicherstellen**
   Split-Horizon, Poison Reverse oder OSPF-Flächen-hierarchien (Area 0 Backbone) implementieren.



ENTSCHEIDUNGSHILFE

Welche Routing-Klasse wird für das aktuelle Netzwerkdesign benötigt?

Verkehr verlässt das eigene Netz ins globale Internet	EGP / BGP mit ASN-Konfiguration und Peering-Filtern wählen.
Internes Firmennetz mit hoher Skalierbarkeit und schnellem Failover	Link-State IGP (OSPF oder IS-IS mit Backbone-Hierarchie) einsetzen.
Sehr kleine, homogene Laborumgebung mit minimaler CPU-Last	Einfaches Distance-Vector-Protokoll oder statische Default-Routen verwenden.

RIPv2 & RIPng (Distance Vector)

1. PROTOKOLLTYP & GRUNDLAGEN



RIP ist ein klassisches Interior Gateway Protocol (IGP) basierend auf dem Distance-Vector-Verfahren (Bellman-Ford-Algorithmus). Router tauschen periodisch ihre vollständige Routingtabelle mit direkt verbundenen Nachbarn aus.

- Interior Gateway Protocol (IGP) für autonome Systeme
- Distance-Vector-Prinzip: Router kennt Distanz und Richtung (Next Hop)
- RIPv2 unterstützt Classless Inter-Domain Routing (CIDR) und Subnetzmasken

2. METRIK & BEGRENZUNG (HOP COUNT)



RIP nutzt ausschließlich den Hop Count (Anzahl durchquerter Router) als Metrik. Die Bandbreite, Latenz oder Zuverlässigkeit von Links werden ignoriert.

- Jeder Routerdurchlauf zählt exakt als 1 Hop
- Maximaler gültiger Hop-Count: 15
- Hop-Count 16 definiert ein unerreichbares Ziel (Infinity)

Skalierungs-Grenze
RIP eignet sich ausschließlich für kleine Netze mit maximal 15 Routern auf einem Datenpfad.

3. UPDATE-MECHANISMEN & ADRESSEN



Aktualisierungen erfolgen periodisch oder ereignisgesteuert. Im Gegensatz zu RIPv1 (Broadcast) arbeiten RIPv2 und RIPng mit Multicast-Adressierung.

- RIPv2 sendet Updates an IPv4-Multicast: 224.0.0.9 (UDP-Port 520)
- RIPng sendet Updates an IPv6-Multicast: FF02::9 (UDP-Port 521)
- Triggered Updates: Sofortige Meldung bei Topologieänderungen

4. RIP-TIMER IM DETAIL



Das Zeitverhalten von RIP wird über vier standardisierte Timer gesteuert, um Routinginformationen aktuell zu halten und veraltete Pfade sicher zu bereinigen.

- Update-Timer (30 s): Reguläres Intervall für den Tabellenaustausch
- Invalid-Timer (180 s): Zeit bis Route als ungültig markiert wird
- Holddown-Timer (180 s): Sperrzeit gegen vorzeitige Neuakzeptanz schlechterer Pfade
- Flush-Timer (240 s): Zeit bis zum endgültigen Löschen aus der Routing-Tabelle

5. SCHLEIFENVERMEIDUNG (LOOP PREVENTION)



Distance-Vector-Protokolle sind anfällig für Routing-Schleifen (Count-to-Infinity). RIP implementiert drei Kernverfahren zur Schleifenunterdrückung.

- Split Horizon: Eine Route wird niemals über das Interface zurückgemeldet, über das sie gelernt wurde
- Poison Reverse: Bekanntgabe einer ausgefallenen Route mit Metrik 16 über das Empfangs-Interface
- Holddown-Timer: Verhindert Routing-Flapping bei temporär instabilen Verbindungen

6. AUTHENTIFIZIERUNG & SICHERHEIT



Um Man-in-the-Middle- und Hijacking-Angriffe zu erschweren, verfügt RIPv2 über integrierte Sicherheitsmechanismen für Nachbarschafts-Updates.

- Klartext-Passwort (unsicher, anfällig für Sniffing)
- MD5-Kryptografie (Authentifizierung der RIP-Pakete zwischen Routern)
- Keine Abwärtskompatibilität zu IPv2- (separater Routing-Prozess)

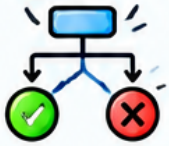
7. RIPNG FÜR IPV6-NETZWERKE



RIP next generation (RIPng) adaptiert die Kernlogik von RIP für moderne IPv6-Infrastrukturen bei Beibehaltung der Bellman-Ford-Prinzipien.

- Unterstützung reiner IPv6-Präfixe und Link-Local-
- Kommunikation über UDP-Port 521 an All-RIP-Routers Multicast FF02::9
- Keine Abwärtskompatibilität zu RIPv2-Payl… (separater Routing-Prozess)

8. PROTOKOLL-ENTSCHEIDUNGSHILFE



Bewertung, wann der Einsatz von RIP im Netzwerkdesign noch zweckmäßig ist und wann moderne Protokolle (OSPF/EIGRP/BGP) gewählt werden müssen.

- Vorteile: Sehr geringer Speicher-/CPU-Bedarf, minimale Konfiguration
- Nachteile: Langsame Konvergenz, maximale Netztiefe 15 Hops, ineffiziente Metrik

Ist RIP das passende Routing-Protokoll für das Zielnetzwerk?

✓ Kleines Netz mit weniger als 15 Hops und homogener Bandbreite
↓
RIPv2 oder RIPng einsetzen für unkompliziertes Setup ohne Link-State-Komplexität.

✗ Netzwerk mit mehr als 15 Hops oder redundanten Links unterschiedlicher Geschwindigkeit
↓
Link-State-Protokoll wie OSPF oder IS-IS wählen, da RIP Bandbreite ignoriert.

EIGRP
(ENHANCED INTERIOR GATEWAY ROUTING PROTOCOL)

1. PROTOKOLL-KLASSIFIKATION & GRUNDLAGEN

EIGRP ist ein hochentwickeltes erweitertes Distance-Vector-Routing-Protokoll (oft als Hybridprotokoll bezeichnet). Es wurde ursprünglich von Cisco entwickelt und arbeitet direkt auf IP-Ebene (IP-Protokollnummer 88) ohne TCP- oder UDP-Header.

- **Kategorie:** Advanced Distance-Vector / Hybrid Interior Gateway Protocol (IGP).
- **Kapselung:** Läuft direkt über IP (Protokollnummer 88), arbeitet unabhängig von TCP/UDP.
- **Updates:** Sendet partielle, getriggerte Routing-Updates nur bei Topologieänderungen statt periodischer Voll-Updates.
- **Nachbarschaften:** Etabliert explizite Nachbarbeziehungen via Multicast (224.0.0.10 für IPv4 bzw. FF02::A für IPv6).

PRAXIS-HINWEIS
Weil EIGRP standardmäßig keine vollständigen periodischen Tabellen-Broadcasts sendet, spart es drastisch Bandbreite gegenüber klassischem RIP.

2. DUAL: FINITE STATE MACHINE & LOOP-FREIHEIT

Das Herzstück von EIGRP bildet der Diffusing Update Algorithm (DUAL). Er garantiert eine mathematisch beweisbare Schleifenfreiheit (Loop-Free Topology) zu jedem Zeitpunkt und ermöglicht extrem schnelle Konvergenz ohne Wartezeiten.

- **Ziel:** Verhindert Routing-Schleifen direkt auf algorithmischer Basis.
- **Passive State:** Normaler, stabiler Betriebszustand einer Route; Pfad ist berechnet und weiterleitungsbereit.
- **Active State:** Route wird aktiv neu berechnet (DUAL sendet Query-Pakete an Nachbarn, falls kein Backup existiert).
- **SIA (Stuck-in-Active):** Problemzustand, wenn eine Abfrage von Nachbarn nicht rechtzeitig quittiert wird.

3. METRIK: FD & RD/AD

DUAL stützt seine Routing-Entscheidungen auf zwei zentrale Distanzwerte, um primäre Pfade und schleifenfreie Ausweichpfade transparent voneinander abzugrenzen.

- **Reported Distance (RD) / Advertised Distance (AD):** Die vom benachbarten Next-Hop-Router berechnete Gesamtkosten-Distanz zum Zielnetzwerk.
- **Feasible Distance (FD):** Die lokal berechnete Gesamtdistanz vom eigenen Router über den jeweiligen Nachbarn bis zum Zielnetz.
- **Berechnungslogik:** FD entspricht den Verbindungskosten zum Nachbarn plus der vom Nachbarn gemeldeten RD.

FD = Kosten_zum_Nachbarn + RD(Nachbar)

Verbindungskosten + Vom Nachbarn gemeldete RD

8. PRAXIS & TROUBLESHOOTING-WORKFLOW

Strukturierte Überprüfung von Nachbarschaften, Topologiedaten und Weiterleitungstabellen im operativen Netzwerkbetrieb.

- **Schritt 1 (Nachbarn prüfen):** show ip eigrp neighbors – Status, Haltezeit (Holdtime) und Interface-Bindung verifizieren.
- **Schritt 2 (Topologie & Metriken prüfen):** show ip eigrp topology – Prüfen von Successor, Feasible Successor, FD und RD-Werten.
- **Schritt 3 (Routing-Tabelle inspizieren):** show ip route eigrp – Installierte Pfade (Kennzeichnung 'D') und Load-Balancing validieren.
- **Schritt 4 (Fehlerbehandlung):** Bei fehlender Nachbarschaft AS-Nummer, K-Werte, MTU, Subnetzmasken und Authentifizierung abgleichen.

SCHNELL-MERKER
Routing-Buchstabe 'D' in Cisco IOS steht für EIGRP (abgeleitet vom DUAL-Algorithmus, da 'E' historisch für EGP reserviert war).

SCHRITT-FÜR-SCHRITT

1. **Nachbarschaft analysieren**
   Mit 'show ip eigrp neighbors' sicherstellen, dass Hello-Pakete empfangen werden und die Nachbarschaft im Up-Status verbleibt.
2. **DUAL-Topologie & Feasible Successor abgleichen**
   Mittels 'show ip eigrp topology all-links' prüfen, welche Alternativrouten die Feasibility Condition (RD < FD) erfüllen.
3. **Unequal-Cost Tuning prüfen**
   Über den Variance-Multiplikator validieren, ob valide Feasible Successors proportional in die FIB/Routing-Tabelle übernommen werden.

PRÜFENDE FELDER
Geprüfte Autonomous System (AS) Nummer: _____
Successor Interface & aktuelle Feasible Distance (FD): _____
Gültige Feasible Successors (Next-Hop und RD): _____

SCHRITT-FÜR-SCHRITT

1. **Nachbarschaft analysieren**
   Mit 'show ip eigrp neighbors' sicherstellen, dass Hello-Pakete empfangen werden und die Nachbarschaft im Up-Status verbleibt.
2. **DUAL-Topologie & Feasible Successor abgleichen**
   Mittels 'show ip eigrp topology all-links' prüfen, welche Alternativrouten die Feasibility Condition (RD < FD) erfüllen.
3. **Unequal-Cost Tuning prüfen**
   Über den Variance-Multiplikator validieren, ob valide Feasible Successors proportional in die FIB/Routing-Tabelle übernommen werden.

PRÜFENDE FELDER
Geprüfte Autonomous System (AS) Nummer: _____
Successor Interface & aktuelle Feasible Distance (FD): _____
Gültige Feasible Successors (Next-Hop und RD): _____

ENTSCHEIDUNG
Wird ein Alternativpfad bei Link-Ausfall sofort ohne Unterbrechung aktiv?

- Ja, RD des Nachbarn ist kleiner als FD des primären Pfades → Feasible Successor existiert. Sofortiges Failover im Passive State ohne Query-Pakete.
- Nein, RD ist größer oder gleich der bisherigen FD → Kein Feasible Successor vorhanden. DUAL wechselt in Active State und sendet Query-Pakete zur Topologieberechnung.

6. URANSPORT: RELIABLE TRANSPORT PROTOCOLL (RTP)

EIGRP stützt sich EIGRP aufsetzt, bringt es sein eigenes auf Verbindungsprotokoll. Die Gewichtung einzelner Parameter wird über fünf S-Werte (K1 bis K5) gesteuert.

- **Standerd Diswichtung:** K1 = 1 (Bandbreite), K2 = 0 (Last), K3 = 1 (Verzögerung/Delay), K4 = 0 (Zuverlässigkeit), K5 = 0 (MTU-Faktor), zum Zeinetzwa.
- **Feasible Distanct (FD):** Die lokal berechnete Gesamtdistanz vom eigenen Verzöigee den
- **Berechnungslogik:** Dyntsprichte den Lardindungs-Zuverlässigkeit sind standardmäßig inaktiv, um Flapping und Neuberechnungs-Kaskaden zu vermeiden.
- **Nachbarschaftsvoraussetzung:** Die K-Werte müssen auf allen benachbarten Routern exakt übereinstimmen.

7. UNEQUAL-COST LOAD BALANCING

Eines der herausragenden Alleinstellungsmerkmale von EIGRP ist die Fähigkeit, Datenverkehr über Pfade mit unterschiedlichen Metrikkosten dynamisch aufzuteilen.

- **Equal-Cost Load Balancing (ECMP):** Standardmäßig aktiv für bis zu 4 Pfade (anpassbar) mit identischen Metrikwerten.
- **Unequal-Cost Load Balancing:** Ermöglicht Lastverteilung über Pfade mit ungleichen Kosten mittels des Befehls 'variance N'.
- **Variance-Regel:** Ein Feasible Successor wird genutzt, wenn gilt: Metrik(FS) <= N * Metrik(Successor).
- **Verkefrsverteilung:** Pakete werden proportional umgekehrt zu den Pfadkosten verteilt (schnellere Pfade transportieren mehr Daten).



5. COMPOSITE METRIC & K-WERTE

EIGRP untzt eine zusammengesezzte Metrik basierend auf Verbindungseigenschaften. Die Gewichtung einzelner Parameter wird über fünf **K-Werte** (K1 bis K5) gesteuert.

- **Standard-Gewichtung:** K1 = 1 (Bandbreite), K2 = 0 (Last), K3 = 1 (Verzögerung/Delay), K4 = 0 (Zuverlässigkeit), K5 = 0 (MTU-Faktior).
- **Klassische Formel:** Metrik = 256 * ((10^7 / minimale Bandbreite in kbit/s) + kumulierte Verzögerung in Zehner-Mikrosekunden).
- **Stabilitätsregel:** Dynamische Werte wie Last und Zuverlässigkeit sind standardmäßig inaktiv, um Flapping und Neuberechnungs-Kaskaden zu vermeiden.
- **Nachbarschaftsvorauseztzung:** Die K-Werte müssen auf allen benachbarten Routern exakt übereinstimmen.

Standard-K-Werte
K1 = 1 K2 = 0 K3 = 1
K4 = 0 K5 = 0

6. TRANSPORT: RELIABLE TRANSPORT PROTOCOLL (RTP)

Da EIGRP nicht auf TCP aufsetzt, bringt es sein eigenes Transportprotokoll (RTP) mit, um die verlässliche Zustellung kritischer Steuerungsnachrichten zu organisieren.

- **Pakettypen:** Hello (Nachbar-Erkennung, unzuverlässig), Update (Routendaten, zuverlässig), Query (Suchenfrage, zuverlässig), Reply (Antwort, zuverlässig), ACK (Quittung, unzuverlässig).
- **Zuverlässigkeit:** Zuverlässige Pakete erfordern eine explizite Bestätigung (ACK) durch den Empfänger mit Sequenznummern.
- **Multicast & Unicast:** Updates werden primär an Multicast gesendet; bleibt ein ACK aus, erfolgt Retransmission gezielt per Unicast.

OSPF: GRUNDLAGEN UND AREA-KONZEPT

1. LINK-STATE-GRUNDLAGEN

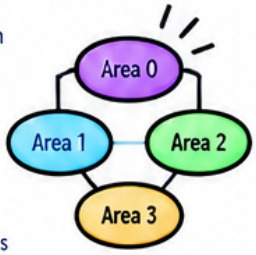
Open Shortest Path First (OSPFv2) ist ein offenes Link-State-Routing-Protokoll (Interior Gateway Protocol, IGP), das auf dem Dijkstra-Algorithmus (Shortest Path First) basiert. Jeder Router bildet eine vollständige Topologiekarte der eigenen Routing-Domäne ab.



- Verwendet Link-State Advertisements (LSAs) zur Verteilung von Topologieinformationen
- Aufbau einer einheitlichen Link-State Database (LSDB) innerhalb einer Area
- Metrik basiert primär auf Verbindungskosten (Cost = Referenzbandbreite / Schnittstellenbandbreite)
- Schnelle Konvergenz ohne Routing-Schleifen im Vergleich zu Distance-Vector-Verfahren

2. HIERARCHISCHE AREA-STRUKTUR

OSPF unterteilt autonome Systeme in logische Zonen (Areas), um die LSDB-Größe zu begrenzen und SPF-Neuberechnungen einzudämmen.



- Backbone-Area (Area 0 / 0.0.0.0): Zentraler Transitbereich, mit dem alle anderen Zonen verbunden sein müssen
- Standard-Areas: Reguläre Teilnetze, die intern detaillierte Topologiedaten austauschen
- Reduktion des Speicherbedarfs und LSA-Flutens über Gebietsgrenzen hinweg
- Routenaggregation an Zonengrenzen minimiert Routingtabellen

3. OSPF-ROUTER-ROLLEN

Router übernehmen in einer Multi-Area-Topologie spezifische Aufgaben basierend auf ihrer Schnittstellenplatzierung.



- Internal Router (IR): Alle aktiven Schnittstellen liegen innerhalb derselben OSPF-Area
- Backbone Router (BR): Verfügt über mindestens ein Interface in Area 0
- Area Border Router (ABR): Verbindet eine oder mehrere Standard-Areas mit der Backbone-Area
- Autonomous System Boundary Router (ASBR): Tauscht Routing-Informationen mit externen Netzwerken aus (z. B. BGP oder statische Routen)

4. HELLO-PROTOKOLL & ADJAZENZ

Das OSPF-Hello-Protokoll dient der dynamischen Nachbarschaftserkennung und kontinuierlichen Verbindungsüberwachung.



- Versand periodischer Hello-Pakete an die Multicast-Adresse 224.0.0.5
- Übereinstimmung von Hello-/Dead-Intervallen, Area-ID und Subnetzmaske ist zwingend erforderlich
- MTU-Größe und Authentifizierungsparameter müssen auf beiden Schnittstellenseiten matchen
- Verhindert fehlerhafte Adjazenzbildungen bei Konfigurationsabweichungen

5. OSPF-NACHBARSCHAFTSZUSTÄNDE

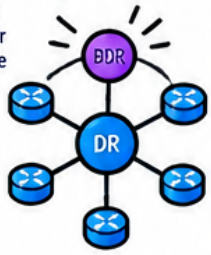
Zwischen zwei OSPF-Routern durchläuft der Verbindungsaufbau sieben sequenzielle Zustände bis zur vollständigen Synchronisation.

1. **Down bis Init**
   Startzustand ohne empfangene Hellos. Nach Erhalt des ersten Hello-Pakets wechselt der Router in 'Init'.
2. **2-Way**
   Bidirektionale Kommunikation etabliert; Router sieht eigene Router-ID in der Nachbarliste. Auf Broadcast-Netzen erfolgt hier die DR/BDR-Wahl.
3. **ExStart & Exchange**
   Aushandlung des Master/Slave-Verhältnisses und Austausch von Database Description (DBD)-Paketen zur Prüfung der LSDB.
4. **Loading & Full**
   Anforderung fehlender Details via Link-State Request (LSR) und Update (LSU). Im Zustand 'Full' sind beide LSDBs synchron.



6. DR- UND BDR-WAHL IM BROADCAST-NETZ

In Multi-Access-Netzwerken reduziert die Wahl von Designated Router (DR) und Backup Designated Router (BDR) die Anzahl der Nachbarschaftsbeziehungen von $n*(n-1)/2$ auf eine sternförmige Struktur.



- **Wahlkriterium 1:** Höchste OSPF-Schnittstellenpriorität (Default: 1, Wert 0 schließt von Wahl aus)
- **Wahlkriterium 2:** Höchste Router-ID (manuell konfiguriert, sonst höchste Loopback-IP, sonst höchste physische IP)
- **DRother**-Router etablieren vollständige Adjazenz ("Full") nur mit DR und BDR
- Kommunikation untereinander verbleibt im Zustand "2-Way"

Wichtiger Praxis-Hinweis

Die DR/BDR-Wahl ist **nicht-präemptiv:** Ein nachträglich hinzugefügter Router mit höherer Priorität übernimmt die Rolle erst nach einem OSPF-Prozess-Neustart.

7. OSPF-MULTICAST-ADRESSEN

OSPFv2 nutzt reservierte IPv4-Multicast-Adressen für effizienten Nachrichtenaustausch ohne Broadcast-Belastung.



- **224.0.0.5 (AllSPFRouters):** Spricht alle OSPF-fähigen Router auf dem Segment an
- **224.0.0.6 (AllDRouters):** Dedizierte Adresse für Nachrichten an DR und BDR
- **DRother**-Knoten senden Updates an 224.0.0.6; der DR vertieft sie über 224.0.0.5 an alle weiter
- Entlastet Endgeräte und OSPF-Knoten von unnötiger Paketverarbeitung

8. OSPF-VERIFIKATION & FEHLERDIAGNOSE

Strukturierte Überprüfung von OSPF-Schnittstellen und Adjazenzproblemen in der Praxis.

- **Prüfbefehl:** Nachbarschaftsstatus (show ip ospf neighbor)
- **Prüfbefehl:** OSPF-Schnittstellenparameter & Timer (show ip ospf interface)
- **Prüfbefehl:** Link-State-Datenbankstruktur (show ip ospf database)

Bleibt der Nachbarschaftsstatus im Zustand "Init" oder "ExStart" hängen?

- → Verharrt **in Init** — Unidirektionale Verbindung oder Paketfilter: Prüfen, ob Multicast 224.0.0.5 in beide Richtungen erlaubt ist und Schnittstellen-Timer exakt übereinstimmen.
- → Verharrt in **ExStart/Exchange**struktur — MTU-Konflikt: Schnittstellen-MTU auf beiden Seiten abgleichen oder 'ip ospf mtu-ignore' für Diagnosezwecke evaluieren.

OSPF: NACHBARSCHAFTSBEZIEHUNGEN, LSAs UND LSDB

1. OSPF-GRUNDPRINZIP & LSDB



Open Shortest Path First (OSPF) ist ein standardisiertes Link-State-Routing-Protokoll (Interior Gateway Protocol). Jeder Router ermittelt die vollständige Netzwerktopologie und speichert sie in der Link-State-Datenbank (LSDB).

- **Link-State-Prinzip:** Router teilen ihren lokalen Verbindungsstatus allen Routern innerhalb derselben OSPF-Area mit.
- **Identische Topologie:** Nach erfolgreicher Konvergenz besitzen alle Router einer Area eine exakt identische LSDB.
- **Dijkstra-Algorithmus (SPF):** Berechnet auf Basis der LSDB den kürzesten kreisfreien Pfad (Shortest Path Tree) zu jedem Zielnetzwerk.
- **Metrik Kosten (Cost):** Basiert standardmäßig auf der Schnittstellen-Bandbreite (Referenzbandbreite / Bandbreite).

Link-State vs. Distanzvektor
Im Gegensatz zu Distanzvektor-Protokollen (z. B. RIP) kennen OSPF-Router nicht nur die Richtung und Entfernung zum Ziel, sondern die gesamte Topologie-Karte des Bereichs.

2. ROUTER-ID & HELLO-PAKETE



Die Router-ID (RID) identifiziert jeden OSPF-Router im Netzwerk eindeutig. Hello-Pakete (OSPF-Pakettyp 1) dienen der Entdeckung und Überwachung von Nachbarn auf einem gemiensamen Übertragungsmedium.

- **RID-Bestimmung:** Manuell konfiguriert (höchste Priorität), sonst höchste IPv4-Adresse auf Loopback-Interfaces, zuletzt höchste aktive physische IP.
- **Hello-Multicast:** Versendung alle 10 s (Broadcast) an 224.0.0.5 (AllSPFRouters); Dead-Interval beträgt standardmäßig das 4-Fache (40 s).
- **Parameter-Übereinstimmung:** Hello/Dead-Timer, Area-ID, Subnetzmaske und Authentifizierung müssen zwingend übereinstimmen.
- **Keepalive-Mechanismus:** Bleibt ein Hello innerhalb des Dead-Intervalls aus, gilt die Nachbarschaft als unterbrochen.

3. NACHBARSCHAFTSPHASEN (DOWN BIS 2-WAY)



Der Aufbau einer OSPF-Adjazenz durchläuft definierte Zustände. Die ersten Phasen etablieren die bidirektionale Sichtbarkeit zweier benachbarter Systeme auf dem Übertragungssegment.

- **Down:** Anfangszustand; keine Hello-Pakete empfangen.
- **Init:** Hello empfangen, eigene RID noch nicht enthalten.
- **Attempt:** Nur in NBMA-Netzen; Hello an statische Nachbarn.
- **2-Way:** Bidirektionale Kommunikation bestätigt; eigene RID in Nachbarliste. In Broadcast-Netzen startet hier DR/BDR-Wahl.

3 Schritte zur 2-Way-Nachbarschaft

1. Hello versenden – Router A sendet Hello mit eigener RID an Multicast 224.0.0.5.
2. Init-Status – Router B empfängt das Hello und trägt Router A im Zustand *Init* ein.
3. Bidirektionale Bestätigung – Router B antwortet mit Hello, das Router As RID enthält; Zustand wechselt zu 2-Way.

4. ADJAZENZ-PHASEN (EXSTART BIS FULL)



Nach Erreichen des 2-Way-Zustands synchronisieren voll adjazente Nachbarn ihre Link-State-Informationen bis zur vollständigen Übereinstimmung der Datenbanken.

- **ExStart:** Master/Slave-Rolle und initiale Sequenznummer (höhere RID wird Master).
- **Exchange:** Austausch von Database Description (DBD)-Paketen (mit Kurzübersichten aller behannten LSAs).
- **Loading:** Fehlende/ veraltete Einträge per LSR anfordern und per LSU empfangen.
- **Full:** Vollständige Adjazenz; LSDBs sind identisch.

2-Way vs. Full Adjazenz
Auf Multiaccess-Segmenten erreichen normale Router (DROther) untereinander nur den Status 2-Way. Der Zustand *Full* wird ausschließlich mit DR und BDR aufgebaut.

5. DR- UND BDR-WAHL



In Broadcast- und NBMA-Netzen verhindert die Wahl eines Designated Routers (DR) und Backup Designated Routers (BDR) eine quadratische Zunahme von Adjazenz-Beziehungen.

- **Problem:** Bei n Routern entstünden ohne DR n*(n-1)/2 Adjazenzen, was hohen Rechendruck und Übertragungs-Overhead erzeugt.
- **Wahlkriterien:** Höchste OSPF-Schnittstellenpriorität gewinnt (Standard: 1; Wert 0 schließt von der Wahl aus); bei Gleichstand die höchste RID.
- **Nicht-präemptiv:** Ein nachträglich hinzugefügter Router mit höherer Priorität verdrängt einen bestehenden DR/BDR nicht.
- **Multicast-Adressen:** DR/BDR lauschen auf 224.0.0.6; alle anderen Router empfangen Updates über 224.0.0.5.

6. LINK-STATE ADVERTISEMENT (LSA) TYPEN 1 BIS 5



Topologie-Informationen werden in spezialisierten LSA-Datenstrukturen verpackt, die je nach Bereich und Ursprung unterschiedliche Gültigkeitsgrenzen aufweisen.

- **Typ 1 (Router LSA):** Von jedem Router generiert; beschreibt die eigenen Schnittstellen, Verbindungskosten und Nachbarn innerhalb der lokalen Area.
- **Typ 2 (Network LSA):** Vom DR im Multiaccess-Segment generiert; listet alle mit diesem Teilnetz verbundenen Router.
- **Typ 3 (Summary LSA):** Vom ABR erzeugt; kündigt Netzwerk-Präfixe aus einer Area in eine andere an.
- **Typ 4 (ASBR-Summary LSA):** Vom ABR erzeugt; teilt anderen Areas den Pfad und die Metrik zum ASBR mit.
- **Typ 5 (AS-External LSA):** Vom ASBR erzeugt; transportiert extern umverteilte Routen (z. B. aus BGP, statischem Routing).

7. LSDB-SYNCHRONISATION & FLOODING



Ändert sich ein Verbindungszustand, sorgt zuverlässiges Flooding für eine verzögerungsfreie und konsistente Aktualisierung aller Router. Unmittelbar benachbarten Router.

- **LSU und LSAck:** Link-State Updates (LSU) enthalten, konkrete LSAs und werden, Verbindungskosten und Nachbarn innerhalb der lokalen Area.
- **Flooding-Verfahren.** Neues DR im Multiaccess-Segment gennant ist Sequenznummen und Alter) wird andeen Router.
- **Typ-AlSummary LSA):** Vom ABR erzeugt; umverteilte Netzwerk-Präfixe aus einer Area in eine andere an.
- **Typ 4 (ASBR-Summary LSA):** Vom ABR erzeugt; teilt anderen Areas den Pfad und die Metrik zum ASBR mit.
- **Typ 5 (AS-External LSA):** Vom ASBR erzeugt; transportiert extern umverteilte Routen (z. B. aus BGP, statischem Routing).

Stabilität durch OSPF-Areas
Durch Aufteilung in Backbone (Area 0) und Standard-Areas begrenzen Typ-1- und Typ-2-LSAs das Flooding auf den jeweiligen Bereich, was CPU und RAM entlastet.

8. DIAGNOSE & FEHLERBEHEBUNG



Strukturierte CLI-Befehle und Entscheidungsregeln ermöglichen die schnelle Eingrenzung von Störungen beim Aufbau von OSPF-Nachbarschaften.

- **show ip ospf neighbor:** Nachbar-RID, Status (Full/2-Way/Init), DR/BDR-Rolle sowie die Schnittstelle.
- **show ip ospf database:** Vorhandene LSAs nach Typen.
- **show ip route ospf:** Interne (O), inter-area (O IA) und externe Routen in der RIB.
- **Häufige Ursachen für State-Hänger:** MTU-Mismatch führt typischerweise zu Endlosschleifen im ExStart/Exchange.

Lokale OSPF Router-ID & Area-Zuordnung:	
Erkannte Nachbarn & Adjazenzstatus (Ziel: Full oder 2-Way):	
Prüfung von Timer- und MTU-Konfiguration bei Störungen:	

Nachbar bleibt deuarheft im Status 'ExStart' oder 'Exchange' hängen?

MTU auf beiden Seiten der Verbindung ungleich	→ MTU-Werte angleichen oder 'ip ospf mtu-ignore' konfigurieren.
Doppelte Router-IDs vorhanden	→ Router-IDs überprüfen und eindeutige Werte vergeben.
Paketfragmentierung oder Firewall blockiert Unicast/DBD	→ Sicherstellen, dass OSPF-Pakettyp 2 (DBD) und Unicast nicht verworfen vernerfen werden.



INTERMEDIATE SYSTEM TO INTERMEDIATE SYSTEM (IS-IS) – LINK-STATE IGP

1. GRUNDKONZEPT & PROTOKOLLTYP



IS-IS ist ein Link-State-Routing-Protokoll (IGP), das von der ISO standardisiert und via RFC 1195 (Integrated IS-IS) für IP adaptiert wurde. Es läuft direkt auf Schicht 2 (Data Link) via eigene ISO-PDUs.

- Arbeitet direkt auf Layer 2 ohne IP-Header-Abhängigkeit
- Link-State-Topologie-Synchronisation via Dijkstra-SPF
- Immun gegen IP-Layer-Angriffe und IP-Spoofing-Schwächen
- Breit eingesetzt im Internet-Backbone und Service-Provider-Netzen

2. ADRESSIERUNG (CLNS & NET)



IS-IS nutzt herkunftsmäßig den OSI-Netzwerkdienst CLNS. Jedes System wird über einen Network Entity Title (NET) identifiziert, der aus Area-ID, System-ID und N-SEL (00) besteht.

- NET-Format: [Area-ID (1-13 Bytes)] + [System-ID (6 Bytes)] + [N-SEL (1 Byte = 00)]
- System-ID muss innerhalb der gesamten IS-IS-Domäne eindeutig sein
- Geräteorientierte Adressierung statt schnittstellenbasierter IP-Adressierung
- Beispiel: 49.0001.1921.6800.1001.00

3. HIERARCHIE: LEVEL 1 & LEVEL 2



Die Netzwerkarchitektur wird in zwei hierarchische Ebenen gegliedert, wobei Router-Grenzen im Gegensatz zu OSPF nicht auf Interfaces, sondern auf ganzen Geräten liegen.

- Level 1 (L1): Intra-Area-Routing innerhalb eines zusammenhängenden Bereichs
- Level 2 (L2): Inter-Area-Backbone-Routing zwischen verschiedenen Areas
- L1/L2-Kombirouter fungieren als Übergangsknoten (Border Routers)
- Strikte Trennung der Link-State-Datenbanken je Level

4. PROTOCOL DATA UNITS (PDUS)



Der Informationsaustausch erfolgt über standardisierte Protokolldateneinheiten (PDUs) direkt in Ethernet-Frames (LLC/SNAP).

- IIH (IS-IS Hello): Aufbau und Halten von Nachbarschaften
- LSP (Link State PDU): Verbreitung topologischer Zustandsdaten
- CSNP (Complete Sequence Number PDU): Datenbank-Vollabgleich
- PSNP (Partial Sequence Number PDU): Anforderung fehlender LSPs & Acknowledgment

5. TLV-ARCHITEKTUR & MULTI-TOPOLOGY



IS-IS transportiert Routing-Informationen in flexiblen Typ-Länge-Wert-Feldern (Type-Length-Value), was eine nahtlose Erweiterbarkeit ermöglicht.

- Einfache Erweiterung ohne Protokollneuentwicklung
- Natives Multi-Protocol-Routing: IPv4, IPv6 und MPLS Traffic Engineering
- TLV 128/130 (IPv4 Reachability) & TLV 236 (IPv6 Reachability)
- Multi-Topology Routing zur unabhängigen Berechnung von IPv4- und IPv6-Pfaden

6. SP-EINSATZ & SEGMENT ROUTING



In modernen Telco- und ISP-Netzen dient IS-IS als skalierbares Fundament für Transport- und Steuerungsarchitekturen.

- Hervorragende Skalierbarkeit für zehntausende Präfixe im Backbone
- Keine Abhängigkeit von funktionsfähigem IP-Stack beim Booten
- Ideale Basis für MPLS-LDP und Segment Routing (SR-MPLS / SRv6)
- BGP-Prefix-Independent Convergence (BGP-PIC) und Fast-Reroute-Support (TI-LFA)

7. VERGLEICH: IS-IS VS. OSPF



Beide Protokolle basieren auf Dijkstras SPF-Algorithmus, unterscheiden sich jedoch grundlegend in Architektur und Pakettransport.

- Transport: IS-IS direkt auf L2; OSPF über IPv4/IPv6-Protokollnummer 89
- Bereichsgrenzen: IS-IS auf Router-Ebene; OSPF auf Schnittstellen-Ebene (ABR)
- Erweiterbarkeit: IS-IS extrem agil via TLVs; OSPF erforderte OSPFv3 für IPv6
- Metrik: IS-IS standardmäßig flach/konfigurierbar (Wide Metrics); OSPF bandbreitenbasiert

8. ZUSAMMENFASSUNG & PRAXIS-FAZIT



IS-IS ist das robuste Rückgrat von Service-Provider- und Cloud-Backbones. Dank Schicht-2-Betrieb und TLVs bleibt es die bevorzugte Wahl für hochskalierbare Segment-Routing-Netze.

- Standard für großflächige Carrier- und ISP-Infrastrukturen
- Wartungsfreundlich durch sauberes Zweiebenen-Konzept (L1/L2)
- Zukunftssicher für IPv6 und SDN-basierte Netzwerkarchitekturen

BGP ARCHITEKTUR UND PEERING – MINDMAP

1. BGP ROLLE & ZWECK



Verbindet Tausende unabhängige Internetdienstanbieter, Rechenzentren und Konzerne zu einem weltweiten IP-Netz und regelt den Datenverkehr an den Außengrenzen.

- Skalierbarkeit für über 900.000 weltweite Routen
- Policy-basiertes Routing statt reinem Latenzvergleich
- Prävention von Routing-Schleifen über das AS_PATH-Attribut

2. AUTONOME SYSTEME (AS) & ASN



Jedes Netzwerk im globalen Routing besitzt eine ASN, vergeben von Regional Internet Registries (RIRs wie RIPE NCC).

- Public ASN: Weltweit eindeutig für Transit und Peering
- Private ASN: Reservierte Bereiche (z. B. 64512–65534) für interne Zwecke
- AS-Grenzen definieren administrative und sicherheitsrelevante Zonen

3. eBGP vs. iBGP ARCHITEKTUR



BGP unterscheidet strikt zwischen Peering über Systemgrenzen hinweg und internem Routing innerhalb desselben autonomen Systems.

- eBGP (External): Verbindung zwischen zwei unterschiedlichen AS (Standard TTL=1)
- iBGP (Internal): Routenaustausch innerhalb desselben AS (Full-Mesh oder Route Reflector)
- Next-Hop-Verhalten: eBGP ändert den Next-Hop standardmäßig, iBGP belässt ihn unverändert

8. BGP-SICHERHEIT & RPKI



Klassisches BGP vertraut Ankündigungen ungeprüft, weshalb moderne Sicherheitsmechanismen unerlässlich sind.

- BGP Hijacking: Fälschliche Ankündigung fremder IP-Präfixe leitet Verkehr um
- RPKI (Resource Public Key Infrastructure): Kryptografische Validierung der Routen-Herkunft (ROA)
- GTSM & MD5/TCP-AO: Schutz der BGP-Session gegen Spoofing und Session-Reset-Angriffe

4. TCP-PORT 179 SESSION-AUFBAU



Anders als viele Interior Gateway Protokolle untzt BGP eine zuverlässige Punkt-zu-Punkt-Verbindung über TCP auf Port 179.

- Kein eigener Transport-Zuverlässigkeits-mechanismus nötig, BGP verlässt sich auf TCP
- Unicast-Verbindung: Nachbarn müssen explizit per IP konfiguiert werden
- BGP-Nachrichtentypen: OPEN, UPDATE, KEEPALIVE und NOTIFICATION

BGP ARCHITEKTUR UND PEERING

7. PEERING-ARTEN & INTERNET EXCHANGE



Netzbetreiber tauschen Daten entweder über direkte Verträge oder an zentralen Knotenpunkten aus.

- Transit: Kostenpflichtige Anbindung an Upstream-Provider für weltweite Erreichbarkeit
- Settlement-Free Peering: Gegenseitiger kostenloser Datenaustausch auf Gegenseitigkeit
- IXP (Internet Exchange Point): Physische Hochleistungs-Switches für Multi-Peer-Austausch

BGP KERNKONZEPT & AUTONOME SYSTEME

BGP ist das primäre Pfadvektor-Routingprotokoll des globalen Internets. Es steuert, wie voneinander unabhängige Netzwerke – sogenannte Autonome Systeme (AS) mit eindeutiger ASN – Erreichbarkeitsinformationen für IP-Präfixe austauschen und Routing-Entscheidungen nach administrativen Richtlinien treffen.

- Pfadvektor-Prinzip: Überträgt vollständige AS-Pfade zur Vermeidung von Schleifen
- Autonomes System (AS): Einheitliche Routing-Domäne unter zentraler Verwaltung
- ASN (Autonomous System Number): 16-Bit oder 32-Bit Kennung für jedes Netz
- Routing-Entscheidungen basieren primär auf Business-Policies statt rein technischer Metriken



5. BGP FINITE STATE MACHINE (FSM)



Eine BGP-Session durchläuft sechs definierte Zustände, bevor Routen ausgetauscht werden können:

- Idle: Startzustand, wartet auf Start-Event
- Connect: Wartet auf TCP-Verbindungsauftau
- Active: Neuer Verbindungsversuch nach Fehlschlag
- OpenSent: BGP-OPEN-Nachricht versendet
- OpenConfirm: Wartet auf KEEPALIVE des Nachbarn
- Established: Vollständig aktiv, Austausch von UPDATEs

7. BGP SCHNELLÜBERSICHT & TROUBLESHOOTING



Diagnose-Leitfaden für Netzwerkadministratoren bei BGP-Verbindungsproblemen:

- Prüfen der TCP-Verbindung zu Port 179 (Firewall-Freigaben und Layer-3-Erreichbarkeit)
- Session-Status 'Active' deutet meist auf TCP-Handshake-Probleme hin
- ASN-Fehlkonfiguration führt zu NOTIFICATION-Resets
- Route Reflectors nutzen, wenn iBGP-Vollvermaschung nicht skaliert

Praxistipp für Administratoren

Wenn ein BGP-Nachbar im Status 'Active' verharrt, ist meist kein BGP-Fehler ursächlich, sondern TCP-Port 179 wird blockiert oder die IP-Konnektivität zum Peer ist unterbrochen.

Schritte zur Fehlerbehebung:

1. **Layer 3 prüfen**
   Sicherstellen, dass die Peer-IP per Ping und Routing-Table erreichbar ist.
2. **Port 179 freigeben**
   Firewall-Regeln für eingehende und ausgehende TCP-Sessions auf Port 179 validieren.
3. **Session-Status abfragen**
   Mittels 'show ip bgp summary' prüfen, ob der Status Established erreicht wird.

BGP Nachbarschaft bleibt im Zustand 'Idle' oder 'Active' stehen?

Status "Active"

TCP-Konnektivität und Firewall-Regeln auf Port 179 prüfen; ACLs auf Interface untersuchen.

Status "Idle"

Konfiguration aktivieren ('no shutdown' auf BGP-Neighbor) und Layer-3-Route zum Peer prüfen.

BGP-Pfadattribute & Pfadauswahlalgorithmus

1. WAS IST BGP-PFADAUSWAHL?



Das Border Gateway Protocol (BGP) steuert das Routing zwischen autonomen Systemen (AS). BGP wählt Routen nicht nach minimalen Hops oder Bandbreite, sondern anhand einer geordneten Kette standardisierter Pfadattribute (Path Attributes).

- **Path-Vector-Routing:** Vermeidung von Routing-schleifen durch Verfolgung kompletter AS-Pfade.
- **Attributbasiert:** Jedes BGP-Update transportiert Attribute zur Pfadbewertung.
- **Deterministisch:** Der Algorithmus bricht beim ersten Attribut ab, das einen klaren Sieger liefert.

Wichtiger Merksatz
BGP evaluiert Pfadattribute streng sequenziell. Ein tieferes Attribut wird nur geprüft, wenn alle vorherigen Werte absolut identisch sind.

2. WEIGHT (PROPRIETÄR / LOKAL)



Weight ist ein herstellerspezifisches Attribut (z. B. Cisco), das nur lokal auf dem jeweiligen Router gilt und niemals in BGP-Updates an Nachbarn weitergegeben wird.

- Wertebereich: 0 bis 65.535 (Standard für lokal generierte Routen: 32.768, sonst 0).
- Regel: Höherer Wert gewinnt (Highest Weight preferred).
- Einsatz: Schnelle Beeinflussung des lokalen ausgehenden Datenverkehrs auf einem einzelnen Gerät.

3. LOCAL PREFERENCE



Local Preference ist ein standardisiertes, diszipliniertes Attribut, das innerhalb des gesamten autonomen Systems (IBGP) kommuniziert, aber niemals über eBGP-Grenzen exportiert wird.

- Standardwert: Üblicherweise 100.
- Regel: Höchster Wert gewinnt (Highest Local-Pref).
- Einsatz: Steuerung des primären
- Einsatz: Steuerung des primären Ausgangs-Gateways für den gesamten ausgehenden AS-Traffic.

4. LOKAL GENERIERTE ROUTEN & AS-PATH



Wenn Weight und Local Preference identisch sind, bevorzugt BGP selbst generierte Pfade (via 'network' oder 'redistribute' gegenüber BGP-gelernten), gefolgt von der AS-Path-Länge.

- **AS-Path-Länge:** Kürzeste Sequenz von autonomen Systemen gewinnt.
- **Loop Prevention:** Eknennt der Router die eigene AS-Nummer im Pfad, verwirft er das Update.
- **AS-Path Prepending:** Künstliche Pfadverlängerung zur Drosselung eingehenden Verkehrs.

BGP PFADAUSWAHL & ATTRIBUTE

BEST-PATH SELECTION ALGORITHM

6. ORIGIN TYPE & MED (MULTI-EXIT DISCRIMINATOR)



Origin kennzeichnet den Ursprung der Route (IGP < EGP < Incomplete). MED beeinflusst, über welche Verbindung Nachbarn Traffic in das lokale AS leiten sollen.

- Origin-Priorität: IGP (i) wird vor EGP (e) und Incomplete (?) bevorzugt.
- MED-Regel: Niedrigster Wert gewinnt (Lowest MED preferred).
- Eigenschaft: MED wird an direkte eBGP-Peers übergeben, aber von diesen nicht weiterpropagiert.

6. PEER-TYP & IGP-METRIK ZUM NEXT-HOP



BGP unterscheidet zwischen extern gelernten und intern gelernten Nachbarschaften und untst die Metrik des Interior Gateway Protocols (z. B. OSPF/IS-IS) als Kriterium.

- eBGP vor iBGP: Externe Pfade werden intern gelernten Pfaden vorgezogen.
- Next-Hop-Metrik: Niedrigste IGP-Kosten zum BGP-Next-Hop gewinnen.
- Hot-Potato-Routing: Pakete werden schnellstmöglich an das nächstgelegene Exit übergeben.

8. BEST-PATH ALGORITHMUS & PRAXIS-CHECK



Führen Sie die Pfadauswahlprüfung Schritt für Schritt durch, um Fehlkonfigurationen und unerwünschtes Traffic-Engineering auf BGP-Routern zu diagnostizieren.

- Prüfen: ist der Next-Hop ereichbar? (Grundvorausetzung für die Evaluation).
- Schrittfolge: Weight -> Local-Pref -> Local Originated -> AS-Path -> Origin -> MED -> eBGP/IBGP -> IGP-Metrik -> Router-ID.
- Befehl: 'show ip bgp <prefix>' zeigt alle konkurrierenden Pfade und den gewählten Best-Path (>).

Troubleshooting-Tipp
Wird ein Pfad unerwartet nicht gewählt, prüfen Sie zuerst mit "show ip route", ob der Next-Hop im IGP auflösbar ist (Next-Hop Reachability).

Schritt-für-Schritt-Anleitung

1. **Schritt 1: Next-Hop Validierung**
   Sicherstellen, dass der BGP Next-Hop über die lokale Routing-Tabelle auflösbar ist. Ungültige Next-Hops werden sofort disqualifiziert.
2. **Schritt 2: Weight & Local-Pref Vergleich**
   Prüfen, ob lokale Priorisierungen vorliegen. Der höchste Weight-Wert gewinnt; bei Gleichstand gewinnt der höchste Local-Pref-Wert.
3. **Schritt 3: AS-Path & Origin Analyse**
   Vergleich der Anzahl an autonomen Systemen im AS-Path. Bei gleicher Länge den Origin-Code prüfen (IGP vor Incomplete).
4. **Schritt 4: MED & Nachbar-Typ Auswertung**
   Auswertung von MED (niedriger Wert) und Bevorzugung von eBGP gegenüber iBGP, gefolgt von der IGP-Metrik zum Next-Hop.

Diagnose-Formular

Ziel-Präfix / Test-Netzwerk

Verglichene Pfade (Next-Hop A vs. Next-Hop B)

Entscheidendes Kriterium im Best-Path-Algorithmus

7. TIE-BREAKER (BGP-ROUTER-ID & PEER-IP)



Besteht nach allen Pfadattributen weiterhin Gleichstand, greifen deterministische Tie-Breaker, um eine anleeutige Routing-Entscheidung zu erzwingen.

- Älteste Route: Bevorzugung der stabilsten bestehenden eBGP-Route.
- Niedrigste BGP-Router-ID: Bevorzugt den Nachbarn mit der kleinsten Router-ID (IPvA-Format).
- Niedrigste Peer-IP-Adresse: Letzter Entscheidungsfaktor bei multiplen Peering-Sessions.

Welches Attribut entscheidet bei zwei Routen mit identischer Local Preference?

1. Route A wurde lokal auf dem Router generiert, Route B via eBGP empfangen.
   → Wähle Route A (Lokal generierte Route hat Vorrang vor gelernten Routen).
2. Beide Routen extern empfangen, aber Route A hat AS-Path (65001 65002], Route B hat (65003).
   → Wähle Route B (Kürzere AS-Path-Länge gewinnt).
3. AS-Path-Länge identisch, aber Route A hat Origin IGP (i) und Route B Incomplete (?).
   → Wähle Route A (IGP hat Vorrang vor Incomplete).

BGP-SKALIERUNG: ROUTE REFLECTORS & KONFÖDERATIONEN

1. DAS PROBLEM: IBGP FULL-MESH



BGP verlangt standardmäßig ein vollständiges internes Mesh zur Loop-Prävention, was in wachsenden Netzen zu massiven Skalierungsproblemen führt.

- Formel für iBGP-Peering-Sessions: N * (N - 1) / 2 bei N Routern
- Split-Horizon-Regel: Ein von iBGP gelernter Pfad darf nicht an andere iBGP-Peers weitergereicht werden
- Enormer Konfigurations- und Ressourcenaufwand bei Hunderten Routern im selben autonomen System

2. ROUTE REFLECTOR PRINZIP



Ein Route Reflector (RR) bricht die klassische iBGP-Split-Horizon-Regel kontrolliert auf und verteilt Routen selektiv an Clients.

- RR leitet Routen zwischen Clients und Non-Clients nach festen Weiterleitungsregeln weiter
- Clients benötigen nur iBGP-Sitzungen zum Route Reflector, nicht mehr untereinander
- Verringert die Anzahl notwendiger TCP-Verbindungen (Port 179) drastisch von $O(N^2)$ auf $O(N)$

3. LOOP-PRÄVENTION: ORIGINATOR-ID



Um Schleifen bei reflektierten Updates zu verhindern, nutzt BGP spezifische BGP-Pfadattribute.

- ORIGINATOR_ID wird vom ersten RR gesetzt und entspricht der BGP-Router-ID des Initiators
- Empfängt ein Router eine Route mit seiner eigenen ORIGINATOR_ID, verwirft er dieses Update sofort
- Bleibt über kaskadierte Route Reflector Reflektionen hinweg unverändert erhalten

4. CLUSTER-ID & CLUSTER-LISTE



Mehrere redundante Route Reflectors bilden gemeinsame Cluster, die durch Attribute abgesichert werden.

- CLUSTER_LIST fungiert analog zum AS_PATH auf Cluster-Ebene
- Jeder RR hängt seine Cluster-ID an die CLUSTER_LIST an, bevor er die Route reflektiert
- Wird die eigene Cluster-ID in der Liste entdeckt, wird die Route zur Vermeidung von Routing-Loops ignoriert

5. AUTONOMOUS SYSTEM CONFEDERATIONS



Konföderationen unterteilen ein großes autonomes System (AS) architektonisch in kleinere Sub-AS-Einheiten.

- Großes öffentliches AS wird intern in private Sub-Autonomous-Systems zerlegt
- Nach außen hin präsentiert sich das gesamte Netzwerk weiterhin als eine einzige einheitliche AS-Nummer
- Erfordert kein globales Full-Mesh, sondern kombiniert eBGP-ähnliches Peering intern mit lokalem iBGP

6. AS_CONFED_SEQUENCE ATTRIBUTE



Die Pfadverwaltung innerhalb von Konföderationen verhindert Schleifen zwischen den Sub-AS-Segmenten.

- AS_PATH nutzt interne Segmenttypen: AS_CONFED_SEQUENCE und AS_CONFED_SET
- Sub-AS-Nummern werden beim Verlassen des Gesamtsystems vor dem externen eBGP-Export gestrippt
- Next-Hop-, MED- und Local-Preference-Attribute bleiben über Sub-AS-Grenzen hinweg erhalten

7. DESIGNVERGLEICH: RR VS. KONFÖDERATION



Entscheidungsmatrix zur Auswahl der passenden Skalierungsarchitektur im Netzwerkdesign.

- Migration: Route Reflector ist modular und ohne Topologie-Neustrukturierung schrittweise einführbar
- Konföderation erfordert strikte Neugruppierung aller Router und Sub-AS-Zuweisung
- Kombination: In sehr großen Tier-1-Provider-Netzen werden RRs häufig innerhalb von Sub-AS-Konföderationen genutzt

ARCHITEKTUR-HINWEIS

Route Reflectors sind heute der De-facto-Standard in den meisten Enterprise- und ISP-Netzen, da Konföderationen bei Migrationen komplexer in der Handhabung sind.

Welche Skalierungsmethode eignet sich für Ihre Netzwerktopologie?

Bestehendes flaches iBGP-Netz mit Bedarf an schneller Skalierung ohne Redesigg	Historisch getrennte administrative Domänen oder Carrier-Zukäufe
↓	↓
Einstaz von redundanten Route Reflectors mit identischer Cluster-ID pro POP	Implementierung einer BGP-Konföderation mit privaten Sub-AS-Zuweisungen

8. ZUSAMMENFASSUNG & BEST PRACTICES



Kernregeln für den stabilen Betrieb von BGP in großem Maßstab.

- Mindestens zwei Route Reflectors pro Cluster für Ausfallsicherheit und Redundanz bereitstellen
- Cluster-ID einheitlich pro redundantes Paar konfigurieren, um Loop-Detektion abzusichern
- Out-of-Band-RR bevorzugt für reine Control-Plane-Reflektion ohne Transit-Traffic einsetzen
- IGP-Metriken (OSPF/IS-IS) präzise pflegen, um suboptimales BGP-Routing durch RRs zu vermeiden

ROUTE REDISTRIBUTION UND ROUTING-SCHLEIFEN-PRÄVENTION

1. GRUNDLAGEN DER REDISTRIBUTION

Route Redistribution bezeichnet das kontrollierte Einspeisen von Routing-Informationen aus einer Routing-Domäne in ein anderes Routing-Protokoll.



- Protokollgrenzen verhinden: Austausch zwischen OSPF, EIGRP, BGP und statischen Routen.
- Grenzrouter (ASBR): Vermittelt an Schnittstellen zweier Routing-Verfahren.
- Unterschiedliche Algorithmen: Überbrückt Distance-Vector- und Link-State-Konzepte.

2. ADMINISTRATIVE DISTANZ (AD)

Die Administrative Distanz dient Routern als Vertrauensindex bei der Auswahl des besten Pfads zwischen konkurrierenden Protokollen.



- Direkt verbunden: AD 0 (höchste Vertrauensstufe).
- Statische Route: AD 1.
- EIGRP (intern): AD 90.
- OSPF: AD 110.
- RIP: AD 120; External BGP: AD 20.

8. SCHRITT-FÜR-SCHRITT ANWENDUNG & VALIDIERUNG

Strukturierter Ablauf zur sicheren Aktivierung der Umverteilung im Produktivnetz.



1. Bedarfsanalyse & Prefix-Definition
   Identifizieren, welche Subnetze transportiert werden müssen, und strikte Prefix-Listen erstellen.
2. **Seed-Metrik festlegen**
   Sinnvolle Standard- oder protokollspezifische Metriken für Zielprotokolle konfigurieren.
3. **Route-Tagging aktivieren**
   Route-Maps mit eindeutigen Tags versehen, um Pfad-Rückläufe zu erkennen.
4. Routing-Tabellen auf unerwartete AD-Werte und Routing-Flapping mit Diagnostools überwachen.

Konfigurierte ASBR-Router / Schnittstellen:

Verwendetes Route-Tag zur Loop-Verhinderung:

3. METRIK-KONVERTIERUNG & SEED-METRIKEN

Da Protokolle Pfadkosten unterschiedlich berechnen, muss bei der Umverteilung eine passende Startmetrik (Seed-Metrik) zugewiesen werden.



- Inkompatible Logik: OSPF nutzt Bandbreite (Cost), RIP zählt Hop-Counts (max. 15).
- EIGRP-Metrik: Basiert auf Bandbreite, Verzögerung, Zuverlässigkeit und Last.
- Manuelle Definition: Ohne explizite Seed-Metrik verwerfen manche Protokolle Routen als unerreichbar.



ROUTE REDISTRIBUTION & LOOP-PRÄVENTION

4. RISIKO: ROUTING-SCHLEIFEN

Bei gegenseitiger (beidseitiger) Umverteilung über mehrere Grenzrouter drohen Feedback-Loops und suboptimale Pfade.



- Route Feedback: Eine Route wird in Domäne B gelernt und fälschlich zu A re-injiziert.
- Suboptimales Routing: Geringere AD-Werte täuschen überlegene Pfade vor.
- Blackholing: Pakete kreisen endlos und verbrauchen Bandbreite bis zum TTL-Ablauf.



Achtung bei Multi-Point Redistribution
Findet die Umwerteilung an mehr als einem Router statt, ist zwingend eine Filterung erforderlich, um Loop-Bildung zu verhindern.

7. ENTSCHEIDUNGSWEGWEISER: FILTER-METHODE

Wählen Sie anhand der Topologie die passende Absicherung gegen Loops.



Welche Topologie liegt zwischen den Routing-Domänen vor?

Ein einziger Grenzrouter (Single-Point)
Einfache Seed-Metrik und Prefix-Listen genügen; Schleifenbildung ist physikalisch unwahrscheinlich.

Zwei oder mehr Grenzrouter (Multi-Point)
Route-Tagging via Route-Maps konfigurieren und AD-Anpassungen vornehmen, um Route-Feedback zu blockieren.

5. ROUTE-FILTERING & PREFIX-LISTEN

Gezielte Filtertechniken steuern präzise, welche Netzwerkpräfixe zwischen den Protokollen geteilt werden dürfen.



- Prefix-Listen: Schnellere und präzisere Adress- und Subnetzmaskenprüfung als Standard-ACLs.
- Route-Maps: Modulare Regelwerke mit 'match'- und 'set'-Befehlen zur Attributsteuerung.
- Default-Deny: Best Practice sieht vor, nur explizit genehmigte Netze zu redistribuieren.

6. ROUTE-TAGGING ZUR PRÄVENTION

Route-Tags markieren Präfixe numerisch beim Verlassen einer Domäne, um deren Re-Injektion an anderer Stelle auszuschließen.



- Präfix markieren: Beim Exportieren von OSPF nach EIGRP wird ein Tag (z. B, 99) gesetzt.
- Eingangsfilter: Am zweiten Router werden alle Routen mit Tag 99 verworfen.
- Schleifenblockade: Verhindert bidirektionale Rückkopplung zuverlässig.

FHRP-Architektur: HSRP, VRRP und GLBP

1. GRUNDPRINZIP & PROBLEMSTELLUNG

Endgeräte in Subnetzen konfigurieren üblicherweise ein einziges Standard-Gateway. Fällt dieser Layer-3-Hop aus, bricht der externe Datenverkehr ab. FHRP bündelt mehrere physische Router zu einem virtuellen Gateway mit geteilter IP- und MAC-Adresse.

- **Single Point of Failure:** Ein einzelner physikalischer Router gefährdet das Subnetz
- **Virtuelle Identität:** Bereitstellung einer gemeinsamen VIP (Virtual IP) und VMAC
- **Transparenter Failover:** Endgeräte bemerken keinen physischen Routerausfall
- **Schicht-Einordnung:** Arbeitet auf Layer 3 zur Absicherung des lokalen Zugangs

PRAXIS-HINWEIS
DHCP verteilt als Default-Gateway stets die VIP der Redundanzgruppe, niemals die physikalische IP-Adresse eines einzelnen Routers.

2. CISCO HSRP (HOT STANDBY ROUTER PROTOCOL)

Cisco-proprietäres Redundanzprotokoll. Eine Gruppe definiert genau einen aktiven Router (Active) und einen Bereitschafts-Router (Standby). Weitere Gruppenmitglieder verbleiben im Listen-Status.



- **Rollenverteilung:** Genau 1 Active Router, 1 Standby Router, restliche Router im Listen-Status
- **Multicast-Kommunikation:** HSRPv1 nutzt 224.0.0.2 (UDP 1985), HSRPv2 nutzt 224.0.0.102
- **Virtuelle MAC v1:** 0000.0c07.acXX (wobei XX die HSRP-Gruppennummer in Hex darstellt)
- **Virtuelle MAC v2:** 0000.0c9f.fXXX für bis zu 4096 Redundanzgruppen

3. STANDARDISIERTES VRRP (V2 & V3)

IETF-Standard (RFC 5798/3768), herstellerunabhängig einsetzbar. Ein Master-Router übernimmt das Forwarding, während ein oder mehrere Backup-Router den Status überwachen.

- **Terminologie:** Unterscheidet strikt swischen Master Router und Backup Routern
- **IP-Nutzung:** Kann die physische Interface-IP direkt als VIP verwenden (Priority 255)
- **Multicast & Protokoll:** Nutzt IP-Protokoll 112 an Multicast-Adresse 224.0.0.18
- **VRRPv3-Erweiterung:** Unterstützt nativ IPv4 und IPv6 mit Subsekunden-Timern

4. CISCO GLBP (GATEWAY LOAD BALANCING)

Erweitert Redundanz um echte aktive Lastverteilung über denselben IP-Standard-gateway-Eintrag auf Endgeräten, ohne separate Subnetze oder Spanning-Tree-Tricks.



- **AVG (Active Virtual Gateway):** Ein gewählter Router beantwortet ARP-Anfragen
- **AVF (Active Virtual Forwarder):** Bis zu 4 Router leiten gleicheisttig Pakete weiter
- **Dynamische MAC-Zuweisung:** AVG verteilt unterschiedliche VMACs an ARP-Clients
- **Algorithmen:** Round-Robin, Host-Dependent oder gewichtete Verteilung (Weighted)

FIRST HOP REDUNDANCY PROTOCOLS (FHRP: HSRP, VRRP, GLBP)



6. FAILOVER-MECHANISMEN & EINSTELLUNGEN

Ein stabiler Failover erfordert korrekte Konfiguration von Prioritäten, Preemption und Schnittstellenüberwachung.

- **Prioritätswahl:** Höchste Priority gewinnt (Standardwert meist 100)
- **Preempt-Funktion:** Zwingend erforderlich, damit primärer Router nach Reboot Rolle zurückholt
- **Interface Tracking:** Reduziert Priorität bei Ausfall des Uplinks zur Vermeidung von Blackholes
- **Hello & Hold Timer:** Müssen auf allen Gruppen-mitgliedern identisch konfiguriert sein

ACHTUNG BEI PREEMPT
Ohne Tracking und Preempt bleibt ein degradierter Router aktiv, selbst wenn sein WAN-Uplink tot ist.

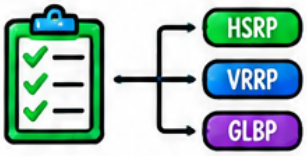
7. FEHLERBEHEBUNG & BEST PRACTICES

Typische Fehlkonfigurationen und strukturierte Diagnose im operativen Netzwerkbetrieb.

- **Duplicate IP Detection:** Prüfen, ob VIP versebentlich physisch vergeben wurde
- **VLAN/Trunk Mismatch:** Fehlende Übertragung von Multicast-Hellos führt zu Split-Brain
- **Preempt Delay:** Verzögerung aktivieren, bis Routing-Tabellen nach Neustart konvergiert sind
- **show standby / show vrrp:** Status, Timer und virtuelle MACs systematisch verifizieren

8. ZUSAMMENFASSUNG & ENTSCHEIDUNG

Protokollauswahl für redundante Gateways auf Basis der Betriebsanforderungen.



- **Multi-Vendor-Umgebung:** Ausschiedlich VRRPv2 bzw. VRRPv3 implementieren
- **Reine Cisco-Infrastruktur mit hohem Durchsatz:** GLBP für automatische Lastverteilung
- **Konservatives Cisco-Netzwerk:** HSRPv2 mit Subsekunden-Timern und Interface Tracking
- **Zero-Trust & Segmentierung:** FHRP-Authentifizierung zur Absicherung gegen Rogue-Router nutzen

WELCHES FHRP-PROTOKOLL PASST ZUR NETZWERKINFRASTRUKTUR?

Heterogene Switch- und Router-Hardware verschiedener Hersteller →	VRRPv3 standardisiert konfigurieren und Subsekunden-Timer für schnellen Failover nutzen.
Reine Cisco-Topologie mit Bedarf an simultaner Bandbreiten-auslastung beider Uplinks →	GLBP implementieren, AVG/AVF-Rollen zuweisen und Round-Robin-Balancing aktivieren.

MPLS: Architektur & Label-Header

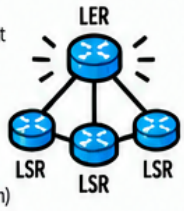
1. Was ist MPLS?

Multiprotocol Label Switching (MPLS) ist eine paketvermittelnde Technologie für Hochleistungsnetze, die zwischen Schicht 2 (Sicherungsschicht) und Schicht 3 (Vermittlungsschicht) angesiedelt ist. Anstatt langwierige IP-Routingtabellen bei jedem Zwischenstopp vollständig zu durchsuchen, leitet MPLS Datenpakete anhand kurzer, fester Kennzeichnungen – sogenannter Labels – ultraschnell durch die Netzinfrastruktur.

- **Protokollunabhängig:** Unterstützt IPv4, IPv6 sowie Ethernet-Frames als Nutzlast
- **Schicht-2.5-Einordnung:** Befindet sich zwischen dem Data-Link- und Network-Header
- **Hohe Effizienz:** Schnelles Label-Swapping statt aufwendigem Longest-Prefix-Match

2. Router-Rollen im MPLS-Netz

Ein MPLS-Netzwerk unterscheidet strikt zwischen Randknoten und Kernknoten, um die Weiterleitungskomplexität optimal aufzuteilen.



- **LER (Label Edge Router):** Steht am Netzwerkrand, klassifiziert eingehenden IP-Verkehr und fügt Labels hinzu oder entfernt sie
- **Ingress-LER:** Eingangsknoten, der IP-Pakete empfängt und mit dem ersten MPLS-Label versieht (Push-Operation)
- **Egress-LER:** Ausgangsknoten, der das letzte Label entfernt und das ursprüngliche IP-Paket an das Zielnetz ausliefert (Pop-Operation)
- **LSR (Label Switching Router):** Kernrouter, der Pakete ausschließlich anhand des Labels mit Höchstgeschwindigkeit weiterleitet (Swap-Operation)

3. Der 32-Bit Shim-Header

Der MPLS-Header ist exakt 32 Bit (4 Bytes) groß und wird wie ein Zwischenkeil (Shim) direkt vor den IP-Header geschoben. Er gliedert sich in vier präzise definierte Felder:

- **Label (20 Bit):** Der egentliche Bezeichner für den Weiterleitungspfad (Wertebereich 0 bis 1.048.575)
- **TC / EXP (3 Bit):** Traffic Class (früher Experimental), gentutzt für Quality of Service (QoS) und Priorisierung
- **S / BoS (1 Bit):** Bottom-of-Stack-Flag; signalisiert mit Wert 1, dass dies das letzte Label im Stack ist
- **TTL (8 Bit):** Time-to-Live; identisch zur IP-TTL zur Schleifenvermeidung, wird bei jedem Hop dekrementiert

Shim-Header Aufbau



= 32 Bit Gesamtgröße

4. Forwarding Equivalence Class (FEC)

Eine Forwarding Equivalence Class (FEC) fasst Datenpakete zusammen, die über denselben Pfad und mit derselben Dienstgüte durch das MPLS-Netzwerk transportiert werden.

- **Zuordnung am Ingress-LER:** Nur der Eingangsknoten analysiert die IP-Zieladresse und weist das Paket einer FEC zu
- **Einheitliche Behandlung:** Alle Pakete derselben FEC erhalten dasselbe Weiterleitungs-Label
- **Ressourcenschonend:** Der Netzwerk-Core muss keine routingbasierten Einzelfallentscheidungen treffen

5. Label-Operationen: Push, Swap, Pop

Während ein Paket den MPLS-Pfad (Label Switched Path, LSP) durchläuft, führen Router drei grundlegende Aktionen mit den Headern aus:

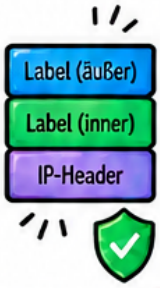
- **Push:** Hinzufügen eines oder mehrerer Labels am Ingress-LER oder für hierarchische Tunnel
- **Swap:** Austausch des eingehenden Labels durch ein neues ausgehendes Label im Core-LSR anhand der LFIB
- **Pop:** Entfernen des obersten Labels am Egress-LER vor der IP-Auslieferung
- **PHP (Penultimate Hop Popping):** Optimierung, bei der der vorletzte Router das Label entfernt, um den Egress-LER zu entlasten



6. Label-Stacking & Tunneling

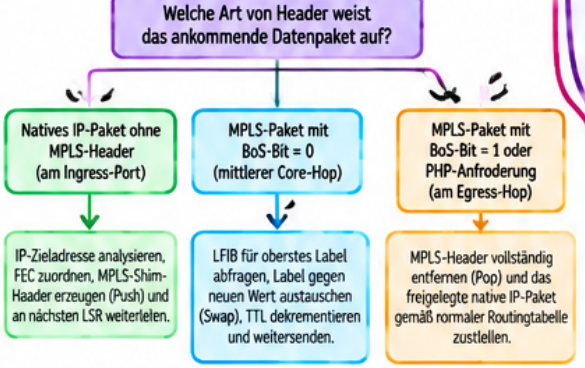
MPLS erlaubt das Stapeln mehrerer Labels übereinander. Die Router verarbeiten dabei immer nur das äußerste Label, was komplexe Netzwerkkonstrukte ermöglicht.

- **Äußeres Label (Transport):** Steuert den Transport durch das Provider-Backbone
- **Inneres Label (VPN/Service):** Identifiziert das spezifische Kundennetzwerk oder den Dienst am Zielknoten
- **Bottom-of-Stack (BoS):** Bit ist 0 für übergeordnete Transport-Labels und springt beim innersten Service-Label auf 1
- **Einsatzgebiete:** BGP/MPLS-VPNs (L3VPN), Carrier Supporting Carrier (CSC) und Fast Reroute (FRR)



7. Praxis-Workflow: Weiterleitung entscheiden

Entscheidungsbaum zur schnellen Einordnung eingehender Frames an einem Router-Interface im MPLS-Netz:



8. Zusammenfassung & Merkregel

MPLS kombiniert die Intelligenz des Routings auf Schicht 3 mit der Geschwindigkeit des Vermittelns auf Schicht 2.

- MPLS arbeitet mit 32-Bit-Shim-Headern (20 Bit Label, 3 Bit TC, 1 Bit S, 8 Bit TTL)
- Ingress pusht, LSR swappt, Egress poppt das Label
- Labels ermöglichen Traffic Engineering, QoS-Garantien und getrennte MPLS-VPNs
- Pakete derselben FEC folgen deterministisch demselben Label Switched Path (LSP)

Prüfungs-Merkregel

Push am Eingang, Swap im Kern, Pop am Ausgang.
Das BoS-Bit zeigt mit einer 1 das Ende des Label-Stapels an.

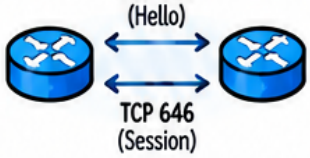
MPLS LDP & Signalisierung (Mindmap)

MPLS LDP & SIGNALISIERUNG



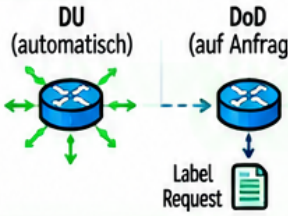
1. LDP DISCOVERY

- UDP-Hellos an 224.0.0.2 (Port 646) für Discovery.
- TCP-Session (Port 646) für Label-Informationen.
- Parameter-Austausch (Keepalive, Modus).



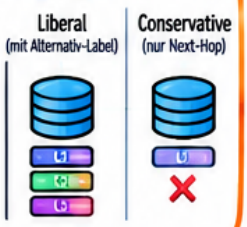
2. DU VS. DOD MODUS

- DU: Automatische Verteilung aller Labels an Nachbarn.
- DoD: Label Request pro FEC, bei Bedarf.
- Praxis: DU ist Standard (schnellere Konvergenz).



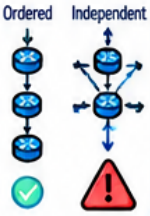
3. RETENTIONS MODI

- LLR: Alle Labels speichern, auch nicht-Next-Hop.
- CLR: Nur Next-Hop-Label speichern, Rest verwerfen.
- Tradeoff: LLR = mehr RAM, aber schnelleres Failover.



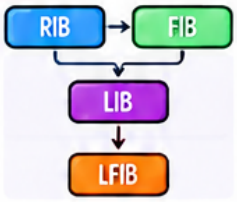
4. KONTROLLMODI

- Ordered: Erst nach Downstream-Label oder Egress.
- Independent: Sofort lokale Labels für alle FECs.
- Risiko: Blackholing bei Independent möglich.



5. TABELLEN: RIB, FIB, LIB, LFIB

- RIB: IGP-Routingtabelle (Next-Hop).
- FIB: Forwarding-Tabelle (Push am Ingress).
- LIB: LDP-Datenbank (alle Labels).
- LFIB: Hardware-Tabelle (Swap/Pop).



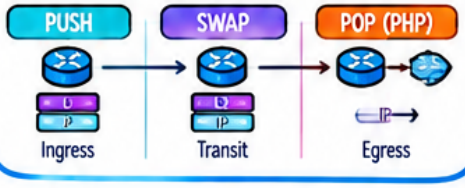
6. IGP-LDP-SYNCHRONISATION

- Problem: IGP routet, LDP noch nicht.
- Mechanismus: IGP Max-Metric (65535) auf betroffenen Link.
- Wirkung: Link wird vom SPF gemieden.
- Fallback-Timer: Nutzung nach Timeout.



7. FORWARDING OPERATIONEN

- PUSH (Ingress): MPLS-Label vor IP.
- SWAP (Transit): Label ersetzen.
- POP (Egress/PHP): Label entfernen (Implicit Null Label 3).



8. TROUBLESHOOTING & LFIB VERIFIKATION

- Nachbarn: show mpls ldp neighbor.
- Bindings: show mpls ldp bindings [prefix].
- Hardware: show mpls forwarding-table.
- Traceroute: traceroute mpls ipv4 [prefix].



ENTSCHEIDUNGSLOGIK: LDP-ARCHITEKTUR & PARAMETERWAHL

Welche Konfigurationsparameter und Betriebsarten passen zu Ihren Netzwerkzielen?

1	Fokus auf minimale Konvergenzzeit nach Linkausfall im Core.	DU + LLR + IGP-LDP-Sync auf allen Core-Links.
2	Fokus auf minimalen Speicher- und Signalisierungs-Overhead.	CLR oder Targeted LDP für End-to-End-Dienste.
3	Verhinderung von Paketverlust bei Reboots oder Wartung.	LDP Graceful Restart (RFC 3478) + IGP-LDP Sync (Holdown-Timer).

PRAKTISCHE ÜBUNGSAUFGABE: TABELLEN-ZUORDNUNG

Tragen Sie die Zuständigkeiten und Beispieldaten für einen Transit-LSR in Ihrem Labornetzwerk ein.

FEC / Ziel-IP-Präfix (z. B. 10.200.1.0/24)

Lokal zugewiesenes In-Label (aus show mpls ldp bindings)

Gelerntes Out-Label vom IGP-Next-Hop Router

LFIB-Eintrag: Incoming Label -> Operation (Swap/Pop) -> Outgoing Interface

MPLS LAYER 3 VPNs (L3VPN / RFC 2547bis)

1. GRUNDPRINZIP & ARCHITEKTUR

MPLS Layer 3 VPNs ermöglichen es Netzbetreibern, über eine gemeinsame Backbone-Infrastruktur mehrere logisch getrennte Kundennetze mit überlappenden privaten IPv4/IPv6-Adressräumen zu transportieren. Die Trennung erfolgt auf Routing-Ebene durch Virtual Routing and Forwarding.

- **Peer-to-Peer-VPN:** Kundenrouter tauschen Routen direkt mit dem Provider Edge (PE) aus.
- Keine Punkt-zu-Punkt-Tunnelfluten wie bei reinem IPsec oder GRE nötig.
- Der Provider-Core (P-Router) bleibt komplett frei von Kundenrouten (BGP-free Core).

BGP-FREE CORE
Core-Router (P) schalten Pakete rein über innere/äußere MPLS-Labels (Label Swapping) und benötigen keine Routen- oder VPN-Kenntnisse der Kunden.

2. ROUTER-ROLLEN (CE, PE, P)

Die L3VPN-Architektur definiert strikt getrennte Rollen für Geräte an den Netzgrenzen und im Kern:

- **CE (Customer Edge):** Router beim Kunden, spricht Standard-Routing (Static, OSPF, BGP) zum PE; hat keine MPLS-Kenntnis.
- **PE (Provider Edge):** Betreiber-Router am Netzrand; verwaltet Kunden-VRFs, bindet CE an und spricht MP-BGP mit anderen PEs.
- **P (Provider Router):** Transit-Router im Backbone; schaltet Pakete nur anhand von MPLS-Labels via LDP oder RSVP-TE.



3. VRF (VIRTUAL ROUTING & FORWARDING)

VRF virtualisiert die Routing-Tabelle auf dem PE-Router analog zu VLANs auf Layer 2.

- Jeder Kunde erhält eine dedizierte Routing- und Forwarding-Instanz (VRF-Tabelle).
- Überlappende IP-Netze (z. B. beide Kunden nutzen 10.0.0.0/24) existieren kollisionsfrei nebeneinander.
- Schnittstellen zum CE werden fest genau einer Kunden-VRF zugewiesen.



4. ROUTE DISTINGUISHER (RD)

Der Route Distinguisher ist ein 64-Bit-Präfix, das einer IPv4-Adresse vorangestellt wird, um sie global eindeutig zu machen.

- Formel: RD (8 Byte) + IPv4-Präfix (4 Byte) = 12-Byte VPN-IPv4-Adresse.
- Typische Formate: ASN:nn (z. B. 65000:100) oder IP:nn.
- Verhindert, dass identische IP-Adressen verschiedener Kunden im MP-BGP kollidieren.



Achtung: RD steuert kein Routing
Der RD sorgt ausschließlich für Eindeutigkeit im MP-BGP. Er bestimmt nicht, in welche Kunden-VRF eine Route importiert wird.

5. ROUTE TARGETS (RT) & POLICY

Route Targets sind erweiterte BGP-Communities (BGP Extended Communities), die die Verteilung und Annahme von Routen steuern.

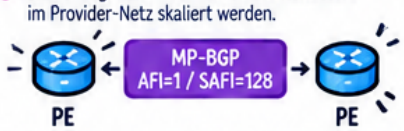
- Export-RT: Taggt VPN-IPv4-Routen beim Verlassen der lokalen VRF ins MP-BGP.
- Import-RT: Bestimmt, welche über MP-BGP empfangenen VPNv4-Routen in die lokale VRF geladen werden.
- Ermöglicht flexible Topologien wie Mesh, Hub-and-Spoke oder Extranet-Freigaben.



6. MULTIPROTOCOL BGP (MP-BGP)

MP-BGP transportiert VPNv4-Routen samt zugehöriger Labels und Attribute zwischen den PE-Routern über das Service-Provider-Netz.

- **Adressfamilie:** BGP AFI=1 (IPv4), SAFI=128 (VPNv4 Unicast).
- **Signalisierung:** Transportiert BGP Next-Hop, Route Targets und das vom Egress-PE zugewiesene VPN-Label.
- **Skalierung:** Kann über BGP Route Reflectors im Provider-Netz skaliert werden.



7. ZWEI-LABEL-FORWARDING (DATA PLANE)

Die Weiterleitung von Kundenpaketen durch das MPLS-Backbone erfolgt über einen 2-stufigen Label-Stack.

- **Outer Label (Transport-Label):** Durch LDP oder RSVP verteilt; bringt das Paket hop-by-hop vom Ingress-PE zum Egress-PE.
- **Inner Label (VPN-Label):** Durch MP-BGP signalisiert; identifiziert am Egress-PE die spezifische Ziel-VRF oder das Ziel-Interface.
- **Penultimate Hop Popping (PHP):** Letzter P-Router entfernt das Transport-Label; Egress-PE liest direkt das VPN-Label.



8. ZUSAMMENFASSUNG & TROUBLESHOOTING

Systematische Verifikation von L3VPNs erfordert die getrennte Betrachtung von Control Plane und Data Plane.

- Schritt 1: PE-CE-Routing und VRF-Interface-Zuordnung prüfen.
- Schritt 2: MP-BGP VPNv4-Nachbarschaften und RT-Import/Export abgleichen.
- Schritt 3: LDP-Transport-Labels im Core und VPN-Label-Zuweisung verifizieren.

Schnelltipp zur Fehlersuche
Stimmen RD und RT? Bei fehlenden Routen im MP-BGF liegt die Ursache fast immer an abweichenden import-Route-Targets.

Wird der Kundenverkehr über das MPLS-Backbone erfolgreich weitergeleitet?

Nein, Routen fehlen in der VRF des Egress-PE	[illegible]	Ja, Kommunikation funktioniert einwandfrei
Prüfe MP-BGP VPNv4 Peering und kontrolliere Übereinstimmung von Export-RT des Senders mit Import-RT des Empfängers.	Prüfe LDP/RSVP Transport-LSP zwischen den PE-Loopbacks; kontrolliere MTU für MPLS-Label-Overhead.	Dokumentiere VRF-Namen, Route Distinguisher (RD) und Route Targets (RT) im Netzplan.



LAYER-2-VPNS: PSEUDOWIRE, VPLS UND EVPN

1. GRUNDPRINZIP VON LAYER-2-VPNS

Layer-2-VPNs koppeln geografisch getrennte lokale Netzwerke (LANs) über ein IP- oder MPLS-Weitverkehrsnettwerk (WAN), sodass verbundene Standorte auf Sicherungsschicht-Ebene transparent wie im selben Broadcast-Segment agieren.



- Transparenz: Vermittlung von Ethernet-Frames inklusive VLAN-Tags über Provider-Backbones
- Protokollunabhängigkeit: Ermöglicht IP-, Nicht-IP- und Multicast-Transport zwischen Standorten
- Kapselung: L2-Payload wird in MPLS-Labels oder IP-Tunnel (GRE/VXLAN) verpackt

ABGRENZUNG ZU LAYER-3-VPNS
Im Gegensatz zu L2-VPNs (wie BGP/MPLS IP-VPNs) routet das Provider-Netzwerk keine Kunden-IP-Pakete, sondern leitet reine Ethernet-Frames auf Schicht 2 weiter.

2. PSEUDOWIRE & EOMPLS

Pseudowire (PW) stellt eine Punkt-zu-Punkt-L2-Verbindung über ein paketvermittelndes Netzwerk bereit. Ethernet-over-MPLS (EoMPLS) nutzt dafür einen statischen oder per LDP signalisierten Label-Stack.

- Punkt-zu-Punkt-Architektur: Emuliert eine Standeitung bzw. ein virtuelles Ethernet-Kabel
- Zwei-Label-System: Tunnel-Label leitet durch den Kern, VC-Label identifiitert den Service
- Signalisierung: Aufbau typischer[illegible] Targeted LDP (RFC 4447)



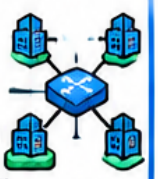
3. ATOM: ANY TRANSPORT OVER MPLS

AToM verallgemeinert das Pseudowire-Konzept, um beliebige L2-Technologien wie Ethernet, ATM, Frame Relay oder HDLC über ein einheitliches MPLS-Backbone zu transportieren.

- Technologie-Agilität: Ermöglicht Migration historischer WAN-Strecken auf modernen MPLS-Kern
- Kapselungsvorschriften: Standardisierte Header-Übersetzung gemäß RFC 4905 / RFC 4906
- Modulares Framing: Control Word sorgt für Sequenzierung und Erkennung von Paketfehlern

4. VPLS: MEHRPUNKT-ETHERNET

Virtual Private LAN Service (VPLS) erweitert L2-VPNs von reinen Punkt-zu-Punkt-Strecken zu einer virtuellen Multi-Point-Switching-Architektur für verteilte Standorte.



- Multipoint-to-Multipoint: Standorte verhalten sich wie an einem einzigen Switch angeschlossen
- Data-Plane MAC-Learning: Provider-Edge-Router (PE) lernen MAC-Adressen aus eintreffenden Frames
- Signalisierungsvarianten: LDP-basiert (Martini-Modell) oder BGP-basiert (Kompella-Modell)

5. SCHWÄCHEN KLASSISCHER VPLS-DESIGNS

Da VPLS wie ein klassischer Ethernet-Switch agiert, erbt es architektonische Nachteile von Flood-and-Learn-Mechanismen im großflächigen Carrier-Betrieb.

- Unbekanntes Unicast-Flooding: Belastet Backbone-Bandbreite bei neuen Adressen erheblich
- Loop-Vermeidung: Erfordert Split-Horizon im Full-Mesh oder komplexe Spanning-Tree-Interaktionen
- Multihoming-Grenzen: Aktives Multi-Homing ohne redundante Schleifen ist stark limitiert

BGP-ALTERNATIVE
Zur Skalierung von L2-Netzen wurde die MAC-Adressverwaltung aus der Datenebene in die BGP-Steuerungsebene verlagert.

6. BGP EVPN STEUERUNGSEBENE

Ethernet VPN (EVPN) nutzt Multi-Protocol BGP (MP-BGP) als deklarative Control Plane, um MAC- und IP-Adressen strukturiert per Routing-Protokoll zu verteilen.

- Control-Plane-Learning: Kein Data-Plane-Flooding zum reinen Auffinden von MAC-Adressen nötig
- Route-Types: Spezifische BGP-EVPN-Routentypen für MAC-Advertisement, Auto-Discovery und Multicast
- Aktive Multi-Homing: [illegible]
- All-Active Multi-Homing: Lastverteilung über redundante Anbindungne (Ethernet Segment ID)



7. AUSWAHLENTSCHEIDUNG FÜR L2-VPN-TECHNOLOGIEN

Die Auswahl der geeigneten L2-VPN-Technologie richtet sich nach Topologie, Skalierungsbebarf und Betriebsmodell.

- Punkt-zu-Punkt vs. Multipoint
- Flooding-Toleranz und Skalierungsanforderung
- Underlay-Kapselung (MPLS vs. VXLAN)

Welche Topologie und Lastanforderung besteht für die Standortvernetzung?

Ausschließlich 2 Standorte als dedizierte Punkt-zu-Punkt-Kopplung	Pseudowire / EoMPLS wählen; minimale Signalisierungskomplexität ohne Notwendigkeit für MAC-Learning im Provider-Netz.
Mehrere Standorte mit Bedarf an direktem Any-to-Any L2-Austausch und geringer Skalierung	VPLS einsetzen, sofern das Backbone für Unicast-Flooding ausgelegt ist und kein komplexes All-Active Multi-Homing erforderlich ist.
Moderne Rechenzentrums- oder Enterprise-Kopplung mit Multi-Homing und optimaler Skalierung	BGP-EVPN einsetzen; Adressverteilung über MP-BGP reduziert Flooding und unterstützt elastische All-Active-Pfade.

8. ZUSAMMENFASSUNG & EVOLUTION

Die historische Evolution von L2-VPNs zeigt den klaren Wandel von einfachen Punkt-zu-Punkt-Tunneln über flutende Multi-Point-Netze hin zu hochgradig kontrollierten Routing-Ebenen.

- Pseudowire (EoMPLS/AToM): Die Basis für Punkt-zu-Punkt-L2-Tunneling
- VPLS: Der Schritt zum LAN-Switching über WAN mit datenebenenbasiertem Lernen
- EVPN: Der moderne Standard mit BGP-basierter Adressverteilung und robuster Schleifenfreiheit

EoMPLS (AToM) → VPLS → EVPN

SEGMENT ROUTING (SR-MPLS & SRV6)

1. GRUNDPRINZIP: SOURCE ROUTING

Segment Routing verlagert den Routing-Pfadstatus direkt in den Paket-Header beim Ingress-Router. Zwischenknoten im Backbone müssen keinen individuellen Pfadstatus mehr pro Datenstrom vorhalten, wodurch Netzwerktopologien drastisch vereinfacht und hochgradig skalierbar werden.



- Ingress-Knoten legt die vollständige Segment-Liste (Segment List) fest
- Transit-Router führen deterministische Operationen aus: PUSH, CONTINUE, NEXT
- Zustandsloses Backbone ohne Per-Flow-Status in Transitknoten

2. SEGMENT-TYPEN: PREFIX-SID & ADJACENCY-SID

Die Weiterleitung stützt sich auf standardisierte Identifier (Segment Identifier / SID), die global oder lokal ausgewertet werden.



- **Prefix-SID:** Global eindeutige Kennung für einen Zielknoten oder ein Loopback-Präfix; Weiterleitung erfolgt via Shortest Path (ECMP)
- **Node-SID:** Spezifische Prefix-SID, die einen Router eindeutig identifiziert
- **Adjacency-SID:** Lokal gültige Kennung für einen spezifischen Link zwischen zwei Nachbarroutern zur Erzwingung expliziter Pfade

3. DATENPFAD: SR-MPLS (MPLS DATA PLANE)

SR-MPLS nutzt bewährte MPLS-Weiterleitungsmechanismen ohne neue Hardware-Anforderungen.

- SIDs werden direkt als 20-Bit MPLS-Labels codiert
- Segment List wird als Label-Stack auf den Paket-Header geschoben
- Kompatibel mit existierender MPLS-Hardware und Forwarding Information Bases (FIB)



4. DATENPFAD: SRV6 (IPV6 DATA PLANE)

SRv6 integriert Segment Routing nativ in das IPv6-Protokoll über standardisierte Extension-Header.

- SIDs sind vollständige 128-Bit IPv6-Adressen (Locator:Function:Arguments)
- Nutzung des Segment Routing Headers (SRH, IPv6 Routing Type 4)
- Segment List wird sukzessive durch Weiterleitung und Segments Left Pointer abgearbeitet
- Ermöglicht programmierbare Netzwerkfunktionen (Service Chaining) ohne MPLS-Overhead



5. PROTOKOLL-ELIMIINIERUNG: ENTFALL VON LDP & RSVP-TE

Segment Routing verenifacht die Netzwerkarchitektur durch die Abschaffung redundanter Signalisierungsprotokolle im Control Plane.

- Verteilung von SIDs erfolgt direkt durch Erweiterungen in IGP (IS-IS, OSPF) und BGP
- LDP (Label Distribution Protocol) entfällt vollständig
- RSVP-TE entfällt: Traffic Engineering ohne zustandsbehaftete Tunnel und Soft-State-Signalisierung



6. TRAFFIC ENGINEERING & TI-LFA SCHUTZ

Mithilfe deterministischer Source-Pfade und moderner Schutzmechanismen wird Hochverfügbarkaiit unterhalb von **50 ms** erreicht.

- Topology-Ideal für gewachsnse Alternate (TI-LFA): 100 % Pfadadceckung gegen Link- und Node-Ausfälle
- Lokale Backup-Pfade werden Clouds berechnet und bei Verbindungsabbruch sofort aktiviert
- Granulare Pfadsteuerung (SLA-basiert) für Latenz, Bandbreite oder administrative Ausschlüsse

1. Topologie- und SID-Lernen



Der Ingress-Router empfängt die Netzwerktopologie und Prefix-/Adjacency-SIDs über die IGP-Erweiterungen (OSPF/IS-IS).

2. Pfadberechnung und Kapselung



Der Pfad wird lokal berechnet (oder via SDN-Controller empfangen): der Ingress-Knoten kapselt das Datenpaket mit dem SID-Stack.

3. Segmentbasierte Weiterleitung



Transit-Router leiten das Paket anhand des obersten aktiven Segments weiter und vererbeiten den Stack zustandslos bis zum Zielknoten.

7. ENTSCHEIDUNGSMATRIX: SR-MPLS ODER SRV6?

Wählen Sie die geeignete Segment-Routing-Technologie basierend auf bestehender Infrastruktur und Zielanforderungen.

- **SR-MPLS:** Ideal für gewachsene Provider- und Core-Netze mit vorhandenen MPLS-Routern
- **SRv6:** Optimal für moderne Cloud-, Telco-Edge- und reine IPv6-Netze mit hohem Bedarf an Service Chaining

Welche Daten-Plane-Infrastruktur soll vorrangig eingesetzt werden?

Bestehende Hardware unterstützt nur 20-Bit MPLS-Label-Switching → **SR-MPLS einsetzen:** Beibehaltung der MPLS FIB, Deaktivierung von LDP/RSVP-TE, Migration auf IGP-SID-Erweiterungen.

Reines IPv6-Backbone oder Integration von Rechenzentren und Network Functions (NFV) → **SRv6 implementieren:** Segment Routing Header (SRH) aktivieren, Service Chaining über 128-Bit Funktions-SIDs abbilden.

8. ZUSAMMENFASSUNG & MERKMALE

Kompakter Überblick über Kernmerkmale und Nutzen von Segment Routing in modernen Weitverkehrs- und Unternehmensnetzen.



- Skalierbarkeit: Kein Flow-Status im Backbone-Kern
- Flexibilität: Nahtlose Unterstützung von Best-Effert-Routing und striktem Traffic Engineering
- Ausfallsicherheit: Schnelle 50ms-Umschaltung durch TI-LFA
- Zukunffssicherheit: Direkte Basis für programmierbare Software-Defined Networks (SDN)

Geplante Migrationsdomäne (z. B. Core, WAN, Rechenzentrum):

Evaluierter Datenpfad (SR-MPLS vs. SRv6) und Begründung:

TCP-Header und Verbindungsaufbau

TCP: Header & Verbindung

1. Grundprinzip von TCP

Das Transmission Control Protocol (TCP) arbeitet auf der Transportschicht (Schicht 4) und garantiert eine verlässliche, reihenfolgerichtige und byteorientierte Datenübertragung zwischen zwei Endpunkten.

- **Verbindungsorientiert:** Vor dem ersten Datenaustausch erfolgt zwingend ein logischer Verbindungsaufbau.
- **Zuverlässigkeit:** Verlorene oder beschädigte Segmente werden automatisch neu angefordert (ARQ).
- **Fluss- und Staukontrolle:** Passt das Übertragungstempo dynamisch an Empfängerpuffer und Netzwerkzustand an.

2. Adressierung & Ports

TCP nutzt 16-Bit-Portnummern zur Identifikation von Quell- und Zielprozessen auf einem Host. Zusammen mit der IP-Adresse bildet ein Port einen eindeutigen Netzwerk-Socket.

- **Quell-Port (16 Bit):** Identifiziert den anfragenden Prozess beim Client (oft flüchtiger Ephemeral Port).
- **Ziel-Port (16 Bit):** Adressiert den Zielserver-Dienst (z. B. Port 80 für HTTP, Port 443 für HTTPS).
- **Socket-Paar:** Eindeutige 4er-Kombination aus Quell-IP, Quell-Port, Ziel-IP und Ziel-Port definiert jede Verbindung.

3. Sequenz- & ACK-Nummern

Zwei 32-Bit-Zähler gewährleisten lückenlose Sortierung und Bestätigung des kontinuierlichen Byte-Stroms in beide Übertragungsrichtungen.

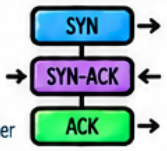
- **Sequence Number (32 Bit):** Bestimmt die Byte-Position des ersten Nutzdatenbytes dieses Segments im Gesamtdatenstrom.
- **Acknowledgment Number (32 Bit):** Bestätigt alle Bytes bis dorthin und nennt die nächste erwartete Byte-Sequenznummer.
- **Kumulative Bestätigung:** Ein einziges ACK bestätigt alle zuvor fehlerfrei empfangenen Bytes der Gegenseite.

4. Steuerungs-Flags im Header

Einzelne Bits im Steuerfeld signalisieren den Zustand des Segments und instruieren die Protokoll-Zustandsmaschine beider Endsysteme.

- **SYN (Synchronize):** Initialisiert Verbindung und synchronisiert Start-Sequenznummern.
- **ACK (Acknowledge):** Markiert das Bestätigungsfeld als gültig (bei fast allen Paketen nach SYN gesetzt).
- **FIN (Finish):** Leitet den geordneten Verbindungsabbau der sendenden Richtung ein.
- **RST (Reset):** Bricht eine ungültige oder verweigerte Verbindung hart und ohne Pufferleerung ab.

5. Drei-Wege-Handshake



Der reguläre Verbindungsaufbau synchronisiert Sequenznummern und Reservierungen zwischen Client und Server in exakt drei Schritten.

- **Client sendet SYN:** Sendet eigene Startsequenznummer (ISN Client = x) mit aktivem SYN-Flag.
- **Server antwortet SYN-ACK:** Bestätigt x+1 (ACK), sendet eigene Startsequenznummer (ISN Server = y) und SYN.
- **Client sendet ACK:** Bestätigt y+1 mit aktivem ACK-Flag; die Verbindung ist nun im Zustand ESTABLISHED.

SYN-Flood-Schwachstelle
Werden SYN-Anfragen gesendet, aber das abschließende ACK unterschlagen, belegt der Server Ressourcen im SYN_RECEIVED-Zustand. Gegenmaßnahme: SYN-Cookies.

6. Fluss- & Steuerfelder

Neben Identifikation und Bestätigung enthält der TCP-Basisheader Felder zur Pufferverwaltung und Fehlerkontrolle.

- **Data-Offset (4 Bit):** Header-Länge in 32-Bit-Wörtern (Standard ohne Optionen: 20 Byte / Wert 5).
- **Window Size (16 Bit):** Empfangsfenster (Flow Control), signalisiert freie Pufferkapazität in Byte.
- **Checksum (16 Bit):** Prüfsumme über Pesudo-IP-Header, TCP-Header und Nutzdaten zur Integritätsprüfung.
- **Urgent Pointer (16 Bit):** Zeigt auf vorrangig zu behandelnde Notfalldaten (nur bei gesetztem URG-Flag).

7. Verbindungsabbau

Neil TCP voll-duplexfähig ist, muss jede Datenübertragungsrichtung separat über FIN und ACK geschlossen oder via RST abgebrochen werden.

- **Data-Wege-Terminierung:** Seite A sendet FIN = Seite B bestätigt ACK. Seite B sendet eigenes FIN = Seite A bestätigt ACK.
- **Halboffener Zustand:** Nach dem ersten FIN kann die Gegenstelle weiterhin Daten senden, bis sie selbst FIN schickt.
- **TIME-WAIT-Zustand:** Der Initiator wartet das 2-fache. Maximum Segment Lifetime (2MSL), um verspätete Segmente abzufangen.

8. Kernpunkte & Vergleich

TCP garantiert Datenintegrität auf Kosten von Protokoll-Overhead und Latenz. Es bildet das Rückgrat zuverlässiger Internetanwendungen.

- **Zuverlässigkeit vor Tempo:** Garantiert Vollständigkeit, im Gegensatz zum verbindungslosen User Datagram Protocol (UDP).
- **Overhead:** Mindestens 20 Byte Header (ohne Optionen) im Vergleich zu lediglich 8 Byte bei UDP.
- **Häufigste Einsatzbereiche:** Webverknér (HTTP/HTTPS), Dateiübertragung (SFTP/FTP), E-Mail (SMTP/IMAP) und Remote Shell (SSH).

Praxis-Analyse: Verbindungsstatus

Bestimmen Sie anhand beobachteter TCP-Flags im Netzwerk-Trace das vorliegende Verbindungsereignis.

Welche Flag-Kombination ist im erfassten TCP-Header aktiv?	Nur SYN gesetzt (ACK = 0)	Sowohl SYN als auch ACK gesetzt	RST gesetzt (mit oder ohne ACK)	FIN und ACK gesetzt
	Verbindungsinitiierung: Client leitet Handshake ein. Auf SYN-ACK von Port prüfen.	**Handshake-Antwort:** Zielhost akzeptiert Verbindung. Erwartet finales ACK.	**Verbindungsabweisung oder harter Abbruch:** Port geschlossen oder Firewall blockiert.	Geordneter Verbindungsabbau: Sender hat Datentransfer abgeschlossen.

TCP-Flusssteuerung und Überlastkontrolle (Congestion Control)

1. GRUNDPRINZIP: FLUSS- VS. ÜBERLASTKONTROLLE

Flusssteuerung (Flow Control) und Überlastkontrolle (Congestion Control) lösen zwei grundverschiedene Engpassprobleme auf Transportschichtebene (L4):

- **Flusssteuerung:** Schützt ausschließlich den Ziel-Host davor, von schnellen Datenmengen des Senders im Empfängspuffer überflutet zu werden (End-to-End).
- **Überlastkontrolle:** Schützt Router, Switches und Zwischenstrecken im gesamten Transitnetz vor Datenstau und Paketverlust (Network-Wide).
- **Sender-Regel:** Das effektiv nutzbare Sendefenster W berechnet sich stets aus dem Minimum beider Mechanismen: W = min(rwnd, cwnd).

MERKSATZ FÜR DIE PRAXIS
rwnd signalisiert die Aufnahmekapazität der Gegenstelle; cwnd schätzt die freie Bandbreite des Netzwerks.

2. SLIDING WINDOW & RECEIVE WINDOW (RWND)

TCP nutzt dynamische Schiebefenster (Sliding Windows) für kontinuierlichen Datentransfer ohne permanentes Stop-and-Wait je Segment:

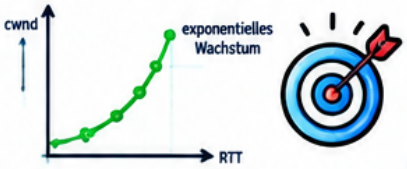
- **Advertised Window:** Der Empfänger meldet fortlaufend im TCP-Header (Feld Window Size) freie Pufferbytes via rwnd.
- **Schiebemechanismus:** Sobald Bytes quittiert (ACK) und von der Anwendung aus dem Empfängspuffer gelesen werden, rückt das Fenster nach rechts.
- **Zero Window Probe:** Meldet der Empfänger ein Fenster von 0 Bytes (rwnd = 0), stoppt der Sender und sendet zyklisch 1-Byte-Probes zur Statusprüfung.



3. SLOW START PHASE (EXPONENTIELLES WACHSTUM)

Zu Verbindungsbeginn oder nach schwerem Timeout kennt der Sender die Netzkapazität nicht und startet mit konservativer Sondierung:

- **Initial Window:** Startet typischerweise mit 1 bis 10 MSS (Maximum Segment Size, initial oft initcwnd = 10 gem. RFC 6928).
- **Verdopplung:** Für jedes erfolgreich empfangene ACK wächst cwnd um 1 MSS (effektive Verdopplung von cwnd pro RTT).
- **Schwellenwert (ssthresh):** Slow Start endet exakt, wenn das Congestion Window den Schwellenwert ssthresh erreicht.



4. CONGESTION AVOIDANCE (ADDITIVE INCREASE)

Erreicht cwnd den ssthresh-Wert, wechselt TCP in die Congestion Avoidance zur stabilen Bandbreitenannäherung:

- **Lineares Wachstum:** cwnd erhöht sich nur noch um circa 1 MSS pro voller RTT, statt sich exponentiell zu verdoppeln.
- **AIMD-Prinzip:** Additive-Increase Multiplicative-Decrease sorgt für faire Bandbreitenverteilung unter konkurrierenden TCP-Flows.
- **Grenzbereich:** Der Sender tastet sich schrittweise an die Sättigungsgrenze heran, bis Paketverlust oder Latenzspitzen auftreten.



5. FAST RETRANSMIT & FAST RECOVERY

Ermöglicht Reparatur einzelner Paketverluste, ohne auf den trägen Retransmission Timeout (RTO) warten zu müssen:

- **3 Duplicate ACKs:** Treffen drei identische Bestätigungen für dasselbe Segment ein, gilt das Folgesegment sicher als verloren.
- **Fast Retransmit:** Das fehlende Datensegment wird sofort neu übertragen, ohne auf den Ablauf des RTO-Timers zu warten.
- **Fast Recovery:** ssthresh wird halbiert, cwnd auf ssthresh gesetzt; TCP verbleibt in Congestion Avoidance statt Rückfall auf cwnd = 1.



6. KLASSISCHE VS. MODERNE ALGORITHMEN (RENO, CUBIC, BBR)

Vergleich der etablierten Algorithmen zur Überlastkontrolle und ihrer Steuerungsmetriken:

- **TCP Reno:** Klassisches verlustbasiertes AIMD; halbiert cwnd bei Paketverlust und startet linearen Wiederanstieg.
- **TCP CUBIC:** Standard in vielen Linux-Systemen; wirzt kubische Wachstumsfunktion basierend auf vergangener Zeit seit dem letzten Verlust (ideal für High-BDP-Netze).
- **Google BBR:** Modellbasiert statt rein verlust-basiert; misst kontinuierlich maximale Bandbreite und minimale RTT zur Vermeidung von Bufferbloat.



7. ENTSCHEIDUNGSLOGIK BEI PAKETVERLUST

Systematischer Ablauf zur Feststellung und Behandlung von Übertragungsstörungen im Datenstrom:

- **Auslöser identifizieren:** 3 Duplicate ACKs deuten auf isolierten Paketverlust hin; RTO-Ablauf deutet auf schweren Netzzusammenbruch hin.
- **Zustandsübergang ausführen:** Entweder Fast Recovery einleiten oder Rückfall in Slow Start mit cwnd = 1 MSS.
- **ssthresh anpassen:** Halbiert stets die bisherige Übertragungsrate als Sicherheitsgrenze.

Welches Verlustsignal registriert der TCP-Sender?

3 Duplicate ACKs empfangen (Gegenstelle meldet Lücke) →	Fast Retransmit ausführen, ssthresh = cwnd / 2 setzen, cwnd = ssthresh einstellen und in Fast Recovery / Congestion Avoidance bleiben.
Retransmission Timeout (RTO) läuft ab ohne jedes ACK →	Schweren Stau annehmen: ssthresh = cwnd / 2 setzen, cwnd radikal auf 1 MSS reduzieren und vollständigen Slow Start neu starten.

8. ZUSAMMENFASSUNG & ANALYSE-CHECKLISTE

Praxis-Checkliste für Wireshark- und Netzwerk-Troubleshecoting bei TCP-Übertragungsengpässen:

- **Fenstergrenze prüfen:** Ist 'TCP Window Full' oder 'ZeroWindow' im Trace sichtbar? Wenn ja, liegt der Engpass primär beim Empfänger (rwnd).
- **Retransmissions analysieren:** Treten Timeouts (RTO) oder Duplicate ACKs auf? RTO signalisiert Router-Drop oder Leitungsabriss im Transit.
- **Algorithmus verifizieren:** Prüfen, ob CUBIC, Reno oder BBR aktiv ist (sysctl net.ipv4.tcp_congestion_control).
- **Bufferbloat ausschließen:** Steigen die Ping-Laufzeiten unter Volllast massiv an, füllen sich Zwischenpuffer ohne rechtzeitiges Throttling.

PRAXIS-TIPP FÜR PAKETANALYSEN
In Wireshark liefert der Graph 'tcptrace' (unter Statistics > TCP Stream Graphs) eine sofortige Visualisierung von cwnd- und rwnd-Verläufen.

TCP FLUSSSTEUERUNG & ÜBERLASTKONTROLLE

rwnd vs cwnd
rwnd = Empfänger-Puffer
cwnd = Netzwerk-Bandbreite

USER DATAGRAM PROTOCOL (UDP)

1. PROTOKOLL-KERN & ROLLE

Das User Datagram Protocol (UDP) agiert auf Schicht 4 (Transportschicht) des OSI-Modells als leichtgewichtiges, zustandsloses Übertragungsprotokoll.

- **Verbindungslos:** Datenübertragung erfolgt ohne vorherigen Verbindungsaufbau (kein Drei-Wege-Handshake).
- **Keine Fluss- oder Stauüberwachung:** Pakete werden ohne dynamische Drosselung sofort an das Netz übergeben.
- **Geringer Protokoll-Overhead:** Ermöglicht maximale Durchsatzraten und minimale Latenzzeiten.

2. 8-BYTE-HEADER-ARCHITEKTUR

Der UDP-Header ist mit einer festen Größe von exakt 8 Byte (64 Bit) bewusst minimalistisch konstruiert und in vier 16-Bit-Felder gegliedert.

- **Source Port (16 Bit):** Optionaler Port der sendenden Anwendung (Rückkanal).
- **Destination Port (16 Bit):** Zielport des empfangenden Dienstes zur Adressierung.
- **Length (16 Bit):** Gesamtlänge des Datagramms in Byte (Header plus Nutzlast; Minimalwert: 8).
- **Checksum (16 Bit):** Prüfsumme zur Fehlererkennung über Pesudo-Header, Header und Nutzdaten.

UDP-HEADER (8 BYTE)	
Source Port (16 Bit)	Destination Port (16 Bit)
Length (16 Bit)	Checksum (16 Bit)

Fester Header-Vergleich
Während TCP mindestens 20 Byte Header mit variablen Optionen erfordert, benötigt UDP durchgehend exakt 8 Byte.

3. VERBINDUNGSLOSES PRINZIP (UNRELIABLE)

UDP verfolgt das Best-Effort-Prinzip und garantiert weder die Ankunft noch die korrekte Reihenfolge versendeter Pakete.

- **Keine Bestätigungen (ACKs):** Der Sender erhält keine Empfangsquittung.
- **Kein Reordering:** In falscher Reihenfolge eintreffende Datagramme werden nicht auf Schicht 4 sortiert.
- **Keine automatische Neuübertragung (ARQ):** Verlorene Pakete werden verworfen und nicht nachgefordert.

4. PORT-MULTIPLEXING & ADRESSIERUNG

Über 16-Bit-Portnummern (Wertebereich 0 bis 65535) ermöglicht UDP die parallele Adressierung unterschiedlicher Anwendungen auf demselben Rechner.

- **Well-Known Ports (0–1023):** Reserviert für Standarddienste (z. B. DNS Port 53, DHCP Ports 67/68).
- **Registered Ports (1024–49151):** Für registrierte Benutzeranwendungen und herstellerspezifische Dienste.
- **Dynamische/Private Ports (49152–65535):** Werden von Clients temporär als Quellports initiiert.

5. CHECKSUM & PSEUDO-HEADER

Die UDP-Prüfsumme dient der Integritätsprüfung gegen Bitfehler und verknüpft Netzwerk- sowie Transportschichtdaten.

- **IPv4 vs. IPv6:** Unter IPv4 optional (Wert 0x0000 bedeutet inaktiv), unter IPv6 zwingend vorgeschrieben.
- **Pseudo-Header-Einbindung:** Quell-IP, Ziel-IP, Protokollnummer (17 bzw. 0x11) und UDP-Länge fließen in die Berechnung ein.
- **Einerkomplement-Summe:** Erkennt versehentliche Adressierungs- und Nutzdatenfehler während der Übertragung.

Pseudo-Header
Quell-IP / Ziel-IP
Protokoll (17 / 0x11)
UDP-Länge

↓

Checksum

6. TYPISCHE ECHTZEIT-EINSATZFELDER

UDP wird bevorzugt eingesetzt, wenn geringe Latenz wichtiger ist als vollständige Fehlerfreiheit.

- **DNS (Port 53):** Schnelle Namensauflösung mit Einzelschritt-Anfrage und -Antwort.
- **DHCP (Ports 67/68):** Lokale Netzwerkkonfiguration per Broadcast ohne bestehende Verbindung.
- **VoIP & Videokonferenzen:** Audio- und Videostreams via RTP, wo verlorene Pakete unbemerkt übersprungen werden.
- **Online-Gaming:** Übermittlung hochfrequenter Positions- und Zustandsdaten in Echtzeit.

7. SECURITY & ANGRIFFSSZENARIEN

Das Fehlen eines Verbindungsstatus macht UDP anfällig für Missbrauch bei Denial-of-Service-Angriffen.

- **IP-Spoofing:** Quell-IP-Adressen können ohne Handshake gefälscht werden, da keine Antwortprüfung erfolgt.
- **Amplification Attacks:** Angriffe auf offene DNS- oder NTP-Server erzeugen asymmetrisch große Antwortmengen auf kleine Anfragen.
- **Port-Scanning:** Offene UDP-Ports reagieren oft stumm, während geschlossene Ports ein ICMP Port Unreachable zurücksenden.

Sicherheitsaspekt
UDP bietet standardmäßig keine Authentifizierung oder Verschlüsselung; Sicherheitsmechanismen müssen auf Anwendungsebene (z. B. DTLS) implementiert werden.

8. PROTOKOLL-ENTSCHEIDUNGSMATRIX & ANALYSE

Nutzen Sie diesen Leitfaden zur Auswahl des Transportschichtprotokolls und prüfen Sie den Datenstrom systematisch.

1. **Verbindungsanforderung definieren**
   Klären, ob Latenzminimierung (UDP) oder garantierte Vollständigkeit (TCP) das Hauptkriterium ist.
2. **Header- und Port-Analyse in Wireshark**
   UDP-Datagramm im Paketmitschnitt isolieren, 8-Byte-Header verifizieren und Prüfsummenvalidierung kontrollieren.

Geprüfter UDP-Dienst & Zielport:

Festgestellte Paketverlustrate & Latenz:

Benötigt die Anwendung garantierte Zustellung oder minimale Übertragungsverzögerung?

- Minimale Latenz und Toleranz gegenüber gelegentlichem Paketverlust → UDP wählen (z. B. Live-Streaming, DNS-Lookup, Gaming-Telemetrie).
- Vollständige und sequenztreue Datenübertragung zwingend erforderlich → TCP wählen (z. B. Dateiübertragung via SFTP/HTTPS, Datenbanktransaktionen).

SCTP und QUIC: Moderne Transportprotokolle

1. GRUNDLAGEN & MOTIVATION



Klassische Protokolle wie TCP und UDP stoßen bei modernen Webanwendungen und verteilten Systemen an funktionale Grenzen.

- TCP liefert einen zuverlässigen Bytestrom, leidet jedoch unter Head-of-Line-Blocking bei Paketverlusten
- UDP bietet minimale Latenz und verbindungslose Übertragung, besitzt jedoch keinerleli Zuverlässigkeits- oder Flusskontrollmechanismen
- Moderne Anforderungen erfordern Multiplexing mehrerer Datenströme und nahtlose Mobilität über wechselnde IP-Netze

Ermittelte RTT beim Verbindungsaufbau (ms): _____

Geprüfte Firewall-Regeln für Transportpfad (UDP/SCTP): _____

2. SCTP: ARCHITEKTUR & MULTI-STREAMING



Das Stream Control Transmission Protocol (SCTP) überträgt nachrichten-gebundene Daten über getrennte unabhängige Ströme.

- Multi-Streaming: Mehrere logische Nachrichtenströme teilen sich eine einzige Assoziation
- Kein striktes Head-of-Line-Blocking zwischen unterschiedlichen Streams bei partiellem Paketverlust
- Erhalt von Nachrichtengrenzen (Message-Framing) direkt auf Transportschichtebene

3. SCTP: MULTI-HOMING & REDUNDANZ



SCTP unterstützt die Bindung mehrerer Netzwerkadressen pro Endpunkt zur Erhöhung der Ausfallsicherheit.

- Verbindungsendpunkte können mehrere IP-Adressen (Schnittstellen) in einer Assoziation führen
- Automatischer Pfadwechsel auf alternative IP-Verbindungen bei Verbindungsabbrüchen ohne Verbindungsneustart
- Traditionell intensiver Einsatz in hochverfügbaren Telekommunlkationsnetzen und Signalisierungsnetzen (SS7/SIGTRAN)

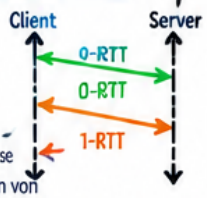
4. QUIC: HTTP/3 & UDP-BASIS



QUIC setzt auf dem User Datagram Protocol (UDP) im User-Space auf, um die Blockade durch starre Middleboxen im Internet zu umgehen.

- Standard-Transportbasis für das modrene Webprotokoll HTTP/3 zur Beschleunigung des Datenaustauschs
- Umgeht Netzwerk-Ossifikation, da Middleboxen UDP-Pakete passieren laesen, während neue Protokolle oft gefiltert werden
- Vollständige Handhabung von Flusskontrolle, Paketwiederholung und Congestion Control oberhalb von UDP

5. QUIC: 0-RTT VERBINDUNGSAUFBAU



QUIC optimiert den Latenzaufwand bei Verbindungsaufnahme durch kombinierte Handshake-Verfahren drastisch.

- 1-RTT-Handshake kombiniert Transport- und Sicherheitsvereinbarung in einer einzigen Hin- und Rückreise
- 0-RTT-Wiederaufnahme ermöglicht das Senden von Anwendungsdaten bereits im ersten Datenpaket bei bekannten Servern
- Signifikante Latenzreduktion gegenüber klassischem TCP-Handshake mit nachgelagertem TLS-Austausch

6. QUIC: INTEGRIERTES TLS 1.3



Verschlüsselung und Authentifizierung sind bei QUIC nicht optional aufgesetzt, sondern integraler Bestantdeil des Headers und Payloads.

- Standardmäßige Integration von TLS 1.3 sichert Nutzdaten sowie nahezu alle Header-Felder gegen Manipulation ab
- Middleboxen im Transportpfad können Verbindungs-metadaten weder unbemerkt modifizeiren noch analysieren
- Schutz gegen Manipulation von Sequenz- und Flusskontrollinformationen durch Dritte

Sicherheitsstandard

Im Gegensatz zu TCP, bei dem TLS nachträglich aufgesetzt wird, ist QUIC ohne Verschlüsselung nicht betrelbbar.

7. DIREKTER VERGLEICH & PROTOKOLL-EVALUATION



Entscheidungsmätrix zur Auswiall des geeigneten Transportprotokolls basierend auf Netziinfrastruktur und Anwendungszweck.

Welches Protokoll erfüllt die Anforderungen Ihres Einsatzszenarios?

- Fokus auf Hochverfügbarkeit mit Multi-Homing in kontrollierten Träger- oder Carrier-Netzwerken → **SCTP wählen:** Bietet Multi-Homing auf Betriebssystemebene und nachrichtenorientiertes Framing ohne UDP-Kapselung.
- Optimierung von Weblateex, mobilem Roaming und Interope-rabilität über reguläre Internet-Gateways → **QUIC / HTTP/3 wählen:** Integriretes TLS 1.3, 0-RTT-Verbindungsaufbau und problemlose Passage gängiger Firewalls via UDP.

MODERNE TRANSPORTSCHICHT: SCTP VS QUIC

NETZWERK-PORTS & MULTIPLEXING

1. WAS SIND PORTS & MULTIPLEXING?

Ports sind 16-Bit-Zahlen (0 bis 65535) auf der Transportschicht (Layer 4), die es einem Betriebssystem erlauben, Netzwerkverkehr präzise dem richtigen Prozess oder Dienst zuzuordnen.

- Ermöglicht Service-Multiplexing: Parallele Web-, Mail- und SSH-Sitzungen über ein einziges physisches Netzwerkkabel und eine IP-Adresse.
- Ein Endpunkt wird durch eine Socket-Adresse (Kombination aus IP-Adresse und Portnummer) eindeutig im Netzwerk adressiert.
- Demultiplexing leitet eingehende Pakete anhand der Ziel-Portnummer im TCP/UDP-Header an den zuständigen Socket weiter.
- Verhindert Datenkollisionen zwischen gleichzeitig laufenden Netzanwendungen auf demselben Host.

2. IANA-PORTBEREICHE IM DETAIL

Die Internet Assigned Numbers Authority (IANA) unterteilt den 16-Bit-Portbereich in drei standardisierte Klassen, um Konflikte zwischen Systemdiensten und temporären Sitzungen zu vermeiden.

- **Well-Known Ports (0–1023):** Reserviert für privilegierte Standarddienste des Betriebssystems (z. B. HTTP 80, HTTPS 443, SSH 22).
- **Registered Ports (1024–49151):** Registriert für spezifische Herstellerdienste und Datenbanken (z. B. MySQL 3306, RDP 3389).
- **Dynamic / Private Ports (49152–65535):** Ephemere Ports für ausgehende Client-Sitzungen; werden dynamisch vergeben und nach Sitzungsende freigegeben.

0 – 1023	1024 – 49151	49152 – 65535
Well-Known Ports	Registered Ports	Dynamic / Private Ports

3. DER NETZWERK-SOCKET (IP:PORT)

Ein Socket bildet die softwareseitige Schnittstelle zwischen Transportschicht und Anwendung. Er definiert die logische Endstelle einer zweiseitigen Netzwerkkommunikation.

- **Syntax:** IPv4-Notation '192.168.1.50:443' oder IPv6 in eckigen Klammern '[2001:db8::1]:443'.
- 5-Tupel zur Eindeutigkeit: Protokoll (TCP/UDP), Quell-IP, Quell-Port, Ziel-IP, Ziel-Port.
- Erlaubt Webservern, tausende Client-Verbindungen gleichzeitig auf demselben Zielport 443 fehlerfrei zu trennen.



4. EPHEMERE QUELLPORTS IN DER PRAXIS

Wenn ein Client einen Webserver aufruft, weist der Kernel ihm automatisch einen temporären (ephemeren) Port als Absender-Port zu.

- Dynamische Zuweisung: Betriebssystem wählt freien Port oberhalb von 1024 bzw. aus 49152–65553.
- Rückkanal: Der Server sendet Antwortpakete exakt an diesen ephemeren Quellport zurück.
- Lebenszyklus: Nach Verbindungsende und TCP-TIME_WAIT-Intervall wird der Port für neue Streams wiederverwendet.



5. BEISPIEL: MULTIPLEXING BEIM SURFEN

Analyse zweier gleichzeitiger Browser-Tabs auf einem Client (192.168.1.100), die denselben Webserver (93.184.216.34) ansteuern.

- Verbindung 1 (Tab A): 192.168.1.100:51020 -> 93.184.216.34:443 (TCP)
- Verbindung 2 (Tab B): 192.168.1.100:51021 -> 93.184.216.34:443 (TCP)
- Multiplexing-Ergebnis: Obwohl Ziel-IP und Ziel-Port identisch sind, trennt das 5-Tupel beide Streams vollkommen isoliert.



6. SICHERHEIT: PORT-SCANNING & FIREWALLS

Offene Ports signalisieren lauschende Dienste und stellen potezeielle Angriffsvektoren für Denial-of-Service- oder Exploit-Angriffe dar.

- Port-Scans (z. B. SYN-Scan): Angreifer prüfen Ziel-IPs auf aktive TCP/UDP-Ports ab, um Software-Versionen zu identifizieren.
- Firewalling & Filterung: Blockieren ungenutzter Ports an Gateways verhindert das Eindringen in interne Netzsegmente.
- Port-Forwarding: Kontrollierte Weiterleitung externer Gateway-Ports an interne private IP-Adressen (NAT-Traversal).



7. PRAXIS-ANALYSE MIT NETSTAT & SS

Schritt-für-Schritt-Anleitung zur Überprüfung aktiver Ports und Sockets auf dem eigenen Rechner ohne Zusatzinstallation.

1. **Terminal öffnen**
   Öffnen Sie die Eingabeaufforderung (PowerShell unter Windows) oder eine Terminal-Shell unter Linux/macOS.
2. **Befehl ausführen**
   Geben Sie **'netstat -ano'** (Windows) oder **'ss -tulnp'** (Linux) ein, um alle lauschenden Ports und bestehenden Verbindungen anzuzeigen.
3. **Lokale Adresse & Port prüfen**
   Identifizieren Sie in der Spalte 'Lokale Adresse' die Notation IP:Port (z. B. 0.0.0.0:80 für Webserver oder 127.0.0.1:3306 für Datenbanken).
4. **Status & PID zuordnen**
   Prüfen Sie den Status ('LISTEN' für wartende Serverdienste, 'ESTABLISHED' für aktive Streams) und vergleichen Sie die Prozess-ID (PID).

Sicherheitshinweis für Privilegierte Ports

Unter Linux erfordert das Binden von Ports unterhalb von 1024 Root-Rechte (CAP_NET_BIND_SERVICE). Dies schützt Standarddienste vor unberechtigter Übernahme durch reguläre Benutzerprozesse.

8. ZUSAMMENFASSUNG & MERKREGEL

Kompakte Orientierungshilfe zur schnellen Zuordnung und Unterscheidung von Ports und Protokollen im Alltag.

- IP-Adresse steuert das Zielgerät an (Brief an das Gebäude), Portnummer steuert den Zielprozess an (Brief an das Zimmer).
- Well-Known Ports (0–1023) für Serverdienste; Ephemere Ports (>49151) für ausgehende Client-Sitzungen.
- Multiplexing sorgt für reibungslosen Parallelbetrieb hunderter Streams über denselben physischen Netzwerkkanal.

IP-MULTICAST & IGMP

1. MULTICAST-GRUNDLAGEN & KONZEPT

IP-Multicast ermöglicht eine effiziente Punkt-zu-Mehrpunkt-Kommunikation. Anstatt Pakete einzeln an jeden Empfänger zu klonen (Unicast) oder an alle Stationen zu fluten (Broadcast), wird ein einzelner Datenstrom versendet, der sich nur an Verzweigungspunkten im Netz vervielfältigt.

- One-to-Many Übertragungsmuster spart wertvolle Sender- und Link-Bandbreite.
- Empfänger treten dynamisch einer spezifischen Multicast-Gruppe bei.
- Sender benötigt keine Liste der einzelnen Empfänger-IPs.
- Typische Einsatzgebiete: Live-Video-Streaming, Audio-Feeds, Routing-Updates.

2. IPv4-MULTICAST-ADRESSBEREICH (KLASSE D)

Für Multicast ist der IPv4-Klasse-D-Bereich 224.0.0.0/4 reserviert (Binärpräfix 1110, Bereich 224.0.0.0 bis 239.255.255.255). Er unterteilt sich in standardisierte Segmente für Routing und lokale Anwendungen.

- 224.0.0.0/24: Link-Local (z. B. 224.0.0.1 alle Systeme, 224.0.0.2 alle Router, TTL=1).
- 224.0.1.0 bis 238.255.255.255: Global Scoped Addresses für weltweites Routing.
- 232.0.0.0/8: Source-Specific Multicast (SSM).
- 239.0.0.0/8: Administratively Scoped (private Netze, analog zu RFC 1918).

2. LAYER-2-MAPPING (ETHERNET-MAC)

IPv4-Multicast-Pakete werden auf Layer 2 in spezielle Ethernet-MAC-Adressen gekapselt. Die IANA besitzt das OUI-Präfix 01:00:5E, wobei das höchstwertige Bit der folgenden 24 Bit fest auf 0 gesetzt ist.

- Feste Basis: 01:00:5E:00:00:00 bis 01:00:5E:7F:FF:FF (23 nutzbare Bit).
- Die unteren 23 Bit der 28-Bit-Multicast-IP werden direkt in die MAC kopiert.
- 5 IP-Bits verfallen: 32 verschiedene IP-Multicast-Adressen teilen sich dieselbe MAC.
- Netzwerkkarten filtern auf L2 vor, der Host-IP-Stack prüft die exakte Ziel-IP.

8. MULTICAST-ZUSAMMENFASSUNG & KERNREGELN

Multicast optimiert Netzwerkkapazitäten durch intelligentes Weiterleiten. Die saubere Verzahnung von L3-Adressen, L2-Mapping und Switch-Snooping ist die Basis für staible Streams.

- IPv4-Adressbereich: 224.0.0.0/4 (Klasse D), Hostbeitritt via IGMP.
- L2-Ethernet: Abbildung in MAC-Bereich 01:00:5E:xx:xx:xx mit 23 Bit Übertrag.
- Protokolle: IGMPv2 für schnelles Verlassen (Leave), IGMPv3 für Quellfilter (SSM).
- Infrastruktior: IGMP-Snooping schützt das lokale Netzwerk vor Broadcast-Flooding.

4. IGMPv1 & IGMPv2 SIGNALISIERUNG

Das Internet Group Management Protocol (IGMP) regelt den Gruppenbeitritt zwischen Endgeräten (Hosts) und dem lokalen Multicast-Router auf Layer 3.

- IGMPv1: Query vom Router, Membership Report vom Host, Abgang nur über Timeout.
- IGMPv2: Einüfhrung der expliziten Leave Group Nachricht für schnellen Stream-Stopp.
- Group-Specific Query in IGMPv2 zur gezielten Bestandsabfrage einzelner Gruppen.
- Querier Election: Router mit der niedrigsten IP-Adresse übernimmt die Abfrage.

7. FEHLERANALYSE & SICHERHEITSASPEKTE

Fehlkonfigurationen bei Multicast führen häufig zu Datenverlust oder Netzwerklähmung. Gezielte Prüfungen grenzen Störungen auf L2 und L3 ein.

- Kein Querier aktiv: Ohne periodische Queries schalten Switches Snooping-Ports stumm.
- MAC-Adresskolllisionen: Überlappende L2-Adressen erfordern genaue L3-Inspektion.
- Multicast-Flooding: Fehlendes IGMP-Snooping führt zu Volllast auf WLAN/Access-Ports.
- Sicherheitsfilter: IGMP-Snooping mit Port-Security schützt vor Rogue-Streams.

PRAXIS-HINWEIS

Ohne aktiven IGMP-Querier im Subnetz verwirft IGMP-Snooping nach Ablauf des Timers die Gruppenmitgliedschaften und unterbricht den Multicast-Stream.

6. IGMP-SNOOPING AUF LAYER-2-SWITCHES

Standardmäßig berbandeln Layer-2-Switches Multicast-Frames wie Broadcasts und fluten alle Ports. IGMP-Snooping analysiert den IGMP-Steuerverkehr und schaltet Ports gezielt frei.

- Switch lauscht passiv auf IGMP-Reports und Leave-Nachrichten an allen Ports.
- Aufbau einer Forwarding-Table: Multicast-Frames nur an Ports mit Empfängern leiten.
- Vermeidet Netzüberlastung und Flooding an Endgeräten ohne Empfangsinteresse.
- Erfordert im VLAN einen aktiven IGMP-Querier (Router oder Switch mit Querier-Funktion).



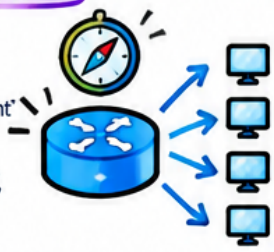
5. IGMPv3 & SOURCE-SPECIFIC MULTICAST (SSM)

IGMPv3 erweitert das Gruppenmanagement um quellenspezifische Filter. Hosts können gezielt angeben, von welchen Quell-IPs sie Multicast-Daten empfangen möchten.

- INCLUDE-Modus: Datenfluss wird nur von explizit benannten Quell-IPs akzeptiert.
- EXCLUDE-Modus: Daten von blockierten Quell-IPs werden verworfen.
- Wesentliche Grundlage für SSM (Source-Specific Multicast im Bereich 232.0.0.0/8).
- Verbesserte Sicherheit und Ressourcenentlastung, da Fehlsender blockiert werden.

MULTICAST ROUTING: PIM-SM & PIM-DM

1. WAS IST PIM?



Protocol Independent Multicast (PIM) ist eine Protokollfamilie für die effiziente Verteilung von Datenströmen an mehrere Empfänger gleichzeitig. "Protocol Independent" bedeutet, dass PIM keine eigenen Unicast-Routingtabellen aufbaut, sondern bestehende Routingtabellen (z. B. aus OSPF, IS-IS oder BGP) für Forwarding- und Loop-Prevention-Entscheidungen nutzt.

- **Zielgruppe:** Multicast-Gruppenübertragungen wie Video-Streaming, Telemetrie oder Finanzmarktdaten
- **Ressourcenschonung:** Pakete werden erst an Verzweigungspunkten im Netz vervielfältigt
- **Topologiebasis:** Nutzt Unicast-Metriken für den Reverse Path Forwarding (RPF) Check

RP-IP-Adresse & Redundanz-Methode (Statisch/BSR/Anycast)

RPF-Interface und Nachbarstatus (PIM Neighbor Check)

2. VERTEILERBÄUME & BASISBEGRIFFE

Multicast stützt sich auf zwei Baumstrukturen: Shared Trees (*,G) mit gemeinsamem Wurzelknoten und Source Trees (S,G), die direkt an der Multicast-Quelle wurzeln.

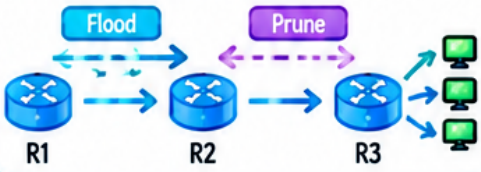
- **(*,G) Notation:** Beliebige Quelle (*) sendet an konkrete Gruppe (G)
- **(S,G) Notation:** Spezifische Quell-IP (S) sendet an konkrete Gruppe (G)
- **Shortest Path Tree (SPT):** Optimaler, direkter Pfad von Quelle S zu jedem Empfänger
- **RPF-Check:** Verwirft Multicast-Pakete, wenn sie nicht über das Interface eintreffen, das zur Quelle führt



3. PIM DENSE-MODE (PIM-DM)

PIM-DM folgt der Annahme, dass nahezu alle Subnetze Multicast-Empfänger besitzen ("Push"-Ansatz). Der Modus eignet sich primär für dichte LAN-Umgebungen.

- **Flood-and-Prune:** Multicast-Verkehr wird anfangs ungefragt an alle Nachbar-Router geflutet
- **Prune-Nachrichten:** Router ohne lokale Empfänger senden Prunes flussaufwärts
- **Graft-Mechanismus:** Meldet sich ein Empfänger neu an, reaktiviert ein Graft den Pfad sofort
- **Nachteil:** Wiederkehrendes periodisches Fluten erzeugt unnötige Bandbreiten- und CPU-Last



4. PIM SPARSE-MODE (PIM-SM)

PIM-SM arbeitet nach dem "Pull"-Prinzip und setzt voraus, dass Empfänger Verkehrsströme explizit anfordern. Dies ist der Standard für moderne Enterprise-Netze.

- **Rendezvous Point (RP):** Zentraler Koordinator im Netzwerk für Multicast-Quellen und Empfänger
- **Expliziter Beitritt:** Last-Hop-Router senden PIM-Join (*,G) in Richtung des zuständigen RP
- **Verkehrsfluss:** Quelle registriert sich beim RP; Daten fließen zunächst über den Shared Tree
- **Skalierbarkeit:** Bandbreite wird nur in Pfaden verbraucht, an denen aktive Empfänger lauschen



5. RENDEZVOUS POINT IN PIM-SM

PIM-SM verbindet die Einfachheit des Shared Trees mit gekapselt des PIM Register an den RP, während Empfänger denselben RP via Sinetnog Deet zusammenn

- **Register-Stop:** Sobald der native Datenpfad steht, weist der erstem den Quell-Router an, das Kapseln zu beenden
- **RP-Auffindung:** Der Last-Hop-Router sendet statisch oder dynamisch via Auto-RP oder BSR (Bootstrap Router)
- **Redundanz:** Anycast-RP mit MSDP oder PIM-BSR sichert den Ausfall einzelner RPs ab

Achtung bei RP-Platzierung
Ein suboptimal platzierter RP erzeugt Hairpinning und Latenzen, bevor der SPT-Switchover greift. Platzieren Sie den RP im Backbone nahe den Quellen.

5. RENDEZVOUS POINT (RP) MECHANIK

Der RP fungiert als Treffpunkt. Quellen senden Pakete gekapselt via PIM Register an den RP, während Empfänger denselben RP via Shared Tree (*,G) anbinden.

- **PIM Register:** First-Hop-Router kapselt Daten in Unicast an den RP, bis der RP den Pfad übernimmt
- **Register-Stop:** Sobald der native Datenpfad steht, weist der RP den Quell-Router an, die Quell-IP
- **Routenhoden:** Empfänger Fixere spedet gifact (dor/dyamie Sirdt Switchover auf best folder Tree

1	2	3	4
IGMP-Join empfangen	**(*,G) Join zum RP**	**Quelle registriert Daten**	**SPT-Umschaltung**
Empfänger meldet Gruppenbeitritt via IGMP an den Last-Hop-Router.	Last-Hop-Router baut Shared Tree zum zustandigen Rendezvous Point auf.	Quelle sendet Daten via First-Hop-Router gekapselt im PIM-Register an den RP.	Last-Hop-Router initiiert direkten (S,G)-Join zur Quelle für minimale Latenz.

6. SPT-SWITCHOVER IN PIM-SM

PIM-SM verbindet die Einfachheit des Shared Trees mit der Effizienz des Shortest Path Trees durch automatisches Umschalten.

- **Initial:** Empfänger empfängt Pakete über den (*,G)-Baum vom zentralen RP
- **Schwellenwert:** Erreicht der Datenstrom ein Limit (oft ab erstem Paket), lernt der Router die Quell-IP
- **Switchover:** Der Last-Hop-Router sendet einen (S,G)-Join direkt zur Quelle und baut den SPT auf
- **Pruning RP:** Nach erfolgreichem SPT-Aufbau wird der Pfad über den RP beschnitz direkrune (*,G))

1	2	3	4
IGMP-Join empfangen	**(*,G) Join zum RP**	**Quelle registriert Daten**	**SPT-Umschaltung**
Empfänger meldet Gruppenbeitritt via IGMP an den Last-Hop-Router.	Last-Hop-Router baut Shared Tree zum zustandigen Rendezvous Point auf.	Quelle sendet Daten via First-Hop-Router gekapselt im PIM-Register an den RP.	Last-Hop-Router initiiert direkten (S,G)-Join zur Quelle für minimale Latenz.

7. ZUDUSAUSWAHL: DM ODER SM?

Kompakte Rekapitullation der PIM passend zur Tophiogien Verifikation im Feldeinsat; der Tellienhmer.

- **PIM-DM:** Empfänger fast überall, kleine Netze, keine RP-Infrastruktur gewünscht
- **PIM-SM:** Empfänger verstreut, mittlere bis große Enterprise-/WAN-Netze, strenge Bandbreitenkontrolle

Befinden sich Multicast-Empfänger in nahexu jedem Subnetz des Netzwerks?

Ja	Nein
Dichte Abdeckung im lokalen Campus-LAN	**Selektive oder verteilte Empfänger (WAN / Großnetz)**
PIM-DM evaluieren, beachten Sie jedech periodisches Fluten und Prune-Zyklen.	PIM-SM mit redundantem RP (Auto-RP/BSR) und SPT-Switchover implementieren.

MLD IN IPV6: MULTICAST LISTENER DISCOVERY

1. WAS IST MLD?

Multicast Listener Discovery (MLD) ist das zentrale IPv6-Steuerungsprotokoll zur Verwaltung von Multicast-Gruppenmitgliedschaften auf dem lokalen Link. Es ist das direkte IPv6-Gegenstück zum IPv4-Protokoll IGMP.

- **Funktion:** Ermöglicht IPv6-Routern zu erkennen, welche Multicast-Adressen auf angebundenen Links von Hosts aktiv empfangen werden.
- **Link-Lokalität:** MLD operiert ausschließlich im lokalen Subnetz; MLD-Nachrichten werden von Routern nicht über Subnetzgrenzen weitergeleitet.
- **Kapselung:** Integriert in ICMPv6 mit vorgeschriebenem IPv6 Hop-by-Hop Router Alert Option Header zur prioritären Prüfung.
- **Basis:** MLDv1 basiert konzeptionell auf IGMPv2; MLDv2 entspricht der Funktionalität von IGMPv3.

SCHLÜSSELFUNKTION

IPv6 erstezt IPv4-Broadcast vollständig durch zielgerichteten Multicast. MLD stellt sicher, dass Multicast-Pakete nur an Interfaces gesendet werden, die sie aktiv anfordern.

2. MLDv1 VS. MLDv2

Die beiden Protokollversionen unterscheiden sich grundlegend in der Filterfähigkeit bezüglich der Quelladressen (Source-Filtering).

- **MLDv1 (RFC 2710):** Unterstützt Any-Source Multicast (ASM). Ein Host meldet Interesse an einer Multicast-Gruppe an, unabbängig vom Sender.
- **MLDv2 (RFC 3810):** Führt Source-Specific Multicast (SSM) ein. Hosts spezifizieren gewünschte oder unerwünschte Quell-IP-Adressen.
- **Filter-Modi in MLDv2:** INCLUDE-Modus (akzeptiert nur gelistete Quellen) und EXCLUDE-Modus (blockiert gelistete Quellen, akzeptiert alle anderen).
- **Abwärtskompatibilität:** MLDv2-Router unterstützen MLDv1-Hosts automatisch durch Umschalten auf Kompatibilitätsmodus.

3. ICMPv6-NACHRICHTENTYPEN

MLD definiert spezifische ICMPv6-Nachrichtentypen für Abfragen, Beitritte und Austritte im lokalen Segment.

- **Typ 130 – Multicast Listener Query:** Vom Router gesendet zur Inventarisierung (General Query, Group-Specific oder Group-and-Source-Specific in MLDv2).
- **Typ 131 – Multicast Listener Report (MLDv1):** Vom Host gesendet, um das Abonnieren einer Multicast-Adresse zu signalisieren.
- **Typ 132 – Multicast Listener Done (MLDv1):** Vom Host gesendet (an ff02::2), wenn er eine Multicast-Gruppe verlässt.
- **Typ 143 – Version 2 Multicast Listener Report:** Bündelt Gruppen- und Quellfilter-Zustände in einer einzigen Nachricht.

4. SOLICITED-NODE MULTICAST

Eine essentielle IPv6-Anwendung von Multicast ist die Adressauflösung und Duplikaterkennung über Solicited-Node-Multicast-Adressen.

- **Präfix & Format:** Bildet sich aus ff02::1:ff00:0/104 kombiniert mit den niederwertigsten 24 Bit der jeweiligen IPv6-Unicast- oder Anycast-Adresse.
- **Einsatzzweck:** Ersetzt ARP-Broadcasts durch Neighbor Solicitation (NDP) und Duplicate Address Detection (DAD). Solicitation (NDP) und Duplicate Address Detection (DAD).
- **MLD-Registrierung:** Jeder IPv6-Knoten muss seiner eigenen Solicited-Node-Multicast-Adresse beitreten und diesen Zustand via MLD verwalten.
- **Hardware-Effizienz:** NIC-Filter und Switches filtern unbeteiligte Hosts auf MAC-Ebene heraus.

5. ROUTER- & HOST-INTERAKTION

Der standardisierte Ablauf zwischen Listener und Querier sichert den kontinuierlichen und bandbreitenschonenden Datenfluss.

- **Querier-Wahl:** Der Router mit der numerisch niedrigsten Link-Local-IPv6-Adresse (fe80::) wird aktiver Querier.
- **General Query:** Regelmäßige Abfrage an ff02::1 (All-Nodes) zur Erfassung aktiver Abonnenten.
- **Report Suppression (MLDv1):** Zufälliger Antwort-Timer verhindert Paketkollisionen; der schnellste Host unterdrückt redundante Berichte anderer.
- **State Tracking (MLDv2):** Router verwalten explizite Zustände je Interface, Gruppe und Quellfilter ohne Unterdrückung.

ABLAUF IN 3 SCHRITTEN

1. **Initialer Gruppenbeitritt**
   Host sendet unaufgefordert einen MLD-Report an die betroffene Multicast-Gruppe, sobald ein Prozess den Datenstrom anfordert.
2. **Periodische Abfrage**
   Querier-Router sendet in festen Intervallen General Queries an ff02::1, um die Listenerschaft zu überpüfen.
3. **Gruppenaustritt & Pruning**
   Host sendet 'Done' (MLDv1) bzw. State-Change-Report (MLDv2). Router stoppt die Weiterleitung nach unbeantworteter Query.

6. MLD-SNOOPING IN SWITCHES

Layer-2-Switches nutzen MLD-Snooping, um Multicast-Frames gezielt nur an interessierte Ports auszuliefern anstatt sie zu fluten.

- **L2-Problem:** Multicast-IPv6-Pakete werden standardmäßig auf Layer 2 wie Broadcast bebandet, wenn der Switch MLD nicht interpretiert.
- **Snooping-Tabelle:** Switch analysiert ICMPv6-MLD-Pakete und mappt Multicast-MACs (33:33:xx:xx:xx:xx) auf konkrete Switchports.
- **Router-Port-Erhennung:** Switch leitet MLD-Reports suvelläßsig an Ports weiter, an denen Multicast-Router ektannt wurden.
- **Entlastung:** Verhindert Überlastung leistungsschwacher Clients durch unangeforderten Multicast-Traffic.



7. TYPISCHE FEHLERQUELLEN & TROUBLESHOOTING

Häufige Konfigurations- und Filterfehler können den IPv6-Multicast-Verkehr empfindlich stören.

- **ICMPv6-Firewall-Blockaden:** Das pauschale Blockieren von ICMPv6 auf Hosts oder Firewalls unterbricht MLD und zerstört damit IPv6-Konnektivität.
- **Fehlender Querier:** Wenn im L2-Segment kein IPv6-Router aktiv ist, schaltet MLD-Snooping ohne konfigurierten Querier Ports nach Timeout stumm.
- **Hop-by-Hop Extension Header Drop:** Manche veraltete L3-Geräte verwerfen Pakete mit Router-Alert-Option fälschlicherweise.
- **Link-Local-Konflikte:** Unvollständige oder gestörte fe80::-Adressen verhindern die ordnungsgemäße Querier-Wahl.

ACHTUNG BEI FIREWALL-REGELN

ICMPv6-Nachrichtentypen 130, 131, 132 und 143 dürfen im lokalen Link niemals verworfen werden, da sonst Neighbor Discovery und Multicast ausfallen.

8. ZUSAMMENFASSUNG & PRAXIS-CHECKLISTE

MLD ist das unverzichtbare Fundament für IPv6-Multicast und grundlegende Netzwerkfunktionen wie DAD und Adressauflösung.

- MLD = IPv6-Äquivalent zu IGMP (MLDv1 = IGMPv2, MLDv2 = IGMPv3).
- Kapselung erfoigt transparent in ICMPv6 mit lokaler Link-Gütigkeit.
- Solicited-Node Multicast bildet das Rückgrat der Adressauflösung.
- MLD-Snooping auf Layer-2-Switches ist zwingend für sauberes Traffic-Management erforderlich.

PRAXIS-CHECKLISTE

Geprüftes Netzwerksegment / VLAN-ID: _____

Aktiver MLD-Querier IPv6-Adresse (fe80::): _____

Status MLD-Snooping auf Switches (Aktiv / Inaktiv / Querier-Modus): _____

Beobachtete Multicast-Gruppen (z. B. ff02::1, ff02::1:ffxx:xxxx): _____

Quality of Service (QoS): Grundlagen und Dienstgütemodelle

1. WAS IST QOS?



Quality of Service (Dienstgüte) bezeichnet Verfahren zur Priorisierung von Netzwerkdatenströmen, um verbindliche Übertragungseigenschaften wie Latenz und Bandbreite für geschäftskritische Anwendungen verlässlich zu garantiieren.

- **Ziel:** Gezielte Steuerung von Netzwerkressourcen bei Engpässen
- **Vermeidung:** Verdrängung zeitkritischer Nutzdaten durch Massendownloads
- **Fokus:** Vorhersehbare Dienstgüte für Sprache, Video und Leitdaten

2. KERNMETRIKEN



Netzwerkleistung wird durch vier fundamentale Übertragungsmetriken bestimmt, die bei Überlastung ohne QoS-Regeln sofort degradieren.

- **Bandbreite:** Verfügbare Übertragungskapazität in Bit pro Sekunde (Bit/s)
- **Latenz:** Paketlaufzeit (One-Way oder Round-Trip-Time) vom Sender zum Empfänger
- **Jitter:** Statistische Schwankung der Paketlaufzeit, kritisch für Audio/Video
- **Paketverlust:** Anteil verworfener IP-Pakete bei Pufferüberlauf an Routern/Switches

8. TRAFFIC SHAPING VS. POLICING



Verkehrsregulierende Mechanismen, die vertragliche Bandbreitengrenzen (Committed Information Rate) durchsetzen.

- **Policing:** Verwirft überschüssige Pakete sofort oder markiert sie herab (verursacht TCP-Retransmissions)
- **Shaping:** Puffert Lastptitzen zwischen und glättet den Datenstrom (erhöht Latenz, vermeidet aber Paketverlust)
- **Praxis:** Shaping am WAN-Uplink des Kunden, Policing am Ingress-Interface des Internet Service Providers

3. BEST-EFFORT-MODELL



Das Standardübertragungsmodell des klassischen IP-Netzes ohne Reservierung oder Bevorzugung bestimmter Sender.

- **Prinzip:** Alle Datenpakete erhalten identische Priorität nach FIFO (First-In, First-Out)
- **Garantie:** Keine Zusicherungen bezüglich Ankunftszeit, Durchsatz oder Verlustrate
- **Einsatz:** Unkritischer Datenverkehr wie Dateiübertragungen, Web-Browsing oder System-Updates



7. WARTESCHLANGEN & VERWURF



Algorithmen steuern Pufferverwaltung und Paketabfertigung an Router-Schnittstellen zur Beherrschung von Überlastungen.

- **Queuing:** Priority Queuing (PQ), Weighted Fair Queuing (WFQ) und Class-Based WFQ (CBWFQ)
- **Low Latency Queuing (LLQ):** Strikte Prioritätswarteschlange für Echtzeit-Audiopakete
- **Congestion Avoidance:** WRED (Weighted Random Early Detection) verwirft gezielt TCP-Pakete vor Pufferüberlauf Providers

4. INTEGRATED SERVICES (INTSERV)



IntServ bietet harte Bandbreitengarantien durch zustandsbehaftete Reservierung etlang des gesamten Übertragungswegs vor Beginn des Datenstroms.

- **Protokoll:** RSVP (Resource Reservation Protocol) signalisiert Ressourcenanfragen
- **Vorteil:** Absolute Servicegarantie für unterbrechungsfreie Verbindungen
- **Limitierung:** Geringe Skalierbarkeit im Internet-Backbone durch Verbindungszustände in jedem Router

6. KLASSIFIZIERUNG & MARKIERUNG



Mechanismen zur Identifikation und Kennzeichnung von Datenströmen am Übergabepunkt in das lokale oder weite Netzwerk.

- **Schicht 2:** IEEE 802.1p Priority Code Point (PCP, 3 Bit im VLAN-Tag)
- **Schicht 3:** IP Precedence (3 Bit) oder modernes IP DSCP (6 Bit)
- **Trust Boundary:** Vertrauensgrenze, an der Markierungen von Endgeräten validiert oder überschrieben werden

5. DIFFERENTIATED SERVICES (DIFFSERV)



DiffServ ist der skalierbare Branchenstandard: Datenströme werden an Netzwerkgrenzen in Dienstklassen eingeteilt und hop-by-hop priorisiert.

- **Klassifizierung:** Markierung über das 6-Bit DSCP-Feld (Differentiated Services Code Point) im IP-Header
- **PHB (Per-Hop Behavior):** Standardsierte Behandlungsklassen wie Expedited Forwarding (EF) und Assured Forwarding (AF)
- **Skalierbarkeit:** Kernrouter prüfen nur das Header-Feld, ohne individuelle Verbindungszustände zu speichern

PRAXIS-CHECKLISTE: QOS-MODELLWAHL



Leitfaden zur Festlegung der passenden Dienstgütestrategie für Unternehmens- und Campus-Netzwerke.

- Best-Effort reicht für geschlossene Gigabit-LANs mit geringer Dauerauslastung ohne VoIP.
- DiffServ ist die Standardarchitektur für Campus-, Rechenzentrums- und WAN-Umgebungen.
- VoIP-Pakete zwingend mit EF (DSCP 46) markieren und in LLQ-Queue einspeisen.
- Signalisiere Datenströme erst ab verifizierten Switch-Ports (Trust Boundary).

HINWEIS ZUR SICHERHEIT

QoS erzeugt keine zusätzliche Bandbreite, sondern verteilt vorhandene Kapazitäten. Nicht authentifizierte Endgeräte dürfen DSCP-Tags niemals unkontrolliert setzen, da Denial-of-Service-Angriffe durch Traffic-Monopolisierung möglich sind.

QoS & PAKETMARKIERUNG



1. GRUNDLAGEN DER KLASSIFIZIERUNG

Die Dienstgüte (Quality of Service, QoS) identifiziert und unterteilt Netzwerkverkehr am Netzeingang in definierte Serviceklassen.



- Identifikation anhand von IP-Adressen, TCP/UDP-Ports oder VLAN-Tags
- Zuweisung des Verkehrs in definierte Dienstklassen (z. B. Sprache, Video, Best-Effort)
- Grundvoraussetzung für Priorisierung, Bandbreitenreservierung und Queueing

2. LAYER-2-MARKIERUNG: 802.1P PCP (COS)

Auf der Sicherungsschicht erfolgt die Priorisierung direkt im Ethernet-Frame innerhalb des 802.1Q-VLAN-Tags.



- Class of Service (CoS) nutzt das 3-Bit Priority Code Point (PCP)-Feld
- Wertebereich von 0 (Best-Effort) bis 7 (Netzwerk-Kontrollverkehr)
- CoS geht beim Weiterleiten über Layer-3-Routergrenzen hinweg verloren

3. HISTORISCHES LAYER 3: TYPE OF SERVICE (TOS)

Das ursprüngliche IPv4-Headerfeld zur Dienstgüte-Definition definierte grundlegende Prioritäten über 8 Bit.



- IP Precedence (IPP) nutzte die ersten 3 Bits (Werte 0 bis 7)
- Bits 3 bis 5 dienten als Flags für Verzögerung, Durchsatz und Zuverlässigkeit
- Wurde durch moderne DiffServ-Standards (RFC 2474) abgelöst

4. MODERNES LAYER 3: DIFFSERV & DSCP

Differentiated Services nutzt das neu definierte 8-Bit-DS-Feld im IP-Header für granulare Verkehrskontrolle.



- DSCP (Differentiated Services Code Point) belegt die ersten 6 Bits (64 Werte)
- Die verbleibenden 2 Bits dienen der Explicit Congestion Notification (ECN)
- DSCP bleibt auch über geroutete Netze hinweg erhalten

5. PHB-STANDARDS (PER-HOP BEHAVIORS)

PHBs legen fest, wie Netzwerkknoten markierte Pakete bei Weiterleitung und Pufferung konkret behandlen.



- Default Forwarding (DF / Best-Effort): Standardweiterleitung ohne Garantien
- Expedited Forwarding (EF / DSCP 46): Minimale Latenz und Jitter für VoIP-Payload
- Assured Forwarding (AF): 4 Klassen mit jeweils 3 Drop-Precedences (z. B. AF41, AF31)

6. TRUST BOUNDARIES & MAPPING

Netzwerkgeräte definieren Grenzen, ab denen Markierungen vertraut oder neu gesetzt werden.

- Trust Boundary: IP-Telefone und Server gelten oft als vertrauenswürdig, Benutzer-PCs als unvertrauenswürdig
- Unvertraute Pakete werden am Access-Switch auf DSCP 0 zurückgesetzt (Remarking)
- CoS-zu-DSCP- und DSCP-zu-CoS-Mapping stellt konsistente QoS über Layer-2/3-Übergänge sicher



PRAXIS-MERKSATZ

Klassifiziere und markiere Datenpakete immer so nah wie möglich an der Datenquelle (Edge), um Ressourcen im Core-Netzwerk zu schonen.

7. WORKFLOW: 4 SCHRITTE ZUR QoS-MARKIERUNG

Strukturierte Vorgehensweise zur Implementierung verlässlicher Klassifizierung und Markierung im Netzwerk.



1. **Verkehrsströme analysieren**
   Echtzeitdaten (VoIP, Video) von geschäftskritischen Daten und reinem Best-Effort-Traffic anhand von Ports und Quell-IPs trennen.
2. **Trust Boundary etablieren**
   Switch-Ports konfigurieren: Endgeräte-Ports untrusted setzen, Uplinks und IP-Telefon-Verbindungen als trusted deklarieren.
3. **Paketmarkierung durchführen**
   Access Control Lists (ACLs) oder Class-Maps anwenden, um Pakete mit DSCP (z. B. EF für Sprache, AF31 für Video) zu markieren.
4. **Queuing und Policing zuweisen**
   Auf Egress-Schnittstellen Priority-Queues für DSCP EF und Weighted-Fair-Queuing für AF-Klassen bereitstellen.

8. ENTSCHEIDUNGSMATRIX: VERKEHR ZUORDNEN

Entscheidungslogik zur Zuweisung des passenden DSCP-Wertes bei der Konfiguration von QoS-Policies.



Welche Anforderungen an Latenz und Verlusttoleranz hat der Datenstrom?

Echtzeit-Sprachverkehr (VoIP Audio)	→	DSCP 46 (EF)
Interaktives Video oder geschäftskritische Datenbankabfragen	→	DSCP AF41 oder AF31
Standard-Websurfen, Datei-Downlonds oder unbekannter Datenverkehr	→	DSCP 0 (Best-Effort)

QoS-Mechanismen: Queuing, Scheduling, Policing und Shaping

1. Grundprinzipien von QoS

Quality of Service steuert Datenströme bei Engpässen auf Netzwerk-Interfaces. Ziel ist die gezielte Minimierung von Verzögerung (Delay), Laufzeitschwankungen (Jitter) und Paketverlust.

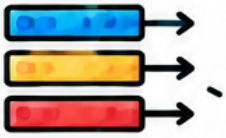
- Bandbreite priorisieren statt unkontrolliert verwerfen
- Klassifikation am Netzwerkeingang via DSCP/CoS
- Entscheidend für Echtzeitanwendungen wie VoIP und Video



2. FIFO & Priority Queuing (PQ)

FIFO (First In, First Out) leitet Pakete strikt nach Eingangsreihenfolge weiter und bietet keinerlei Bevorzugung. PQ richtet mehrere feste Prioritätsklassen ein.

- FIFO: Keine Differenzierung, Standard ohne QoS-Konfiguration
- PQ: Hohe Klassen werden immer zuerst vollständig geleert
- Gefahr bei PQ: Niedrigere Warteschlangen können verhungern (Starvation)



3. Weighted Fair Queuing (WFQ)

WFQ teilt Bandbreite dynamisch und fair zwischen aktiven Flows auf, ohne dass Zugriffsklassen manuell vorkonfiguriert werden müssen.

- Verhindert, dass bandbreitenintensive Ströme kleine Ströme blockieren
- Kleine Pakete (z. B. TCP ACKs, DNS) werden schneller bedient
- Automatische Zuweisung basierend auf IP-Präzedenz oder Header-Werten



4. Class-Based WFQ (CBWFQ)

CBWFQ erweitert WFQ um benutzerdefinierte Verkehrsklassen mit garantierten Bandbreitenanteilen je Schnittstelle.

- Definition von Klassen über Access-Listen oder DSCP-Werte
- Jeder Klasse wird ein prozentualer oder absoluter Durchsatz garantiert
- Unbenutzte Bandbreite wird dynamisch auf andere Klassen umverteilt



5. Low Latency Queuing (LLQ)

LLQ kombiniert die Bandbreitengarantie von CBWFQ mit einer strikten Prioritätswarteschlange (PQ) für absolut zeitkritischen Datenverkehr.

- Definierter Standard für Voice over IP (VoIP)
- Strikte Priorität mit integriertem Policing zum Schutz anderer Klassen
- Ermöglicht minimale Paketlaufzeiten und extrem niedrigen Jitter



6. Traffic Policing

Policing überwacht die Einhaltung konfigurierter Übertragungsraten und greift bei Überschreitung unmittelbar hart ein.

- Überzählige Pakete werden sofort verworfen (Drop) oder ummarkiert (Remark)
- Erzeugt keinen künstlichen Puffer-Delay
- Führt bei TCP durch Paketverlust zu Fensterrücknahme und Datendrosselung



7. Traffic Shaping

Shaping glättet Verkehrsspitzen, indem überschüssige Pakete temporär in einem Puffer zwischengespeichert und gleichmäßig ausgesendet werden.

- Verhindert Paketverlust an Engpässen durch kontrollierte Verzögerung
- Erfordert Pufferspeicher und erzeugt messbaren Zusatz-Delay
- Typischer Einsatz am Übergang von LAN- zu WAN-Verbindungen



8. Token-Bucket-Algorithmus

Mathematisches Modell zur Durchsatzmessung für Policing und Shaping, das Burst-Größen und Dauerübertragungsraten präzise definiert.

- Tokens füllen den Eimer kontinuierlich mit fester Committed Information Rate (CIR)
- Für jedes gesendete Datenpaket wird ein entsprechendes Token-Guthaben verbraucht
- Ermöglicht kontrollierte Bursts bis zur maximalen Eimergröße (Bc)



Vergleichsregel

Policing schneidet Spitzen sofort ab (Drop/Remark). Shaping puffert und verzögert Pakete für ein gleichmäßiges Signalprofil.

QoS: ÜBERLASTVERMEIDUNG (RED & WRED)

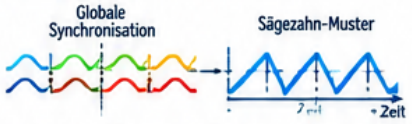
1. GRUNDPRINZIP DER KONGESTIONSVERMEIDUNG

Überlastvermeidung (Congestion Avoidance) setzt präventiv an, bevor Router-Puffer vollständig vollaufen. Während Congestion Management (Queuing) regelt, wie Pakete geordnet den Puffer verlassen, entscheidet die Überlastvermeidung darüber, welche Pakete beim Pufferzulauf verworfen oder markiert werden.

- Ziel: Verhinderung von Pufferüberläufen (Bufferbloat) und langen Latenzen.
- Arbeitet am Puffer-Eingang des Routers (Buffer Management).
- Signalisierung an Sender zur proaktiven Reduktion der Datenrate.

2. DAS TAIL-DROP-PROBLEM

Standardmäßig greift Tail Drop: Ist die Ausgangswarteschlange voll, werden ausnahmslos alle nachfolgenden eintreffenden Pakete verworfen. Dies führt zu gravierenden Ineffizienzen im Netzwerkverkehr.



- Globale TCP-Synchronisation: Hunderte TCP-Sessions verlieren gleichzeitig Pakete und halbieren zeitgleich ihr Congestion Window.
- Sägezahn-Muster: Der Netzwerkdurchsatz schwankt extrem zwischen Überlast und Leerlauf.
- Verhungern (Starvation): Einzelne aggressive Datenströme verdrängen reaktive TCP-Verbindungen.

Achtung bei Tail Drop
Tail Drop erzeugt periodische Leistungseinbrüche im gesamten Netz, da synchronisierte Verbindungen die Bandbreite nie stabil auslasten.

3. RANDOM EARLY DETECTION (RED)

RED verwirft stochastisch einzelne Pakete bereits bei beginnender Pufferfüllung, lange bevor die Puffer komplett überläuft. Dadurch reduzieren nur einzelne TCP-Quellen ihr Senderating.

- Glättung des Pufferstands durch exponentiell gewichteten gleitenden Durchschnitt (Average Queue Length).
- Verhindert das Schwingen bei kurzzeitigen Bursts normaler Paketfolgen.
- Aufbrechen der globalen Synchronisation: Nur selektierte Verdrängen drosseln ihren Durchindungen.

4. RED SCHWELLENWERTE UND WAHRSCHEINLICHKEIT

Die Paketverwerfung bei RED folgt drei definierten Phasen basierend auf der berechneten durchschnittlichen Warteschlangenlänge:

- Unter Min-Threshold: Kein Verwerfen (Drop-Wahrscheinlichkeit = 0 %).
- Zwischen Min- und Max-Threshold: Linearer Anstieg der Verwerfungswahrscheinlichkeit von 0 % bis Max-P.
- Über Max-Threshold: Rückfall auf 100 % Verwerfung (Tail Drop für alle nachfolgenden Pakete).



5. WEIGHTED RED (WRED)

WRED erweitert RED um Quality-of-Service-Differenzierung. Schwellenwerte und Verwerfungswahrscheinlichkeiten werden dynamisch anhand von Prioritätsfeldern im IP-Header festgelegt.

- Klassifizierung über IP Precedence (3 Bits) oder DSCP (Differentiated Services Code Point, 6 Bits).
- Niedrig priorisierter Best-Effort-Verkehr hat niedrigere Schwellenwerte und wird früher verworfen.
- Missionskritischer Datenverkehr bleibt bei beginnender Last unberührt im Puffer.

DSCP (6 Bits)

AF11 | AF21 | AF23 | EF

6. EXPLICIT CONGESTION NOTIFICATION (ECN)

ECN ermöglicht Überlastsignalisierung ganz ohne gezielten Paketverlust. Es verwendet die beiden letzten Bits des Traffic-Class-/TOS-Feldes im IPv4/IPv6-Header zusammen mit TCP-Flags.

- Knoten setzt CE-Bit (Congestion Experienced), statt das Paket via RED/WRED zu droppen.
- Empfänger quittiert Überlast im TCP-ACK via ECE (ECN-Echo).
- Sender verringert Congestion Window und bestätigt via CWR (Congestion Window Reduced).

IP-Header (IPv4/IPv6)

...	TOS / Traffic-Class	...	ECN: CE	ECN: ECT

TCP-Flags

...	ECE	CWR	...

Praxis-Tipp: ECN-Voraussetzung
ECN funktioniert verlustfrei nur, wenn Sender, Router und Empfänger ECN-fähig sind. Fehlt die Unterstützung, greift WRED automatisch auf Paket-Drop zurück.

7. VERGLEICH DER VERFAHREN

Entscheidungsübersicht zum Einsatz der jeweiligen Pufferverwaltungsstrategie in modernen Enterprise- und Service-Provider-Netzwerken.

- Tail Drop: Minimale CPU-Last, aber unkontrollierbare Jitter- und Synchronisationsprobleme.
- Klassisches RED: Verhindert globale Synchronisation, unterscheidet jedoch keine Dienstklassen.
- WRED: Standard für differenzierte Enterprise-QoS-Konzepte mit IP Precedence / DSCP.
- **WRED + ECN**: Optimal für latenzsensitive TCP-Anwendungen ohne unnötigen Paketverlust.

Welche Puffer-Strategie passt zu Ihrem Netzwerkszenario?

Keine QoS-Priorisierung erforderlich, nur Vermeidung globaler TCP-Synchronisation	Standard-RED aktivieren und Schwellenwerte an Round-Trip-Time (RTT) anpassen.
Multiservice-Netzwerk mit DSCP/VoIP und transaktionalen Daten	WRED konfigurieren: AF-Klassen (Assured Forwarding) mit gestaffelten Drop-Wahrscheinlichkeiten versehen.
Hochmoderne Data-Center- oder Cloud-Umgebung mit TCP-Lastspitzen	WRED in Verbindung mit ECN aktivieren, um Leitungen ohne reinen Paketverlust auszureizen.

8. ZUSAMMENFASSUNG & BEST PRACTICES

Kompakter Leitfaden für die erfolgreiche Implementierung von Überlastvermeidungsstrategien in aktiven Netzwerk-Komponenten.

- Niemals WRED auf Voice-Warteschlangen (Priority Queues) anwenden; Voice verlangt striktes Policing/LLQ.
- Puffergrößen realsitisch dimensionieren, um Bufferbloat an Engpässen zu vermeiden.
- ECN netzwerkweit evaluieren, um Durchsatz bei interaktiven Anwendungen zu maximieren.

4 Schritte zur Umsetzung

1. **Schritt 1: Verkehrsklassen analysieren**
   Identifizieren Sie geschäftskritische TCP-Ströme, Voice-Daten und Best-Effort-Verkehr auf den Schnittstellen.
2. **Schritt 2: WRED-Profile definieren**
   Legen Sie Minimal- und Maximalschwellen für unterschiedliche DSCP-Drop-Precedences (z. B. AF21 vs. AF23) fest.
3. **Schritt 3: ECN-Unterstützung zuschalten**
   Aktivieren Sie ECN im WRED-Profil, um kompatiblen Hosts verlustfreie Drosselung zu ermöglichen.
4. **Schritt 4: Warteschlangen-Telemetrie überwachen**
   Prüfen Sie Drop-Counter und Puffer-Füllstände via Interface-Statistiken, um Schwellenwerte feinabzustimmen.

WLAN-GRUNDLAGEN: FUNK, KANÄLE & ANTENNENTECHNIK

1. 2,4-GHZ-BAND (ISM)



2400 – 2483,5 MHz



2,4 GHz

- 13 Kanäle im europäischen Raum mit 5 MHz Kanalabstand.
- Typische Signalbandbreite von 20 MHz je Kanal.
- Exakt drei überlappungsfreie 20-MHz-Kanäle nutzbar: Kanal 1, 6 und 11.

2. 5-GHZ-BAND (UNII)



19 überlappungsfreie 20-MHz-Kanäle



- Geringere Interferenzdichte als im 2,4-GHz-Bereich.
- Unterstützt Kanalbündelung auf 40, 80 und 160 MHz.
- DFS (Dynamic Frequency Selection) und TPC (Transmit Power Control) zwingend auf UNII-2/UNII-2-Extended.

3. 6-GHZ-BAND (Wi-Fi 6E / 7)



5945 – 6425 MHz



6 GHz

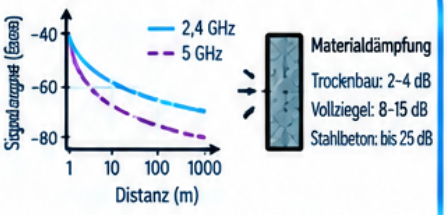
- Bis zu 24 zusätzliche 20-MHz-Kanäle bzw. breite 80/160/320-MHz-Blöcke.
- Keine Abwärtskompatibilität zu älteren IEEE-802.11b/g/n/ac-Clients erforderlich.
- Geringere Reichweite durch erhöhte Absorption an Wänden und Decken.

4. KANALBREITEN & BONDING



- 20 MHz: Industriestandard für dichte Client-Umgebungen (High Density).
- 40 MHz: guter Kompromiss im 5-GHz-Band ohne übermäßige Kanalüberlappung.
- 80 / 160 / 320 MHz: maximaler Einzelclient-Durchsatz, primär in störungsarmen Heimnetzen sinnvoll.

5. FREIRAUMDÄMPFUNG (FSPL)



- Signalenergie verteilt sich kugelförmig: Verdopplung der Distanz = 6 dB Verlust.
- 5 GHz verliert im freien Raum etwa 6 bis 7 dB mehr Pegel als 2,4 GHz bei gleicher Distanz.
- Materialdämpfung wie angegeben.

6. ANTENNENCHARAKTERISTIKA



Omnidirektional (Rundstrahler) | Direktional (Richtantenne)

- Omnidireiktional: 360-Grad-Abdeckung in der horizontalen Ebene (Donut-Form).
- Direktional: Fokus in eine Vorzugsrichtung für Punkt-zu-Punkt-Strecken oder Hallen.
- MIMO: mehrere Antennen für parallele Übertragung via Raummultiplex.

7. SENDELEISTUNG, EIRP UND GRENZWERTE

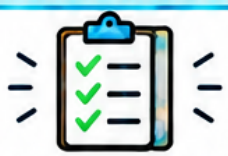


$$EIRP = P_{TX} - L_K + G_A$$

P_{TX} = Sendeleistung
L_K = Kabeldämpfung
G_A = Antennengewinn

- 2,4 GHz EU-Limit: maximal 100 mW (20 dBm) EIRP.
- 5 GHz EU-Limit: 200 mW (23 dBm) für UNII-1/UNII-2; bis zu 1000 mW (30 dBm) auf UNII-2-Extended mit DFS/TPC.
- dBm-Skala: 0 dBm entspricht 1 mW; jede Erhöhung um 3 dB verdoppelt die Leistung.

8. PRAXIS-CHECKLISTE



- 2,4 GHz: nur Kanal 1, 6 oder 11; kein 40-MHz-Bonding.
- Im 5-GHz-Bereich 20 oder 40 MHz für Büroumgebungen.
- DFS-Kanäle überwachen.
- Antennenausrichtung und Montagehöhe auf Endgeräte abstimmen.

Ausbreitung von Funkwellen:
Dämpfung · Reflexion · Streuung · Beugung

Entscheidungsmatrix: Frequenzband- und Kanalwahl

Welche primäre Anforderung bestimmt das Einsatzszenario der Funkzelle?

1	Große Distanzen, viele Wände oder IoT-Geräte ohne 5-GHz-Support	→ 2,4 GHz mit 20 MHz Kanalbreite. Nur Kanal 1, 6 oder 11.
2	Hohe Client-Dichte im Büro mit moderaten Durchsatzanforderungen	→ 5 GHz mit 20 oder 40 MHz Kanalbreite. Nachbarzellen auf getrennte UNII-Kanäle.
3	Punkt-zu-Punkt-Richtfunkstrecke im Außenbereich über mehrere hundert Meter	→ 5 GHz UNII-2-Ext mit Richtantennen, aktivem DFS/TPC und EIRP-Grenzwerte.
4	Sehr hohe Datenraten für moderne Arbeitsplätze mit Wi-Fi 6E/7	→ 6 GHz mit 80 oder 160 MHz Kanalbreite bei direkter Sichtverbindung.

WLAN-Feldmessungs- und Konfigurationsprotokoll

Erfassen Sie die Funkparameter für einen installierten Access Point zur Sicherstellung einer störungsfreien Funkabdeckung.

Access Point Standort & Gerätekennung (MAC / BSSID):

Verwendetes Frequenzband (2,4 GHz / 5 GHz / 6 GHz) & Kanalnummer:

Eingestellte Kanalbreite (20 / 40 / 80 / 160 MHz) & DFS-Status:

Gemessener Signalpegel (RSSI in dBm) und Grundrauschen (Noise Floor):

Antennentyp, geschätzter Antennengewinn (dBi) und Montagehöhe:

IEEE 802.11 WLAN-STANDARDS (WIFI 1 BIS WIFI 7)

1. FRÜHE GENERATIONEN

- IEEE 802.11b (WiFi 1 / 1999): bis 11 Mbit/s, 2,4 GHz, DSSS/CCK
- IEEE 802.11a (WiFi 2 / 1999): bis 54 Mbit/s, 5 GHz, OFDM
- IEEE 802.11g (WiFi 3 / 2003): bis 54 Mbit/s, 2,4 GHz, Mischbetrieb aus OFDM und DSSS



2. WIFI 4 (802.11N)

- MIMO-Technologie
- 2,4/5 GHz Dualband
- 40 MHz Kanalbreite
- bis 600 Mbit/s



3. WIFI 5 (802.11AC)

- 5 GHz nur
- 256-QAM
- Downlink MU-MIMO
- 80/160 MHz Kanalbreite



4. WIFI 6/6E (802.11AX)

- OFDMA
- 1024-QAM
- 6 GHz Band
- High Density



5. WIFI 7 (802.11BE)

- 320 MHz Kanalbreite
- 4096-QAM (4K-QAM)
- MLO (Multi-Link Operation)
- 16x16 MIMO



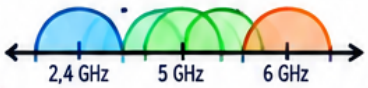
7. MIMO & BEAMFORMING

- Spatial Streams
- Beam Steering
- Array Diversity



8. SPEKTRUMSPLANUNG

- 20–320 MHz Kanalbündelung
- DFS (Radarvermeidung)
- CCI (Interferenzkontrolle)



ZENTRALER ÜBERBLICK: IEEE 802.11 STANDARD-FAMILIE

Normenreihe IEEE 802.11 definiert die Bitübertragungs- und MAC-Schicht für drahtlose lokale Netzwerke (WLAN). Seit 1997 entwickelte sich die Funktechnologie von rudimentären Raten bis zu Multi-Gigabit-Systemen über drei Frequenzbänder.

- **Frequenzbereiche:** 2,4 GHz (hohe Reichweite, hohe Dämpfung/Überlastung), 5 GHz (mehr Spektrum, geringere Störung) und 6 GHz (breite Kanäle ohne Legacy-Ballast)
- Zentrale Normierungsinstanzen: IEEE (technische Spezifikation) und Wi-Fi Alliance (Zertifizierung und Endkundenbezeichnungen von WiFi 1 bis 7)
- Grundlegende Architektur: Trennung in physikalische Übertragung (PHY) und Medienzugriffssteuerung (MAC mit CSMA/CA)

Kanalüberlappung im 2,4-GHz-Band

Im 2,4-GHz-Band stehen in Europa 13 Kanäle im 5-MHz-Raster zur Verfügung. Bei klassischen 20-MHz-Kanalbreiten existieren nur drei überschneidungsfreie Kanäle (meist 1, 6 und 11), weshalb Neuinstallationen vorrangig auf 5 GHz und 6 GHz setzen.

Praxis-Checkliste: WLAN-Standard & Frequenz-Audit

Nutzen Sie diese Prüfpunkte zur systematischen Erfassung und Bewetrung bestehender WLAN-Infrastrukturen vor Ort.

Checkliste

- Aktueller Standard des Access Points (WiFi 5, WiFi 6 oder WiFi 7)
- Konfigurierte Kanalbreiten pro Band (2,4 GHz: strikt 20 MHz; 5 GHz: 20/40/80 MHz)
- Prüfung der DFS-Ereignisse im Systemlogbuch des Controllers
- Anteil aktiver Legacy-Clients (802.11b/g-Geräte, die Kanalzeit blockieren)
- Aktivierung von WPA3-Personal oder WPA3-Enterprise (zwingend für WiFi 6E/7)

So gehen Sie vor

1. **Schritt 1: Spektrumanalyse durchführen**
   Messen Sie die Signaldämpfung (RSSI in dBm) und den Signal-Rausch-Abstand (SNR) an typischen Arbeitsplätzen auf 2,4 GHz, 5 GHz und 6 GHz.
2. **Schritt 2: Mindestdatenrate festlegen**
   Deaktivieren Sie niedrige Basisdatenraten (z. B. 1, 2, 5.5, 11 Mbit/s) im WLAN-Controller, um Roaming zu beschleunigen und Sendepausen zu reduzieren.
3. **Schritt 3: Antennenkonfiguration abstimmen**
   Prüfen Sie, ob Clients MU-MIMO und Beamforming unterstützen, und positionieren Sie Access Points ohne metallische Abschattung.

Geprüfter Standort / Gebäudeabschnitt:

Festgestellte dominierende Standards & Kanalbreiten:

Identifizierte Interferenzen oder DFS-Abschaltungen:

Entscheidungshilfe

Welche Kanalbreite soll im 5-GHz-Band konfiguriert werden?

- **Hohe Client-Dichte / viele benachbarte Access Points** → Konfigurieren Sie maximal 20 MHz oder 40 MHz Kanalbreite, um Co-Channel-Interferenzen zu verhindern und freie Kanäle zu gewährleisten.
- **Geringe Dichte / hohe Durchsatzanforderung pro Client** → Aktivieren Sie 80 MHz (oder 160 MHz nur bei garantiert ungestörtem Spektrum und verifiziertem DFS-Freiraum).

WLAN-TOPOLOGIEN & KOMPONENTEN

802.11 ARCHITEKTUR

1. BSS & IBSS (Grundlagen)



- Der Basic Service Set (BSS) bildet die kleinste Zelle eines Infrastruktur-WLANs mit einem zentralen Access Point (AP).
- BSSID: Eindeutige Kennung der Funkzelle, entspricht typischerweise der MAC-Adresse des AP-Funkmoduls.
- IBSS (Independent BSS): Ad-hoc-Modus ohne AP, bei dem Stationen direkt per Peer-to-Peer kommunizieren.

2. ESS & DS (Erweiterung)



- Ein Extended Service Set (ESS) verknüpft mehrere Basis-Zellen zu einem übergreifenden Firmen- oder Campusnetz.
- Distribution System (DS): Das verbindende Backbone-Netz (üblicherweise Ethernet/Switches).
- SSID: Einheitlicher Netzwerkname über alle verbundenen Access Points für Endanwender.

8. WIRELESS MESH



- Netzwerktopologie ohne durchgehende Ethernet-Verkabelung der einzelnen Zugangsknoten.
- Root AP (RAP): Physisch per Kabel an das LAN/Backbone angebundener Ankerknoten.
- Mesh AP (MAP): Nutzt ein separates 5-GHz- oder 6-GHz-Funkband als dynamischen Backhaul-Uplink zum nächsten Knoten.

3. AUTONOMOUS APs



- Eigenständige "Fat APs", die sämtliche WLAN- und Sicherheitsfunktionen lokal auf dem Gerät verarbeiten.
- Lokale Konfiguration: Jeder AP speichert Verschlüsselungs-Keys, SSIDs und Zugriffsfilter autark.

7. ROAMING-Topologien



- Der nahtlose Übergang mobiler Endgeräte zwischen verschiedenen Funkzellen innerhalb eines Netzwerks.
- Layer-2-Roaming: Client wechselt AP innerhalb desselben IP-Subnetzes ohne IP-Neuvergabe.
- Layer-3-Roaming: APs liegen in unterschiedlicher Subnetzen; Mobility-Tunnel erhalten die ursprüngliche Client-IP aufrecht.

4. LIGHTWEIGHT APs (LAP)



- "Thin APs" übernehmen primär echtzeitkritische Funkoperationen, während Managementfunktionen ausgelagert sind.
- Split-MAC-Architektur: AP wickelt RF-Verschlüsselung und Beaconing ab, Routing/Policies liegen zentral.
- Zero-Touch: Bezieht Konfiguration und Firmware automatisch beim Booten vom Controller.

6. WIRELESS LAN CONTROLLER (WLC)



- Das zentrale Steuerungselement moderner Unternehmensnetze für Richtlinien, RF-Management und Sicherheit.
- Radio Resource Management (RRM): Dynamische Anpassung von Sendeleistung und Kanalwahl zur Störungsvermeidung.
- Sicherheitsdurchsetzung: Zentrale Authentifizierung (802.1X/RADIUS) und netzweite Gastzugangs-Isolation.

5. CONTROLLER-PROTOKOLLE (LWAPP / CAPWAP)



- Standardisierte Tunnel-Protokolle verbinden Lightweight APs über Layer 2 oder Layer 3 mit dem zentralen Controller.
- Control Plane: UDP-Port 5246 (CAPWAP) verschlüsselt mit DTLS für Management- und Konfigurationsbefehle.
- Data Plane: UDP-Port 5247 tunnelt den eigentlichen Nutzdatenverkehr der Clients zum Controller.

ARCHITEKTUR-ENTSCHEIDUNGSLOGIK



Leitfaden zur Auswahl der passenden WLAN-Struktur nach Skalierung und Verkabelungsverfügbarkeit.

PRAXIS-HINWEIS

In modernen Netzen hat CAPWAP (RFC 5415/5416) das ältere proprietäre LWAPP vollständig abgelöst.

Welche WLAN-Architektur ist für den geplanten Standort erforderlich?

Standort hat < 5 APs und keine zentrale Netzwerkverwalltung

→ Einsatz von Autonomous APs (Fat APs) mit lokaler Konfiguration je Gerät.



Enterprise-Umgebung mit > 10 APs, Roaming-Bedarf und zentraler Policy

→ Controller-basierte Architektur mit Lightweight APs und CAPWAP-Tunnelung zum WLC.



Weitläufiges Areal oder Außenbereich ohne LAN-Kabel an jedem Montagepunkt

→ Wireless Mesh Architektur mit dedizierten Root APs und Funk-Backhaul über Mesh APs.



WLAN-Medienzugriff: CSMA/CA, RTS/CTS & IFS-Strukturen

1. Geteiltes Medium & Funkkanäle



WLAN nutzt elektromagnetische Funkwellen als ungebundenes Übertragungsmedium. Da alle Stationen in derselben Funkzelle dieselbe Frequenz teilen, müssen Senderechte streng koordiniert werden.

- Halbduplex-Betrieb: Ein WLAN-Transceiver kann konstruktionsbedingt nicht zeitgleich auf demselben Kanal senden und empfangen.
- Kollisionen im Äther: Gleichzeitige Aussendungen überlagern sich und zerstören die übertragenen Datenrahmen unwiderruflich.
- Dämpfung & Reichweite: Signalstärken nehmen mit der Entfernung stark ab, wodurch Stationen einander nicht immer direkt wahrnehmen.

2. Warum nicht CSMA/CD?



Im klassischen kabelgebundenen Ethernet erkennt eine Netzwerkkarte Signalüberlagerungen direkt auf der Leitung. In Funknetzwerken scheitert dieser Kollisionserkennungsansatz aus physikalischen Gründen.

- Eigenrauschen überdeckt Fremdsignale: Die eigene Sendeleistung überstrahlt ankommende fremde Signale am Empfänger vollständig.
- Kein Collision Detection (CD): Der Sender kann während der Übertragung nicht mithören, ob ein anderer Sender parallel aktiv ist.
- Präventionsprinzip (CA): Statt Kollisionen im laufenden Betrieb abzubrechen, setzt WLAN auf Kollisionsvermeidung vor dem Senden.

Physikalische Grenze
Da WLAN-Karten beim Senden taub für andere Funksignale sind, muss jede erfolgreiche Übertragung explizit per Bestätigung (ACK) quittiert werden.

3. CSMA/CA Grundablauf



Carrier Sense Multiple Access with Collision Avoidance regelt den geregelten Kanalzugriff Schritt für Schritt nach festen Prüfungs- und Warteintervallen.

- Physisches Trägerprüfen: Messung der HF-Signalstärke auf dem Kanal (Clear Channel Assessment / CCA).
- Logisches Trägerprüfen: Auswertung des Network Allocation Vector (NAV) anhand reservierter Zeiten im MAC-Header.
- Zufallszeit (Backoff): Verhindert, dass alle wartenden Stationen unmittelbar nach Freiwerden des Kanals zeitgleich loslaufen.

Der Ablauf im Detail

1. **Kanal abhören**
   Die sendewillige Station prüft via Carrier Sense, ob das Übertragungsmedium aktuell frei von Funkverkehr ist.
2. **Inter-Frame Space abwarten**
   Bleibt das Medium für die Dauer des vorgeschriebenen Intervalls (DIFS bzw. AIFS) ununterbrochen frei, beginnt die Backoff-Phase.
3. **Zufallstimer dekrementieren**
   Der Backoff-Timer zählt in Slots herunter, solange der Kanal frei ist. Wird der Kanal belegt, friert der Zähler temporär ein.
4. **Datenrahmen übertragen**
   Erreicht der Zähler den Wert 0, sendet die Station ihren Frame ab und wartet nach SIFS auf das Empfangs-ACK.

4. Inter-Frame Spaces (IFS) & Priorisierung



Inter-Frame Spaces definieren exakte Schutzabstände zwischen Übertragungen. Unterschiedliche Wartezeiten erzeugen eine deterministische Priorisierung von Steuernachrichten.

- SIFS (Short Inter-Frame Space): Kürzester Abstand für zeitkritische Antworten wie ACKs, Clear-to-Send (CTS) und Polling-Antworten.
- PIFS (PCF Inter-Frame Space): Mittleres Intervall für koordinierte Zugriffe durch den Access Point bei zentralisierter Steuerung.
- DIFS (DCF Inter-Frame Space): Standard-Warteintervall für gewöhnliche Datenpakete im unkoordinierten Wettbewerbsbetrieb.
- EIFS (Extended IFS): Längstes Intervall, greift bei fehlerhaft oder unvollständig empfangenen Rahmen zur Neusynchronisation.



5. Das Problem der versteckten Station

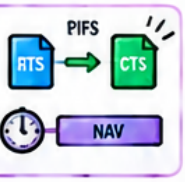


Das Hidden-Node-Problem entsteht, wenn zwei entfernte Stationen denselben zentralen Access Point erreichen, sich gegenseitig jedoch außerhalb der Funkreichweite befinden.

- Keine gegenseitige Erkennung: Station A und B hören einander nicht ab und stufen den Kanal als frei ein.
- Kollision am Access Point: Senden beide gleichzeitig an den AP, treffen die Wellenfronten zeitgleich ein und interferieren.
- Verdeckte Verluste: Ohne Gegenmaßnahme steigen Paketverlustrate und Retransmissions extrem an, was den Durchsatz einbrechen lässt.

Praxis-Konsequenz
Reines CSMA/CA versagt bei versteckten Stationen, da die Trägerprüfung (Carrier Sense) lokal fälschlicherweise Freigabe signalisiert.

6. RTS/CTS Mechanismus & NAV



Der 4-Wege-Handshake Request to Send / Clear to Send reserviert das Medium explizit vor der eigentlichen Nutzdatenübertragung über einen logischen Reservierungszähler.

- RTS-Anfrage: Sender schickt ein kurzes Kontrollpaket an den Empfänger mit Angabe der benötigten Sendedauer.
- CTS-Antwort: Empfänger sendet CTS zurück; alle Stationen im Umkreis des Empfängers hören diese Nachricht verbindlich mit.
- NAV (Network Allocation Vector): Lauschende Stationen setzen ihren internen virtuellen Timer auf "belegt" und schweigen.
- RTS-Schwellenwert (Threshold): Kurze Frames werden ohne RTS übertragen; große Frames nutzen den Overhead gezielt zur Kollisionsabsicherung.

Soll für ein Datenpaket der RTS/CTS-Handshake ausgelöst werden?

Paketgröße überschreitet den konfigurierten RTS-Threshold	Paketgröße liegt unterhalb des RTS-Thresholds
Initiiere RTS-Frame mit Sendedauer-Reservierung im Header und warte nach SIFS auf CTS vom Access Point.	Sende Nutzdatenrahmen direkt nach Ablauf von DIFS und Backoff-Timer ohne vorherige Kanalreservierung.

7. Koordinationsfunktionen: DCF vs. EDCA



Der IEEE 802.11 Standard differenziert zwischen reinem Zufallswettbewerb und Dienstgüte-gesteuerter Priorisierung nach Anwendungstypen.

- DCF (Distributed Coordination Function): Basis-Wettbewerbsverfahren, bei dem alle Stationen gleichberechtigt um Sendezeit konkurrieren.
- PCF (Point Coordination Function): Zentral gesteuertes Polling durch den AP (in der Praxis selten implementiert).
- EDCA (Enhanced Distributed Channel Access): QoS-Erweiterung (802.11e/WMM) mit vier Access Categories (Sprache, Video, Best Effort, Background).
- Differenzierte Parameter: Höher priorisierter Datenverkehr erhält kürzere AIFS-Wartezeiten und kleinere Contention Windows (CW).

8. Exponentieller Backoff & Retry-Limit



Bleibt eine Übertragungsbestätigung aus, greift ein deterministischer Backoff-Algorithmus zur schrittweisen Entlastung des Funkkanals.

- Contention Window (CW): Das Zufallsfenster startet bei CWmin (z. B. 15 oder 31 Zeitschlitzen) und wählt einen Zufallswert.
- Exponentielle Verdopplung: Bei jedem Fehlversuch ohne Empfang eines ACK verdoppelt sich das Fenster (CW = (CW + 1) * 2 - 1) bis zu CWmax.
- Retry Counter & Drop: Nach Überschreiten des maximalen Wiederholungslimits (Short/Long Retry Limit) wird der Rahmen verworfen und der Zähler zurückgesetzt.

Netzwerk-Diagnostik
Hohe Retransmission-Raten und anschwellende Contention Windows deuten direkt auf HF-Interferenzen oder verdeckte Stationen hin.

Aktueller CWmin / CWmax Wert der Schnittstelle

Konfigurierter RTS-Threshold (in Bytes)

Beobachtete Frame-Verlustrate / Retry-Rate (%)

WLAN-Sicherheit: WEP, WPA, WPA2 und WPA3-Verfahren

WLAN-Sicherheit: Funkverschlüsselung



1. WEP (Wired Equivalent Privacy)



- **Verschlüsselung:** RC4-Stromchiffre mit 40-Bit- oder 104-Bit-Schlüssel
- **Schwachstelle:** Zu kurzer 24-Bit-Initialisierungsvektor (IV) führt zu rascher IV-Wiederholung
- **Integrität:** CRC-32 ist linear und schützt nicht vor gezielten Paketmanipulationen
- **Status:** Veraltet und in wenigen Minuten per Airplay/Aircrack-ng entschlüsselbar

2. WPA & TKIP



- **TKIP:** Temporal Key Integrity Protocol mischt Paketschlüssel dynamisch
- **Schlüssellänge:** 128-Bit-Chiffrierschlüssel plus erweiterter 48-Bit-IV
- **Message Integrity Check:** Michael-Algorithmus zur Integritätsprüfung
- **Schwachstelle:** Beck-Tews- und Ohigashi-Kurokawa-Angriffe zeigten strukturelle Schwächen des TKIP-Designs

3. WPA2 & AES-CCMP



- **Verschlüsselung:** CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol)
- **Algorithmus:** Symmetrische Blockchiffre AES mit 128-Bit Schlüssellänge
- **Zwei Betriebsmodi:** WPA2-Personal (PSK) und WPA2-Enterprise (IEEE 802.1X/EAP)
- **Robustheit:** Datenübertragung gilt bei starkem AES als sicher

4. Schwachstellen im WPA2-Handshake



- **Offline-Wörterbuchangriff:** Passiver Mitschnitt des 4-Wege-Handshakes erlaubt Brute-Force-Attacken gegen schwache Passwörter
- **Deauthentifizierungs-Angriff:** Ungeschützte Management-Frames ermöglichen DoS und erzwungene Re-Authentifizierungen
- **KRACK (2017):** Key Reinstallation Attacks nutzten Fehlverhalten bei der Nonce-Wiederverwendung aus

5. WPA3-Personal & SAE



- **SAE-Verfahren:** Simultaneous Authentication of Equals ersetzt den fehleranfälligen PSK-Austausch
- **Protokollbasis:** Dragonfly-Key-Exchange (Zero-Knowledge-Proof-Mechanismus)
- **Forward Secrecy:** Schutz vergangener Sitzungen bei Schlüsselkompromittierung
- **Wörterbuchschutz:** Passwörter nicht mehr ohne Netzinteraktion offline durchprobierbar

6. WPA3-Enterprise & CNSA



- **Schlüssellängen:** 192-Bit-Sicherheitsmodus gemäß Commercial National Security Algorithm (CNSA) Suite
- **Verschlüsselung:** GCMP-256 (Galois/Counter Mode Protocol)
- **Integrität & Hashing:** GMAC-256 sowie HMAC-SHA-384 für Authentifizierung und Frame-Schutz
- **Management-Schutz:** Verbindlicher Einsatz von PMF

7. OWE (Enhanced Open)



- **Funktionsweise:** Verschlüsselung ohne vorherige Passworteingabe mittels Diffie-Hellman-Schlüsselaustausch
- **Schutz:** Verhindert passives Schnüffeln (Sniffing) im lokalen Funknetzwerk
- **Grenzen:** Keine gegenseitige Authentifizierung, Schutz vor Man-in-the-Middle-Angriffen erfordert zusätzliche Ebenen (z. B. TLS)

8. PMF & Migration



- **Schutzbereich:** Schützt Deauthentifizierungs-, Disassoziierungs- und Action-Frames
- **WPA3-Pflicht:** PMF ist unter WPA3 zwingend vorgeschrieben, bei WPA2 optional
- **Übergangsmodus:** WPA2/WPA3-Mixed-Mode erleichtert die Migration älterer Endgeräte, birgt jedoch Downgrade-Risiken

Praxis-Checkliste: WLAN-Sicherheitsaudit

Leitfaden zur Überprüfung und Absicherung von Funknetzwerken im Heimbereich oder Unternehmensnetzwerk.

1. **Schritt 1: Legacy-Verfahren deaktivieren**
   Im Access Point oder Controller prüfen, ob WEP und WPA/TKIP vollständig abgeschaltet sind. Reine AES-CCMP- oder SAE-Modi erzwingen.
2. **Schritt 2: PMF-Status konfigurieren**
   Protected Management Frames (802.11w) auf "Required" setzen, sofern alle Clients dies unterstützen, mindestens jedoch auf "Capable".
3. **Schritt 3: WPA3-Tauglichkeit der Clients evaluieren**
   Endgeräte auf Unterstützung für WPA3-Personal (SAE) prüfen. Mixed-Mode nur temporär für Altsysteme betreiben.
4. **Schritt 4: Gast- und offene Netze absichern**
   Öffentliche Zugänge von rein offenen SSIDs auf OWE (Enhanced Open) migrieren und Gastnetze per VLAN isolieren.

Welches Verfahren ist für das Zielnetzwerk optimal?

Modernes Netz mit aktuellen Endgeräten (ab ca. 2019/2020)	WPA3-Personal (SAE) Only aktivieren; PMF verbindlich erzwingen.
Heterogene Umgebung mit älteren Laptops/IoT-Geräten	WPA2/WPA3 Mixed Mode nutzen oder IoT-Geräte in ein separates WPA2-AES-VLAN auslagern.
Öffentlicher Hotspot ohne Zugangspasswort	OWE (Enhanced Open) konfigurieren, um Sniffing im Äther zu unterbinden.

Netzwerkzugangskontrolle mit IEEE 802.1X und EAP

1. GRUNDPRINZIP IEEE 802.1X

Portbasierte Netzzugangskontrolle sichert physische Switch-Ports und WLAN-Verbindungen gegen unautorisierten Zugriff ab.

- Blockiert Datenverkehr auf Layer 2 vor erfolgreicher Identitätsprüfung
- Trennt logisch den unkontrollierten vom kontrollierten Datenpfad
- Verhindert das unbefugte Anstecken fremder Hardware an Netzwerkdosen



2. DIE DREI KERNEROLLEN

Die 802.1X-Architektur verteilt Aufgaben strikt auf drei Instanzen.

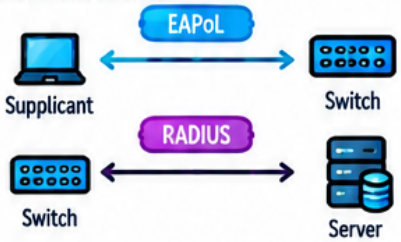
- Supplicant: Client-Endgerät mit Authentifizierungssoftware
- Authenticator: Switch oder WLAN-Access-Point als Gateway-Wächter
- Authentication Server: Zentraler RADIUS-Server zur Regelprüfung



3. EAP-TRANSPORTMEDIEN

Das Extensible Authentication Protocol wird über verschiedene Protokollstrecken transportiert.

- EAPoL (EAP over LAN): Kapselung zwischen Supplicant und Switch
- RADIUS (UDP 1812/1813): Kapselung zwischen Switch und Server
- Authenticator fungiert als Übersetzer ohne EAP-Paketinhalte zu öffnen



4. EAP-METHODEN IM VERGLEICH

Die Auswahl der Authentifizierungsmethode bestimmt Sicherheit und Zertifikatsaufwand.

- EAP-TLS: Höchste Sicherheit durch gegenseitige X.509-Zertifikate
- PEAP: TLS-Tunnel vom Server, Client nutzt Benutzername/Passwort
- EAP-TTLS: Flexibler Server-Tunnel mit diversen inneren Protokollen



5. SCHRITT-FÜR-SCHRITT ABLAUF

Chronologischer Ablauf einer erfolgreichen Netzwerkauthentifizierung:

1. **Verbindung & EAPoL-Start**
   Client verbindet sich physisch und sendet EAPoL-Start oder reagiert auf EAP-Request/Identity des Switches.
2. **Identitätsweiterleitung**
   Supplicant liefert Identität via EAPoL an den Switch; dieser leitet sie in einem RADIUS-Access-Request an den AAA-Server weiter.
3. **EAP-Verhandlung & Tunnel**
   Server fordert EAP-Methode an; Client und Server tauschen kryptografische Handshakes direkt über den Switch-Relay aus.
4. **Freigabe des Switch-Ports**
   Server sendet RADIUS-Access-Accept mit Sitzungsschlüsseln; Switch öffnet den Port für regulären IP-Datenverkehr.

6. RADIUS-POLICY-ZUWEISUNG

Nach erfolgreicher Prüfung steuert der RADIUS-Server dynamisch Netzwerkattribute.

- Dynamische VLAN-Zuweisung: Verschieben in Mitarbeiter- oder Gastnetze
- Downloadbare ACLs (dACLs): Portspezifische Filterregeln
- Sitzungsdauer-Begrenzung und periodische Re-Authentifizierung



7. FEHLERBEHANDLUNG & FALLBACK

Strategien für nicht authentifizierte oder inkompatible Geräte:

- Gast-VLAN: Internetzugriff ohne LAN-Ressourcenzugriff
- MAC Authentication Bypass (MAB): Fallback für Drucker und IoT
- Quarantäne-VLAN bei ungültigen Anmeldedaten oder Policy-Verstößen



MAB-Sicherheitshinweis
MAC-Adressen können gefälscht werden; MAB bietet geringeren Schutz als echte 802.1X-Zertifikate.

8. ZUSAMMENFASSUNG & PRAXIS-CHECK

Prüfkriterien für eine belastbare IEEE 802.1X-Infrastruktur im Unternehmensnetzwerk.

- RADIUS-Server hochverfügbar mit sekundärem Backup auslegen
- Client-Zertifikate über PKI und MDM automatisiert ausrollen
- Switch-Ports standardmäßig auf "Unauthorizod" konfigurieren
- Accounting (RADIUS Accounting) für lückenlose Audits aktivieren



Verwendete EAP-Methode im Netzwerk:

Konfiguriertes Fallback-Verfahren (z. B. Gast-VLAN / MAB):

IEEE 802.1X & EAP NETZWERKZUGANGS-KONTROLLE

WAN-TECHNOLOGIEN & MODEMS

1. LETZTE MEILE (LOCAL LOOP)



- Die sogeanante 'Letzte Meile' (Teilnehmeranschlussleitung / TAL) beschreibt den physischen Streckenabschnitt von der Vermittlungsstelle bzw. dem Kabelverteiler bis zum Gebäude des Endkunden.
- Traditionell verlegte Kupfer-Doppeladern der analogen Telefonie
- Starke Signaldämpfung und Übersprechen (Crosstalk) über zunehmende Leitungslänge
- Hoher Investitionsbedarf für den Austausch durch moderne optische Fasern

2. ADSL2+ & VDSL2 (KUPFER-BREITBAND)



- DSL nutzt vorhandene verdrillte Telefon-Kupferadern mit diskreter Mehrtonmodulation (DMT) oberhalb des Sprachfrequenzbandes.
- ADSL2+ (ITU G.992.5) arbeitet asymmetrisch mit bis zu 24 Mbit/s im Frequenzbereich bis 2,2 MHz.
- VDSL2 (ITU G.993.2) erweitert das Frequenzspektrum auf bis zu 30 MHz (Profil 30a) für Datenraten von bis zu 100 Mbit/s bei kurzen Leitungslängen.
- ADSL2+: Download bis 24 Mbit/s, Upload bis 1-3 Mbit/s, Spektrum bis 2,2 MHz
- VDSL2: Bis zu 100 Mbit/s symmetrisch/asymmetrisch über Bandprofile (z. B. 17a, 30a)
- Starke Abhängigkeit der Durchsatzrate von Entfernung und Leitungsquerschnitt

3. VECTORING & G.FAST (SUPERVECTORING)



- Vectoring (ITU G.993.5): Echtzeit-Messung und Auslöschung von Übersprechstörungen (Far-End Crosstalk) mittels Gegenphasensignalen (bis 100 Mbit/s)
- **Supervectoring 35b**: Frequenzbereich bis 35 MHz für Übertragungsraten von bis zu 300 Mbit/s
- **G.fast** (ITU G.9700/G.9701): Frequenzen bis 106 MHz bzw. 212 MHz für Gigabit-Raten auf sehr kurzen Kupferdistanzen (< 250 Meter)

4. KABELNETZE (DOCSIS)



- DOCSIS (Data Over Cable Service Interface Specification) nutzt das hybride Glasfaser-Koaxialnetz (HFC). Im Vergleich zu Telefonkabeln bieten Koaxialkabel eine hohe Schirmung und Bandbreite, teilen sich jedoch als Shared Medium die Übertragungsstrecke in Clustern.
- DOCSIS 3.0: Kanalbündelung (Channel Bonding) mehrerer 8-MHz-Kanäle für Hunderte Mbit/s
- DOCSIS 3.1: OFDM-Subträger und LDPC-Fehlerkorrektur für bis zu 10 Gbit/s Downstream
- DOCSIS 4.0 (Full Duplex / Extended Spectrum): Symmetrische Multi-Gigabit-Übertragung
- Architektur: CMTS (Cable Modem Termination System) am Kopfende steuert die Modems

5. FTTC, FTTB & FTTH (TOPOLOGIEN)



- Glasfaser-Ausbaustufen unterscheiden sich darin, wie nah die optische Faser an das Endgerät herangeführt wird und wo der Medienübergang auf Kupfer stattfindet.
- FTTC (Fiber to the Curb): Glasfaser bis zum Multifunktionsgehäuse/Kabelverzweiger am Straßenrand; Weiterführung über bestehende Kupfer-TAL mit VDSL2/Vectoring
- FTTB (Fiber to the Building): Glasfaser bis in den Gebäudekeller; interne Hausverteilung über G.fast, VDSL oder strukturiertes Ethernet.
- FTTH (Fiber to the Home): Durchgehende Glasfaserleitung bis in die Wohnung; optischer Abschluss direkt an der OTO-Dose (Optical Telecommunications Outlet)

6. PASSIVE OPTICAL NETWORKS (PON)



- PON (Passive Optical Networks) nutzen ungespeiste optische Splitter (Prismen), um ein Einzelfasersignal vom Hauptverteiler auf typischerweise 32 oder 64 Teilnehmeranschlüsse aufzuteilen.
- OLT (Optical Line Terminal): Zentrales Vermittlungssystem am Netzknoten des Anbieters
- Optischer Splitter: Rein passives Element ohne eigene Stromversorgung im Feld
- ONT/ONU (Optical Network Terminal/Unit): Modemeinheit beim Kunden zur Lichtsignal-Wandlung
- WDM (Wavelength Division Multiplexing): Getrennte Wellenlängen für Up- und Downstream

7. GPON VS. XGS-PON



- GPON (ITU-T G.984): Asymmetrisch mit 2,488 Gbit/s Downstream und 1,244 Gbit/s Upstream; Wellenlängen bei 1490 nm (Down) und 1310 nm (Up)
- XGS-PON (ITU-T G.9807.1): Vollständig symmetrisch mit 10 Gbit/s im Down- und Upstream
- Koexistenz: GPON und XGS-PON können über denselben passiven Splitter betrieben werden, da XGS-PON abweichende optische Fenster nutzt (1577 nm Down / 1270 nm Up)

8. ZUSAMMENFASSUNG & VERGLEICH



- Der WAN-Zugang bestimmt Bandbreite, Latenz und Stabilität der Internetanbindung. Während Kupfer-DSL durch Frequenzdämpfung stark reichweitenabhängig ist und Koaxialkabel typische Shared-Medium-Eigenschaften aufweisen, garantieren PON-Glasfasernetze Skalierbarkeit und Zukunftssicherheit über optische Multiplexverfahren.
- xDSL: Bewährtes Kupfernetz, bis 300 Mbit/s (Supervectoring), stark distanzabhängig
- DOCSIS: Breitbandiges HFC-Koaxnetz, bis Gigabit-Downstream, geteilte Kopfstellen-Bandbreite
- FTTH/PON: Durchgängige optische Faser, symmetrische Gigabit-Raten, minimale Latenzen

WAN-Architektur & Modems



Das Wide Area Network (WAN) bindet lokale Kundennetze (LANs) über Telekommunikationsinfrastrukturen an das weltweite Internet an. Während ein LAN digitale Rohdatenrahmen überträgt, fungiert das Zugangsmodem (Modulator/Demodulator) als Signalwandler für physikalische WAN-Trägermedien wie Zweidraht-Kupfer, Koaxialkabel oder Glasfasern.

- Demodulation und Modulation von Hochfrequenzsignalen an der Netzgrenze
- Wandlung analoger Hochfrequenzträger in standardisierte Ethernet-Frames (Schicht 2)
- Übergabepunkt zwischen Provider-Zugangsnetz und internem Teilnehmer-Router
- Breitbandanbindung über differenzierte physikalische Medien und Protokollstandards

Abgrenzung: Modem vs. Router

Das reine Breitbandmodem wandelt ausschließlich physikalische Leitungssignale in Ethernet-Frames um (OSI Schicht 1/2). Erst der nachgeschaltete IP-Router übernimmt Adressierung, NAT, Firewall und Routing (OSS Schicht 3).

WAN-Diagnose, Auswahlmatrix & Dokumentation

Praxis-Checkliste: WAN-Anschlussanalyse

Prüfen Sie bestehende WAN-Infrastrukturen und identifizieren Sie Technologie sowie Medienübergabepunkte vor Ort.

- Physische Anschlussdose ermitteln: TAE (Kupfer-Doppelader), BNC/Multimedia-Dose (Koax) oder OTO-Dose (LC/APC-Glasfaser)
- Hardware-Grenzstelle bestimmen: Reine Modembetriebsart (Bridge Mode) versus kombiniertes Integriertes Zugangsgerät (IAD)
- Technologie-Identifikation: VDSL2-Vectoring-Profil, DOCSIS-Kanalbündelung oder PON-Protokolltyp (GPON/XGS-PON)
- Signalgüte erfassen: Dämpfungswerte (dB), Signal-Rausch-Abstand (SNR) und unkorrigierbare Leitungsfehler (CRC)

Praxis-Tipp für Messungen

Prüfen Sie bei Performance-Problemen stets die Schicht-1-Verbindungswerte der Modemschnittstelle (SNR-Margin und Dämpfung), bevor Sie Fehler im lokalen LAN oder Router vermuten.

Technologie-Auswahlmatrix für WAN-Zugänge

Leitfaden zur Evaluierung des geeigneten WAN-Trägermediums anhand von Standortbedingungen und Durchsatzanforderungen.

- Verfügbarkeit der physischen Zuleitung im Gebäude prüfen
- Anforderungen an Symmetrie und Upload-Kapazität definieren
- Latenzempfindlichkeit für Echtzeitanwendungen und VPNs einbeziehen

Welche physische WAN-Anbindung erfüllt die Standortanforderungen?

FTTH/Glasfaser bis in die Räume verfügbar	Koaxialkabel (Kabelnetz) mit DOCSIS 3.1 vorhanden	Nur bestehende Kupfer-Doppelader (Telefonleitung) vorhanden
Einsatz von XGS-PON/GPON via ONT. Bietet höchste Ausfallsicherheit, minimale Latenz und symmetrische Bandbreiten bis zu 10 Gbit/s.	Kabelmodem-Installation. Kostengünstige Multi-Megabit-Downstreams; Upload und Latenz konnen in Spitzenzeiten variieren (Shared Medium).	VDSL2-Supervectoring oder G.fast Modem nutzen. Kurze Leitungslängen zum DSLAM für stabile Bandbreiten sicherstellen.

WAN-Infrastruktur Dokumentationsprotokoll

Verwenden Sie dieses strukturierte Protokoll zur Erfassung der WAN-Leitungsparameter und Hardwarekonfiguration an Ihrem Anschluss.

- Vollständige Erfassung der Schicht-1- und Schicht-2-Parameter
- Referenzwerte für spätere Störungsdiagnosen festhalten

WAN-Technologie (z. B. VDSL2 35b / DOCSIS 3.1 / XGS-PON)	
Modem-Typ & Seriennummer / PON-Modem-ID	
Leitungskapazität Downstream / Upstream (Soll vs. Ist in Mbit/s)	
Signal-Rausch-Abstand (SNR / Störabstandsmarge) & Leitungsdämpfung (dB)	
Netzabschluss-Schnittstelle (Bridge-Mode / VLAN-ID / PPPoE / IPoE)	

Traditionelle WAN-Protokolle: HDLC, PPP und PPPoE

1. WAN-Grundlagen & Punkt-zu-Punkt-Verbindungen



Punkt-zu-Punkt-Verbindungen bilden das Fundament klassischer Weitverkehrsnetze (WAN). Sie verbinden zwei dedizierte Router-Schnittstellen über serielle Leitungen, Glasfaser oder getunnelte Zugangsstrecken direkt miteinander, ohne dass Vermittlungsknoten auf Layer 2 kollidieren.

- **Dedizierte serielle Leitungen:** Feste Bandbreite zwischen exakt zwei Endpunkten ohne Medienkonflikte.
- **Schicht-2-Kapselung:** WAN-Frames packen Schicht-3-Pakete (z. B. IPv4/IPv6) für die physikalische Übertragung ein.
- **Fehlererkennung:** Zyklische Redundanzprüfung (CRC) stellt sicher, dass beschädigte Frames verworfen werden.
- **Protokollvielfalt:** Historische proprietäre Standards versus offene herstellerunabhängige Kapselungsverfahren.

2. High-Level Data Link Control (HDLC)



HDLC ist ein synchrones Schicht-2-Protokoll mit Bitorientierung. Während der ISO-Standard keine Mehrprotokollfähigkeit auf demselben Link vorsieht, fügt proprietäres Cisco-HDLC ein eigenes Typfeld hinzu.

- **Bit-Stuffing:** Verhindert Fehldeutungen des Flag-Begrenzers (01111110) durch automatisches Einfügen einer Null nach fünf Einsen.
- **Frame-Aufbau:** Flag (1 Byte), Adresse (1 Byte), Steuerung (1 Byte), Nutzdaten, Frame Check Sequence (FCS, 2–4 Bytes).
- **Herstellerbindung:** Cisco-HDLC ergänzt einen 2-Byte-Code für das Netzwerkprotokoll und ist inkompatibel zu Standard-HDLC anderer Hersteller.
- **Geringer Overhead:** Schlanker Protokollkopf ohne integrierte Authentifizierungs- oder dynamische Adressierungsfunktionen.

Interoperabilitätsfalle bei HDLC

Standard-HDLC unterstützt keine parallele Kapselung verschiedener Schicht-3-Protokolle auf einer Verbindung. Zwischen Geräten unterschiedlicher Hersteller scheitert HDLC häufig am proprietären Typfeld. Für herstellerübergreifende Links ist PPP erforderlich.

3. Point-to-Point Protocol (PPP) Architektur



PPP löste herstellerspezifische Beschränkungen ab. Es standardisiert eine modulare Architektur aus Rahmenkapselung, Link Control Protocol (LCP) und mehreren Network Control Protocols (NCP).

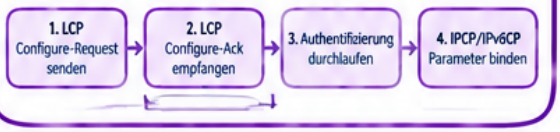
- **Herstellerunabhängiger RFC-Standard:** Garantiert Interoperabilität auf synchronen und asynchronen seriellen Schnittstellen.
- **Mehrprotokollfähig:** Transportiert simultan IPv4, IPv6, und Legacy-Protokolle über dieselbe physikalische Verbindung.
- **Verbindungsüberwachung:** Unterstützt Magic Numbers zur Schleifenerkennung und Link Quality Monitoring (LQM).
- **Geringer Overhead:** Schlanker mehrerer Leitungen (Multilink PPP) und hardwarenahe Compression direkt im Framing.

4. PPP-Phasen: LCP & NCP Aushandlung



Der Verbindungsaufbau bei PPP folgt einem strikten Zustandsautomaten. Erst nach erfolgreicher LCP-Parameterabstimmung und optionaler Authentifizierung konfigurieren die zuständigen NCPs die Schicht-3-Parameter.

- **Phase 1 - LCP Link Establishment:** Aushandlung von MTU/MRU, Erkennung geschlossener Schleifen und Wahl der Authentifizierungsmethode.
- **Phase 2 - Optionale Link-Qualitätsprüfung:** Messung der Leitungsstabilität vor Freigabe höherer Protokollschichten.
- **Phase 3 - Authentifizierung:** Identitätsprüfung via PAP oder CHAP vor Gewährung des Netzzugangs.
- **Phase 4 - NCP Konfiguration:** IPCP vergibt dynamisch IPv4-Adressen und DNS-Server; IPv6CP initialisiert Interface Identifier.



5. Authentifizierung: PAP versus CHAP



PPP bietet zwei standardisierte Authentifizierungsverfahren für Zugangskontrolle. Die Wahl des Mechanismus entscheidet über die Sicherheit gegen Abhören und Replay-Attacken auf der Leitungsstrecke.

- **PAP (Password Authentication Protocol):** Zweiter Handshake; überträgt Benutzername und Passwort unverschlüsselt im Klartext.
- **CHAP (Challenge Handshake Authentication Protocol):** Drei-Wege-Handshake mit Nonce, geheimem Schlüsseel und kryptografischem MDS-Hash.
- **Wiederholte Challenges:** CHAP kann während bestehender Sitzungen periodisch wiederholt werden, um Session Hijacking zu unterbinden.
- **Sicherheitsbewertung:** PAP gilt als unsicher bei kompromittierten Übertragungsmedien; CHAP schützt das Geheimnis vor passiven Sniffern.

Sicherheitsvergleich: PAP vs. CHAP

Verwenden Sie PAP ausschließlich bei Altgeräten ohne Krypto-Unterstützung. Bei CHAP verlässt das geteilte Kennwort niemals das Gerät; übertragen wird lediglich der Hash aus Challenge-Wert und Shared Secret.

6. PPPoE im Breitbandzugang (DSL/FTTx)



Point-to-Point Protocol over Ethernet (PPPoE, RFC 2516) tunnelt PPP-Pakete durch Ethernet-Broadcast-Frames. Es ermöglicht Internet-Service-Providern (ISPs), Authentifizierung, Abrechnung und IP-Zuweisung über geteilte Glasfaser- oder Kupfernetze abzuwickeln.

- **Ethernet-Kapselung:** Packt PPP-Frames in standardmäßige Ethernet-Frames mit EtherType 0x8863 (Discovery) und 0x8864 (Session).
- **MTU-Reduktion auf 1492 Bytes:** Der 8-Byte-PPPoE-Header verringert die nutzbare Standard-Ethernet-MTU von 1500 auf 1492 Bytes.
- **MSS Clamping:** Router müssen die TCP Maximum Segment Size auf typischerweise 1452 Bytes begrenzen, um Fragmentierungsprobleme zu verhindern.
- **Abrechnung & Rate-Limiting:** Ermöglicht RADIUS/AAA-gestützte Abrechnung und Bandbreitenkontrolle am Breitband-Zugangsserver (BRAS/BNG).

7. PPPoE Discovery- & Session-Aufbau



Vor dem eigentlichen Datenaustausch durchläuft PPPoE eine vierstufige Discovery-Phase zur Ermittlung der Server-MAC-Adresse und Zuweisung einer eindeutigen Sitzungs-ID.

- **PADI (PPPoE Active Discovery Initiation):** Client sendet Broadcast zur Suche nach verfügbaren Zugangsservern (Access Concentrator).
- **PADO (PPPoE Active Discovery Offer):** Ein oder mehrere Access Concentratoren antworten per Unicast mit ihren Dienstattributen.
- **PADR (PPPoE Active Discovery Request):** Client wählt einen Server aus und ferdert per Unicast den Start einer Session an.
- **PADS (PPPoE Active Discovery Session-confirmation):** Server bestätigt die Anfrage und vergibt die eindeutige Session-ID.
- **PADT (PPPoE Active Discovery Terminate):** Beendet eine aktive Session explizit von Client- oder Serrveseite.

8. Protokollvergleich & Praxis-Checkliste



Überprüfen Sie WAN- und Breitbandschnittstellen anhand technischer Kernparameter, um Fehlkonfigurationen bei MTU, Authentifizierung und Frame-Kapselung auszuschließen.

- **Kapselungsprüfung:** Kapselungsmodus auf Schnittstellenebene beidseitig identisch setzen (HDLC vs. PPP).
- **CHAP-Secret-Abgleich:** Gleicher Pre-Shared Key und passender Hostname auf lokalem und entferntem Router hinterlegt.
- **MTU/MSS-Audit:** Bei PPPoE-Schnittstellen IP MTU 1492 sowie **ip tcp adjust-mss** 1452 im Forwarding-Pfad validieren.
- **LCP/IPCP-Statuskontrolle:** Zustand "Open" für LCP und die jeweiligen NCPs in den Diagnosemeldungen verifizieren.

Gegenstellen-Hostname / Router-ID:

Konfigurierte Schicht-2-Kapselung (HDLC / PPP / PPPoE):

Authentifizierungsmethode & Status (None / PAP / CHAP):

Schnittstellen-MTU & TCP-MSS-Einstellung:

SD-WAN ARCHITEKTUR & KOMPONENTEN

1. GRUNDPRINZIP & ENTKOPPLUNG

Traditionelle WAN-Strukturen binden Weiterleitungsentscheidungen fest an physische Router. SD-WAN trennt Steuerungslogik von der Hardware.



- Ablösung manueller Router-Konfigurationen pro Standort
- Overlay-Netzwerk kapselt Datenverkehr über IPsec-Tunnel
- Agile Bereitstellung neuer Standorte ohne MPLS-Wartezeiten

2. CONTROL PLANE

Das logische Gehirn des SD-WAN. Verantwortlich für Routing-Tabellen, Verschlüsselungsschlüssel und Netzwerktopologie.



- Zentralisierte Steuerungseinheit (z. B. vSmart-Architektur)
- Verteilt Routing- und Sicherheitsrichtlinien an Edge-Geräte
- Entlastet lokale Router von komplexen Routing-Berechnungen

3. DATA PLANE (VEDGE / CEDGE)

Die Weiterleitungsebene vararbeitet und transportiert den produktiven Benutzerverkehr basierend auf Controllervorgaben.



- Physische oder virtuelle Router (vEdge / cEdge) an Standorten
- Paketprüfung, IPsec-Verschlüsselung und Hardware-Forwarding
- Laufende Messung von Paketverlust, Latenz und Jitter

4. MANAGEMENT & ORCHESTRIERUNG

Zentrale Schnittstellen für Administration, Bereitstellung und automatische Standort-Registrierung.



- Single Pane of Glass für Monitoring und Audit (z. B. vManage)
- Orchestrierungs-Instanz authentifizert Router (z. B. vBond)
- Automatisches Zero-Touch Provisioning (ZTP) für neue Knoten

5. TRANSPORTUNABHÄNGIGKEIT

Das Overlay nutzt parallele Verbindungen transparent und aggregiert Bandbreite flexibel über mehrere Provider.



- Gleichzeitige Nutzung von MPLS, Breitband-Internet und 4G/5G
- Kostenoptimierung durch Verlagerung unkritischer Lasten
- Vermeidung von Vendor-Lock-in einzelner Telekommunikationsanbieter

6. ANWENDUNGSBASIERTES ROUTING

Entscheidungen über den Verbindungsweg fallen in Echtzeit anhand von Anwendungstyp und Link-Qualitätswerten.



- Priorisierung latenzkritischer Daten (z. B. VoIP, Videokonferenzen)
- Dynamischer Failover bei Schwellwertüberschreitung von Jitter/Loss
- Direct Internet Access (DIA) für SaaS-Dienste wie Microsoft 365

7. INTEGRIERTE SICHERHEIT & IPSEC

Sicherer Transport über ungesicherte öffentliche Netze ohne zusätzliche Standalone-Appliances.



- Automatisierter Austausch von IPsec-Schlüsseln über Control Plane
- Zonale Next-Gen-Firewall und Segmentierung direkt am Edge
- Integrierte Filterung gegen Bedrohungen am Standort-Breakout

8. KURZE ZUSAMMENFASSUNG

SD-WAN ersetzt starre WAN-Konzepte durch programmierbare, transportunabhängige Netzwerke mit zentraler Kontrolle.



- Drei Ebenen: Management, Control Plane, Data Plane
- Höhere Zuverlässigkeit durch Multi-Transport-Redundanz
- Deutliche Kostensenkung gegenüber reinen MPLS-Strukturen

Zentrales Konzept: SD-WAN Architektur

Software-Defined WAN (SD-WAN) abstrahiert traditionelle Weitverkehrsnetze durch die Entkopplung von Kontroll- und Weiterleitungsebene. Anstelle starrer MPLS-Leitungen ermöglicht SD-WAN ein dynamisches, softwaregesteuertes Overlay-Netzwerk über beliebige Übertragungsmedien hinweg mit zentraler Richtlinienverwaltung.

- Entkopplung von Hardware und Routing-Intelligenz
- Dynamisches Overlay-Netzwerk über heterogene Transportwege
- Zentrale Richtlinienvergabe statt lokaler Box-by-Box-Konfiguration

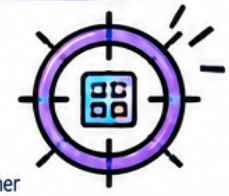


Architektur-Merksatz

Im SD-WAN entscheidet der zentrale Controller (Control Plane) über Routen und Pfade, während Router vor Ort (Data Plane) rein den tatsächlichen Paketversand ausführen.

SD-WAN BETRIEB: APPLICATION-AWARE ROUTING & PATH SELECTION

1. APPLICATION-AWARE ROUTING



Application-Aware Routing (AAR) identifiziert Netzwerkverkehr anhand konkreter Anwendungen statt reiner Ziel-IP-Adressen und Portnummern. Die Engine klassifiziert Pakete durch Deep Packet Inspection (DPI) und leitet Datenströme anhand anwendungsspezifischer Richtlinien weiter.

- Erkennung von SaaS-Diensten, VoIP und internen Workloads in Echtzeit
- Abkehr von statischen Routing-Tabellen hin zu geschäftsorientierten Policies
- Zuordnung von Prioritätsklassen zu geschäftskritischen Applikationen

2. SLA-MONITORING IM LAUFENDEN BETRIEB



SD-WAN-Edge-Router überwachen kontinuierlich die Qualität aller verfügbaren Transportverbindungen. Bidirektionale Messsonden ermitteln permanent Metriken, um Verletzungen definierter Service Level Agreements (SLA) sofort zu identifizieren.

- Latenz (One-Way / Round-Trip Time): Laufzeit von Datenpaketen
- Jitter: Schwankungen der Paketlaufzeit, entscheidend für Audio/Video
- Paketverlustrate: Prozentsatz verlorener Pakete je Messintervall

3. DYNAMIC PATH SELECTION (DPS)



Dynamic Path Selection wählt in Echtzeit den optimalen Pfad für jede Anwendungssitzung. Bei einer Leitungsverschlechterung schwenkt das System Datenströme unterbrechungsfrei auf alternative Verbindungen um.

- Nutzung heterogener WAN-Verbindungen (MPLS, Breitband-Internet, 4G/5G)
- Automatische Pfad-Auswahl anhand aktueller SLA-Erfüllung
- Vermeidung von Verbindungsabbrüchen bei Leitungsstörungen (Brownouts)

4. DIRECT INTERNET BREAKOUT (DIA)



Direct Internet Breakout ermöglicht Außenstellen den direkten Zugriff auf vertrauenswürdige Internet- und Cloud-Dienste, ohne den Datenverkehr über das zentrale Rechenzentrum umzuleiten.

- Entlastung teurer MPLS- und VPN-Kernverbindungen
- Signifikante Latenzreduktion für Microsoft 365, Webkonferenzen und Cloud-Apps
- Integrierte Sicherheitsüberprüfung am lokalen Edge-Knoten

5. CLOUD-ONRAMPING ARCHITEKTUREN



Cloud-Onramping bindet Außenstellen direkt und hochperformant an Public-Cloud-Umgebungen (AWS, Azure, GCP) und Cloud-Sicherheitsplattformen (SSE/SASE) an.

- Automatisierte Tunnelterminierung in virtuellen Cloud-Routern (vEdges)
- Optimaler Zugang zu SaaS-Gateways über nächstgelegene Cloud-PoPs
- Zentral überwerchte Ende-zu-Ende-Verschlüsselung bis in die Cloud VPCs

6. OVERLAY-TUNNELING & TRANSPORTUNABHÄNGIGKEIT



SD-WAN entkoppelt logische Netzwerkfunktionen von der physischen Infrastruktur. Das Overlay-Netzwerk nutzt IPsec- oder WireGuard-Tunnel über beliebig gemischte physische Underlay-Netze hinweg.

- Sichere Ende-zu-Ende-Verschlüsselung über ungesicherte öffentliche Netze
- Abstraktion des physischen Providers (carrier-neutrales Design)
- Zentral gesteuerter Schlüsselaustausch über die SD-WAN-Control-Plane

7. TRAFFIC-STEERING ENTSCHEIDUNGSMATRIX



Konfigurationslogik zur automatischen Pfadwahl nach Anwendungsanforderung:

- VoIP & Videokonferenzen: Primär MPLS; Fallback auf Internet-Overlay nur bei strikter Einhaltung von Jitter < 20 ms
- SaaS & Office-Tools: Bevorzugt Direct Internet Breakout (DIA); lokales Security-Filtering aktiv
- Batch-Backups & Dateitransfers: Günstiges Breitband-Internet ohne Echtzeit-SLA

BETRIEBSHINWEIS

Dämpfungszeiten (Hysterese) konfigurieren, um 'Flapping' – ständiges Hin- und Herschalten zwischen Leitungen bei Grenzwerten – wirksam zu verhindern.

8. KERNMETRIKEN



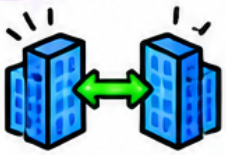
Intelligentes SD-WAN kombiniert Messung, Policy und flexible Tunnelarchitekturen, um Benutzererfahrung und Betriebseffizienz zu maximieren.

- Kontinuierliche BFD/SLA-Telemetrie steuert Pfadentscheidungen unterbrechungsfrei
- Direct Internet Breakout minimiert Latenzen und entlastet das Rechenzentrum
- IPsec-Overlay entkoppelt Sicherheit und Routing vom Underlay-Provider

VPN: ARCHITEKTUREN & PROTOKOLLE

1. SITE-TO-SITE

- Verbindet zwei feste Firmenstandorte oder Rechenzentren transparent miteinander.
- Router oder Security-Gateways terminieren den Tunnel auf beiden Seiten.



2. REMOTE ACCESS

- Ermöglicht einzelnen mobilen Endgeräten den gesicherten Zugriff auf das Unternehmensnetzwerk.
- Erfordert Client-Software oder TLS-fähigen Webbrowser.
- Strikte Authentifizierung (oft via 2FA/MFA).



3. OVERLAY- VS. UNDERLAY-MODELL

- Underlay: Öffentliches Internet oder Provider-Routing (reiner Transport).
- Overlay: Geschütztes virtuelles Subnetz mit eigenen Routing-Tabellen.
- Unabhängigkeit: Interne Netzstrukturen bleiben nach außen verborgen.



4. L2 VS. L3 TUNNELING

- Layer 2 (z. B. L2TP, VXLAN): Überträgt komplette Ethernet-Frames, unterstützt Non-IP und Broadcasts.
- Layer 3 (z. B. IPsec, WireGuard): Routet IP-Pakete direkt, höhere Effizienz und Skalierbarkeit.



5. IPSEC

- Besteht aus IKEv2 (Schlüsselaustausch), ESP (Verschlüsselung) und AH (Authentifizierung).
- Zwei Modi: Transport- und Tunnelmodus.
- Universell einsetzbar, jedoch komplex in Konfiguration und NAT-Traversal.



6. SSL / TLS

- Nutzung von TCP/UDP-Ports wie Port 443; durchdrjngt Firewalls problemlos.
- OpenVPN als modularer Standardclient; clientlose Varianten im Browser.
- Feingranulare Zugriffskontrolle auf einzelne Webapplikationen.



7. WIREGUARD

- Fest definierte moderne Kryptografie-Primitives (z. B. ChaCha20-Poly1305, Curve25519).
- Betrieb im Linux-Kernelspace für minimalen Overhead.
- Einfaches Konfigurationsmodell mit Public-Key-Routing.



8. GRE

- Erlaubt den Transport von Multicast- und dynamischem Routing-Traffic (z. B. OSPF/BGP).
- Keine native Verschlüsselung oder Authentifizierung (Klartext).
- Wird häufig mit IPsec kombiniert (GRE-over-IPsec).





ENTSCHEIDUNGSMATRIX: VPN-ARCHITEKTUR WÄHLEN

Leitfaden zur zielgerichteten Auswahl der geeigneten Topologie und des Protokolls für spezifische Netzwerkanforderungen.

1 Bedarfsanalyse Standort vs. Endgerät
Definieren Sie, ob zwei Rechenzentren gekoppelt werden (Site-to-Site) oder Endgeräte ins Netz gelangen sollen (Remote Access).

2 Routing- und Protokollprüfung
Bestimmen Sie, ob Routingprotokolle (GRE nötig) oder reine IP-Nutzlast (IPsec/WireGuard) transportiert werden.

3 Sicherheits- und Performanceabwägung
Wählen Sie WireGuard für maximale Performance, IPsec für klassische Enterprise-Gateways und SSL/TLS für restriktive Netze.

Geplantes Einsatzszenario (z. B. Home-Office-Anbindung)	Gewählte Topologie (Site-to-Site oder Remote Access)	Ausgewähltes Protokoll und Begründung

Welche primäre Anforderung bestimmt Ihr VPN-Szenario?

Feste Verbindung zweier Unternehmensstandorte mit Firewall-Routern	Setzen Sie auf ein Site-to-Site IPsec-VPN im Tunnelmodus oder GRE-over-IPsec bei dynamischem Routing.
Mobile Außendienst-Laptops hinter restriktiven Hotel- und Gast-Firewalls	Wählen Sie ein TLS/SSL-basiertes Remote-Access-VPN über Port 443 oder einen verwalteten WireGuard-Client.
Übertragung von Layer-2-Broadcasts oder Nicht-IP-Frames über weite Strecken	Nutzen Sie Layer-2-Tunneling (L2TP/bridged VPN) unter Berücksichtigung des erhöhten MTU-Overheads.

GRE & DMVPN

Overlay-Tunneling & Multipoint-Skalierung



1. GRUNDLAGEN VON GRE



Generic Routing Encapsulation (GRE, RFC 2784) ist ein universelles Tunneling-Protokoll zur Kapselung verschiedener Netzwerkprotokolle in Standard-IP-Pakete.

- **Protokoll-Typ:** IP-Protokollnummer 47 (direkt auf IP-Ebene aufgesetzt)
- **Overhead:** Fügt 24 Byte hinzu (20 Byte neuer Outer-IP-Header + 4 Byte GRE-Header)
- **Punkt-zu-Punkt:** Standard-GRE verbindet exakt zwei Endpunkte über statische IP-Adressen
- **Keine native Verschlüsselung:** GRE überträgt Nutzdaten und Header im Klartext

2. ROUTING-TRANSPORT & MULTICAST



Ein Hauptvorteil von GRE gegenüber reinem IPsec-Tunnelmodus ist die native Unterstützung für Routing-Protokolle und Multicast-Verkehr.

- **Multicast-Unterstützung:** Erlaubt den Transport von Hello-Paketen für Routing-Nachbarschaften
- **Protokollunabhängig:** Transportiert OSPF, EIGRP, BGP sowie IPv6 über reine IPv4-Netze
- **Overlay-Routing:** Trennt logische Netzwerktopologie (Tunnel) von der physischen Transportebene
- **Kombination mit IPsec:** GRE-over-IPsec ermöglicht Routing-Updates bei vollständiger Verschlüsselung

3. DMVPN-ARCHITEKTUR



Dynamic Multipoint VPN (DMVPN) skaliert Punkt-zu-Punkt-GRE-Verbindungen zu einer flexiben Hub-and-Spoke- oder Spoke-to-Spoke-Architektur.

- **Hub-and-Spoke:** Zentrale Kopfstelle (Hub) verwaltet dynamische Tunnel zu verteilten Niederlassungen (Spokes)
- **Skalierbarkeit:** Spokes benötigen nur eine Tunnel-Schnittstelle und statische Hub-Informationen
- **Direkte Verbindungen:** Spoke-to-Spoke-Tunnel bauen sich bei Bedarf dynamisch auf und wieder ab
- **Konfigurationsreduktion:** Kein manueller n*(n-1)/2 Tunnel-Aufwand im gesamten Mesh-Netz

4. MULTIPOINT GRE (mGRE)



Multipoint GRE ermöglicht es einer einzelnen physischen Schnittstelle, mehrere GRE-Tunnel gleichzeitig zu terminieren.

- **Single-Interface-Prinzip:** Ein einziges Tunnel-Interface bedient mehrere entfernte Gegenstellen
- **Dynamische Zielauflösung:** Ziel-IP wird nicht statisch im Interface verdrahtet, sondern via NHRP ermittelt
- **Ressourcenschonung:** Reduziert IP-Subnetz-Verbrauch und Schnittstellenanzahl drastisch
- **Broadcast/Multicast-Handling:** Erlaubt Pseudobroadcast-Replikation für dynamische Routingprotokolle

5. NHRP (NEXT HOP RESOLUTION PROTOCOL)

Das Next Hop Resolution Protocol (RFC 2332) fungiert als dynamisches Adressbuch für DMVPN-Umgebungen.

- **Adress-Mapping:** Ordnet private Tunnel-IP-Adressen den öffentlichen Transport-IPs zu
- **NHRP Registration:** Spokes melden ihre aktuelle öffentliche IP beim Start an den Hub (NHS)
- **NHRP Resolution:** Spokes fragen den Hub nach der echten IP anderer Spokes für direkte Kommunikation
- **Client/Server-Modell:** Hub agiert als Next Hop Server (NHS), Spokes agieren als Next Hop Clients (NHC)



6. DMVPN-PHASEN 1 BIS 3

DMVPN entwickelte sich in drei Architekturschritten mit zunehmender Flexibilität und Routing-Optimierung.

- **Phase 1:** mGRE nur auf Hub, Spokes nutzen Standard-GRE; gesamter Datenverkehr läuft über Hub
- **Phase 2:** mGRE auf Hub und Spokes; dynamische Spoke-to-Spoke-Tunnel, Routing-Informationen bleiben erhalten
- **Phase 3:** NHRP-Redirect und NHRP-Shortcut; optimale Spoke-to-Spoke-Pfade ohne Routingtabellen-Überlastung



7. SICHERHEIT & ABSICHERUNG (IPsec)



Da weder GRE noch DMVPN über eigene Verschlüsselung verfügen, ist der Schutz über IPsec essenziell.

- **IPsec Protection:** Anbindung via IPsec-Profile direkt an das virtuelle mGRE-Tunnel-Interface
- **Transportmodus:** Spart 20 Byte Overhead, da GRE bereits einen neuen IP-Header bereitstellt
- **Authentifizierung:** Zertifikate oder Pre-Shared Keys sichern Registrierung und Paketaustausch ab
- **Crypto Maps überflüssig:** Dynamisches IPsec-Profil schützt jeden entstehenden dynamischen Tunnel

Achtung: MTU und Fragmentierung

GRE (24 Byte) und IPsec (ca. 50-70 Byte) reduzieren die effektive Nutzlastgröße (MSS/MTU). Zur Vermeidung von Paketfragmentierung muss 'ip mtu 1400' und 'ip tcp adjust-mss 1360' auf Tunnelinterfaces konfiguriert werden.

8. ZUSAMMENFASSUNG & BEST PRACTICES



GRE und DMVPN bilden das Rückgrat moderner softwaredefinierter Weitverkehrsnetze und hybrider WAN-Strukturen.

- GRE kapselt Routingprotokolle, liefert jedoch keinerlei Vertraulichkeit oder Datenintegrität
- DMVPN vereint mGRE, NHRP und IPsec zu einer hochgradig skalierbaren Mehrendpunkt-VPN-Architektur
- NHRP löst die Zuordnung von logischen Tunnel-IPs zu dynamischen öffentlichen IP-Adressen
- Optimale Dimensionierung von MTU und MSS verhindert Performance-Einbußen durch Fragmentierung

Mindmap: IPsec-Architektur (AH, ESP und Sicherheitsassoziationen)

IPSEC-ARCHITEKTUR: SCHICHT-3-SICHERHEIT

AH, ESP, SAs & MODI

1. GRUNDLAGEN DER IPSEC-ARCHITEKTUR



IPsec (Internet Protocol Security) schützt IP-Pakete direkt auf Vermittlungsebene (Schicht 3). Es stellt Vertraulichkeit, Integrität und Replay-Schutz für alle darüberliegenden Schichten bereit.

- **Schicht-3-Absicherung:** Schützt beliebige Transportprotokolle wie TCP und UDP transparent ohne Anpassung von Anwendungsprogrammen.
- **Sicherheitsdienste:** Datenursprungsauthentifizierung, Schutz vor unbefugter Modifikation und optionale kryptografische Verschlüsselung.
- **Standard-Architektur:** Definiert durch RFC-Standards als modulares Framework für moderne VPNs.

PRAXIS-HINWEIS
Da IPsec auf Schicht 3 arbeitet, müssen Endanwendungen nicht modifiziert werden, um von Verschlüsselung und Integritätsschutz zu profitieren.

2. AUTHENTICATION HEADER (AH)



Das Protokoll AH (IP-Protokollnummer 51) garantiert Paketintegrität und Herkunftsbeglaubigung, bietet jedoch keine Nutzdatenverschlüsselung.

- **Integritätsnachweis:** Verifiziert den IP-Payload und unveränderliche Header-Felder über einen kryptografischen Hash (ICV).
- **Keine Vertraulichkeit:** Nutzdaten verbleiben im Klartext lesbar und werden nicht verschlüsselt übertragen.
- **NAT-Inkompatibilität:** Scheitert bei Netzwerkadressübersetzung (NAT), da veränderte IP-Adressen den Prüfwert ungültig machen.

3. ENCAPSULATING SECURITY PAYLOAD (ESP)



ESP (IP-Protokollnummer 50) bietet neben Integrität und Authentifizierung vor allem Vertraulichkeit durch die symmetrische Verschlüsselung des Payloads.

- **Verschlüsselung:** Kapselt und verschlüsselt die Datenlast mit modernen Algorithmen wie AES-GCM oder ChaCha20-Poly1305.
- **Integrität & Herkunft:** Authentifiziert den verschlüsselten Nutzdatenbereich sowie den ESP-Header mittels Integritätsprüfwert.
- **Praxisstandard:** Bildet die primäre Säule moderner Site-to-Site- und Remote-Access-Tunnelarchitekturen.

4. SICHERHEITSASSOZIATIONEN (SA) & DATENBANKEN



Eine Security Association (SA) bildet den vertraglichen Sicherheitskontext mit Schlüsseln, Algorithmen und Parametern für eine gerichtete Kommunikation.

- **Einbahnstraße:** Für eine bidirektionale Duplex-Verbindung sind mindestens zwei eigenständige SAs (Inbound/Outbound) zwingend nötig.
- **SAD (Security Association Database):** Verwaltet aktive kryptografische Parameter, Sequenznummern und Schlüssel pro Verbindung.
- **SPD (Security Policy Database):** Bestimmt anhand von Paket-Selektoren, ob Traffic verworfen, ungeschützt weitergeleitet oder via IPsec verarbeitet wird.

5. SECURITY PARAMETER INDEX (SPI) & REPLAY-SCHUTZ



Der SPI ist ein 32-Bit-Identifikator im IPsec-Header, der gemeinsam mit der Ziel-IP und dem Protokoll eine eindeutige Zuordnung zur aktiven SA herstellt.

- **32-Bit-Selektor:** Ermöglicht dem Empfänger das blitzschnelle Nachschlagen der korrekten Entschlüsselungs- und Prüfparameter in der SAD.
- **Anti-Replay-Fenster:** Eine monoton steigende 32-Bit- oder 64-Bit-Sequenznummer verhindert das Wiedereinspielen abgefangener Pakete.ung.
- **Sliding-Window:** Empfänger prüft anhand eines Gleitfensters, ob eintreffende Sequenznummern bereits verarbeitet oder zu alt sind.

6. TRANSPORTMODUS VS. TUNNELMODUS



IPsec operiert in zwei Betriebsarten, die bestimmen, wie Original-Header und Nutzdaten gekapselt und im Netz geroutet werden.

- **Transportmodus:** Schützt primär End-to-End-Verbindungen zwischen zwei Hosts; der ursprüngliche IP-Header bleibt unverändert sichtbar.
- **Tunnelmodus:** Kapselt das komplette Original-IP-Paket in einen neuen äußeren IP-Header; typisch für Gateway-zu-Gateway-VPNs.
- **Overhead:** Der Tunnelmodus erzeugt durch den zusätzlichen äußeren Header mehr Protokolloverhead, verbirgt aber interne Netztopologien.

Welcher IPsec-Modus muss für das vorliegende Szenario konfiguriert werden?

Zwei Standort-Gateways verbinden private Subnetze über ein öffentliches Netz	Tunnelmodus einsetzen: Vollständige Kapselung der internen Original-IP-Pakete mit neuem öffentlichen Gateway-Header.
Zwei bekannte Endgeräte kommunizieren direkt miteinander ohne Subnetz-Maskierung	Transportmodus einsetzen: Ursprünglicher IP-Header bleibt erhalten, ESP/AH wird direkt zwischen IP und Transport-Header eingefügt.

7. SCHLÜSSELAUSTAUSCH VIA IKE (IKEV1 / IKEV2)



Internet Key Exchange (IKE) automatisiert die Authentifizierung und das Aushandeln kryptografischer Schlüssel für die SAs über UDP-Port 500 und 4500.

- **Phase 1 / IKE SA:** Authentifiziert Gegenstellen und etabliert einen geschützten Verwaltungskanal (Diffie-Hellman-Schlüsseltausch).
- **Phase 2 / Child SA:** Handelt unter Schutz der ersten Phase die konkreten unidirektionalen IPsec-SAs für Nutzdatenverbindungen aus.
- **IKEv2-Vorteile:** Signifikant reduzierter Handshake-Overhead, integrierte NAT-Traversal-Unterstützung und höhere Stabilität bei IP-Wechseln.

IKEv2 STANDARD
IKEv2 ersetzt veraltetes IKEv1 weitestgehend, da es Latenzen im Handshake minimiert und NAT-Traversal (NAT-T via UDP 4500) direkt unterstützt.

8. PRÜF- UND ANWENDUNGSCHECKLISTE IPSEC



Leitfaden zur strukturierten Fehleranalyse, Konfiguration und Parameterprüfung bei IPsec-Verbindungen in der Netzwerkpraxis.

- **Protokollfreigabe in Firewalls:** Sicherstellen, dass ESP (IP 50), AH (IP 51) und IKE (UDP 500 / UDP 4500) passieren dürfen.
- **Übereinstimmende Parameter:** Identische Verschlüsselungsschiffren, Hash-Verfahren, Diffie-Hellman-Gruppen und Lifetime-Werte beider Gegenstellen.
- **MTU und MSS berücksichtigen:** Kapselungsoverhead erfordert oft Anpassung der TCP-MSS (Maximum Segment Size), um Paketfragmentierung zu vermeiden.

Welches Blackhole-Umgebung entsprechende Szenario konfiguriert werden?

Zwei Standort-Gateways verbinden private Subnetze über ein öffentliches Netz	Tunnelmodus einsetzen: Vollständige Kapselung der internen Original-IP-Pakete mit neuem öffentlichen Gateway-Header.
Zwei bekannte Endgeräte kommunizieren direkt miteinander ohne Subnetz-Maskierung	Transportmodus einsetzen: Ursprünglicher IP-Header bleibt erhalten, ESP/AH wird direkt zwischen IP und Transport-Header eingefügt.

8. PRÜFMRT: ANWENDUNGSCHECKLISTE IPSEC



Und Parameterprüfung bei IPsec-Verbindungen in der Netzwerkpraxis. Gemäß [illegible]

- **Protokollfreigabe in Firewall:** [illegible] (IP 51) und IKE (UDP 500 oder Sicherstellen, passieren dürfen.
- **Übereinstimmende Parameter:** identische Verschlüsselungschiffren, Hash-Verfahren, Diffie-Hellman-Gruppen und Lifetime-Werte beider Gegenstellen.
- **MTU [illegible]:** Kapselungsoverhead erfordert oft Anpassung der TCP-MSS (Maximum Segment Size), um

MTU/MSS Blackhole Vermeidung
Tunnel-Overhead vergrößert Pakete über das typische Ethernet-MTU-Limit von 1500 Bytes hinaus. Reduzieren Sie die MSS am Gateway auf ca. 1360-1400 Bytes.

Gegenstellen-IP & Tunnelmodus (Tunnel vs. Transport):

Verwendetes Protokoll (ESP / AH) & Verschlüsselungsalgorithmus:

Aushandlungsstatus (IKE-SA aktiv / Child-SA SPI-Werte):

Angewandte Firewall-Regeln (UDP 500, UDP 4500, IP 50):

IPsec-Schlüsselaustausch: IKEv1 vs. IKEv2 Aushandlungsphasen

1. GRUNDPRINZIP INTERNET KEY EXCHANGE (IKE)

Das IKE-Protokoll automatisiert die sichere Authentifizierung und Schlüsselverwaltung für IPsec-Tunnel über UDP-Port 500 und 4500.



- Dynamische Schlüsselaushandlung statt statisch hinterlegter Vorab-Schlüssel
- Aufbau von Security Associations (SAs) mit kryptografischen Parametern
- Nutzung von UDP-Port 500 (Basis) und UDP 4500 für NAT-Traversal

PRAXIS-HINWEIS
Ohne NAT-Traversal (NAT-T) blockieren Router mit Adressübersetzung IPsec-Pakete häufig aufgrund modifizierter IP-Header.

2. IKEV1 PHASE 1: DER MANAGEMENT-TUNNEL

Phase 1 etabliert den geschützten IKE-SA-Kanal zur sicheren Übertragung nachfolgender Kontrollnachrichten.

- Main Mode: 6 Pakete im bidirektionalen Austausch mit voller Identitätsverschleierung
- Aggressive Mode: 3 Pakete für schnellen Verbindungsaufbau, überträgt Identitäten unverschlüsselt
- Vereinbarung von Verschlüsselung, Hash-Funktion, Authentifizierungsmethode und DH-Gruppe



3. DIFFIE-HELLMAN-GRUPPEN (DH)

Diffie-Hellman berechnet ein gemeinsames Geheimnis über ein unsicheres Medium, ohne dass der geheime Schlüssel selbst übertragen wird.



- DH-Gruppe 1 (768 Bit) und DH-Gruppe 2 (1024 Bit) gelten heute als kryptografisch unsicher
- DH-Gruppe 14 (2048 Bit) bildet den modernen Mindeststandard für klassische Modulare Exponentialverfahren
- DH-Gruppen 19, 20 und 21 setzen auf elliptische Kurven (ECDH) mit höherer Effizienz und Sicherheit

SICHERHEITSWARNUNG
Vermeiden Sie DH-Gruppen kleiner als 14 (unter 2048 Bit Schlüssellänge), um Downgrade-Angriffe auszuschließen.

4. KRYPTOGRAFISCHE SUITES IM TUNNEL

Jede Sicherheitsassoziation kombiniert vier algorithmische Kernfunktionen zu einer verbindlichen Cipher Suite.

- Symmetrische Verschlüsselung: AES-CBC (128/256 Bit) oder modernes AES-GCM
- Integritätsprüfung: HMAC-SHA-256 oder im AEAD-Verfahren durch AES-GCM integriert
- Authentifizierung: Pre-Shared Keys (PSK) für einhache Setups oder digitale RSA/ECDSA-Zertifikate



5. IKEV1 PHASE 2: QUICK MODE

Im Quick Mode handeln die Tunnel-Endpunkte die eigentlichen IPsec-SAs für den Nutzdatentransport (ESP/AH) aus.

- Austausch von exakt 3 verschlüsselten Paketen innerhalb der bestehenden Phase-1-SA
- Festlegung von Traffic-Selektoren (Subnetze, Host-Adressen, Quell- und Zielports)
- Optionales Perfect Forward Secrecy (PFS) über erneuten DH-Austausch für frische Sitzungsschlüssel



6. IKEV2: INITIAL-AUSTAUSCH (IKE_SA_INIT & IKE_AUTH)

IKEv2 ersetzt die komplexen Phase-1/2-Modi durch einen standardisierten, kompakten 4-Pakete-Austausch.

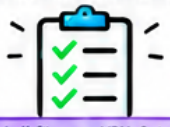
- IKE_SA_INIT (2 Pakete): Aushandlung kryptografischer Parameter und DH-Schlüsseltausch unverschlüsselt
- IKE_AUTH (2 Pakete): Verschlüsselte Authentifizierung der Endpunkte und Erstellung der ersten Child-SA
- Halbiert die Latenzzeit des Tunnelaufbaus gegenüber dem klassischen IKEv1 Main Mode



7. PROTOKOLLVERGLEICH & MOBILITY

IKEv2 behebt fundamentale Schwächen von IKEv1 und optimiert die Verbindung für dynamische Netze.

- Integriertes NAT-Traversal ohne separate Erweiterungs-Aushandlung
- MOBIKE-Unterstützung (RFC 4555) für unterbrechungsfreie IP-Wechsel bei mobilen Endgeräten
- Eingebaute Anti-DDoS-Cookies gegen Denial-of-Service auf den Schlüsselaustausch



Welches Protokoll für neue VPN-Gateways wählen?

- Gegenstelle unterstützt moderne Standards und dynamische Clients → Konfigurieren Sie IKEv2 mit MOBIKE und AES-GCM für maximale Stabilität und Effizienz.
- Legacy-Gegenstelle zwingt älteren Softwarestand → Nutzen Sie IKEv1 ausschließlich im Main Mode mit DH-Gruppe >= 14 und aktiver PFS.

8. DIAGNOSE & STATUS-CHECK

Verifizierung des Tunnelstatus auf Firewall- und Router-Konsolen zur Fehlerbehebung.

- Prüfung der aktiven Phase-1/IKE-SA auf beiden Peers
- Verifikation der Child-SA/Phase-2-Security Associations
- Analyse von Paketencapsulation und Drop-Countern

TYPISCHER FEHLER
Mismatch in Phase-2-Traffic-Selektoren oder DH-Gruppen führt zu hängendem Verbindungsaufbau ohne Klartext-Fehlermeldung.

DURCHFÜHRUNG

1. Phase-1-Aushandlung prüfen
2. Phase-2-Child-SAs verifizieren
3. Traffic und Drop-Counter beobachten

TESTFELDER

Gegenstellen-IP / FQDN:

Genutzte DH-Gruppe & Verschlüsselungssuite:

Festgestellter SA-Status & Notizen:

SSL/TLS & WIREGUARD VPN

1. GRUNDPRINZIP: SSL/TLS-VPN

SSL/TLS-VPNs nutzen Transport Layer Security zur Absicherung des Netzwerkverkehrs.



- Arbeitet typischerweise auf Schicht 4/5 des Netzwerkmodells.
- Nutzung von Port 443 ermöglicht problemloses Passieren von Firewalls.
- Verschlüsselt TCP- oder UDP-Sitzungen mit asymmetrischem Schlüsselaustausch.
- Weit verbreitet für flexible Fernzugriffe (Remote Access).

2. CLIENTLESS VS. CLIENT-BASIERT

Zwei grundlegende Betriebsmodi bestimmen Reichweite und Funktionsumfang.



- Clientless (Web-VPN): Zugriff via Standard-Browser via HTTPS/NTMLS.
- Clientless begrenzt auf Web-Apps und definierte Port-Weiterleitungen.
- Client-basiert: Installierter Agent stellt virtuelle TUN/TAP-Netzwerkkarte bereit.
- Client-basiert routet vollständigen Subnetz- und IP-Verkehr transparent.

3. OPENVPN TUNNELBETRIEB

OpenVPN ist der bekannteste quelloffene Vertreter für TLS-gesicherte Tunnel.



- Unterstützt TUN (Layer 3 Routing) und TAP (Layer 2 Ethernet-Bridging).
- Wahlweise über TCP (hohe Stabilität bei Firewalls) oder UDP (geringere Latenz).
- TCP-over-TCP-Problem vermeiden: Paketverlust führt zu doppelter Flusskontrolle.
- Authentifizierung über X.509-Zertifikate, TLS-Auth oder Benutzertoken.

4. WIREGUARD ARCHITEKTUR

WireGuard bietet eine moderne, schlanke Alternative zu klassischen VPNs.



- Direkte Implementierung im Linux-Kernel für minimalen Kontextwechsel.
- Nur ca. 4.000 Codezeilen erleichtern Audits und reduzieren Angriffsfläche.
- Verbindungsloser Tunnelbetrieb auf Basis fester UDP-Pakete.
- Zustandsloses Verbindungsmodell mit extrem schnellem Roaming.

5. WIREGUARD KRYPTOGRAFIE

Feste, moderne Krypto-Suite ohne unsichere Verhandlungsphasen (Cipher Agility).



- Noise Protocol Framework: Schlankes 1-RTT-Handshake-Modell.
- Curve25519: Elliptische Kurven für schnellen ECDH-Schlüsselaustausch.
- ChaCha20-Poly1305: Authentifizierte symmetrische AEAD-Verschlüsselung.
- BLAKE2s: Extrem schnelle kryptografische Hashfunktion.

6. CRYPTOKEY ROUTING

WireGuard verknüpft öffentliche Schlüssel direkt mit erlaubten IP-Adressen.



- AllowedIPs definiert Routing-Tabelle und Filter für jeden Peer.
- Ausgehend: Ziel-IP wählt Peer anhand des AllowedIPs-Bereichs.
- Eingehend: Paket wird verworfen, falls Quell-IP nicht zum Schlüssel passt.
- Eliminiert komplexe Firewall-Regelwerke innerhalb des Tunnel-Treibers.

7. PERFORMANCEVERGLEICH

Strukturelle Unterschiede wirken sich massiv auf Durchsatz und Latenz aus.



- WireGuard: erzielt nahezu Leitungsgeschwindigkeit durch Kernel-Optimierung.
- OpenVPN im Userspace erfordert ständige Kontextwechsel (TUN-Device).
- Verbindungsaufbau bei WireGuard erfolgt in Millisekunden statt mehreren Sekunden.
- Geringerer Akkuverbrauch auf Mobilgeräten bei WireGuard durch Ruhemodus ohne Keepalive-Spam.

8. ENTSCHEIDUNGSMATRIX & PRAXIS

Auswahl des passenden VPN-Typs abhängig von Infrastruktur und Einsatzzweck.



- WireGuard: Ideal für Site-to-Site, Server-Mesh und mobile Clients.
- SSL/TLS (OpenVPN): Bevorzugt bei strikten Proxies oder reinen Browser-Portalen.
- Keine veralteten Cipher-Suites pflegen, sondern Standardvorgaben härten.
- Zero-Trust-Zonierung auch hinter dem VPN-Gateway aufrechterhalten.

Praxishinweis zur Protokollwahl

Vermeiden Sie TCP-over-TCP bei OpenVPN, wenn UDP verfügbar ist. Nutzen Sie WireGuard für performante Standleitungen und OpenVPN bei Firewalls, die nur Port 443/TCP durchlassen.

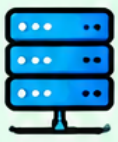
Welches VPN-Protokoll eignet sich für Ihr Netzwerkszenario?



Restriktive Unternehmens-Firewall blockiert alle UDP-Ports

→ Setzen Sie OpenVPN über TCP Port 443 ein, um TLS-Datenverkehr zu imitieren.

Maximale Bandbreite und minimale Latenz für Punkt-zu-Punkt-Kopplung erforderlich



→ Implementieren Sie WireGuard mit Cryptokey Routing und Kernel-Modul.

ETHERNET-SICHERHEITSMECHANISMEN: PORT SECURITY, DHCP SNOOPING UND DAI

1. BEDROHUNGSLAGE AUF LAYER 2



Auf der Sicherungsschicht vertrauen Switches standardmäßig allen Frames. Ohne Schutzmaßnahmen manipulieren Angreifer MAC-Tabellen, initiieren Man-in-the-Middle-Angriffe oder vergiften ARP-Caches im lokalen Segment.

- CAM-Table-Overflow durch massenhaft gefälschte Quell-MAC-Adressen
- Rogue DHCP Server verteilen falsche Standard-Gateways und DNS-Server
- ARP-Spoofing leitet IP-Verkehr unbemerkt über Angreifersysteme um

GRUNDSATZ DER ZUGRIFFSEBENE
Layer-2-Angriffe finden vor IP-Routing und Firewalls statt; Schutz muss direkt am Switchport ansetzen.

2. PORT SECURITY FUNKTIONSWEISE



Port Security beschränkt die Anzahl zulässiger MAC-Adressen an einem physischen Switchport und verknüpft Schnittstellen fest mit autorisierten Endgeräten.

- Begrenzung der maximalen MAC-Adressen (Maximum MACs)
- Statisches Eintragen oder dynamisches Lernen von Geräteadressen
- Sticky MAC speichert gelernte Adressen direkt in der Running-Configuration

3. VIOLATION MODES IM VERGLEICH



Wird das MAC-Limit überschritten oder eine unzulässige Adresse erkannt, löst der Switch eine vorkonfigurierte Schutzreaktion aus.

- Protect: Verwirft unautorisierte Frames stillschweigend ohne Zähler oder SNMP-Trap
- Restrict: Verwirft Frames, erhöht den Violation-Counter und erzeugt einen Syslog-/SNMP-Alarm
- Shutdown: Versetzt den Switchport sofort in den Zustand error-disabled (Standard)

WELCHER VIOLATION-MODUS PASST ZUR NETZUMGEBUNG?

Strikte Zero-Tolerance-Sicherheitsrichtlinie gefordert	Shutdown wählen; Port wird bei Verstoß deaktiviert und erfordert administrativen Reset.
Betrieb muss weiterlaufen, Verstoß soll jedoch auditiert werden	Restrict aktivieren; fremder Datenverkehr wird blockiert, Monitoring schlägt Alarm.

7. IMPLEMENTIERUNG IN 4 SCHRITTEN



Aktivierung und Verknüpfung der Schutzfunktionen in der richtigen Reihenfolge auf dem Access-Switch.

- DHCP Snooping global und per Ziel-VLAN aktivieren
- Trustert Porte: Verbindungen zu echten DHCP-Servern oder Uplinks erlauben DHCP-Offers/Acks
- Untrusted Ports: Reguläre Clientports verwerfen DHCP-Server-Antworten unmittelbar
- Port Security auf Endgeräte-Interfaces mit Sticky-MAC und Restrict/Shutdown scharfschalten

ETHERNET-SICHERHEIT: L2-SCHUTZ

PORT SECURITY · DHCP SNOOPING · DAI

4. DHCP SNOOPING BASISPRINZIP



DHCP Snooping filtert unzulässige DHCP-Nachrichten und unterscheidet Switchports in vertrauenswürdig (trusted) und nicht vertrauenswürdig (untrusted).

- Trusted Ports: Verbindungen zu echten DHCP-Servern oder Uplinks erlauben DHCP-Offers/Acks
- Untrusted Ports: Reguläre Clientports verwerfen DHCP-Server-Antworten unmittelbar
- Verhindert Rogue-DHCP-Server und Man-in-the-Middle-Angriffe im Subnetz

6. DYNAMIC ARP INSPECTION (DAI)



DAI fängt ARP-Pakete auf nicht vertrauenswürdigen Ports ab und verifiziert die Übereinstimmung von Absender-MAC und Absender-IP mit der Snooping-Tabelle.

- Blockiert ARP-Poisoning und unberechtigte Gratuitous-ARP-Meldungen
- Untrusted Ports verwerfen ARP-Pakete ohne passenden Binding-Eintrag
- Trusted Ports (Uplinks und Router-Schnittstellen) leiten ARP ungeprüft weiter

9. DYNAMIC ARP INSPECTION (DAI)



DAI fängt ARP-Pakete auf nicht vertrauenswürdigen Ports ab und verifiziert die Übereinstimmung von Absender-MAC und Absender-IP mit der Snooping-Tabelle.

- Blockiert ARP-Poisoning und unberechtigte Gratuitous-ARP-Meldungen
- Untrusted Ports verwerfen ARP-Pakete ohne passenden Binding-Eintrag
- Trusted Ports (Uplinks und Router-Schnittstellen) leiten ARP ungeprüft weiter

SCHRITT-FÜR-SCHRITT-ABLAUF

1. **Schritt 1: DHCP Snooping aktivieren**
   DHCP Snooping global einschalten, für betroffene VLANs aktivieren und Uplinks zum zentralen DHCP-Server auf 'trust' setzen.
2. **Schritt 2: Binding-Generierung prüfen**
   Mit 'show ip dhcp snooping binding' verifizieren, dass verbundene Clients mit korrekter IP, MAC und Interface registriert werden.
3. **Schritt 3: DAI zuschalten**
   Dynamic ARP Inspection für dieselben VLANs aktivieren; für statische Server bei Bedarf ARP-Access-Lists hinterlegen.
4. **Schritt 4: Port Security konfigurieren**
   An Client-Ports 'switchport port-security', Adresslimit (z. B. 1 oder 2) und Violation-Modus definieren.

8. ZUSAMMENFASSUNG & BETRIEBS-CHECK



Das koordinierte Zusammenspiel der drei Mechanismen etabliert eine geschützte Switching-Infrastruktur auf Zugriffsebene.

- Port Security sichert die physikalische Schnittstelle, gegen MAC-Flutung und unerlaubte Hardware
- DHCP Snooping schützt die IP-Konfigurationsphase und sammelt Identitätsdaten
- DAI garantiert die Integrität der Zuordnung von IP- zu MAC-Adressen im gesamten VLAN

PRAXIS-TIPP FÜR DEN BETRIEB
Rate-Limiting für ARP- und DHCP-Pakete aktivieren, um CPU-Überlastung durch Angriffs-Bursts vorzubeugen.

Audit: Nicht vertrauenswürdige Ports geprüft (Datum / Prüfer)

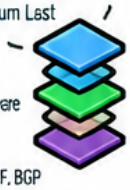
Status: DHCP Snooping Binding Table konsistent (Anzahl aktiver Leases)

CONTROL PLANE POLICING (CoPP) & CPPR



1. ARCHITEKTUR: DIE DREI EBENEN

Moderne Netzwerkgeräte trennen Aufgaben strikt in drei funktionale Schichten, um Last und Sicherheit zu isolieren.



- **Data Plane (Forwarding)**: Verarbeitet Transitverkehr in Hardware (ASICs) ohne CPU-Beteiligung.
- **Control Plane**: Protokolle wie OSPF, BGP und STP berechnen Topologien direkt auf der Haupt-CPU.
- **Management Plane**: Administrativer Zugriff auf das Gerät via SSH, HTTPS, SNMP und Syslog.

2. BEDROHUNG: KONTROLLEBENEN-DOS

Wird die zentrale CPU mit unzulässigen Paketen überflutet, brechen Routing und Gerätezugriff zusammen.



- **CPU-Erschöpfung**: 100 % CPU-Auslastung verhindert reguläre Protokoll-Hellos und Keepalives.
- **Routing-Instabilitäten**: Flapping von BGP- oder OSPF-Nachbarschaften reißt ganze Netzsegmente ab.
- **Verlust der Managementschnittstelle**: SSH-Sessions brechen ab, Reagieren im Incident wird unmöglich.

3. FUNKTIONSWEISE VON COPP

Control Plane Policing definiert die CPU als virtuelle Schnittstelle, auf der QoS-Regeln greifen.

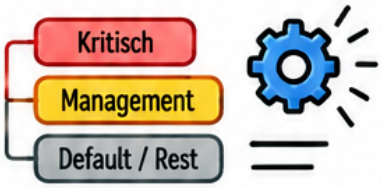
- **Klassifizierung**: Eingehender Datenverkehr wird über strikte Access Control Lists (ACLs) identifiziert.
- **Policing & Rate Limiting**: Erlaubter Verkehr erhält Bandbreitenlimits (Committed Information Rate).
- **Hardware-Filtering**: Ungewollter Datenverkehr wird bereits auf ASIC-Ebene verworfen (Drop).



4. TRAFFIC-KLASSIFIZIERUNG

Effektives Policing erfordert die granulare Aufteilung des Kontrollverkehrs in definierte Klassen.

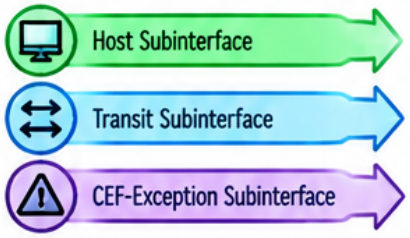
- **Kritisch**: IGP/BGP Routing-Hellos, LACP, BFD und ICMP Unreachable (höchste Priorität).
- **Management**: Autorisierte SSH-Verbindungen, SNMP-Monitoring und NTP-Synchronisation.
- **Undefiniert / Rest**: Unbekannter Verkehr fällt in eine Default-Klasse mit minimaler Bandbreite.



5. CPPR: GRANULARE UNTERSCHNITTELEN

Control Plane Protection verfeinert CoPP durch Aufteilung der Control Plane in drei logische Pfade.

- **Host Subinterface**: Pakete, die direkt an die lokalen IP-Adressen des Geräts gerichtet sind (SSH, BGP).
- **Transit Subinterface**: Datenverkehr, der die CPU für Sonderfunktionen beansprucht (z. B. IP-Optionen).
- **CEF-Exception Subinterface**: Pakete, die nicht per Hardware weitergeleitet werden können (ARP, TTL-Ablauf).



6. IMPLEMENTIERUNGSSCHRITTE

Die Aktivierung von CoPP folgt einem standardisierten, mehrstufigen MQC-Vorgehen (Modular QoS CLI).

1. **Klassifizierung per ACL**
   Erstellen spezifischer Access-Listen für kritische Routing-, Management- und Ausnahmetypen.
2. **Definition der Class-Maps**
   Zuordnung der erstellten ACLs zu modularen Class-Maps zur eindeutigen Verkehrstrennung.
3. **Policing in Policy-Map**
   Konfiguration von Bandbreitengrenzen (Police CIR/Burst) und Aktionen (Transmit, Drop) je Klasse.
4. **Aktivierung an der Control-Plane**
   Bindung der Policy-Map an die Control-Plane-Schnittstelle im Ingress-Pfad.

7. BEST PRACTICES & FALLSTRICKE

Fehlkonfigurationen können fatale DoS-Zustände für das reguläre Netzwerkmanagement hervorrufen.

- **Kein blindes Droppen**: ICMP-Raten begrenzen, aber nicht sperren (Path MTU Discovery benötigt ICMP).
- **BGP/OSPF Schutz**: Rate-Limits für Routing-Protokolle großzügig über dem Normalpeak ansetzen.
- **Zuerst Logging**: Neue Policies vor dem Droppen im Monitoring-Modus auf legitimen Drop-Verkehr prüfen.

Wichtiger Praxishinweis
Testen Sie CoPP-Regeln stets zuerst in einer Staging-Umgebung. Zu restriktive Policen sperren Administratoren aus oder trennen OSPF-Nachbarschaften bei Lastspitzen.

8. ENTSCHEIDUNG & VERIFIKATION

Prüfen Sie bestehende Gerätekonfigurationen anhand des Verifikationsbaums und der Checkliste.

- [ ] Kritische Kontrollprotokolle (BGP, OSPF, LACP) identifiziert und vermessen
- [ ] Management-Zugriffe (SSH, SNMP) auf autorisierte Quellnetze eingegrenzt
- [ ] Ingress-Policy an 'control-plane' erfolgreich gebunden und fehlerfrei aktiv
- [ ] 'show policy-map control-plane' auf unvorhergesehene Paketverluste überwacht

Welche CPU-Schutzmethode passt zu ihrer Plattform?

Hardware unterstützt CPPR mit Subinterfaces	Plattform unterstützt nur Basis-MQC für Control-Plane
CPPR implementieren und separate Policen für Host, Transit und CEF-Exceptions pflegen.	Klassisches CoPP mit Rate-Limiting für Management-, Routing- und Restverkehr anwenden.

Access Control Lists (ACLs): Standard, Extended und Named ACLs

ACCESS CONTROL LISTS (ACLs)

1. WAS IST ES



Access Control Lists (ACLs) sind sequenzielle Regelsammlungen auf Netzwerkgeräten wie Routern und Layer-3-Switches, Sie fungieren als Paketfilter auf den Schichten 3 (Netzwerk) und 4 (Transport) des OSI-Modells, um Datenströme anhand definierter Kriterien zuzulassen oder zu verwerfen.

- Filterung primär über IP-Header (Schicht 3) und TCP/UDP-Header (Schicht 4)
- Zwei Hauptentscheidungen pro Regel: Permit (Durchlassen) oder Deny (Blockieren)
- Wirkt als elementare Sicherheitsmauer direkt auf der Weiterleitungsebene

2. REGELAUSWERTUNG & TOP-DOWN



Pakete werden strikt von oben nach unten (Top-Down) geprüft. Sobald eine Zeile zutrifft, wird die Aktion sofort ausgeführt und die Prüfung beendet. Greift keine explizite Regel, greift am Ende stets das unsichtbare "Implicit Deny".

- Erster Treffer gewinnt (First-Match-Prinzip); nachfolgende Zeilen werden ignoriert
- Spezifische Filterregeln müssen immer vor allgemeinen Regeln stehen
- Implicit Deny am Listenende verwirft jeden nicht ausdrücklicln erlaubten Datenverkehr

3. STANDARD ACLS



Standard-ACLs filtern Datenpakete ausschließlich auf Baiss der Quell-IP-Adresse, Da Zieladresse und Portnummern nicht ausgewertet werden, bieten sie nur eine grobe Verkehrssteuerung.

- Nummernbereiche: 1-99 sowie erweiterter Bereich 1300–1999
- Prüft nur: Source IP Address
- Best Practice zur Platzierung: So nah wie möglich am Zielnetzwerk konfigurieren

4. EXTENDED ACLS



Erweiterte ACLs ermöglichen eine feingranulare Filterung. Sie analysieren Quell- und Ziel-IP-Adressen, IP-Protokolltypen (TCP, UDP, ICMP) sowie optionale Portnummern (z. B. Port 80 HTTP, 443 HTTPS).

- Nummernbereiche: 100–199 sowie erweiterter Bereich 2000-2699
- Prüft: Source-IP, Destination-IP, Protokolltyp, Quell- und Zielports
- Best Practice zur Platzierung: So nah wie möglich an der Datenquelle platzieren

5. NAMED ACLS & EDITIERBARKEIT



Named ACLs erstezen starre Zahlenwerte durch lesbare alphanumerische Bezeichner. Sie erlauben durch automatisierte Sequenznummern (z. B. 10, 20, 30) das gezielte Löschert und Einfügen einzelner Regeln.

- Aussagekräftige Namen (z. B. ACL-DMZ-FILTER) verbessern Nachvollziehbarkeit
- Sequenznummern verhinderro das aufwendige Neuschreiben der kompletten Liste
- Unterstützt sowohl Standard- als auch Extended-Modi in moderner Syntax

6. INGRESS VS. EGRESS FILTERUNG



Eine ACL muss an einer Schnittstelle (Interface) und in einer bestimmten Verkehrsrichtung aktiviert werden. Ingress prüft vor dem Weiterleitungsentscheid, Egress filtert direkt vor dem Verlassen des Interfaces.

- Ingress (In): Prüft eingehende Pakete vor dem Routingprozess; schont Routerressourcen
- Egress (Out): Prüft ausgehende Pakete nach Durchlaufen der internen Routing-Tabelle
- Regel: Maximal eine ACL pro Interface, Protokoll (z: B. IPv4) und Richtung

7. BEST PRACTICES & ANWENDUNG



Fehlerfafte ACLs können legitimen Datenverkehr unterbrechen oder unbemerkt Sicherheitslücken öffnen. Ein methodischer Ablauf bei Konzeption, Test und Implementierung schützt vor Konfigurationsfehlern.

- Wildcard-Masken (Invertierte Subnetzmasken) präzise berechnen (0 = prüfen, 255 = ignorieren)
- Explizite "deny ip any any log" Zeile vor dem Listenende zur Nachverfolgung nutzen
- Änderungen vorab in Testumgebungen simulieren und Verbindungstests durchführen

Platzierungsregel Merksatz

Standard-ACL nah ans Ziel (Destination), um unbeabsichtigtes Blockieren auf anderen Pfaden zu verhindern. Extended-ACL nah an die Quelle (Source), um unerwünschten Datenverkehr sofort am Netzwerkeingang abzufangen.

Welcher ACL-Typ wird für das geplante Vorhaben benötigt?

Nur Quell-IPs müssen geblockt/erlaubt werden
→ Standard-ACL wählen und nahe am Zielnetzwerk zuweisen.

→ Prüfung von Ziel-IP, TCP/UDP-Ports oder Protokollen nötig

→ Extended Named-ACL wählen und nahe an der Datenquelle platzieren.

Schritte

1. **Schritt 1: Kommunikationsmatrix definieren**
   Quellnetze, Zielnetze und benötigte Transportports exakt effassen.
2. **Schritt 2: ACL-Typ & Regeln formulieren**
   Regeln von spezifisch nach allgemein ordnen und Wildcard-Masken ermitelen.
3. **Schritt 3: Interface & Richtung binden**
   ACL mittels Ingress- oder Egress-Befehl dem entsprechenden Interface zuweisen.
4. **Schritt 4: Verifikation & Hit-Counter prüfen**
   Regelzugriffe über Zähler überwachen und unerwartete Paketverluste analysieren.

8. ZUSAMMENFASSUNG & REGELMATRIX



ACLs bieten robuste, ressourceenschonende Basissicherheit auf Netzwerkebene. Sie arbeiten stateless (zustandslos) und unterscheiden sich dadurch grundlegend von Stateful-Inspection-Firewalls.

- Top-Down-Auswertung mit sofortigem First-Match-Ausstieg
- Sequenznummern bei Named ACLs ermöglichen unterbrechungsfreie Wartung
- Implicit Deny stets als Sicherheitsgrundannahme im Design berücksichtigen

Audit: Konfigurierte ACL-Bezeichnung und Interface-Zuordnung

Geprüfte Regelreihenfolge und Spezifitätsabgleich (Notizen)

SPI VS. STATELESS FILTERING

1. GRUNDPRINZIP & VERGLEICH



Paketfilter prüfen Netzwerkpakete an Schnittstellen. Stateless Filter analysieren jedes Paket isoliert anhand statischer Header-Felder, währned Stateful Packet Inspection (SPI) den dynamischen Verbindungsstatus über eine interne Tabelle erfasst.

- **Stateless:** Prüft Quell-/Ziel-IP, Port und TCP-Flags rein isoliert ohne Kontext.
- **SPI:** Verfolgt den gesamten Lebenszyklus einer Verbindung von Initialisierung bis Abbau.
- **Kontextsensitivität:** Antwortpakete werden automatisch legitimiert, wenn eine aktive Sitzung existiert.

2. VERBINDUNGSSTATUSTABELLE (STATE TABLE)



Das Herzstück einer SPI-Firewall ist die dynamische Statustabelle. Jeder initiierte Verbindungsaufbau erzeugt einen Eintrag, der eingehende Antworten automatisch zuordnet.

- **Sitzungs-Tupel:** Protokoll, Quell-IP, Quellport, Ziel-IP, Zielport.
- **Sequenznummern-Validierung:** Abgleich von TCP-Sequenz- und Acknowledgment-Nummern gegen Hijacking.
- **Timeout-Management:** Automatische Bereinigung inaktiver oder geschlossener Sitzungseinträge.

3. TCP-HANDSHAKE-TRACKING



SPI analysiert die TCP-Zustandsübergänge lückenlos während des gesamten Verbindungsaufbaus.

- **SYN:** Client initiiert die Verbindung; Firewall erstellt Status 'SYN_SENT'.
- **SYN-ACK:** Server antwortet; Firewall aktualisiert auf 'SYN_RECEIVED'.
- **ACK:** Handshake abgeschlossen; Status wechselt auf 'ESTABLISHED'.



SICHERHEITSVORTEIL

Unangemeldete TCP-Pakete mit gesetztem ACK- oder FIN-Flag werden von SPI ohne passenden Tabelleneintrag sofort verworfen.

4. PROTOKOLLBESONDERHEITEN: UDP & ICMP



Obwolh UDP und ICMP verbindungslos sind, implementiert SPI eine 'Pseudo-Statefulness'.

- **UDP-Tracking:** Ausgehende UDP-Anfragen öffnen ein zeitlich eng begrenztes Rückmeldefenster für den Zielport.
- **ICMP-Zuordnung:** 'Echo Reply' (Typ 0) wird nur gestattet, wenn zuvor ein passender 'Echo Request' (Typ 8) registriert wurde.
- **Dynamische Schließung:** Erfolgt nach definierter Leerlaufzeit (UDP-Idle-Timeout).

5. RESSOURCENEFFIZIENZ & PERFORMANCE



Der Sicherheitsgewinn von SPI erfordert einen höheren Rechen- und Speicheraufwand gegenüber stateless Filtering.

- **Stateless:** Minimaler RAM- und CPU-Bedarf, ideal für Access Control Lists (ACLs) auf High-Speed-Core-Routern.
- **SPI:** Skaliert mit der Anzahl gleichzeitiger Verbindungen (Concurrent Connections) im Arbeitsspeicher.
- **Session Affinity:** Erfordert, dass Hin- und Rückweg über dieselbe Firewall-Instanz geroutet werden.

7. SICHERHEITSRISIKEN & ANGRIFFSVEKTOREN



Beide Architekturen weisen systemspezifische Angriffsflächen auf Netzwerkebene auf.

- **Stateless-Schwachstelle:** Angreifer können gefälschte ACK-Pakete einschleusen, um statische Regelsätze zu umgehen.
- **State-Table-Exhaustion:** SYN-Flooding zielt darauf ab, die Zustandstabelle der SPI-Firewall durch offene Halb-Verbindungen zu überlasten.
- **Keine Applikationsinspektion:** Weder SPI noch Stateless prüfen standardmäßig Schadcode in legitimen Nutzdaten.



DOS-SCHUTZ

Moderne SPI-Systeme nutzen SYN-Cookies oder aggressive Session-Timeouts, um Tabellenerschöpfung bei DoS-Angriffen abzuwehren.

8. PRÜFUNG & VERIFIKATION



Praxisleitfaden zur Analyse und Diagnose von Paketfiltern im laufenden Netzwerkbetrieb.

1. **Verbindungsaufbau initiieren**
   Starten Sie eine Verbindung vom geschützten Host und kontrollieren Sie das Eintreffen des SYN-Pakets an der Firewall.
2. **State-Table-Eintrag prüfen**
   Verifizieren Sie mit 'conntrack -L' oder Firewall-CLI-Befehlen das Vorhandensein des 5-Tupels und des Status 'ESTABLISHED".
3. **Unerwartete Pakete testen**
   Senden Sie ein unaufgefordertes TCP-ACK-Paket von extern und stellen Sie sicher, dass die Firewall das Paket verwirft (DROP).

Geprüftes Netzwerk-Segment / Firewall-IP

Beobachteter Status-Timeout (TCP / UDP in Sekunden)

7. ARCHITEKTUR-ENTSCHEIDUNGSFINDUNG

Wählen Sie den passenden Filtermechanismus basierend auf Durchsatzanforderungen und Sicherheitsgrenzen im Netzwerklayout.



An welcher Netzwerkposition und mit welcher Priorität soll gefiltert werden?

- Perimeter-Sicherheit mit dynamischen Client-Verbindungen ins Internet
  → Einsatz von SPI (Stateful), um Antwortpakete automatisch zuzuordnen und Ports nach außen geschlossen zu halten.
- Internes High-Throughput-Routing im Core-Netzwerk ohne Speicherengpass
  → Einsatz von Stateless ACLs auf Hardware-Routern für maximale Paketdurchsatzraten ohne Statusverwaltung.

NGFW & DEEP PACKET INSPECTION MINDMAP

NGFW & DEEP PACKET INSPECTION

1. DEFINITION & KERNKONZEPT



- Klassische Paketfilter prüfen lediglich Header-Informationen auf Layer 3 (IP) und Layer 4 (Port/Protokoll).
- Eine NGFW erweitert diese Architektur um die Analyse der Anwendungsebene (Layer 7).
- Unabhängig vom verwendeten Transport-Port identifiziert die NGFW das tatsächliche Protokoll und kontrolliert gezielt Anwendungsfunktionen sowie Nutzdaten.
- **Port-Unbbhängigkeit:** Erkennt Applikationen auch bei Port-Verschleierung oder Dynamic Port Hopping.
- **Kontextbezug:** Verknüpft IP-Verbindungen mit Benutzeridentitäten und Anwendungszuständen.
- **Konsolidierte Sicherheitsfunktionen:** Bündelt Filterung, Antivirus, IPS und Web-Proxy in einer Appliance.

2. LAYER-4-FIREWALL VS. LAYER-7-NGFW



Klassische Firewalls sind blind für Inhalte oberhalb der Transportschicht. NGFWs dekodieren den gesamten Datenstrom zur Laufzeit.

- **Layer-4-Paketfilter:** Untersucht Quell-/Ziel-IP, Protokoll (TCP/UDP) und Ports. Ein Datenstrom über Port 443 wird pauschal als HTTPS gewertet.
- **Layer-7-NGFW:** Rekonstruiert den Datenstrom, validiert Protokollstandards und unterscheidet bspw. legitimen TLS-Verkehr von getunneltem SSH- oder P2P-Datenverkehr.
- **Granularität:** Ermöglicht die Freigabe einer Webanwendung bei gelichzeitigem Blockieren bestimmter Unterfunktionen (z. B. Datei-Upload).

3. DEEP PACKET INSPECTION



Deep Packet Inspection analysiert nicht nur den Paket-Header, sondern zerlegt und untersucht die gesamte Nutzlast (Payload). Mittels Signaturabgleich, Heuristik und Protokollanalyse erkennt die DPI-Engine schadhafte Inhalte, Exploits und Datenafflüsse direkt im Datenstrom.

- Paketstrom-Reassemblierung: Fragmente werden geordert zusammengesetzt, um Evasion-Techniken zu verhindern.
- Signaturabgleich: Durchsucht Nutzdaten nach Mustern bekannter Schadsoftware und Exploits.
- Anomalie-Erkennung: Erkennt Abweichungen von RFC-Standards innerhalb der Protokoll-Payloads.

4. TLS/SSL-ENTSCHLÜSSELUNG



Da der Großteil des modernen Netzwerkverkehrs verschlüsselt ist, bliebt DPI ohne Entschlüsselung wirkungslos. Die NGFW agiert hierbei als transparenter Man-in-the-Middle-Proxy.

- Inbound Inspection: Schützt interne Server, indem die Firewall das Serverzertifikat und den privaten Schlüssel vorhält.
- Outbound Inspection (Gesucht Nutzdaten): Die Firewall terminiert die TLS-Sitzung zum Webserver und stellt eine eigenständige, mit der internen Unternehmens-CA signierte TLS-Dorbindung zum Client her.
- Ausnahmelisten: Datenschutzrelevanter Datenverkehr (z. B. Online-Banking, Medizinportale) wird per Whitelist von der Entschlüsselung ausgenommen.

5. USER-IDENTITY-MAPPING



Statt statsischer IP-Adressen nutzt die NGFW reale Benutzer- und Gruppenidentitäten für Richtlinienentschiedungen. Dies vereinfacht die Rechteverwaltung in dynamischen Netzen wie DHCP- oder WLAN-Umgebungen.

- Directory-Integration: Anbindung an Microsoft Active Directory, LDAP, Kerberos oder RADIUS.
- IP-to-User Mapping: Korrelation von IP-Adressen mit Logins via Event-Logs, Captive Portal oder Endpoint-Agents. Logins via Event-Logs, Captive Portal oder Endpoint-Agents.
- Rollenbasierte Regeln: Definition von Zugriffsrechten direkt für Abteilungen oder Gruppen (z. B. "DevOps" vs. "Vertrieb").

6. INTEGRIERTE IPS-ENGINES



Ein integriertes Intrusion Prevention System (IPS) schützt Systeme vor Ausnettung bekannter Schwachstellen. Es analysiert Netzwerkflüsse in Echtzeit und blockiert Angriffe inline, bevor sie das Zielsystem erreichen.

- **Schwachstellen-Schutz:** Verhindert Exploits gegen ungepatchte Server- und Clientdienste (Virtual Patching).
- **Brute-Force-Abwehr:** Blockiert automatische Anmeldeversuche bei Überschreitung definierter Grenzwerte.
- **Verhaltensanalyse:** Erkennt unübliche Verbindungsversuche wie Portscans oder Command-and-Control-Beacons.

7. FALLEN & BEST PRACTICES



Die Aktivierung von Deep Packet Inspection und SSL-Entschlüsselung erfordert sorgfältige Planung von Rechenrerssourcen und Zertifikatsverteilung.

- **Performance-Einbruch:** Vollständige Entschlüsselung erhöht CPU- und Speicherlast; Hardware-Offloading/ ASICs einplanen.
- **Zertifikatsfehler:** Das Stammzertifikat der NGFW muss auf allen Endgeräten im vertrauenswürdigen Zertifikatsspeicher hinterlegt sein.
- **Recht & Privavsphäre:** Klare Richtlinien für nicht einsehende Kategorien (Finanzen, Gesundheit) zur Wahrung der DSGVO definieren.

8. ZUSAMMENFASSUNG



NGFWs vereinen klassicches Routing und Port-Filterung mit moderner Anwendungs- und Bedrohungserkennung. Durch die Trias aus App-ID, User-ID und Content-ID (DPI) ermöglichen sie präzise und risikobasierte Sicherheitsrichtlinien im Unternehmensnetzwerk.

- Layer-7-Sichtbarkeit schließt blinde Flecken traditioneller Paketfilter.
- DPI und SSL-Inspection sind essenziell zur Erkennung verdeckter Schadsoftware.
- User-Mapping ersetzt starre IP-Regeln durch flexible Identitätskontrolle.

LEITFADEN: PAKETVERARBEITUNG IN DER NGFW

1. 

Ingress & Layer 3/4-Basisprüfung

Das Paket trifft an der Schnittstelle ein. Routing-Tabelle, Quell- und Ziel-IP sowie TCP/UDP-Ports werden gegen elementare Access Control Lists (ACLs) geprüft.

2. 

Stateful Inspection & Sitzungsaufbau

Die Firewall prüft, ob das Paket zu einer bestehenden Session gehört oder einen gültigen TCP-Handshake (SYN) einleitet.

3. 

TLS/SSL-Terminierung (Optional)

Handelt es sich um verschlüsselten Verkehr und greift eine Inspektions-richtlinie, bricht der Proxy die TLS-Sitzung auf und entschlüsselt die Payload zur Untersucdung.

4. 

App-ID & User-ID Ermittlung

Die Engine bestimmt die tatsächliche Anwendung anhand von Protokoll-mustern und ordnet die Quell-IP einem authentifizierten Benutzer zu.

5. 

Content-ID & DPI (IPS / AV / Webfiiter)

Die entschlüsselte Nutzlast wird durch die Signaturen von IPS und Antivirus geprüft. Webfilter prüfen Kategorien und URLs.

6. 

Forwarding oder Drop

Wird keine Bedrohung gefunden und erlaubt die Richtlinie den Zugriff, wird das Paket neu verschlüsselt (falls SSL-Inspection aktiv war) und an die Egress-Schnittstelle weitergeleitet.

Praxis-Hinweis zur Entschlüsselung

DPI auf verschlüsseltem Datenverkehr ohne aktives TLS-Offloading prüft ausschließlich unverschlüsselte Metadaten (wie SNI und IP-Ziele), kann jedoch keine Nutzlast-Signaturen analysieren.

Welche Inspektionsmethode sollte für einen Datenstrom angewendet werden?

- Verkehr ist verschlüsseltes HTTPS, betifft jedoch Banking- oder Patientendaten → Bypass SSL-Inspection: Nur Layer-3/4-Filterung und SNI-Domain-Prüfung anwenden, Nutzdaten unberührt weiterleiten.
- Verkehr ist unverschlüsselt oder generischer Webverkehr von internen Clients → Vollständige DPI mit SSL-Inspection aktivieren, App-ID zuweisen und IPS-/Malware-Signaturen auf der Payload ausführen.

IDS & IPS IM NETZWERK



1. GRUNDPRINZIP UND ZIELSETZUNG



Intrusion Detection Systeme (IDS) und Intrusion Prevention Systeme (IPS) analysieren den Netzwerkverkehr auf bösartige Aktivitäten, Richtlinienverstöße und bekannte Bedrohungsmuster.

- IDS fungiert als passiver Sensor und löst Alarme aus
- IPS steht aktiv im Datenstrom und blockiert Angriffe
- Schutz vor Ausnutzung bekannter Schwachstellen und Malware
- Sichtbarkeit von Bedrohungen auf Paket- und Session-Ebene

2. ERKENNUNGSMETHODEN



Zur Identifikation verdächtiger Aktivitäten setzen Systeme auf zwei komplementäre Verfahren mit spezifischen Stärken und Schwächen.

- Signaturbasiert: Musterabgleich gegen definierte Angriffsdefinitionen
- Hohe Genauigkeit bei bekannten Exploits, blind gegen Zero-Days
- Anomaliebasiert: Abweichung von einer gelernten Baseline des Normalverkehrs
- Erkennt neuartige Muster, neigt jedoch zu Fehlalarmen

3. BETRIEBSMODI: INLINE VS. PROMISCUOUS



Die physische und logische Platzierung bestimmt, ob ein System Angriffe nur bebbachten oder direkt stoppen kann.

- Promiscuous Mode (IDS): TAP oder Switch-Mirror-Port (SPAN) kopiert Verkehr
- Keine Latenz für den regulären Datenverkehr bei Hardware-Ausfall
- Inline Mode (IPS): Datenverkehr fließt direkt durch das System hindurch
- Ermöglicht sofortiges Verwerfen, birgt Risiko von Paketverzögerungen

4. AUTOMATISIERTE ABWEHRMASSNAHMEN

Moderne IPS-Systeme leiten bei verifizierten Alarmen deterministische Reaktionen ein, um Schäden zu verhindern.



- Drop Packet: Verwerfen schädlicher Einzelpakete ohne Benachrichtigung
- TCP Reset (RST): Aktives Beenden der bösartigen TCP-Sitzung beidseitig
- Dynamische Firewall-Regel: Temporäre Blockierung der Quell-IP
- Rate Limiting: Drosselung verdächtigen Volumens zur Schadensbegrenzung

5. FALSE-POSITIVE-MANAGEMENT



Ein geregeltes Vorgehen verhindert, dass legitimer Betriebsverkehr durch Überreaktionen blockiert wird.

- Fehlalarme belasten Support-Teams und gefährden Geschäftsprozesse
- Regelmäßiges Tuning und Deaktivieren unpassender Signatursätze
- Testphase im reinen Alert-Modus vor Aktivierung harter IPS-Drops
- Whitelisting vertrauenswürdiger interner Scanner und Systeme



ACHTUNG BEI TUNING-MASSNAHMEN
Signaturen nicht ungeprüft global abschalten, sondern Pfad und Host gezielt eingrenzen.

6. INTEGRATION IN DIE NETZWERKARCHITEKTUR

Sensoren müssen an kritischen Segmentgrenzen platziert werden, um maximalen Einblick ohne Blindstellen zu gewährleisten.



- Platzierung hinter der Perimeter-Firewall reduziert Signaturrauschen
- Interne Platzierung vor Kernservern schützt vor Lateral Movement
- Bypass-Switches verhindern Netzausfälle bei IPS-Hardwaredefekten
- Traffic-Normalisierung verhindert Evasion durch TCP-Segmentierung

7. PRAXIS-WORKFLOW BEI ALARMIERUNG



Standardisierter Ablauf für Analysten beim Auftreten eines kritischen IPS/IDS-Ereignisses im Monitoring.

1. **Paket-Payload und Header prüfen**
   Quell- und Ziel-IP, Ports sowie Rohdaten auf tatsächliche Angriffsmuster untersuchen.
2. **Systemstatus verifizieren**
   Prüfen, ob das Zielsystem verwundbar ist oder der Exploit ins Leere lief.
3. **Regelanpassung oder Quarantäne**
   Bei Bedrohung Host isolieren; bei Fehlalarm Regeltuning für die Signatur dokumentieren.

8. ZUSAMMENFASSUNG UND KERNREGELN



Wesentliche Leitlinien für den stabilen Betrieb von IDS- und IPS-Infrastrukturen.

- IDS meldet passiv; IPS blockiert aktiv im Leitungsstrang
- Signatur-Updates kontinuierlich einpflegen und versionieren
- Normalisierungs-Engines gegen Fragmentierungs-Tricks vorschalten
- Kritische Blockierregeln vorab im Überwachungsmodus validieren

NETWORK TIME PROTOCOL (NTP)

1. WAS IST ES

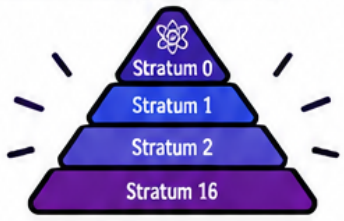
Das Network Time Protocol (NTP) ist ein hierarchisches Netzwerkprotokoll zur hochpräzisen Synchronisation von Systemuhren über paketvermittelte IP-Netzwerke.



- Protokollstandard auf Anwendungsschichtbasis über UDP-Port 123
- Kompensiert variable Paketlaufzeiten und asymmetrische Netzwerkpfade
- Schafft eine global einheitliche Zeitbasis (UTC) für verteilte Rechnernetze
- Ermöglicht Sub-Millisekunden-Genauigkeit in lokalen Netzwerken (LAN)

2. STRATUM-HIERARCHIE

NTP organisiert Referenzzeitquellen in einer baumförmigen Hierarchie von Genauigkeitsstufen, sogenannten Strata (Bereich 0 bis 16).



- Stratum 0: Hochpräzise Zeitreferenzen (Atomuhren, GPS-Empfänger, DCF77)
- Stratum 1: Primäre Zeitserver, direkt physisch an Stratum-0-Geräte angebunden
- Stratum 2: Sekundäre Server, die Zeit über NTP von Stratum-1-Knoten synchronisieren
- Stratum 16: Signalisiert eine vollständig unsynchronisierte oder ungültige Zeitquelle

3. DRIFT & KORREKTURVERFAHREN

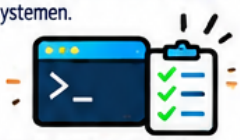
Hardware-Quarzoszillatoren weisen Fertigungstoleranzen und Temperatureinflüsse auf, die kontinuierliche Anpassungen erfordern.



- Clock Drift: Kontinuierliches Vor- oder Nachgehen der lokalen Hardware-Uhr
- Clock Jitter: Statistische Schwankung aufeinanderfolgender Laufzeitmessungen
- Slewing: Sanftes Dehnen oder Stauchen der Systemsekunde via adjtime()
- Stepping: Harter Zeitsprung bei großen Diskrepanzen (Gefahr inkonsistenter Logfolgen)

7. PRAXIS: DIAGNOSE & KONFIGURATION

Prüfung und Pflege des Zeitsynchronisationsstatus auf Client- und Serversystemen.



- chronyc tracking: Ausgabe von Stratum, Drift, Referenzquelle und Offset
- chronyc sources -v: Detaillierte Signalbewertung und Filterzustände der Zeitquellen
- ntpq -p: Klassische Auflistung erreichbarer Peers, Jitter und Paketverzögerungen
- Pool-Redundanz: Konfiguration von mindestens 4 unabhängigen Servern zur Mehrheitsfindung

Schritte zur Diagnose und Konfiguration

1. **Status prüfen**
   Führen Sie 'chronyc tracking' oder 'timedatectl' aus, um aktuellen Offset und Stratum-Wert zu analysieren.
2. **Quellen bewerten**
   Prüfen Sie mit 'chronyc sources', ob Server konsistente Offsets liefern und als synchronisierte Referenz markiert sind.
3. **Offset korrigieren**
   Verhindern Sie abrupte Zeitsprünge im laufenden Betrieb und nutzen Sie 'makestep' nur während der Bootphase.

8. ZUSAMMENFASSUNG & CHECK

Kompakter Leitfaden zur Absicherung und Verifikation der unternehmensweiten Zeitsynchronisation.



- NTP operiert über UDP-Port 123 in einer hierarchischen Stratum-Architektur
- Drift wird sanft per Slewing korrigiert, um Logbuchbrüche zu vermeiden
- Replay-Schutz in Kerberos und TLS-Zertifikatsvalidierung benötigen präzise Uhren
- SIEM-Ereigniskorrelation erfordert netzwerkweit synchrone Zeitstempel

Lokaler NTP-Server / Pool-Adresse

Maximal tolerierter Offset (z. B. Kerberos < 300 s)

Eingesetzte Authentifizierung (NTS / Key-ID)

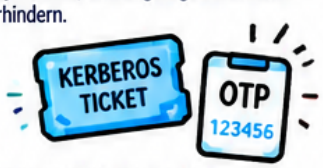
Liegt der ermittelte Zeit-Offset über dem kritischen Schwellenwert von 1000 Millisekunden?

Ja (Offset > 1 s)
Untersuchen Sie Netzwerk-Jitter und Firewall-Regeln für UDP 123. Nutzen Sie kontrolliertes Stepping nur außerhalb der Produktionszeiten.

Nein (Offset stabil im Millisekundenbereich)
Belassen Sie das System im regulären Slewing-Modus und überwachen Sie die Drift über das Monitoring-System.

6. KRYPTOGRAFISCHE VERFAHREN & TOKENS

Moderne Sicherheitsarchitekturen setzen auf synchrone Zeitbasen, um Wiederholungsangriffe (Replay Attacks) und ungültige Zertifikate zu verhindern.



- Kerberos-Tickets: Zeitfenster (Standard: 5 Minuten) zur Abwehr abgefangener Authentifizierungs-Tickets
- TLS-Zertifikate: Gültigkeitsprüfung (NotBefore und NotAfter) schlägt bei Zeitasymmetrie fehl
- TOTP (RFC 6238): Zeitbasierte Einmalkennwörter erfordern synchrone Zeitfenster (oft 30 Sekunden)
- Token-Invalidierung: Zeitnahes Auslaufen von kurzlebigen JSON Web Tokens (JWT)

5. BEDEUTUNG FÜR LOGGING & SIEM

Präzise Zeitstempel sind das fundamentale Rückgrat für jede computerforensische Untersuchung und forensische Zeitleisten.



- Korrelation von Audit-Logs: Zeitliche Verknüpfung von Ereignissen über Firewalls, Proxys und Server
- Chronologische Kausalität: Eindeutiger Nachweis von Angriffsvektoren und Lateral Movement
- SIEM-Alarme: Erkennung zeitkritischer Angriffsmuster und Anomalien in Echtzeit
- Gerichtsverwertbarkeit: Manipulationssichere Zeitreihen für Compliance und Nachweispflichten

PRECISION TIME PROTOCOL (IEEE 1588)



1. GRUNDPRINZIP & ZWECK



PTP (IEEE 1588) synchronisiert Uhren in paketbasierten Netzwerken auf den Sub-Mikrosekundenbereich. Es nutzt Hardware-Zeitstempel auf PHY-/MAC-Ebene, um Software-Latenzen und Jitter auszuschließen.

- Ziel: Deterministische Taktsynchronisation über Ethernet
- Genauigkeit: Typisch < 1 Mikrosekunde (oft wenige Nanosekunden)
- Hardware-Zeitstempelung eliminiert Betriebssystem-Jitter

2. KNOTEN-ROLLEN & TOPOLOGIE



Eine PTP-Hierarchie wird dynamisch via Best Master Clock Algorithm (BMCA) organisiert. Knoten nehmen feste funktionale Rollen ein:

- Grandmaster Clock (GMC): Höchste Referenzzeit (meist GPS/GNSS)
- Boundary Clock (BC): Schlichtet Segmente, trennt Master-/Slave-Ports
- Ordinary Clock (OC): Endgerät mit einfacher Uhr (als Master oder Slave

3. VERZÖGERUNGSMESSUNG

Zwei primäre Methoden ermittelh Paketlaufzeiten und Asymmetrien zwischen Kommunikationspartnern:

- Delay Request-Response (E2E): Misst Gesamtstrecke über alle Hops
- Peer Delay (P2P): Misst Link-Latenz punktuell zwischen direkten Nachbarn
- P2P skaliert robuster in Netzen mit festen Latenzprofilen



4. VIER-ZEITSTEMPEL-VERFAHREN

Der Slave berechnet Uhrenversatz (Offset) und Einweg-Laufzeit (Mean Path Delay) anhand von 4 exakten Zeitstempeln:



- t1 (Master sendet Sync), t2 (Slave empfängt Sync)
- t3 (Slave sendet Delay_Req), t4 (Master empfängt Delay_Req)
- Delay = ((t4 - t1) - (t3 - t2)) / 2;
  Offset = (t2 - t1) - Delay

So funktioniert's – in 4 Schritten:

1. **Schritt 1: Sync & Follow_Up**
   Master sendet Sync (t1 erfasst). Bei Two-Step Clocks folgt Follow_Up mit präsisem t1.
2. **Schritt 2: Delay_Req erfassen**
   Slave empfängt Sync (t2), sendet Delay_Req ab (t3) und speichert lokallen Wert.
3. **Schritt 3: Delay_Resp verarbeiten**
   Master empfängt Delay_Req (t4) und übermittlet t4 via Delay_Resp zurück an den Slave.
4. **Schritt 4: Taktkorrektur**
   Slave errechnet Delay sowie Offset und regelt die lokale Hardwareschwingung (VCO) nach.

5. SWITCH-UNTERSTÜTZUNG (TC)

Normale Netzwerkswitches verursachen Queuing-Jitter. PTP-fähige Transparent Clocks (TC) korrigieren diesen Fehler direkt im Paket:

- End-to-End TC: Addiert switchinterne Verweilzeit (Residence Time)
- Peer-to-Peer TC: Addiert Verweilzeit plus vorgelagerte Link-Latenz
- Korrekturfeld (Correction Field) wird in-flight aktualisiert



Transparent Clock (TC)

6. EINSATZFELDER IN DER PRAXIS

PTP ist der De-facto-Standard in allen Industrien mit harter Echtzeitanforderung:

- 5G-Mobilfunk: Fronthaul-Synchronisation (O-RAN) für Antennengruppen
- Industrieautomatisierung: Deterministische TSN-Netze (IEEE 802.1AS)
- Finanzsektor: MiFID-II-konforme Zeitstempel für Hochfrequenzhandel
- Rundfunk: Unkomprimiertes Audio/Video über IP (SMPTE ST 2110)



7. NTP VS. PTP VERGLEICH



Die Auswahl des Synchronisationsprotokolls hängt vom Genauigkeitsbedarf und der Infrastruktur ab:

- NTP: Millisekundenbereich, rein softwarebasiert, ideal für WAN/Internet
- PTP: Sub-Mikrosekunden, erfordert PTP-Hardware-Switches und lokales Netz
- Overhead: PTP erfordert spezialisierte Netzwerkkarten und Filter

Hardwareunterstützung zwingend

Reines Software-PTP ohne MAC/PHY-Timestamping erreicht selten Genauigkeiten unterhalb von Mikrosekunden, da Betriebssystem-Interrupts Fluktuationen bewirken.

Welches Protokoll für das geplante Vorhaben wählen?

Millisekunden im gerouteten Internet/WAN ausreichend	→ NTP (Network Time Protocol) implementieren; keine Spezialhardware nötig.
Sub-Mikrosekunden in deterministischem LAN gefordert	→ PTP (IEEE 1588 / IEEE 802.1AS) mit Hardware-Timestamp-Switches einsetzen.

8. DIAGNOSE & ARBEITSSCHRITTE



Mess- und Prüfschritte bei der Validierung einer PTP-Architektur im Netzwerk:

- Lock-Status der Grandmaster Clock mit GNSS-Fix prüfen
- Offset-Statistik und Jitter am Slave-Port aufzeichnen
- Transparent-Clock-Korrekturwerte auf allen Switches validieren

GMC Identifikationsnummer (Grandmaster ID) / Quelle:

_____

Gemessener mittlerer Offset (ns / µs) am Slave-Knoten:

_____

Eingesetztes Delay-Verfahren (E2E / P2P) & Begründung:

_____

_____

SNMP (v1, v2c, v3)

1. GRUNDPRINZIPIEN & ARCHITEKTUR

SNMP arbeitet nach dem Manager-Agenten-Prinzip auf der Anwendungsschicht zur Statusabfrage und Configuration.



- Manager (NMS): Zentrale Managementstation sendet Anfragen und empfängt Alarme
- Agent: Software-Dienst auf verwalteten Systemen wie Routern, Switches und Servern
- Transportprotokoll: Nutzt standardmäßig ungesichertes UDP Port 161 (Polling) und UDP Port 162 (Traps)

2. SNMP-OPERATIONEN

Der Datenaustausch erfolgt über standardisierte Protokolldateneinheiten (PDUs) zwischen NMS und Agent.



- GetRequest / GetNextRequest: Abfrage einzelner oder sequentieller Parameterwerte
- GetBulkRequest: Effiziente Massenabfrage größerer Datentabellen (eingeführt mit SNMPv2c)
- SetRequest: Schreibender Zugriff zur direkten Änderung von Geräteparametern
- Trap / InformRequest: Unaufgeforderte Statusmeldungen; Inform erfordert Quittierung

3. MIB & OID-BAUMSTRUKTUR

Der Managemetausch erfolgt Base (MIB) bildet verwaltbare Parameter in einer standardisierten Baumhierarchie ab.



- Struktur: Hierarchischer Objektbaum, definiert mittels Abstract Syntax Notation One (ASN.1)
- OID-Notation: Punktgetrennte Ziffernfolge (z. B. .1.3.6.1.2.1 für die Standard-Internet-MIB-II)
- Hersteller-Zweige: Private Enterprise Numbers (PEN) unter .1.3.6.1.4.1 für herstellerspezifische Werte

4. PROTOKOLLVERSIONEN IM VERGLEICH

Die Protokollversionen unterscheidren sich grundlegend in Leistungsfähigkeit und Sicherheitsarchitektur.



- SNMPv1: Basisversion, unverschlüsselte Klartext-Übertragung, unsichere Community-Strings
- SNMPv2c: Einführung von 64-Bit-Zählern und GetBulk, nutzt jedoch weiterhin Klartext-Communities
- SNMPv3: Umfassende kryptografische Sicherheit mit granularer Zugriffskontrolle und Benutzersperwaltung Werte

5. SNMPV3 SICHERHEITSARCHITEKTUR

SNMPv3 ersetzt fehleranfällige Community-Strings durch modulare Sicherheits- und Autorisierungsmodelle.

- USM (User-based Security Model): Authentifizierung und Verschlüsselung pro Benutzer
- VACM (View-based Access Control Model): Definiert präzise MIB-Teilbäume und Lese-/Schreibrechte
- Sicherheitsstufen: noAuthNoPriv (unsicher), authNoPriv (Integrität/Auth), authPriv (Auth und Verschlüsselung)



6. SICHERHEITSRISIKEN & SCHUTZ

Alte SNMP-Implementierungen stellen erhebliche Angriffsflächen für Informationsabfluss und Manipulation dar.

- Klartext-Risiko: Abhören von Standard-Strings (public/private) mittels Paket-Sniffing
- DoS & Reflection: Missbrauch ungeschützter UDP-Dienste für Distributed-Denial-of-Service-Angriffe
- Härtung: Abschalten ungenutzter SNMP-Dienste, Migration auf SNMPv3 und Absicherung über Management-VLANs



PRODUKTIONHINWEIS

Standard-Community-Strings wie 'public' oder 'private' müssen in jedem Netzwerk sofort deaktiviert oder geändert werden.

7. PRAXISBEISPIEL: SNMPWALK & ABFRAGE

Typischer Ablauf einer SNMPv3-Abfrage zur Ermittlung des Systemnamens und Schnittstellenstatus:

- Befehl: snmpwalk -v3 -l authPriv -u secuser -a SHA -A AuthPass123 -x AES -X PrivPass123 192.168.1.1 1.3.6.1.2.1.1
- Rückgabe: sysDescr (.1.1.0) liefert Hardware- und Betriebssystemdetails des Netzwerkgeräts
- Schnittstellenprüfung: Auslesen von ifInOctets (.1.3.6.1.2.1.2.2.1.10) zur Bandbreitenanalyse



8. ENTSCHEIDUNGSMATRIX PROTOKOLLWAHL

Systematischer Prüfpfad zur Festlegung des sicheren Überwachungsmodus im Produktivbetrieb.



Unterstützt das zu überwachende Zielsystem SNMPv3 mit authPriv?

Ja

Erzwinge SNMPv3 authPriv mit SHA-Authentifizierung und AES-Verschlüsselung; deaktiviere v1/v2c vollständig.

Nein

Isoliere die Abfrage in ein dediziertes, geschütztes Management-VLAN, setze komplexe Community-Strings und erlaube ausschließlich Nur-Lese-Rechte (Read-Only).

SYSLOG (RFC 5424) & LOGGING

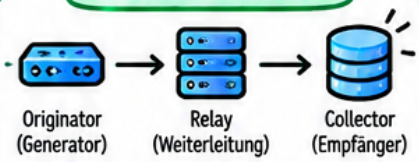
1. GRUNDLAGEN

Das Syslog-Protokoll standardisiert die ereignisbasierte Protokollierung von System- und Netzwerkkomponenten zur zentralen Überwachung und forensischen Nachvollziehbarkeit.

- Definiert in RFC 5424 als herstellerübergreifender Standard für strukturierte Systemmeldungen.
- Zentralisiert Status- und Fehlermeldungen von Routern, Firewalls, Switches und Servern.
- Ermöglicht Sicherheitsaudits, Echtzeit-Monitoring und die Einhaltung regulatorischer Compliance-Anforderungen.

Historischer Hinweis
RFC 5424 erstezt das veraltete Format nach RFC 3164 und bietet standardisierte Zeitstempel sowie strukturierte Daten.

2. ARCHITEKTUR



Ein Syslog-Ökosystem trennt die Erzeugung, den Transport und die Speicherung von Logdaten in spezialisierte funktionale Rollen.

- Originator (Generator): Client-Gerät oder Netzwerkdienst, der das Primärereignis erfasst.
- Relay (Weiterleitung): Vermittelnder Knoten zur Bündelung, Filterung oder kryptografischen Kapselung.
- Collector (Empfänger): Zentraler Syslog-Server oder SIEM-System zur Archivierung und Analyse.

3. HEADER & FORMAT



Jedes Datagramm ist streng hierarchisch aufgebaut, um automatisierte Parser-Verabeitung und einheitliche Ablage zu gewährleisten.

- **PRI (Priority):** Berechnet aus Facility-Code und Severity-Wert.
- **Header:** Enthält Versionsnummer, ISO-8601-Zeitstempel mit Zeitzone, Hostname, App-Name, PID und Message-ID.
- **STRUCTURED-DATA und MSG:** Optional typisierte Schlüssel-Wert-Paare gefolgt von der Freitext-Meldung.

4. SEVERITY LEVELS



Die Schweregrade priorisieren Meldungen numerisch von kritischen Betriebsstörungen bis zur detaillierten Fehlersuche.

- **0 (Emergency) & 1 (Alert):** Vollständiger Systemausfall oder sofortige Intervention zwingend erforderlich.
- **2 (Critical), 3 (Error) & 4 (Warning):** Kritische Fehlerbedingungen, Hardwareausfälle oder drohende Risiken.
- **5 (Notice), 6 (Informational) & 7 (Debug):** Reguläre Statusänderungen, Betriebsereignisse oder Code-Diagnose.

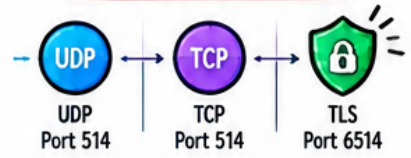
5. FACILITIES

Priority = (Facility × 8) + Severity

Facilities klassifizieren das erzeugende Teilsystem im Betriebssystem oder der Netzwerkkomponente.

- Klassische Werte: auth/authpriv (04/10), daemon (03), kern (00), mail (02), local0 bis local7 (16-23).
- Formel zur Prioritätsbechnung: Priority = (Facility * 8) + Severity.
- Beispiel: authpriv (10) bei Alert (1) ergibt PRI-Wert <81> im Nachriehten-Header.

6. TRANSPORT & TLS



Der Transportweg bestimmt die Integrität, Vertraulichkeit und Zustellsicherheit über unsichere Netzwerkgrenzen.

- **UDP Port 514:** Verbindungslos ohne Bestätigung; minimaler Overhead, jedoch anfällig für Paketverlust und Spoofing.
- **TCP Port 514:** Verbindungsorientiert mit Flusskontrolle; verhindert stillen Paketverlust bei hoher Netzlast.
- **TLS über TCP Port 6514:** Standard nach RFC 5425 für wechselseitig authentifizierte und verschlüsselte Log-Übertragung.

Sicherheitshinweis
Logdaten enthalten häufig vertrauliche IP-Adressen oder Kontonamen. Im WAN- und Cloud-Betrieb ist Syslog über TLS Pflicht.

6. TRANSPORT-ENTSCHEIDUNGSHILFE

Auswahl des geeigneten Transportprotokolls basierend auf Netzwerksegment und Sicherheitsanforderungen.

Welches Transportverfahren erfüllt die Vorgaben des Netzwerkabschnitts?

- Isoliertes internes Management-VLAN ohne sensslile Nutzdaten und geringer Bandbreite → Klassisches UDP 514 oder Standard-TCP 514 verwenden; Fokus auf geringen Komponenten-Overhead.
- Übertragung über geroutete Netze, WAN, DMZ oder standortübergreifende Links → RFC 5425 Syslog over TLS (TCP Port 6514) mit X.509-Zertifikatsauthentifizierung erzwingen.

7. UMSETZUNGSSCHRITTE

Verbindliche Implementierungsabfolge zur Härtung der Log-Übermittlung auf Endgeräten und Relay-Systemen.

1. **Facility und Severity definieren**
   Protokollierungslevel auf dem Gerät konfigurieren (z. B. local0 mit Severity Warning und höher).
2. **Zertifikate hinterlegen**
   Vertrauenswürdiges CA-Zertifikat und Client-Zertifikat für TLS-Gegenstellenauthentifizierung installieren.
3. **Ziel-Collector und Port konfigurieren**
   Syslog-Daemon auf den Collector mit Ziel-Port 6514/TCP unter Angabe des FQDN parametrieren.
4. **Pufferung und PFI-Filterung testen**
   Lokale Warteschlangen für Verbindungsausfälle aktivieren und Testmeldung via Logger-Befehl auslösen.

8. KONFIGURATIONSPROTOKOLL

Dokumentationsbereich zur strukturierten Erfassung von Syslog-Quellen im Auditing.

Hostname / Quell-IP-Adresse

Konfigurierte Facility und Mindest-Severity

Transportmethode (UDP 514 / TCP 514 / TLS 6514)

Zertifikatsfingerabdruck / Gültigkeitsdatum

NETWORK TELEMETRY UND FLOW-MONITORING: NETFLOW, IPFIX UND SFLOW

1. GRUNDPRINZIP: WAS IST FLOW-MONITORING?

Netzwerk-Flow-Monitoring erfasst aggregierte Metadaten von Datenströmen statt vollständiger Paketnutzdaten (Payloads). Ein Datenfluss (Flow) wird klassisch als Folge von IP-Paketen definiert, die innerhalb eines Zeitfensters übereinstimmende Kernmerkmale teilen. Dies ermöglicht bandbreitenschonende Telemetrie bei minimalem Speicheraufwand.

- **Unterscheidung:** Metadaten-Aggregation statt ressourcenintensiver Deep Packet Inspection (DPI)
- **Klassisches 5-Tupel-Kriterium:** Quell-IP, Ziel-IP, Quell-Port, Ziel-Port und Layer-4-Protokoll (TCP/UDP)
- **Flow-Eigenschaften:** Aggregierte Zähler für Pakete, übertragene Bytes, Start- und Endzeitpunkte
- **Einsatzzweck:** Erkennung von DoS-Volumenangriffen, Kapazitätsengpässen und Netzwerk-Scans

DEFINITION EINES DATENFLUSSES
Ein Flow fasst alle Pakete zusammen, die dieselben Adress- und Portparameter nutzen. Flüsse werden beendet, wenn ein Inactivity-Timeout greift oder ein TCP-FIN/RST-Flag erkannt wird.

2. ARCHITEKTUR & ABLAUF DER TELEMETRIE

Die Erfassung und Auswertung von Telemetriedaten erfolgt in einer standardisierten dreistufigen Pipeline aus Erfassungspunkt, Übertragung und zentraler Korrelation.

- **Exporter:** Netzwerkgeräte generieren Flow-Statistiken im laufenden Betrieb
- **Collector:** Zentraler Speicher nimmt UDP-basierte Telemetrie-Pakete auf
- **Analyzer:** SIEM- oder Telemetrie-Tools visualisieren Anomalien und Trends

DER ABLAUF IN 4 SCHRITTEN

1. **Paketbeobachtung am Router/Switch**
   Netzwerkknoten identifizieren Pakete anhand der Header-Informationen und ordnen sie einer Flow-Tabelle zu.
2. **Aggregation & Zähleraktualisierung**
   Byte- und Paketzähler werden für jeden Flow aktualisiert.
3. **Export bei Ablauf oder Verbindungsende**
   Flow-Datensazz wird per UDP an den Collector übertragen.
4. **Indexierung & Forensische Auswertung**
   Collector normalisiert IP-Felder und stellt Daten für Reports bereit.

3. PROTOKOLLVERGLEICH: NETFLOW VS. IPFIX VS. SFLOW

Zur Erfassung von Telemetrie existieren drei dominante Industriestandards mit unterschiedlicher technischer Arbeitsweise.

- **NetFlow (Cisco):** Proprietärer Ursprung (v5 mit festem Format, v9 template-basiert)
- **IPFIX (IETF RFC 7011):** Offener Standard, baut auf NetFlow v9 auf, unterstützt variable Felder und Enterprise-Identifer
- **sFlow (InMon):** Paketbasiertes Sampling (z. B. 1 von 1000 Paketen) direkt im Switch-ASIC mit Header-Extraktion

UNTERSCHIED STATUS VS. SAMPLING
NetFlow und IPFIX aggregieren Zustände aller Pakete im Cache (Stateful), während sFlow statistisch einzelne Pakete samplet (Stateless) und extrem skalierbar für 100G-Backbones ist.

NETWORK TELEMETRY & FLOW-MONITORING

4. PROTOKOLL-AUSWAHL FÜR DIE ANALYSE

Entscheidungsmatrix zur Auswahl des geeigneten Telemetrie-verfahrens je nach Netzwerktopologie und Hardwareausstattung.

- **Stateful Flow-Verfahren** liefern exakte Abrechnungs- und Sicherheitsdaten
- **Sampling-Verfahren** schützen Netzwerk-Hardware vor CPU-Erschöpfung

WELCHES TELEMETRIEPROTOKOLL ERFÜLLT DIE SYSTEMANFORDERUNGEN?

Cisco-Hardware ohne Third-Party-Spezifikationen vorhanden	NetFlow v9 aktivieren; Template-basierten Export zum zentralen Collector konfigurieren.
Multivendor-Umgebung mit Wunsch nach flexiblen Headern (MPLS, VLAN, IPv6)	IPFIX (IETF) implementieren und einheitliche Template-Definitionen festlegen.
Extrem hohe Durchsatzraten (Core-Switching >40 Gbps)	sFlow auf ASIC-Ebene mit adäquater Sampling-Rate (z. B. 1:2048) einrichten.

5. ANWENDUNG IN DER CYBERSECURITY

Flow-Daten bilden das Rückgrat der netzwerkweiten Bedrohungserkennung und forensischen Rekonstruktion nach Sicherheitsvorfällen.

- **DDoS-Erkennung:** Ungewöhnlicher Anstieg von Paketen pro Sekunde mit identischen Ziel-Ports (z. B. SYN-Floods)
- **Port-Scanning:** Ein einzelner Quell-Host erzeugt tausende kurze Flows zu fortlaufenden Zielports innerhalb von Sekunden
- **Data Exfiltration:** Auffällige Zunahme des Outbound-Byte-Volumens über nicht standardisierte Ports oder Protokolle
- **Lateral Movement:** Interne Systeme initiieren ungewohnte Verbindungen zu administrativen Ports (z. B. SSH, RDP, SMB)

6. INTEGRATION IN MONITORING & SIEM

Best Practices zur fehlerfreien Anbindung von Exportern an zentrale Sicherheits- und Netzwerkanalyseplattformen.

- **Collector-Absicherung:** Schutz der unverschlüsselten UDP-Telemetrieströme über isolierte Management-VLANs
- **Cache-Dimensionierung:** Anpassung der aktiven und inaktiven Flow-Timeouts zur Vermeidung von Paket-Drops im RAM
- **Template-Sync:** Sicherstellen, dass IPFIX-Templates regelmäßig an den Collector gesendet werden

ACHTUNG VOR UDP-PAKETVERLUST
Da die meisten Flow-Exporte über verbindungslose UDP-Verbindungen erfolgen, führen Überlastungen des Collectors zu Datenlücken ohne Fehlermeldung.

7. PRAXIS-AUDIT: FLOW-KONFIGURATION PRÜFEN

Prüfbogen für Systemadministratoren und Sicherheitsanalysten zur auditierbaren Überprüfung der Netzwerktelemetrie.

- Dokumentation aller aktiven Exporter und Interface-Zuordnungen
- Validierung der Alarm-Schwellenwerte für verdächtige Flussraten

Geprüfter Router / Core-Switch Hostname & IP: _____

Aktiviertes Export-Protokoll (NetFlow v9 / IPFIX / sFlow): _____

Konfigurierte Sampling-Rate bzw. Flow-Timeout (Sekunden): _____

Zuständiger Collector IP & Port (z. B. UDP 2055 / 4739): _____

Beobachtete Anomalien oder festgestellte Paket-Drops im Flow-Cache: _____

8. FAZIT & ESSENTIELLE KERNREGELN

Kompakte Zusammenfassung der wichtigsten Leitlinien für den verlässlichen Betrieb von Netzwerk-Flow-Monitoring im IT-Betrieb.

- Metadaten genügen für Makroanalysen: Payloads müssen nur bei gezieltem Verdacht via PCAP erfasst werden
- Konsistente Zeitzonen und NTP-Synchronisation auf allen Exportern sind zwingend für forensische Korrelationen
- NetFlow/IPFIX für forensische Details; sFlow für kosteneffizientes Core-Backbone-Capacity-Planning
- Regelmäßige Baseline-Updates durchführen, um False Positives durch legitime Lastspitzen zu minimieren

PORT MIRRORING: SPAN, RSPAN UND ERSPAN



1. WAS IST PORT MIRRORING?



Port Mirroring ist eine essenzielle Switch-Funktion zur unterbrechungsfreien Verkehrsanalyse. Dabei werden Pakete ausgewählter Quellports oder VLANs hardwarenah kopiert und an einen dedizierten Analyseport geleitet, an dem Überwachungstools wie IDS, IPS oder Paket-Sniffer (z. B. Wireshark) angebunden sind.

- Ermöglicht passive Netzwerküberwachung ohne Eingriff in den produktiven Datenfluss.
- Verhindert Beeinträchtigungen des Originalverkehrs durch rein lesenden Abgriff.
- Dient der Fehlersuche, Sicherheitsanalyse und Compliance-Dokumentation.

2. LOKALES SPAN (SWITCHED PORT ANALYZER)



Lokales SPAN spiegelt Datenverkehr innerhalb eines einzelnen physischen Switches. Quellports (Source Ports) und das Ziel (Destination Port) befinden sich auf demselben Gerät.

- Unterstützt Ingress- (eingehend), Egress- (ausgehend) oder bidirektionale Überwachung.
- Keine zusätzliche Kapselung oder Netzwerklast auf Trunk-Verbindungen.
- Einfache Einrichtung für Ad-hoc-Analysen im lokalen Rack.

3. RSPAN (REMOTE SPAN)



RSPAN erweitert das lokale Mirroring über mehrere Layer-2-Switches hinweg. Der gespiegelte Datenverkehr wird in ein eigens reserviertes RSPAN-VLAN eingespeist und über bestehende Trunk-Ports transportiert.

- Erfordert ein dediziertes RSPAN-VLAN mit deaktiviertem MAC-Address-Learning.
- Ermöglicht die Konsolidierung von Analysetools auf zentralen Switches.
- Verkehr bleibt auf dieselbe Layer-2-Broadcast-Domäne beschränkt.

4. ERSPAN (ENCAPSULATED REMOTE SPAN)



ERSPAN kapselt duplizierte Ethernet-Frames in Generic Routing Encapsulation (GRE) und versieht sie mit einem IPv4- oder IPv6-Header. Dadurch kann gespiegelter Datenverkehr über geroutete Layer-3-Netze und WAN-Verbindungen transportiert werden.

- Verwendet IP Protocol 47 (GRE) mit speziellem ERSPAN-Typ-Header.
- Ermöglicht standortübergreifende Paketaufzeichnung in Rechenzentren.
- Erfordert Unterstützung auf Router- oder Switch-Hardware sowie MTU-Prüfung.

5. TECHNISCHER VERGLEICH & EINSATZ



Die Wahl des Mirroring-Verfahrens richtet sich nach Netzwerktopologie, Durchsatz und Entfernung zum Analysetool.

- **SPAN:** Minimale Latenz, kein Overhead, auf einen Switch begrenzt.
- **RSPAN:** Layer-2-Trunks erforderlich, potenzieller Bandbreitenverbrauch auf Uplinks.
- **ERSPAN:** Volle Layer-3-Routbarkeit, erzeugt Zusatz-Header (typisch ca. 50 Byte).

6. PRAXIS-WORKFLOW: MONITORING-SESSION EINRICHTEN



Strukturierter Ablauf zur fehlerfreien Implementierung einer Mirroring-Sitzung in der Praxis:

1. **Bedarf & Ports bestimmen**
   Quellports (SPAN-Source) und Analyse-Port (SPAN-Destination) sowie Verkehrsrichtung (rx, tx, both) definieren.
2. **Bandbreitenprüfung**
   Sicherstellen, dass der Ziel-Port die kumulierte Bandbreite der Quell-Ports aufnehmen kann, um Paketverlust zu vermeiden.
4. **Session konfigurieren**
   Paketmitschnitt am Analyzer starten und prüfen, ob Kontrollframes sowie Nutzlast ohne Pufferüberläufe empfangen werden.

7. TYPISCHE FALLSTRICKE & RISIKEN



Fehlkonfigurationen beim Mirroring können Produktionsnetze überlasten oder Analyseergebnisse verfälschen.

- Oversubscription: Überlastung des Ziell-Ports führt zum unbemerkten Verwerfen gespiegelter Pakete (Drops).
- Layer-2-Loops: RSPAN-VLANs müssen vom normalen Spanning-Tree-Flooding und MAC-Learning isoliert sein.
- MTU-Probleme: ERSPAN fügt Kapselungs-Header hinzu; Überschreitungen führen zu Fragmentierung oder Drop.

Wichtiger Praxis-Hinweis
Auf Destination-Ports wird der reguläre Datenverkehr standardmäßig deaktiviert. Schließen Sie Analyse-Rechner direkt an und betreiben Sie keine aktiven Netzwerkdienste auf diesem Port.

8. ZUSAMMENFASSUNG & ENTSCHEIDUNGSMATRIX



Leitfaden zur Auswahl des optimalen Spiegelungsverfahrens für Netzwerk- und Security-Analysen.

Welches Port-Mirroring-Verfahren passt zu Ihrer aktuellen Infrastruktur?

1. Analysegerät ist am selben physischen Switch wie die Datenquelle angeschlossen.
   → Lokales SPAN wählen: Geringster Aufwand, keine Kapselung, maximale Performance ohne Netzwerklast.
2. Quelle und Ziel befinden sich auf unterschiedlichen Switches desselben Layer-2-Campus.
   → RSPAN konfigurieren: Dediziertes RSPAN-VLAN über Trunks routen und Zielport am Ziel-Switch belegen.
3. Daten müssen über geroutete Netze, Subnetze oder Rechenzentrums-Grenzen fließen.
   → ERSPAN einsetzen: GRE-Tunnel über IP konfigurieren und MTU-Puffergröße auf den Transportpfaden sicherstellen.

NETZWERKANALYSE & PAKET-SNIFFING (WIRESHARK & TCPDUMP)

1. GRUNDLAGEN DES PAKET-SNIFFINGS



Paket-Sniffing bezeichnet das passive oder aktive Mitschneiden von Datenübertragungen auf der Sicherungs- und Vermittlungsschicht. Auf Switched Networks erfordert dies Techniken wie Port-Mirroring (SPAN) oder TAP-Geräte, um Datenströme jenseits von Broadcasts sichtbar zu machen.

- Promiscuous Mode: Aktiviert die Annahme aller Frames unabhängig von der Ziel-MAC-Adresse der Netzwerkkarte.
- Erfassungspunkte: Einsatz an TAP-Ports oder Switched Port Analyzer (SPAN) zur verlustfreien Spiegelung.
- Rechtlicher Rahmen: Nur auf explizit autorisierten Schnittstellen und eigenen Testumgebungen sniffen.

Sicherheits- & Datenschutzhinweis
Unverschlüsselte Nutzdaten (Cleartext) enthalten sensilbe Kennwörter und Sitzungs-IDs. Die Erfassung setzt stets die schriftliche Freigabe des Netzwerkeigentümers voraus.

2. BERKELEY PACKET FILTER (BPF) SYNTAX



Berkeley Packet Filters (BPF) reduzieren die Verarbeitungs- und Speicherlast bereits im Kernelbereich des Betriebssystems, bevor Pakete an den Userspace übergeben werden. Die Syntax unterscheidet Primitiven nach Typ, Richtung und Protokoll.

- Host & Netz: `host 192.168.1.100` schänkt auf eine IP ein; `net 10.0.0.0/24` erfasst das gesamte Subnetz.
- Portfilter: `port 443` oder `portrange 80-88` filtert Quell- und Zielports auf Transportschichtebene.
- Logische Operatoren: Kombiniere Ausdrücke mit `and`, `or` und `not` (bspw. `'tcp and not port 22'`).

Capture-Filter vs. Display-Filter
Capture-Filter (BPF) bestimmen vorab, was gespeichert wird. Display-Filter (Wireshark) filtern die bereits gespeicherten Pakete nachträglich in der GUI.

3. TCPDUMP: WORKFLOW AUF DER CLI



Tcpdump ist der De-facto-Standard für leichtgewichtige, performante Paketerfassung auf Linux- und UNIX-Systemen ohne grafische Oberfläche.

- Schnittstellenprüfung: Auflisten verfügbarer Netzkarten für den Mitschnitt.
- Parametersteuerung: Steuerung von Puffergrößen, Namensauflösung und Dateiausgabe.
- PCAP-Ablage: Schreiben in standardisierte Binärformate zur späteren Tiefenanalyse.

Schritt-für-Schritt-Workflow

1. **Schnittstelle identifizieren**
   Befehl `'tcpdump -D'` ausführen, um Schnittstellennummern und Namen (z. B. eth0, any) abzufragen.
2. **Erfassung starten**
   Mit `"tcpdump -i eth0 -nn -s 0 -v"` starten: `-nn` verhindert DNS- und Portauflösung für maximalen Durchsatz.
3. **BPF anwenden & in PCAP speichern**
   Zielgerichteten Mitschnitt sichern: `"tcpdump -i eth0 -w dump.pcap "tcp port 80 and host 192.168.1.50""`.
4. **Erste Schnellanalyse**
   Schnittstellerdaten inspizieren mit `"tcpdump -r dump.pcap -c 20"` ohne erneute Netzwerklast.

4. WIRESHARK: STRUKTUR & FARBPROFILE



Wireshark bietet ein dreigeteiltes Analysefenster: Paketliste (Paket-Übersicht), Paketdetails (dekodierte Protokollschichten als Baum) und Paketbytes (Hexdump mit ASCII-Darstellung).

- Paketliste: Zeigt fortlaufende Nummer, Zeitstempel, Quell-/Ziel-IP, Protokoll und Kurzinfo.
- Baumansicht: Aufklappbare Protokoll-Header von Frame (Layer 2) bis Nutzdaten (Layer 7).
- Hex-Ansicht: Rohe Byte-Werte des selektierten Felds mit Kennzeichnung im Hexdump.



5. TCP-STREAM-REKONSTRUKTION & FLAGS



TCP ist ein verbindungsorientierter Bytestrom. Wireshark ermöglicht es, einzelne TCP-Pakete anhand ihrer Sequence- und Acknowledgement-Nummern nahtlos zu einem lesbaren Anwendungsstrom zusammensusetzen.

- Drei-Wege-Handshake: Prüfe den Verbindungsaufbau über [SYN], [SYN-ACK], [ACK].
- Stream-Verfolgung: Kontextmenü "Folgen -> TCP-Stream" visualisiert den Dialog zwischen Client (rot) und Server (blau).
- Layer und FIN-Analyse: Erkennt plötzliche Verbindungsabbrüche (RST) gegeneüber regulärem Schließen (FIN).

Wireshark-Filter-Tipp
Nutze `'tcp.flags.reset == 1'`, um abgebrochene Verbindungen sofort zu lokalisieren.

6. SCHICHTENBASIERTE FEHLERDIAGNOSE



Systematische Störungssuche erfolgt von unten nach oben entlang des Schichtenmodells, um Ursachen wie Kabelprobleme, Routingfehler oder Serverstörungen zu isolieren.

- Layer 2 (Data Link): Fehlerhafte MAC-Adressen, Spanning-Tree-Topologiewechsel oder ARP-Misserfolge (Filter: `arp`).
- Layer 3 (Network): Unerreichbare Ziele, TTL Expired Fehlermeldungen (Filter: `icmp`).
- Layer 4 (Transport): TCP-Retransmissions, Zero-Window-Meldungen und Paketverluste (Filter: `tcp.analysis.flags`).
- Layer 7 (Application): Fehlgeschlagene DNS-Auflösungen oder HTTP-Statuscodes 4xx/5xx (Filter: `dns.flags.rcode != 0` or `http.response.code >= 400`).

Welches Symptom dominiert den erfassten Netzwerkverkehr?
Für den Symptomabschnitt

- → Wiederkehrende ICMP "Destination Unreachable" oder "TTL exceeded" Überprüfe Layer 3: Routing-Tabellen, Subnetzmasken-Konfiguration und Firewall-Gateways analysieren.
- → Häufige Meldungen "[TCP Retransmission]" und Latenzspitzen Überprüfe Layer 4 und Interface: Physische MTU-Größen, Switch-Port-Fehler oder Pufferüberläufe untersuchen.
- → Layer 7 (Application): Fehlgeschlagene DNS-Auflösungen oder HTTP-Statuscodes 4xx/5xx (Filter: `dns.flags.rcode != 0` or `http.response.code >= 400` Paket.

Welches Symptom dominiert den erfassten Netzwerkverkehr?
Wiederkehrende ICMP "Destination Unreachable" oder "TTL exceeded" Überprüfe Layer 3: Routing-Tabellen, Subnetzmasken-Konfiguration und Firewall-Gateways analysieren.
→ Häufige Meldungen "[TCP Retransmission]" und Latenzspitzen Überprüfe Layer 4 und Interface: Physische MTU-Größen, Switch-Port-Fehler oder Pufferüberläufe untersuchen.
→ Verbindung wird mit "[TCP RST]" sofort nach SYN quittiert Prüfe Zielhost und Port: Dienst läuft nicht auf dem Zielport oder lokale Host-Firewall blockiert Paket.

7. PRAXIS-CHECKLISTE FÜR DEN PCAP-AUDIT



Strukturierter Ablauf zur Verifizierung verdächtiger oder fehlerfafter Netzwerkübertragungen im Labor oder IT-Betrieb.

- NTP-Zeitsynchronisation vor dem Mitschnitt an allen Messpunkten abgeglichen
- Schnittstellenpuffer ausreichend groß gewählt, um Packet Drops zu verhindern
- Basisfilterung mittels BPF gesetzt, um Speicherplatz und I/O nicht zu überlasten
- Wireshark-Experteninfos (Analyze -> Expert Information) auf Anomalien geprüft
- Wiederholte TCP Dup ACKs und Out-of-Order Segmente protokolliert

8. EINSATZPROTOKOLL & ANALYSENOTIZEN



Dokumentation des Analysevorfalls zur Nachverfolgbarkeit und Fehlerbehebung.

Untersuchte Schnittstelle / IP-Bereich:

Beobachtetes Schichtproblem (L2 / L3 / L4 / L7):

Ermittelte Ursache & empfohlene Abhilfemaßnahme:

NETZWERK-DIAGNOSETOOLS

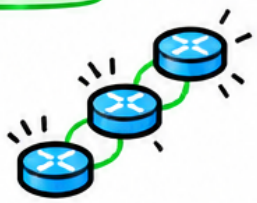
Ping, Traceroute, MTR & Pathping

1. PING & ICMP



- Ping sendet ein ICMP Type 8 (Echo Request) Paket an die Ziel-IP.
- Ein erreichbares System antwortet mit ICMP Type 0 (Echo Reply).
- Messung von RTT und Verbindungsfähigkeit.

2. TRACEROUTE & TTL



- Nutzt das TTL-Feld im IP-Header.
- Router dekrementieren TTL um 1.
- Bei 0: ICMP Type 11 Code 0 (Time Exceeded in Transit).
- Ermittelt Zwischenstationen und Engpässe.

3. MTR ANALYSE



- Echtzeit-Aktualisierung der gesamten Routingkette.
- Genaue Aufschlüsselung von Verlusten pro Hop.
- Erkennt instabile Leitungen und Jitter.

4. PATHPING HYBRID



- Phase 1: Pfadidentifikation über TTL-Ablauf.
- Phase 2: Statistische Belastungsprobe pro Zwischenstation.
- Detaillierte Verlustangaben auf Router- und Verbindungsebene.

5. FEHLERQUELLEN & ICMP-RATENBEGRENZUNG



- ICMP Rate Limiting erzeugt lokalen Schein-Paketverlust.
- Firewalls blockieren ICMP oder bestimmte UDP-Ports (Sternchen).
- Verlust setzt sich auf nachfolgende Hops fort.
- Asymmetrisches Routing kann unterschiedliche Pfade bewirken.

Diagnosetipp

Wenn Hop 4 Paketverlust anzeigt, Hop 5 und das Ziel jedoch 0% Verlust aufweisen, handelt es sich um Drosselung des Routers auf Hop 4 und kein echtes Leitungsproblem.

6. LEITFADEN: TOOL-AUSWAHL FÜR DIE PRAXIS

Wählen Sie das passende Diagnosewerkzeug anhand der vorliegenden Symptome und der Systemumgebung.

- Sofortprüfung der Basisverbindung: Ping
- Topologieermittlung und Bruchstellen: Traceroute
- Intermittierende Abbrüche und Latenzspitzen: MTR

Welches Symptom tritt primär auf?

Kompletter Verbindungsabriss zu einem Ziel	Sporadische Aussetzer, hohe Latenzen oder Voice/Video-Störungen
Zuerst "ping <ziel-ip>" ausführen. Reagiert das Ziel nicht, "traceroute" (Linux) oder "tracert" (Windows) starten, um den lztzten erreichbaren Router zu lokalisieren.	"mtr <ziel-ip>" (oder "pathping" unter Windows) über mindestens 100 Pakete laufen lassen, um Paketverlust und Jitter pro Knoten zu quantifizieren.

7. SCHRITT-FÜR-SCHRITT-DIAGNOSEABLAUF



Strukturierte Fehleranalyse bei Netzwerkproblemen:

- Schritt 1: Lokales Gateway prüfen
- Schritt 2: Öffentliche Referenz-IP testen
- Schritt 3: Pfad zum Zielsystem analysieren
- Schritt 4: Langzeitprüfung bei sporadischen Fehlern

1. **Lokale Schnittstelle und Gateway testen**
   Ping auf Standard-Gateway (z. B. 192.168.1.1).
2. **Zielerreichbarkeit und DNS prüfen**
   Per IP und Hostname pingen. Nur Hostname fehlt → DNS.
3. **Pfadverfolgung starten**
   Traceroute zum Ziel. Letzten antwortenden Router vor Zeitüberschreitungen identifizieren.
4. **Kontinuierliche Hop-Analyse**
   MTR oder Pathping nutzen, um Verluste ab einem Hop auf alle Folge-Hops zu prüfen.

8. PROTOKOLL & NOTIZEN



- Ziel-IP/Hostname notieren.
- Rundlaufzeit und Paketverlust festhalten.
- Auffällige Zwischenstationen markieren.

Netzwerk-Diagnose im Überblick



Zur schnellen Fehlereingrenzung in IP-Netzen existieren spezialisierte Diagnosewerkzeuge. Sie prüfen Erreichbarkeit, ermitteln Zwischenstationen (Hops) und quantifizieren Laufzeitverzögerungen sowie Paketverluste entlang des Übertragungspfads.

- Basisprüfung der Schicht 3: Erreichbarkeit via Echo-Mechanismen
- Pfadverfolgung: Lokalisierung von Zwischenroutern und Engpässen
- Statistische Langzeitmessung: Erkennung von Jitter und partiellem Paketverlust

Hinweis zur Protokollbasis

Diagnosetools stützen sich primär auf das Internet Control Message Protocol (ICMP) sowie transportschichtliche UDP- oder TCP-Proben.

LLDP und CDP: Schicht-2-Nachbarschafts-Erkennung

1. Grundprinzip & Zweck



Link-Discovery-Protokolle arbeiten direkt auf Schicht 2 (Sicherungsschicht). Sie ermöglichen es Netzwerkgeräten, Identitäts-, Port- und Systemdaten zyklisch an direkt verbundene Nachbarn zu senden, ohne IP-Routing oder Schicht-3-Konfigurationen vorauszusetzen.

- LLDP ist der herstellerneutrale Standard gemäß IEEE 802.1AB für heterogene Netze.
- CDP ist Ciscos proprietäres Nachbarschafts-protokoll für Cisco-Switches, Router und IP-Telefone.
- Beide Protokolle arbeiten link-lokal: Pakete werden an speziellen Multicast-Adressen gestoppt und nicht geroutet.

Keine Paketweiterleitung
Pakete von LLDP und CDP verbleiben stets auf dem physikalischen Segment. Switches leiten diese Frames standardmäßig nicht an andere Ports weiter.

2. TLV-Struktur



Sowohl LLDP als auch CDP kapseln alle Informationen in flexiblen TLV-Feldern. Dieses modulare Schema erlaubt das selektive Hinzufügen administrativer und hardwarenaher Metadaten.



- Type (Typ): Identifiziert das Datenfeld (z. B. Chassis-ID, Port-ID, TTL).
- Length (Länge): Gibt die exakte Byte-Länge des nachfolgenden Wertefelds an.
- Value (Wert): Enthält den eigentlichen Nutzdaten-wert wie MAC-Adresse, Portbezeichnung oder Systemname.
- LLDP-End-TLV: Markiert das Frame-Ende verbindlich mit Typ 0 und Länge 0.

3. Pflicht-TLVs & Kernattribute

Jede gültige LLDP-Nachricht muss einen fest definierten Satz an Basisfeldern enthalten, um eine eindeutige Zuordnung eibt das Nachbargeräts zu gewährhrleisten.

- Chassis ID TLV: Eindeutige Kennung des sendenden Geräts (meist Basis-MAC-Adresse).
- Port ID TLV: Identifikator der sendenden Schnittstelle (z. B. Interface-Name oder Port-Index).
- Time to Live (TTL) TLV: Gültigkeitsdauer der Information beim Empfänger (Standard: meist 120 Sekunden).
- Optionale TLVs: System Name, System Capabilities, Management-Adresse und VLAN-Zuordnung.



4. Protokollvergleich

Trotz identischem Anwendungszweck unterscheiden sich beide Standards in Spezifikation, Standardwerten und Standardisierungsgremien.

Merkmal	LLDP	CDP
Standard	IEEE 802.1AB (offen)	Cisco Proprietary (proprietär)
Multicast-Zieladresse	01:80:C2:00:00:0E	01:00:0C:CC:CC:CC
Sendeintervall / TTL	30 s / 120 s	60 s / 180 s
Erweiterungen	LLDP-MED (VoIP/PoE-Profile)	Cisco-VoIP-Appliances



5. LLDP-MED & PoE

LLDP-MED (Media Endpoint Discovery) erweitert LLDP um organisationsspezifische TLVs für Endgeräte wie IP-Telefone, Kameras und Access Points.

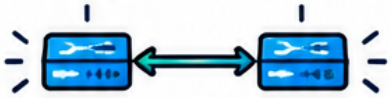
- Voice-VLAN-Zuweisung: Automatisches Einbuchen von IP-Telefonen in dedizierte Sprach-VLANs.
- Dynamisches PoE-Power-Management: Aushandlung von Leistungsaufnahmen in Milliwatt-Schritten.
- Netzwerkrichtlinien: Übermtitlung von QoS- und Layer-2-Priorisierungseinstellungen (CoS/DSCP).
- Inventarisierungsdaten: Übertragung von Seriennummer, Firmware-Stand und Modellbezeichnung.



6. Workflow: Automatisches Port-Mapping

Administratoren rekonstruieren und dokumentieren physische Verbindungstopologien mithilfe der Discovery-Tabellen auf den Switches.

1. **Nachbarschaftstabellen abrufen**
   CLI-Befehl auf dem Core-Switch ausführen (z. B. 'show lldp neighbors' oder 'show cdp neighbors detail').
2. **Lokale zu Remote-Ports korrelieren**
   Lokale Interface-Spalte dem gemeldeten Remote Device ID- und Neighbor Port ID-Feld zuordnen.
3. **Schleihen und Fehlsteckungen identifizieren**
   Unerwartete Uplinks oder parallele Verbindungen mit Spanning-Tree-Topologiedaten abgleichen.
4. **Topologiedatenbank aktualisieren**
   Die extrahierten Chassis- und Port-IDs in das zentrale IP-Management oder Monitoring-System übernehmen.



7. Sicherheitsbewertung & Risiken

Discovery-Protokolle senden unverschlüsselte Klartextinformationen. In nicht vertrauenswürdigen Netzwerkzonen stellen sie ein erbelliches Sicherheitsrisiko dar.

- Reconnaissance: Angreifer lesen Switch-Modelle, IOS-Versionen, IP-Adressen und VLANs passiv aus.
- Poisoning-Angriffe: Gefälschte Discovery-Pakete können Tabellenspeicher von Switches füllen.
- Härtungsempfehlung: LLDP und CDP auf Endnutzer- und Außen-Ports gezielt deaktivieren ('no lldp run', 'no cdp enable').
- Zugangsbeschränkung: Protokolle ausschlißlich auf Trunk-Ports zwischen vertrauenswürdigen Switches belassen.

Best Practice zur Schicht-2-Härtung
Deaktivieren Sie LLDP und CDP grundaställich auf allen Edge-Ports, an denen reguläre Arbeitstpatzrechner oder Drittgeräte angeschlossen sind.



8. Schnellreferenz & CLI-Befehle

Direkte Gegenüberstellung der essenziellen Überprüfungs- und Diagnosebefehle in typischen Switching-Betriebssystemen.

- Global aktivieren: 'lldp run (LLDP) bzw. 'cdp run' (CDP).
- Port-spezifisch steuren: 'lldp transmit' / 'lldp receive' bzw. 'cdp enable'.
- Tabellenanzeige kompakt: 'show lldp neighbors' bzw. 'show cdp neighbors'.
- Vollständige TLV-Details: 'show lldp neighbors detail' bzw. 'show cdp neighbors detail'.



NETZWERK-MINDMAP: AAA-SICHERHEITSARCHITEKTUR – RADIUS VS. TACACS+

AAA-SICHERHEITS-ARCHITEKTUR
RADIUS VS. TACACS+

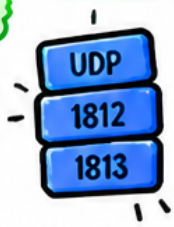
1. GRUNDLAGEN DER AAA-ARCHITEKTUR



Das AAA-Modell bildet das fundamentale Rahmenwerk fuer kontrollierten Netzuggriff und Systemverwaltung ueber drei getrennte Sicherheitsfunktionen.

- **Authentication:** Identitaetspruefung ueber Zugangsdaten (Passwort, Token, Zertifikat).
- **Authorization:** Zuweisung granularer Rechte, Privilegienstufen und Zugriffsrichtlinien nach erfolgreicher Identifikation.
- **Accounting:** Lueckenlose Protokollierung aller Sitzungszeiten, Befehle, uebertragenen Datenmengen und Statusaenderungen.

2. RADIUS-ARCHITEKTUR & FUNKTION



Remote Authentication Dial-In User Service (RADIUS) ist ein offener Standard nach RFC 2865 fuer Netzwerkzugriffskontrolle.

- **Transport:** Nutzt UDP ueber die Ports 1812 (Authentication/Autorisierung) und 1813 (Accounting).
- **Funktionskopplung:** Authentifizierung und Autorisierung sind fest in einer einzigen Anfragesequenz verknuepft.
- **Primaerer Einsatzbereich:** 802.1X-Portauthentifizierung im LAN, WLAN-WPA-Enterprise und VPN-Einwahl.

3. TACACS+-ARCHITEKTUR & FUNKTION

Terminal Access Controller Access-Control System Plus (TACACS+) ist ein auf Geraeteadministration spezialisiertes Protokoll.



- **Transport:** Arbeitet verbindungsorientiert ueber TCP Port 49 mit sicherem Handshake.
- **Modulare Trennung:** Authentifizierung, Autorisierung und Accounting koennen auf voellig separaten Servern betrieben werden.
- **Granulare Befehlsautorisierung:** Jeder einzelne CLI-Befehl auf Netzwerkkomponenten wird vor Ausfuehrung autorisiert.

4. PROTOKOLLVERGLEICH & KERNUNTERSCHIEDE

Ein direkter technischer Vergleich verdeutlicht die unterschiedlichen Schwerpunkte in Netzwerkbetrieb und Geraetemanagement.



- **Transport:** RADIUS verwendet verbindungslose UDP-Pakete; TACACS+ setzt auf zuverlaessiges TCP.
- **Dienstetrennung:** RADIUS buendelt AuthC/AuthZ;
- **Dienstetrennung:** RADIUS buendelt AutbC/AuthZ; TACACS+ trennt alle drei AAA-Funktionen strikt voneinander.
- **Verwendungsfokus:** RADIUS optimiert fuer Network Access (Clients); TACACS+ optimiert fuer Device Administration (Router/Switches).

5. VERSCHLUESSELUNG & SICHERHEITSEBENEN

Die Absicherung der Uebertragung unterscheidet sich grundlegend im Grad der Vertraulichkeit des Nutzdatenstroms.



- **RADIUS-Verschluesselung:** Verschluesselt ausschliesslich das Passwortfeld im Paket mittels MD5 Shared Secret; IP-Header und Attribute bleiben Klartext.
- **TACACS+-Verschluesselung:** Verschluesselt den vollstaendigen Paket-Payload; ledliglich der feste 12-Byte-TACACS-Header bleibt unverschluesselt.
- **Netzwerkschutz:** RADIUS-Verbindungen erfordren bei ungesicherten Strecken zusaetzlichen Schutz wie IPsec oder RadSec (TLS).



Sicherheitshinweis zum Abhoerschutz

RADIUS legt Benutzernamen und Autorisierungsattribute im Klartext offen. In sicherheitskritischen Umgebungen ist TLS/IPsec oder der Einsatz von TACACS+ fuer die Administration zwingend geboten.

6. WORKFLOW: 4-SCHRITTE ZUR AAA-KONFIGURATION

Strukturierte Schrittfolge zur Absicherung einer Netzwerk-komponente ueber einen zentralen AAA-Server.



- Sicherheitsmodell definieren
- Server-Endpunkte anbinden
- Authentifizierungsmethode zuweisen
- Lokalen Rueckfallpfad absichern

1. AAA-Funktion aktivieren
2. Server-Hosts & Shared Secret hinterlegen
3. Authentifizierungs- und Autorisierungs-listen anwenden
4. Lokalen Konsolen-zugang als Fallback absichern

7. PROTOKOLLAUSWAHL: ENTSCHEIDUNGSWEG

Entscheidungsbaum fuer Netzwerkarchitekten zur Bestimmung des geeigneten AAA-Protokolls fuer konkrete Einsatzszenarien.

- Zielgruppe des Zugangs analysieren
- Protokoll nach Einsatzzweck zuweisen

Welches primaere Zugriffsszenario soll im Netzwerk abgesichert werden?

- **Administrativer CLI-Zugriff auf Router, Firewalls und Switches mit granularer Befehlskontrolle** → **TACACS+ auswaehlen** (TCP Port 49, vollstaendige Payload-Verschluesselung, getrennte Befehlsautorisierung).
- **Endgeraete-Zugangskontrolle ueber 802.1X, WLAN-Enterprise oder Client-to-Site-VPN-Tunnel** → **RADIUS auswaehlen** (UDP Port 1812/1813, offener Standard, breite Unterstuetzung fuer Identity-Management).

8. AUDIT- & IMPLEMENTIERUNGSPROTOKOLL

Formular zur lueckenlosen Dokumentation der AAA-Implementierung und Pruefung im Betrieb.



- Zielsystem und IP-Adresse
- Primaerer AAA-Diensttyp
- Transportport und Verschluesselungsstatus
- Funktionspruefung des Fallback-Zugangs

SECURE SHELL (SSHv2) FÜR NETZWERKADMINISTRATION

1. WARUM NICHT TELNET?

- Telnet überträgt Daten als Klartext.
- Passwörter und Befehle können mitgeschnitten werden.
- Keine Verschlüsselung, keine Integritätsprüfung.



2. DREI-SCHICHTEN-ARCHITEKTUR

- Transport Layer: Verbindungsaufbau, Schlüsselaushandlung, Integrität.
- User Authentication Layer: Administrator-Authentifizierung.
- Connection Layer: Multiplexing von CLI, SCP, SFTP über eine Verbindung.



8. HÄRTUNG FÜR ROUTER & SWITCHES

- ACLs: Nur Management-VLANs.
- Timeouts & Limits: z. B. 300 s, max. Fehlversuche.
- OOBM: Getrennt vom Nutzerdatenverkehr.



3. SCHLÜSSELAUSTAUSCH & PFS

- Diffie-Hellman (DH/ECDH): gemeinsamer Sitzungsschlüssel.
- Keine Übertragung des Schlüssels.
- Perfect Forward Secrecy (PFS).



SSHv2 FÜR NETZWERKADMINISTRATION

Sicheres Management von Routern & Switches

7. DATENINTEGRITÄT (HMAC/AEAD)

- HMAC-SHA256: Unverfälschlichkeit.
- AEAD: Verschlüsselung + Integrität in einem Schritt.
- Replay-Schutz: Sequenznummern.



4. SCHLÜSSELKOLOKATION & HOST-KEYS

- TOFU: Host-Key in known_hosts.
- Validierung: Abweichung = Warnung.
- Individuelle RSA- oder Ed25519-Keys.



6. SYMMETRISCHE VERSCHLÜSSELUNG

- AES-GCM oder ChaCha20-Poly1305.
- 3DES und RC4: deaktiviert.
- Geringer Overhead, auch über WAN.



5. CLIENT-AUTHENTIFIZIERUNG

- Public Key: Ed25519 oder RSA.
- Passwort: verschlüsselt, anfällig.
- AAA: RADIUS oder TACACS+.



Zentrales Konzept: SSHv2 in der Netzwerkverwaltung

Secure Shell Version 2 (SSHv2) ersetzt unsichere Klartextprotokolle wie Telnet im Switch- und Router-Management. Es schützt administrative Befehle und Zugangsdaten durchgehend kryptografisch auf Anwendungsebene über TCP-Port 22.

- **Ablösung von Telnet:** Vollständige Unterbindung von Sniffing und Abfangen administrativer Zugangsdaten.
- **Kryptografische Absicherung:** Integrität, Authentifizierung und Vertraulichkeit ab dem Verbindungsaufbau.
- **Standard-Port:** TCP 22 als definierter Zielport für administrative Terminalsitzungen.

Sicherheitshinweis für Netzgeräte

SSHv1 gilt als kryptografisch gebrochen. Auf Routern und Switches ist SSHv1 zwingend zu deaktivieren und ausschließlich SSHv2 zu konfigurieren.

1. Warum nicht Telnet?

Telnet überträgt Benutzerkennung, Passwörter und Konfigurationsbefehle als Klartext im Netzwerk. Diese Daten können im selben Subnetz oder auf Durchgangsroutern mitgeschnitten werden.

- **Keine Verschlüsselung:** Klartext-Payload gefährdet Passwörter.
- **Fehlende Integritätsprüfung:** Man-in-the-Middle-Angriffe und Manipulation.
- **Richtlinie:** Telnet auf VTY-Lines abschalten (transport input ssh).

2. Drei-Schichten-Architektur

SSHv2 ist modular in drei Funkitonsebenen gegliedert, die aufienander aufbauen.

- **Transport Layer:** Kryptografischer Verbindungsaufbau, Serverauthentifizierung, Schlüsselaushandlung, Integrität.
- **User Authentication Layer:** Admin-Authentifizierung (Passwort oder Key).
- **Connection Layer:** Multiplexing (CLI, SCP, SFTP) über eine sichere TCP-Verbindung.

3. Schlüsselaustausch & Forward Secrecy

Der Sitzungsschlüssel wird über Diffie-Hellman ausgehandelt. PFS sorgt für zusätzliche Sicherheit.

- **Diffie-Hellman (DH/ECDH):** Gemeinsamer Sitzungsschlüssel über unsicheres Medium.
- **Keine Übertragung des Schlüssels.**
- **PFS:** Kompromittierung des Host-Schlüssels ermöglicht keine nachträgliche Entschlüsselung.

4. Schlüsselkollokation & Host-Keys

Der Client speichert den Host-Fingerprint lokal, um Manipulationen und Spoofing zu erkennen.

- **TOFU:** Host-Key in known_hosts.
- **Validierung:** Abweichung = Warnung.
- Router/Switches: RSA- oder Ed25519-Keys.

5. Symemtrische Payload-Verschlüsselung

Nach dem Handshake werden alle weiteren Befehle, Banner und Ausgaben verschlüsselt.

- AES-GCM oder ChaCha20-Poly1305.
- 3DES und RC4: strikt deaktiviert.
- Geringer Overhead, auch über WAN.

7. Datenintegrität mit MAC / AEAD

SSHv2 verhindert das Einfügen, Verändern oder Löschen von Befehlen im Datenstrom.

- **HMAC-SHA256:** Unverfälschlichkeit.
- **AEAD:** Verschlüsselung + Integrität.
- **Replay-Schutz:** Sequenznummern.

8. Härtung für Router & Switches

Ein Leitdaden zur Absicherung der virtuellen Terminalleitungen.

- **ACLs:** Nur designierte Management-VLANs.
- **Timeouts & Limits:** z. B. 300 Sekunden, max. Fehlversuche.
- **OOBM:** Physisch oder logisch vom Nutzerdatenverkehr trennen.

So konfigurieren Sie SSHv2 (Schritte)

1. Hostname & Domäne konfigurieren (Entropiebasis für Schlüsselgenerierung).
2. Asymmettrisches Schlüsselpaar erzeugen (RSA oder Ed25519, mind. 2048 Bit).
3. SSHv2 erzwingen und Telnet sperren (ip ssh version 2, transport input ssh).
4. Management-ACL binden (nur autorisierte Admin-IPs, TCP 22).

Prüfprotokoll

- SSHv2-Version und Host-Key-Fingerprint überprüft? ☐
- Telnet auf allen VTY-Ports (0-15) vollständig blockiert? ☐

Entscheidungshilfe

Welche Authentifizierungsmethode soll für die Router-Administration gewählt werden?

- **Zentraler Unternehmensverbund mit Directory-Service vorhanden**
  → AAA an TACACS+ oder RADIUS anbinden.
- **Isoliertes oder dezentrales Netzwerkgerät ohne AAA-Server**
  → Public-Key-Authentifizierung mit individuellem Schlüsselppar.

HTTPS & TLS-TERMINIERUNG IM NETZWERKBETRIEB

1. GRUNDLAGEN VON HTTPS & TLS

HTTPS sichert die HTTP-Übertragung über Port 443 durch Transport Layer Security (TLS) ab. Ziel ist der Schutz vor Manipulation und Lauschangriffen im Netz.

- Verschlüsselung schützt Datenpakete vor Mitlesen im Transit.
- Server-Authentifizierung bestätigt die Identität gegenüber dem Client.
- Integritätsprüfungen verhindern unbemerkte Datenveränderungen.
- Standardport für gesicherte Webservices ist TCP 443.

PROTOKOLL-EVOLUTION
Veraltete SSL-Versionen (2.0/3.0) sowie TLS 1.0 und 1.1 gelten als unsicher und müssen netzwerkweit deaktiviert sein.

2. TLS-HANDSHAKE & SCHLÜSSELAUSTAUSCH

Vor der Übertragung von Nutzdaten handeln Client und Server Verschlüsselungsparameter und Sitzungsschlüssel in einem strukturierten Handshake aus.

- ClientHello initiiert die Verbindung und nennt unterstützte Cipher Suites.
- ServerHello wählt die Cipher Suite und sendet das TLS-Zertifikat.
- Asymmetrische Kryptografie sichert den ersten Schlüsselaustausch.
- Symmetrische Sitzungsschlüssel verschlüsseln den eigentlichen Nutzdatenstrom.

DER HANDSHAKE IN 4 SCHRITTEN

1. ClientHello & ServerHello
   Aushandeln von Version, Algorithmen und Zufallswerten.
2. Zertifikatsvalidierung
   Prüfung von Kette, Gültigkeit und Hostname.
3. Schlüsselaustausch
   Berechnung gemeinsamer Schlüssel (z. B. ECDHE).
4. Finished & Verschlüsselter Datenkanal
   Bestätigung der Integrität und Wechsel auf symmetrisch.

3. ZERTIFIKATE & PUBLIC-KEY-INFRASTRUKTUR (PKI)

X.509-Zertifikate binden kryptografische öffentliche Schlüssel verifizierbar an Domain-Namen und Unternehmensidentitäten.

- Certificate Authority (CA) signiert und garantiert die Echtheit.
- Root- und Intermediate-Zertifikate bilden die Vertrauenskette.
- Domain Validation (DV) prüft Domain-Kontrolle automatisiert.
- Zertifikatssperren werden per CRL oder OCSP abgefragt.

4. CIPHER SUITES & KRYPTOGRAFISCHE STANDARDS

Cipher Suites definieren die Kombination aus Schlüsselaustausch, Authentifizierung, symmetrischer Chiffre und Hashverfahren.

- Forward Secrecy (PFS) stellt sicher, dass vergangene Sitzungen auch bei Key-Leak geschützt bleiben.
- TLS 1.3 vereinfacht die Suiten (z. B. TLS_AES_256_GCM_SHA384) und entfernt unsichere Algorithmen.
- Vermeidung veralteter Chiffren wie RC4, 3DES, CBC-Modi sowie MD5 und SHA-1.
- AEAD-Chiffren garantieren Vertraulichkeit und Integrität.

KONFIGURATIONSPRAXIS
Im modernen Netzwerkbetrieb sollten vorrangig TLS 1.3 und als Faliback TLS 1.2 mit ECDHE und AES-GCM konfiguriert werden.

5. TLS-OFFLOADING & EDGE-TERMINIERUNG

Reverse Proxies, Load Balancer und Application Delivery Controller (ADCs) terminieren TLS am Netzwerkrand zur Entlastung interner Systeme.

- Entlastung interner Applikationsserver von rechenintensiven Krypto-Operationen.
- Zentrale Zertifikatsverwaltung und einheitliche Erneuerung am Border-Gateway.
- Ermöglicht Deep Packet Inspection (DPI) und Web Application Firewalling (WAF).
- Backend-Netze müssen durch Segmentierung (VLAN/mTLS) adäquat geschützt werden.



6. ABSICHERUNG VON ADMIN-SCHNITTSTELLEN

Verwaltungsschnittstellen von Routern, Switches und Firewalls erfordern strikte TLS-Richtlinien und Zugriffskontrollen.

- Deaktivierung unverschlüsselter Protokolle wie HTTP (Port 80) und Telnet (Port 23).
- Einsatz gültiger interner Zertifikate statt ignorierter Self-Signed-Warnungen.
- Erzwingen von HSTS (HTTP Strict Transport Security) gegen Downgrade-Angriffe.
- Kombination mit Out-of-Band-Management (OOBM) und strikten Firewall-Regeln.

7. PRAXIS-CHECKLISTE: TLS-TERMINIERUNG AUDITIEREN

Schrittweises Vorgehen bei der Inbetriebnahme oder Überprüfung eines Netzwerkrandgeräts mit TLS-Terminierung.

- Gültigkeit und Trust-Chain des Zertifikats auf Edge-Geräten verifizieren.
- Cipher Suites auf TLS 1.2/1.3 mit PFS einschränken.
- HTTP-zu-HTTPS-Weiterleitung (301) und HSTS-Header konfigurieren.
- Backend-Kommunikation absichern (Re-Encryption oder dediziertes Management-VLAN).

WELCHES SICHERHEITSNIVEAU ERFORDERT DIE INTERNE BACKEND-STRECKE?

Sensibles Backend oder Zero-Trust-Architektur
TLS-Bridging (Re-Encryption) mit internem Zertifikat oder mTLS zwischen Proxy und Server.

Isoliertes, physikalisch getrenntes Management-VLAN
Klassisches TLS-Offloading zulässig; strikte ACLs und Paketfilterung auf Schnittstellenebene.

8. ZUSAMMENFASSUNG & MERKSÄTZE

Wesentliche Kernpunkte für Administratoren und Netzwerker im täglichen Betrieb.

- HTTPS ist Standard für alle webbasierten Netzwerkdienste und GUIs.
- TLS-Terminierung spart Serverressourcen, verlangt aber Schutz im Backend.
- Nur moderne Protokolle (TLS 1.2/1.3) und PFS-Cipher Suites aktivieren.
- Zertifikatslebenszyklen automatisiert überwachen, um Ausfälle zu vermeiden.

APPLICATION DELIVERY CONTROLLER & SERVER LOAD BALANCING

Der ADC steuert den Datenverkehr, verteilt Anfragen auf mehrere Server und sorgt für hohe Verfügbarkeit, Skalierbarkeit und optimale Antwortzeiten.

1. GRUNDPRINZIP: ADC & SLB



Ein Application Delivery Controller (ADC) steuert als intelligenter Middlebox-Konten den eingehenden Datenverkehr vor Serverfarmen. Server Load Balancing (SLB) verteilt Client-Anfragen gezielt auf mehrere Backend-Server, um Überlastung zu verhindern und Ausfallsicherheit zu garantieren.

- **Single Point of Contact:** Clients kommunizieren primär mit einer virtuellen IP (VIP) des Load Balancers.
- **Entkopplung:** Backend-Server bleiben vor direktem Internetzugriff geschützt und skalierbar.
- **Traffic-Inspektion:** Erweiterte Layer-4 bis Layer-7 Prüfung vor Weiterleitung der Pakete.

2. LAYER-4 VS. LAYER-7 BALANCING



Die Verteilung erfolgt je nach Netzwerkschicht anhand unterschiedlicher Parameter im Paket-Header.

- **Layer 4 (Transport Layer):** Weiterleitung rein nach IP-Adresse und TCP/UDP-Port ohne Einblick in Payload.
- **Layer 7 (Application Layer):** Routing basierend auf HTTP-Headern, URL-Pfaden, Cookies oder Datentypen.
- **Ressourceneinsatz:** L4 bietet extremen Durchsatz; L7 benötigt mehr Rechenleistung für Inhaltsanalyse.

3. STATISCHE & DYNAMISCHE VERTEILALGORITHMEN



Die Auswahl des Zielknotens erfolgt nach festgelegten mathematischen Heuristiken und Systemmetriken.

- **Round Robin:** Reihum-Verteilung ohne Berücksichtigung der aktuellen Serverkapazitäten.
- **Weighted Round Robin:** Bevorzugung leistungsstärkerer Serverknoten über statische Gewichtungsfaktoren.
- **Least Connections:** Zuweisung an den Knoten mit den wenigsten aktiven offenen TCP-Verbindungen.
- **Response Time:** Berücksichtigung der geringsten Latenzzeit bei dynamischer Serverrückmeldung.

4. SESSION AFFINITY & STICKY SESSIONS



Stateful Webapplikationen verlangen oft, dass ein Client während einer Nutzersitzung konsistent an denselben Server gebunden bleibt.

- **Session Affinity:** Bündelung zusammenhängender Anfragen über einen gemeinsamen Bezeichner.
- **Quell-IP-Hash:** Zuweisung per Hashing der Client-IP (anfällig bei NAT-Gateways und Proxys).
- **Cookie-Insertion:** Der ADC setzt ein Tracking-Cookie zur eindeutigen Backend-Zuordnung.

5. HEALTH CHECKS & MONITORING



Kontinuierliche Überwachung stellt sicher, dass ausgefallene Serverfarm-Mitglieider automatisch aus dem Datenpfad entfernt werden.

- **Layer-3 Ping:** Prüft reine ICMP-Erreichbarkeit der Ziel-IP.
- **Layer-4 Port-Check:** Verifiziert erfolgreichen TCP-Drei-Wege-Handshake auf Service-Ports (z. B. Port 443).
- **Layer-7 Health Check:** Sendet echte HTTP-Anfragen (z. B. GET /health) und prüft auf HTTP 200 OK.

6. SSL/TLS OFFLOADING & TERMINATION



Der ADC entlastet Webserver von der kryptografisch aufwendigen Ver- und Entschlüsselung von TLS-Sessions.

- **SSL-Termination:** Handshake und Entschlüsselung am ADC; Klartext-HTTP im internen Netzsegment.
- **SSL-Bridging:** Re-Verschlüsselung zwischen ADC und Server für End-to-End Zero-Trust-Vorgaben.
- **Zentrales Zertifikatsmanagement:** Aktualisierung und Renewal von Zertifikaten an einer zentralen Stelle.

7. HOCHVERFÜGBARKEIT & CLUSTER-BETRIEB



Load Balancer werden redundant betrieben, um keinen Single Point of Failure in der Netzwerkinnfrastruktur darzustellen.

- **Aktiv/Passiv (Failover):** Sekundärer Knoten übernimmt die VIP bei Ausfall via Heartbeat-Protokoll (z. B. VRRP).
- **Aktiv/Aktiv:** Beide ADC-Einheiten verarbeiten gleichzeitig Anfragen und teilen die Gesamsystemlast.
- **Session Synchronization:** Laufende State-Tabellen werden laufend zwischen den Geräten abgegliichen.

8. ZUSAMMENFASSUNG & PRAXIS-CHECKLISTE



Kompakter Leitfaden zur Überprüfung und Implementierung von Lastverteilungsmechanismen im eigenen Netzwerk.

- **Schichtwahl prüfen:** L4 für maximale Paketrate, L7 für URL-Routing und Session-Handling wählen.
- **Algorithmus anpassen:** Least Connections für ungleiche lange Sessions bevorzugen.
- **Tiefe Health Checks etablieren:** Stets Layer-7 Statuscodes statt reiner ICMP-Pings auswerten.
- **Redundanz absichern:** Heartbeat-Verbindungen isolieren und Failover-Zeiten testen.



Praxis-Hinweis für Netzwerker
Ein reiner ICMP-Ping meldet auch dann Erfolg, wenn der Webdienst auf Port 80/443 abgestürzt ist. Health Checks müssen immer die tatsächliche Anwendungsfunktion abfragen.

MINDMAP: FORWARD PROXY VS. REVERSE PROXY ARCHITEKTUREN

1. DEFINITION & GRUNDKONZEPT



Ein Proxy fungiert als vermittelnder Knoten (Middlebox) zwischen Kommunikationspartnern auf Anwendungsebene. Ein Forward Proxy vertritt interne Clients gegenüber externen Webservern, während ein Reverse Proxy interne Webserver gegenüber externen Clients abschirmt.

- **Forward Proxy:** Client-orientiert, fängt ausgehende Anfragen aus dem lokalen Netz ab.
- **Reverse Proxy:** Serwer-orientiert, nimmt eingehende Internet-Anfragen für Webserver-Cluster entgegen.
- **Schnittstellen-Entkopplung:** Beide Varianten trennen die direkte TCP/IP-Sitzung in zwei eigenständige Sitzungen auf.

2. FUNKTIONSWEISE DES FORWARD PROXY



Der Forward Proxy nimmt HTTP/HTTPS-Requests von internen Arbeitsplatzrechnern entgegen, ersetzt die Absender-IP durch seine eigene und leitet die Pakete an das Internet weiter. Die Identität der internen Rechner bleibt für externe Webserver verborgen.

- **Transparenter Proxy:** Leitet Datenverkehr ohne explizite Client-Konfiguration über Routing-Regeln um.
- **Expliziter Proxy:** Browser oder Betriebssystem werden per Proxy-PAC oder fester IP/Port-Angabe konfiguriert.
- **Verbindungsaufbau:** Terminierung der internen Sitzung und Neuaufbau einer externen Sitzung.

8. ARCHITEKTURVERGLEICH & PRAXISREGELN



Die Wahl des richtigen Proxy-Typs hängt von der Schutzrichtung und dem Anwendungsziel ab. Folgende Kernregeln leiten das Netzwerkdesign.

- **Richtung:** Forward schützt/steuert Clients nach außen; Reverse schützt Server nach innen.
- **Sicherheitsperimeter:** Forward Proxys stehen am Client-Gateway; Reverse Proxys in der DMZ vor dem Web-Cluster.
- **Kombinierbrakeit:** Moderne Unternehmensnetze nutzen zeitgleich beide Systeme für durchgängigen Schütz.

3. FUNKTIONSWEISE DES REVERSE PROXY



Der Reverse Proxy ist an der Peripherie des Servernetzwerks platziert. Aus Sicht des externen Nutzers agiert er als der eigentliche Ziel-Webserver. Nach der Anforderungsanalyse leitet er die HTTP-Anfrage an den passenden Backend-Server im internen Netz weiter.

- **Zentraler Einstiegspunkt:** Eine öffentliche IP-Adresse bedient Hunderte interne Applikationsdienste.
- **Netzwerkisolierung:** Backend-Webserver erhalten ausschließlich private IP-Adressen ohne Internet-Routing.
- **Protokollumstezung:** Ermöglicht HTTPS-Terminierung extern und optimierte HTTP/gRPC-Kommunikation intern.



FORWARD PROXY VS. REVERSE PROXY ARCHITEKTUREN

7. LASTVERTEILUNG & HOCHVERFÜGBARKEIT



Diese Kernfunktion des Reverse Proxys vertielt eingehenden Datenverkehr dynamisch auf mehrere Backend-Instanzen, um Überlastung za verhindern und Ausfallsicherheit zu garantieren.

- **Verteilungsalgorithmen:** Round Robin, Least Connections oder IP-Hash zur Sitzungsbindung.
- **Health Checks:** Kontinuielithie Überwachung der Backend-Server; automatsiche in der DMZ vor dem Web-Cluster.
- **SSL/TLS-Offloading:** Rechenintensive Kryptografie wird am Proxy gebündelt, was Backend-Server entlastet.

4. CACHING-MECHANISMEN



Zwischenspeicher entlasten Netzwerkanbindungen und beschleunigen Antwortzeiten drastisch. Forward- und Reverse-Proxies nutzen HTTP-Header, um statische und dynamische Inhalte temporär vorzuhalten.

- **Forward Cache:** Speichert häufig abgerufene Internet-Ressourcen (z. B. Software-Updates) für alle LAN-Clients.
- **Reverse Cache:** Pufferung statischer Assets (Bilder, CSS, HTML) zur Reduzierung der Last auf Backend-Datenbanken.
- **Cache-Validierung:** Steuerung über standardisierte Header wie "Cache-Control", "ETag" und "Expires".

6. ANONYMISIERUNG & IDENTITÄTSSCHUTZ



Die Trennung von Verbindungsketten verschleiert Netzwerkinformationen. Beide Proxy-Arten schützen gezielt unterschiedliche Entitäten vor unerwünschter Aufklärung.

- **Client-Schutz:** Externe Server sehen nur die WAN-IP des Forward Proxys; LAN-Subnetze bleiben unerkennbar.
- **Server-Schutz:** Angreifer sehen weder IP noch Betriebssystem der Backend-Server hinter dem Reverse Proxy.
- **Header-Sanitization:** Entfernung interner Header ("X-Powered-By", "Server") zur Erschwerung von Fingerprinting.

5. INHALTSFILTERUNG & CONTENT INSPECTION



Proxies analysieren den Nutzdatenstrom der Anwendungsschicht (Layer 7). Sie setzen Sicherheits- und Zugriffsrichtlinien durch, die auf Paketfiltern (Layer 3/4) nicht realisierbar sind.

- **URL- & Domain-Filtering:** Blockieren unerwünschter oder bösartiger Websites anhand von Reputationslisten.
- **Malware-Scanning:** Antiviren-Prüfung von ein- und ausgehenden Dateidownloads direkt im Datenstrom.
- **DLP (Data Loss Prevention):** Filterung vertraulicher Informationen in ausgehenden HTTP-POST-Anfragen.

ARCHITEKTUR-ENTSCHEIDUNGSHILFE



Verwenden Sie diesen Entscheidungsbaum, um die passende Proxy-Komponente für Ihre Netzwerkanforderung zu identifizieren.

Welches Schutzziel bzw. welcher Kommunikationspfad soll implementiert werden?



Interne Clients surfen im Internet und Downloads müssen auf Viren geprüft werden.

→ **Implementieren Sie einen Forward Proxy mit integrierter Layer-7-Inhaltsfilterung und Antivirus-Engine am LAN-Gateway.**



Ein Webserver-Cluster im Rechenzentrum soll vor direkten externen Angriffen geschützt und die HTTPS-Last verteilt werden.

→ **Setzen Sie einen Reverse Proxy mit SSL-Offloading und Load Balancing in der demilitarisierten Zone (DMZ) ein.**

Hinweis zur SSL-Inspektion

Beim Einsatz von SSL/TLS-Terminierung auf einem Forward Proxy ist der Rollout interner Stammzertifikate auf allen Clients zwingend erforderlich, um Browser-Sicherheitswarnungen zu vermeiden.

CONTENT DELIVERY NETWORKS (CDN): FUNKTIONSWEISE UND EDGE CACHING



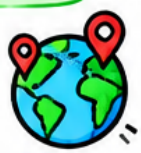
1. GRUNDPRINZIP UND ARCHITEKTUR



Ein Content Delivery Network (CDN) ist ein geografisch verteiltes Nettwerk aus Proxy- und Edge-Servern. Es minimiert Latenzzeiten und reduziert die Belastung des zentralen Ursprungsservers (Origin Server).

- Origin Server: Primäre Datenquelle, hält die Masterkopie aller Daten
- Edge Server (PoP): Weltweit verteilte Caching-Knoten in Nutzer-Nähe
- Latenzminimierung: Reduzierung der Round Trip Time (RTT) für Webassets

2. ROUTING-VERFAHREN IM CDN



Um Client-Anfragen an den optimalen Edge-Server zu leiten, kombinieren CDNs intelligente Routing-Mechanismen auf Netzwerk- und DNS-Ebene.

- Anycast Routing: Identische IP-Adresse an mehreren Standorten via BGP
- GeoDNS: DNS-Server antwortet mit IP des nächstgelegenen PoP basierend auf Client-Standort
- Lastverteilung: Automatische Laststeuerung bei Überlastung einzelner PoPs

3. CACHING-STRATEGIEN UND HEADER



Edge Server speichern Inhalte gemäß standardisierter HTTP-Cache-Header CDNs, um redundante Datenabfragen beim Ursprungsserver zu vermeiden.

- Cache-Control: Steuerung über max-age, public, private und no-store
- ETag & Last-Modified: Validierungs-mechanismen für bedingte HTTP-Anfragen (304 Not Modified)
- Stale-While-Revalidate: Sofortige Auslieferung gecachter Daten bei asynchroner Aktualisierung

4. INHALTSTYPEN: STATISCH VS. DYNAMISCH



CDNs differenzieren zwischen sofort speicherbarer statischen Assets und zustandsbehafteten dynamischen Datenflüssen.

- Statischer Content: HTML, Bilder, CSS, JS und Video-Segmente verbeiben im Cache
- Dynamischer Content: Personalisierte API-Aufrufe und Logins passieren den Cache
- Edge Computing: Ausführung von Serverless-Code (Workers) direkt am PoP

5. CACHE INVALIDATION UND PURGING

Änderungen am Ursprungsserver erfordern gezielte Mechanismen, um veraltete Kopien auf allen Edge-Knoten unmitteblar zu entwerten.

- TTL-Ablauf: Netürliches Verfallen des Caches nach konfigurierter Zeitspanne
- Instant Purge: Gezieltes Löschen per API-Call für Pfade, URLs oder Tags
- Cache Bypassing: Umgehung des Caches via Versions-Parameter in der URL



6. SICHERHEIT AM NETZWERK-EDGE

Durch die Positionierung zwischen Client und Origin dient das CDN als vorgelagertes Schutzschild gegen Angriffe.

- DDoS-Mitigation: Absorbieren massiver Volumendatenströme durch globale Bandbreite
- Web Application Firewall (WAF): Blockieren von SQLi, XSS und bösartigen Bots am Edge
- TLS-Terminierung: Schneller HTTPS-Handshake in geografischer Nutznähe



7. WORKFLOW EINER CDN-ANFRAGE



Vollständiger Lebenszyklus einer Client-Anfrage von der DNS-Auflösung bis zur Antwortzustellung.

1. **Schritt 1: DNS-Auflösung**
   Client sendet DNS-Request und erhält via Anycast/GeoDNS die IP-Adresse des optimalen PoP.
2. **Schritt 2: Edge-Prüfung**
   Client verbnidet sich mit dem Edge Server; dieser prüft seinen lokalen Cache auf Treffer (Cache Hit).
3. **Schritt 3: Origin-Abruf bei Miss**
   Bei Cache Miss holt der PoP die Datei vom Origin Server, speichert sie lokal und liefert sie an den Client.

8. ENTSCHEIDUNGSMATRIX: CACHE-HIT VS. CACHE-MISS

Operativer Ablauf an den PoP-Knoten basierend auf dem Vorhandeneien und der Gültigkeit gecachter Daten.



Praxis-Hinweis
Eine hohe Cache-Hit-Ratio (typisch > 85 %) schont Origin-Ressourcen und sichert minimale Reaktionszeiten.

Liegt das angeforderte Asset im Edge-Cache vor und ist seine Gültigkeit (TTL) noch intakt?

Cache Hit:
Asset im PoP vorhanden und unverändert gültig

Sofortige Auslieferung an den Client direkt vom Edge-Speicher mit minimaler Latenz.

Cache Miss / Stale:
Asset fehlt oder max-age ist abgelaufen

PoP sendet Backend-Anfrage an den Origin Server, erneuert den lokalen Cache und bedient danach den Client.

ANYCAST-ROUTING: KONZEPTE UND ANWENDUNGSBEREICHE

1. DEFINITION & GRUNDPRINZIP



Anycast ist ein Adressierungs- und **Routing-Verfahren**, bei dem **dieselbe IP-Adresse mehreren** physischen Hosts an verschiedenen **Standorten** zugewiesen wird. Das Netzwerk routet **Pakete automatisch** zum topologisch **nächstgelegenen Knoten.**

- **One-to-Nearest:** Ein Sender kommuniziert mit dem nach Routing-Metrik am besten erreichbaren Knoten.
- **Gemeinsame IP:** Mehrere Server nutzen dieselbe Unicast-IP-Adresse ohne Adresskonflikt.
- **Automatische Redundanz:** Fällt ein Standort aus, übernimmt der nächste verfügbare Knoten transparent.

2. BGP- VS. IGP-ANYCAST



Anycast wird sowohl global über das Internet als auch intern innerhalb isolierter Netzwerktopologien implementiert.

- **BGP-Anycast (Global):** Autonome Systeme kündigen dasselbe IP-Präfix über eBGP an; das Internet wählt Routen nach AS-Hop-Count.
- **IGP-Anycast (Lokal):** Nutzung innerhalb eines Rechenzentrums via OSPF oder IS-IS basierend auf Latenz- oder Bandbreitenmetriken.
- **Routing-Konvergenz:** Routenwechsel bei BGP dauern im weltweiten Netz länger als im internen IGP.

8. ARCHITEKTUR-ZUSAMMENFASSUNG



Kompakter Spickzettel für den praktischen Einsatz von Anycast in Netzwerkarchitekturen.

- **Ideal für:** DNS, CDN-Edge, NTP und DDoS-Schutzsysteme.
- **Ungeeignet für:** Lange TCP-Sessions mit großen Datentransfers ohne Failover-Architektur.
- **Faustregel:** Anycast verteilt Routing-Pfade, ersetzt aber keinen lokalen Load-Balancer vor Ort.

Praxis-Hinweis zu Anycast & BGP
Im Internet akzeptieren Tier-1-Provider aus Sicherheits- und Skalierungsgründen typischerweise keine BGP-Präfixe, die kleiner als /24 (IPv4) oder /48 (IPv6) sind.

3. DNS-INFRASTRUKTUR



Das globale Domain Name System (DNS) ist der historisch wichtigete und stabilste Anwendungsfall für globales Anycast.

- **Root- & TLD-Nameserver:** Nahezu alle [illegible] Root-Server-Identitätes (A bis M) bestehen aus hunderten Anycast-Instanzen.
- **UDP-Vorteil:** Einzelne DNS-Anfragen (Request-Response) sind zustandslos und resistent gegen Routenfluktuation.
- **Latenzreduktion:** Anfragen europäischer Nutzer werden direkt in lokalen Rechenzentren beantwortet.

ANYCAST-ROUTING



4. CDN & WEB-BESCHLEUNIGUNG



Content Delivery Networks (CDNs) bringen statische und gecachte Inhalte geografisch nah an die Endbenutzer heran.

- **Edge-PoPs:** Anycast führt HTTP/HTTPS-Traffic [illegible] zum am nächsten liegenden Point of Presences.
- **TCP-Herausforderung:** Route Flapping kann bestehende TCP-Verbindungen abbrechen (Connection Reset).
- **Moderne Mitigierung:** BGP-Tuning, Keep-Alive-Optimierung und QUIC/HTTP3 mindern Verbindungsprobleme.

7. BEREITSTELLUNGS-WORKFLOW



Vier Kernschritte zur Einrichtung eines Anycast-fähigen Edge-Dienstes.

1. **IP-Präfix & ASN bereitstellen**
   [illegible] Einrichtung redundanter Server an Zielstandorten mit identischen Diensten und IP-Bindungen auf Dummy/Loopback-Interfaces.
3. **BGP-Peering & Health Checking**
   Kopplung lokaler Routing-Dämonen (z. B. BIRD oder FRR) mit Upstream-Routern; automatischer Rückzug bei Dienstausfall.
4. **Monitoring & Validierung**
   Laufende Überwachung weltweiter Routing-Pfade und Latenzen mittels global verteilter Test-Probes.

5. DDoS-MITIGIERUNEN & LASTVERTEILUNG



Anycast bildet ein mächtiges Schutzschild gegen voluminöse Denial-of-Service-Angriffe.

1. **Angriffszerstreuung:** Angriffsverkehr von Botnetzen wird auf Dutzende globale Standorte aufgeteilt, statt ein System zu überlasten.
2. **Lokale Filterung:** Bösartiger Datenverkehr wird direkt an den Edge-Knoten verworfen (Scrubbing Centers).
4. **Schutz des Urspriellung:** Der eigentiiche Origin-Server bleibt verborgen und operiert ungestört.

6. BERAUSFORDERUNGEN & RISIKEN



Der Betrieb einer Anycast-Architektur birgt spezifische operative und technische Fallstricke.

- **Zustandsbehaftete Protokolle:** TCP-Handshakes und Dateitransfers können bei Routing-Änderungen mitten im Strom abbrechen.
- **Debugging-Komplexität:** Monitoring und Traceroute-Analysen erfordern standortspezifische Messpunkte (Looking Glasses).
- **Ungleiche Lastverteilung:** BGP-Metriken richten sich nach AS-Pfaden, nicht nach der Serverkapazität oder Netzwerkauslastung.

RECHENZENTRUMS-ARCHITEKTUREN: SPINE-LEAF & CLOS

1. WAS IST ES



Spine-Leaf ist eine zweistufige Netzwerktopologie basierend auf den Prinzipien von Charles Clos. Jeder Leaf-Switch ist redundant mit ausnahmslos jedem Spine-Switch verbunden, wodurch eine blockierungsfreie Fabric entsteht.

- Evolviert aus mehrstufigen Clos-Netzwerken für hohe Skalierbarkeit.
- Ersetzt traditionelle drestufige Hierarchien (Core-Aggregation-Access).
- Jeder Leaf-Switch verbindet Server und Storagesysteme direkt.

2. OST-WEST-TRAFFIC



Moderne Cloud-Workloads wie Microservices, Hadoop und Container-Cluster kommunizieren überwiegend horizontal zwischen Servern (Ost-West), anstatt vertikal nach außen (Nord-Süd). Spine-Leaf minimiert Latenzen und Engpässe für diese horizontalen Datenströme.

- Ost-West-Traffic dominiert über 80 % des Datenverkehrs im RZ.
- Nord-Süd-Verkehr läuft über dedizierte Border-Leaves zum WAN/Internet.
- Verhindert Bandbreitenflaschenhälse auf aggregierten Uplinks.

3. DETERMINISTISCHE LATENZ



In einer Spine-Leaf-Topologie beträgt der Pfad zwischen beliebigen zwei Servern an unterschiedlichen Leaf-Switches exakt denselben Abstand: Server zu Leaf, zu Spine, zu Leaf, zum Zielserver.

- Genau 3 Switch-Hops zwischen beliebigen Server-Endpunkten.
- Keine unvorhersehbaren Verzögerungen durch asymmetrisches Routing.
- Gleichmäßige Dienstqualität (QoS) für zeitsensitive Datenströme.

4. ECMP & BGP/OSPF



Spine-Leaf setzt auf Layer-3-Routing bis zum Leaf-Switch. Equal-Cost Multi-Pathing (ECMP) verteilt Datenpakete gleichmäßig über alle parallelen Spine-Verbindungen, ohne redundante Pfade künstlich abzuschalten.

- BGP (häufig eBGP) oder OSPF steuern die dynamische Pfadwahl.
- ECMP untzt 100 % der installierten Glasfaser-Bandbreite parallel.
- Automatisches Rerouting im Millisekundenbereich bei Link-Ausfall.

5. ABLÖSUNG VON SPANNING TREE



Klassisches Spanning Tree Protocol (STP) blockierte 50 % oder mehr aller Verbindungen zur Schleifenvermeidung. In reinen L3-Fabrics mit Spine-Leaf entfällt STP vollständig.

- Schluss mit inaktiven Standby-Links und verschwendeten Uplinks.
- Keine netzwerkweiten Broadcast-Stürme oder STP-Konvergenzpausen.
- Transparente Skalierung bei voller Fehlertoleranz.

6. SKALIERUNGSPRINZIPIEN



Die Kapazität einer Spine-Leaf-Fabric lässt sich modular und unterbrechungsfrei anpassen, indem spezifische Komponenten unabhängig voneinander erweitert werden.

- Mehr Endgeräte/Server nötig: Neuen Leaf-Switch hinzufügen und an alle Spines anbinden.
- Mehr Fabric-Bandbreite nötig: Zusätzlichen Spine-Switch einsetzen und mit allen Leaves verkabeln.
- Keine Rekonfiguration der bestehenden Server-Verkabelung erforderlich.

7. OVERLAY-NETZWERKE (VXLAN / EVPN)



Um Layer-2-Mobilität für virtuelle Maschinen über die Layer-3-Fabric hiweg bereitzustellen, werden moderne Overlay-Technologien eingesetzt.

- VXLAN kapselt L2-Frames in UDP-Pakete über die
- BGP-EVPN dient als Control-Plane zur Verteilung von MAC- und IP-Routen.
- Ermöglicht Mandantenfähigkeit und flexibles VM-Verschieben ohne L2-Domänen-Risiken.

8. ZUSAMMENFASSUNG & BEST PRACTICES



Spine-Leaf bietet den de-facto Standard für moderne Rechenzentrums-Netzwerke: hochverfügbar, modular skalierbar und maßgeschneidert für massiven horizontalen Datenverkehr.

- Underlay: Robustes L3-Routing mit ECMP über alle Spines.
- Overlay: VXLAN/EVPN für virtualisierte Umgebungen.
- Dimensionierung: Portdichte der Spine-Switches bestimmt die maximale Leaf-Anzahl.



PRAXIS-MERKSATZ

Leaf-Switches sprechen niemals direkt miteinander und Spine-Switches untereinander ebenfalls nicht – jede Verbindung führt immer zwischen Leaf und Spine.

DATA CENTER BRIDGING (DCB) & LOSSLESS ETHERNET

1. WAS IST DATA CENTER BRIDGING (DCB)?



Data Center Bridging (DCB) bezeichnet eine standardisierte Erweiterung des klassischen IEEE 802.1 Ethernet-Standards, um ein verlustfreies Übertragungsmedium bereitzustellen.

- Löst das Problem von Paketverlusten (Packet Drops) bei Überlastung im Switching-Fabric.
- Grundvorauszetzung für konvergente Rechenzentrumsnetze (LAN und SAN auf einer Infrastruktur).
- Ermöglicht den Verzicht auf separate Fibre-Channel-Verkabelungen durch FCoE und RoCE.

Kernziel: Zero Packet Drop
Herkömmliches Ethernet verwirft Pakete bei vollem Puffer (Best Effort). DCB garantiert Pufferverfügbarkeit für kritischen Speicherverkehr.

2. WARUM LOSSLESS ETHERNET BENÖTIGT WIRD



Klassische SAN-Speicherprotokolle und HPC-Cluster stellen gänzlich andere Anforderungen an die Latenz und Zuverlässigkeit als gewöhnlicher Web- und IP-Verkehr.

- Speicherprotokolle wie Fibre Channel tolerieren keine Frame-Verluste ohne massive I/O-Einbrüche.
- TCP-Retransmissions erzeugen untragbare Latenzspitzen für verteilte High-Performance-Berechnungen.
- Reduziert Anschaffungs- und Betriebskosten durch Bündelung von Server-Ports und Switches.

3. PFC – PRIORITY-BASED FLOW CONTROL (802.1Qbb)



PFC erweitert das globale Ethernet-PAUSE-Signal auf einzelne Datenprioritäten (Class of Service).

- Unterteilt einen physischen Link in 8 getrennte logische Prioritätskanäle (CoS 0 bis 7).
- Stoppt gezielt nur überlastete Prioritätsklassen, während unkritischer Verkehr ungehindert weiterfließt.
- Verhindert Head-of-Line Blocking über gemischte Datenströme hinweg.

4. ETS – ENHANCED TRANSMISSION SELECTION (802.1Qaz)



ETS bietet eine flexible und garantierte Bandbreitenzuweisung über Prioritätsgruppen hinweg.

- Definiert garantierte Mindestbandbreiten für Speicher-, Cluster- und Managementverkehr.
- Erlaubt dynamisches Ausleihen ungenutzter Bandbreite an andere Verkehrklassen bei Leerlauf.
- Verhindert das Verhungern (Starvation) von niederpriorem Standard-Traffic.

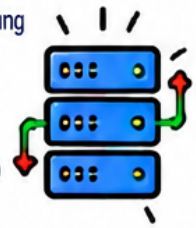
5. DCBX – DCB EXCHANGE PROTOCOL



DCBX ist ein Discovery- und Konfigurationsprotokoll basierend auf LLDP (Link Layer Discovery Protocol).

- Handelt PFC- und ETS-Parameter automatisch zwischen Host (CNA) und Switch-Port aus.
- Sichert eine netzwerkweit konsistente Konfiguration der CoS-Zuweisungen.
- Verhindert Fehlfonfigurationen, die zu Pufferüberläufen oder Deadlocks führen könnten.

6. QCN – QUANTIZED CONGESTION NOTIFICATION (802.1Qau)



QCN dient der proaktiven End-to-End-Stauvermeidung auf Layer 2 im Rechenzentrum.

- Switches erkennen drohende Pufferengpässe frühzeitig vor dem Auslösen von PFC.
- Sendet CNMs (Congestion Notification Messages) direkt zurück an die Quellknoten.
- Quellknoten drosseln die Senderate kontrolliert, um PFC-Verbreitung zu minimieren.

7. HAUPTANWENDUNGEN: FCoE, RoCE UND HPC



Verlustfreies Ethernet bildet das technologische Fundament moderner Storage- und KI-Cluster.

- FCoE (Fibre Channel over Ethernet): Kapselt FC-Frames direkt in Layer-2-Ethernet.
- RoCE v1/v2 (RDMA over Converged Ethernet): Extrem latenzarmer Speicherzugriff für NVMe-oF.
- HPC & Machine Learning: Verlustfreie Synchronisation paralleler Rechenknoten ohne TCP-Overhead.

8. ZUSAMMENFASSUNG & DCB-CHECKLISTE



Praxisleitfaden zur Konfiguration und Validierung von Lossless Ethernet in Rechenzentren.

- End-to-End-PFC-Pfade definieren und Deadlock-Risiken durch strikte Pufferplanung minimieren.
- CoS-Mappings für Speicherverkehr (z. B. CoS 3 für FCoE oder CoS 5 für RoCE) switchweit vereinheitlichen.
- DCBX auf Access-Ports aktivieren und Host-Aushandlung über LLDP-Status prüfen.

Achtung vor PFC-Deadlocks
Zyklische Pufferabhängigkeiten können PFC-Deadlocks erzeugen. Ein sauberes Spanning-Tree- bzw. Leaf-Spine-Design ohne L2-Schleifen ist zwingend erforderlich.

STORAGE AREA NETWORKS: FC vs. iSCSI & NVMe-oF

1. GRUNDLAGEN SAN & BLOCKSPEICHER



Ein Storage Area Network (SAN) ist ein dediziertes Hochgeschwindigkeitsnetzwerk, das Servern Zugriff auf konsolidierten Blockspeicher auf Blockebene bietet.

- **Blockspeicher vs. NAS:** Das Betriebssystem sieht Speicherressourcen wie lokale Festplatten (LUNs / Namespaces) statt Dateifreigaben.
- **Entkopplung:** Trennung von Anwendungs-Compute-Knoten und persistenter physischer Speicherkapazität.
- **Zweck:** Hochverfügbarkeit, unterbrechungsfreie Backups, Server-Clustering und optimierter Datendurchsatz in Rechenzentren.

2. FIBRE CHANNEL (FC) ARCHITEKTUR



Fibre Channel ist der traditionelle Standard für Enterprise-SANs mit deterministischer Leistung und hardwarebasiertem Pufferkredit-System.

- **Dedizierte Fabric:** Erfordert eigene Host-Bus-Adapter (HBA), optische Transceiver und spezialisierte FC-Switches.
- **Verlustfreie Übertragung:** Credit-basiertes Flow Control (Buffer-to-Buffer Credits) verhindert Paketerrluste auf Hardwareebene.
- **Geschwindigkeiten:** Standardmäßig 16GFC, 32GFC und 64GFC mit extrem geringer Latenz und stabiler Dienstgüte.

3. ISCSI: SPEICHER ÜBER ETHERNET



iSCSI kapselt SCSI-Speicherbefehle in standardmäßige TCP/IP-Pakete und nutzt bestehende Ethernet-Infrastruktur ohne Sonderhardware.

- **Transport & Port:** Nutzt TCP-Port 3260 für zuverlässige, reihenfolgetreue Übertragung über TCP/IP.
- **Adressierung:** Identifikation über IQN (iSCSI Qualified Name) oder EUI (Extended Unique Identifier).
- **Wirtschaftlichkeit:** Läuft auf Standard-Netzwerkkarten (NIC) und Standard-Ethernet-Switches, optional mit TCP Offload Engine (TOE).

4. NVME-OF: EXTREME PERFORMANCE



NVMe over Fabrics (NVMe-oF) erweitert das parallele NVMe-Speicherprotokoll über Netzwerkverbindungen für Flash- und All-Flash-Arrays.

- **Parallele Queues:** Unterstützt bis zu 64.000 Warteschlangen mit je 64.000 parallelen Befehlen für minimale CPU-Latenzen.
- **Transportschichten:** NVMe/FC (auf Fibre Channel), NVMe/TCP (Standard-Ethernet) und NVMe-oF über RDMA (RoCEv2, iWARP, InfiniBand).
- **Ziel:** Direkte Speicherzugriffe ohne SCSI-Overhead mit Latenzwerten im Mikrosekundenbereich.

5. PROTOKOLLVERGLEICH & METRIKEN



Direkter technischer Vergleich der Übertragungsverfahren hinsichtlich Latenz, Komplexität, Infrastrukturkosten und Durchsatz.

- **Fibre Channel:** Extrem niedrige Latenz (~10-20 µs), sehr hohe Anschaffungskosten, dedizierte Administration.
- **iSCSI:** Moderate Latenz (~100-250 µs), geringste Kosten durch Standard-LAN-Hardware, gut skalierbar.
- **NVMe-oF:** Ultraniedrige Latenz (<10 µs mit RoCE), extrem hohe IOPS, benötigt moderne Switches mit Flow-Control-Support (PFC/ECN).

Lossless Ethernet Voraussetzung

Für NVMe over RoCEv2 muss das Ethernet-Netzwerk zwingend verlustfrei konfiguriert sein (Priority-based Flow Control und DSCP-basiertes QoS), um Paketverluste und Neuübertragungen zu verhindern.

6. SICHERHEIT & ZUGRIFFSKONTROLLE

Sicherheitsmechanismen zur Abschottung von Speichernetzen gegen unbefugten Zugriff, Spoofing und Datenmanipulation.

- **FC Zoning & LUN Masking:** Isolation von Ports und HBAs im Switch sowie Freigabe spezifischer Speicherbereiche für Hosts.
- **iSCSI Authentifizierung:** Verwendung von CHAP (Challenge Handshake Authentication Protocol) und IPsec-Verschlüsselung.
- **Netztrennung:** Physische oder VLAN-basierte Isolation des Speicherdatenverkehrs vom normalen Client-LAN.



7. WORKFLOW: ISCSI-ANBINDUNG

Schrittfolge zur Einrichtung einer stabilen iSCSI-Blockspeicher-Verbindung zwischen Initiator (Server) und Target (Storage).

1. **Initiator konfigurieren**
   iSCSI-Dienst auf dem Host starten und den eindeutigen IQN-Namen vergeben (z. B. iqn.2024-05.com.firma:srv01).
2. **Netzwerk & MTU anpassen**
   Dedizierte Speicher-Netzwerkadapter einrichten und Jumbo Frames (MTU 9000) durchgängig auf Host und Switch aktivieren.
3. **Target Discovery & Login**
   Ziel-IP des Storage-Systems abfragen (iscsiadm discovery), CHAP-Zugangsdaten hinterlegen und Verbindung herstellen.
4. **Multipathing & Dateisystem**
   MPIO (Multipath I/O) für redundante Pfade aktivieren, Speicher-LUN partitionieren und Dateisystem formatieren.



8. ENTSCHEIDUNGSMATRIX: SPEICHERPROTOKOLL



Leitfaden zur Auswahl des optimalen Speicherprotokolls anhand von Anforderungs- und Budgetkriterien.

Welche Priorität bestimmt die Speicherarchitektur?

Geringes Budget und vorhandene Ethernet-Switches	Bestehende FC-Infrastruktur mit maximaler Verlässlichkeit	Maximale IOPS und minimale Latenz für All-Flash-Arrays
iSCSI mit separatem Speicher-VLAN oder isolierten 10G/25G-Switches wählen.	Fibre Channel (32G/64G) mit dedizierter Fabric und HBA-Redundanz beibehalten.	NVMe-oF (über RoCEv2 oder TCP) für hochmoderne Virtualisierungs- und KI-Workloads einsetzen.

Mindmap: Overlay-Netzwerke & VXLAN

1. Was ist ein Overlay-Netzwerk?

Ein virtuelles logisches Netz, das transparent auf einer physischen Routing-Infrastruktur (dem Underlay) aufsetzt. Es entkoppelt Endsysteme und VM-Mobilität von der physischen Standort-Topologie.



- Physische Topologie: Leaf-Spine-Fabric mit IP-Routing
- Logische Topologie: Direktes Layer-2-Segment über Rechenzentren hinweg
- Entkopplung von MAC-Tabellen auf zentralen Core-Switches

2. Die 4.096-VLAN-Limitierung

Traditionelle VLANs nach IEEE 802.1Q nutzen ein 12-Bit-VLAN-ID-Feld im Ethernet-Header. Dies beschränkt moderne Multi-Tenant-Rechenzentren und Cloud-Provider massiv.

- Maximal 4.094 nutzbare VLAN-IDs pro Schaltnetzwerk
- Mangelnde Skalierbarkeit für Mandanten und Microservices
- Hoher Verwaltungsaufwand für trunked Links im Core



3. VXLAN Network Identifier (VNI)

Der VXLAN-Header stellt ein 24-Bit-Feld für den VNI bereit, das den virtuellen Layer-2-Broadcast-Bereich eindeutig identifiziert und isoliert.

- 2^{24} = 16.777.216 simultane Netzwerksegmente
- Vollständige logische Trennung verschiedener Mandanten
- Flexible Zuordnung von VLAN-Tags am Hypervisor/Switch zu globalen VNIs



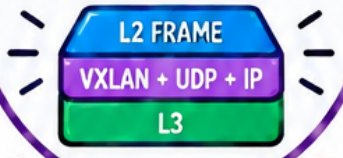
8. Zusammenfassung & Praxischeck

VXLAN ermöglicht moderne Rechenzentrumsnetzwerke, Cloud-Multi-Tenancy und ausfallfreie VM-Migrationen über Layer-3-Grenzen hinweg.

- 16M Segmente statt 4K VLANs
- ECMP-kompatibel dank variablem Quell-UDP-Port
- Wichtigste Voraussetzung: MTU >= 1600 Byte im physischen Netz konfigurieren



Overlay & VXLAN (L2 over L3)



4. VTEP: Knotenpunkte der Kapselung

Virtual Tunnel Endpoints (VTEPs) sind die Schnittstellen, die Pakete kapseln und entkapseln. Sie existieren als Hardware-VTEP (z. B. auf Top-of-Rack Switches) oder Software-VTEP (Hypervisor/Kernel).

- Eingang: Nimmt Standard-L2-Frame auf und fügt VXLAN/UDP/IP-Header an
- Ausgang: Entfernt äußere Header und [illegible]
- Verwaltung von Source-MAC zu Outer-IP-Zuordnungen



7. Control Plane: EVPN-BGP vs. Multicast

Zur Adressauflösung (Broadcast-, Unknown-Unicast- und Multicast-Traffic) existieren zwei fundamentale Betriebsmodi für VXLAN.

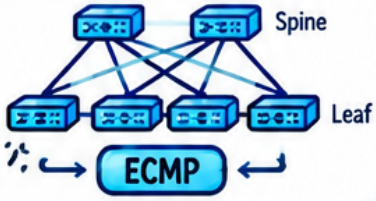
- Multicast Flood-and-Learn: VTEPs nutzen IP-Multicastgruppen zur MAC-Ermittlung
- BGP EVPN (RFC 7432): Standard für Enterprise; nutzt MP-BGP zur proaktiven Verteilung von MAC/IP-Routen ohne unkontrolliertes Flooding



6. Underlay vs. Overlay Routing

Die Rollenverteilung zwischen physischer und logischer Ebene garantiert Ausfallsicherheit und hohen Durchsatz ohne Spanning-Tree-Blockaden.

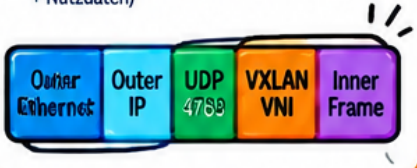
- Underlay: Robustes IP-Routing (meist BGP oder OSPF) mit Equal-Cost Multi-Path (ECMP)
- Overlay: Unabhängiges Layer-2/Layer-3-Bridging zwischen virtuellen Instanzen
- Ausfallsicherheit: Verbindungsausfälle fängt das Underlay unterbrechungsfrei ab



5. Aufbau des VXLAN-Paketheaders

Das ursrgrüngliche Ethernet-Datenpaket wird komplett geschachtelt transportiert. Von außen nach innen betrachtet entsteht folgende Schichtung:

- Outer Ethernet Header (MAC Quelle/Ziel des nächsten IP-Hops)
- Outer IP Header (Quell- und Ziel-IP der beiden beteiligten VTEPs)
- Outer UDP Header (IANA-Zielport 4789, variabler Quellport für Hash-ECMP)
- VXLAN Header (8 Byte mit Flags und 24-Bit VNI)
- Inner L2 Frame (Original Payload: L2-Header + IP + Nutzdaten)



MTU-Größenanpassung erforderlich

Durch den zusätzlichen VXLAN-Header (8 Byte), UDP-Header (8 Byte), äußeren IP-Header (20 Byte) und äußeren Ethernet-Header (14 Byte) entstehen **50 bis 54 Byte Overhead**. Im Underlay-Netzwerk müssen Jumbo Frames (mindestens 1600 Byte MTU) konfiguriert werden, um IP-Fragmentierung zu verhindern.

Praxis-Leitfaden & VTEP-Konfigurationsprotokoll

Entscheidungsbaum: Netzwerksegmentierung im RZ

Wählen Sie das passende Kapselungs- und Segmentierungsmodell basierend auf Ihren Skalierungsanforderungen.

Welche Anforderungen bestehen an Mandantenanzahl und Netzwerk-Infrastruktur?

Unter 4.000 Segmente & rein lokales Layer-2-Switching



Klassisches IEEE 802.1Q VLAN einsetzen.

Keine Anpassung der MTU oder UDP-Kapselung notwendig.

Große Cloud-/Hypervisor-Umgebung mit dynamischer VM-Migration über L3-Spine-Leaf



VXLAN mit BGP-EVPN Control Plane implementieren.

Physisches Underlay auf mindestens 1600 Byte MTU (Jumbo Frames) einstellen.

Praxis-Konfigurationsprotokoll: VXLAN & VTEP

Dokumentieren Sie die Parameter für die VTEP-Bereitstellung und die Underlay-Überprüfung.

1 Underlay-MTU prüfen



Ping mit Do-Not-Fragment-Bit (DF) und Paketgröße 1550 Byte über alle Spine- und Leaf-Strecken testen.

2 VTEP Loopback-IPs konfigurieren



Dedizierte /32-Loopback-Adressen für jeden VTEP einrichten und im Underlay-IGP (OSPF/BGP) ankündigen.

3 VNI-Mapping definieren

VLAN	VNI
10	10010
20	10020
30	10030

Lokale VLANs den globalen VXLAN Network Identifiers (VNIs) zuweisen.

4 Control-Plane-Status validieren



EVPN-Peering oder Multicast-Join für BUM-Traffic verifizieren und MAC-Tabelle abgleichen.

Lokale VTEP IP-Adresse (Loopback):	
Zugeordnete VNI (z. B. 10010) & lokales VLAN:	
Geprüfte Underlay-MTU (Bytes):	
Control-Plane Modus (Multicast / BGP-EVPN):	

BGP EVPN (RFC 7432) als Data-Center-Control-Plane

1. Definition & Standardisierung

BGP EVPN (Ethernet Virtual Private Network) ist ein standardisiertes Control-Plane-Protokoll nach RFC 7432, das Multiprotocol BGP (MP-BGP) nutzt, um Layer-2-MAC- und Layer-3-IP-Erreichbarkeitsinformationen über moderne IP-Underlays (z. B. VXLAN oder MPLS) zu verteilen.



- RFC 7432: Offener Standard für herstellerunabhängige Fabrics
- MP-BGP-Erweiterung (AFI 25, SAFI 70) für Routing & Switching
- Ablösung proprietärer Flood-and-Learn-Mechanismen im Rechenzentrum

2. Trennung von Control- & Data-Plane

Die Netzwerkarchitektur trennt logische Signalisierung präzise vom physischen Datenverkefr. BGP EVPN steuert die Adressverteilung, während Kapselungsprotokolle den eigentlichen Transport übernehmen.



- Control-Plane: BGP EVPN tauscht MAC- und IP-Routen per BGP-Updates aus
- Data-Plane: VXLAN kapselt L2-Frames in L3-UDP-Pakete (Port 4789)
- Kein Broadcast-Fluten nötig: Adressauflösung erfolgt kontrolliert

3. Wichtige EVPN-Routentypen

BGP EVPN definiert spezifische Network Layer Reachability Information (NLRI)-Routentypen für die präzise Steuerung von Host- und Netzwerkrouten.



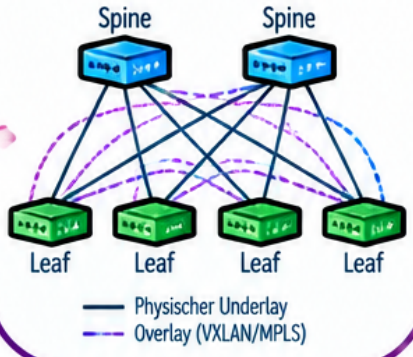
- Typ 2: MAC/IP Advertisement Route für Host-Erreichbarkeit
- Typ 3: Inclusive Multicast Ethernet Tag für BUM-Handling
- Typ 5: IP Prefix Route für mandantenfähiges Inter-Subnet-Routing

4. Spine-Leaf & Data-Center-Vorteile

In modernen Spine-Leaf-Topologien (Clos-Netzwerke) maximiert EVPN die Resilienz, Bandbreite und Flexibilität virtueller Maschinen und Container-Cluster.



- All-Active Multi-Homing via Ethernet Segment Identifier (ESI)
- Optimale Pfadnutzung durch Equal-Cost Multi-Path (ECMP)
- Eliminierung von Spanning-Tree-Blockaden in Rechenzentren



5. Integriertes Routing & Bridging (IRB)

EVPN unterstützt effizientes Weiterleiten zwischen unterschiedlichen virtuellen Subnetzen direkt auf den Leaf-Switchen (VTEPs).



- Asymmetrisches IRB: Routing auf Ingress-Switch, Bridging auf Egress
- Symmetrisches IRB: Routing auf Ingress und Egress via Transit-VNI
- Verhindert Hairpinning-Traffic über zentrale Core-Router

6. Mandantenfähigkeit & Skalierbarkeit

Durch die Kombination mit Virtual Routing and Forwarding (VRF) und VNIs ermöglicht EVPN die vollständige Isolierung tausender Mandanten.



- VRF-Instanzen trennen Routingtabellen logisch auf Layer 3
- VNIs (VXLAN Network Identifiers) bieten bis zu 16 Millionen Segmente
- Skalierbare Route Reflector-Topologien im BGP-Underlay

7. Schnell-Check & Implementierungsentscheidung

Prüfen Sie anhand der Kernparameter, ob BGP EVPN die passende Control-Plane-Architektur für Ihre Netzwerkanforderung darstellt.



ARCHITEKTUR-HINWEIS
BGP EVPN erfordert solide Kenntnisse im IP-Underlay-Routing (z. B. OSPF/IS-IS/eBGP), um zuverlässig als Overlay zu fungieren.

Welche Netzwerkanforderung liegt im Rechenzentrum vor?

- Multi-Tenant Cloud oder verteilte Spine-Leaf Fabric
  → BGP EVPN mit VXLAN-Kapselung implementieren, um dynamische MAC/IP-Verteilung und ESI Multi-Homing zu nutzen.
- Kleines statisches Campus-Netzwerk ohne Mandantentrennung
  → Klassisches L2/L3-VLAN-Design oder simples Routing ohne EVPN-Overlay prüfen, um Komplexität zu reduzieren.

8. Zusammenfassung & Kernpunkte

Kompakte Übersicht über den Nutzen von BGP EVPN als moderne Steuerungs- und Kontrollschicht im Rechenzentrumsnetzwerk.



- Standardsiert nach RFC 7432 für offene, herstellerübergreifende Netze
- Ersetzt 'Data-Plane Learning' durch planbare 'Control-Plane Signalisierung'
- Kombiniert L2-Mobilität, L3-Routing und Mandantenisolierung optimal

SDN & OpenFlow: Control-Plane-Entkopplung

1. Grundprinzip: Planes-Trennung



Klassische Router vereinen Weiterleitung und Wegberechnung auf demselben Gerät. SDN bricht diese Bindung auf und trennt das Netzwerk in drei eigenständige Funktionsebenen.

- **Data Plane (Datenebene):** Reine Paketweiterleitung in Hardware (ASICs/TCAM).
- **Control Plane (Steuerungsebene):** Entscheidet über Routingpfade und Richtlinien.
- **Management Plane:** Bereitstellung von Konfiguration, SSH, SNMP und Web-GUIs.

KERNUNTERSCHIED
Herkömmliche Switche treffen Routing-Entscheidungen autonom; in SDN empfängt der Switch fertige Anweisungen von einer zentralen Instanz.

2. Architektur-Ebenen



Die SDN-Architektur gliedert Netzwerksysteme in ein hierarchisches Schichtenmodell mit standardisierten Kommunikationsschnittstellen.

- **Infrastructure Layer:** Physikalische und virtuelle Switche (Forwarding Elements).
- **Control Layer:** Zentralisierter Controller als logisches Betriebssystem des Netzes.
- **Application Layer:** Geschäftsanwendungen für Monitoring, Firewalling und Load Balancing.

3. Der SDN-Controller



Der Controller bildet das softwarebasierte Gehirn. Er aggregiert den globalen Netzwerkstatus und programmiert Topologien dynamisch vor.

- **Zentrale Sicht:** Vollständige globale Topologie- und Verbindungstransparenz.
- **Logisch zentralisiert:** Kann zur Hochverfügbarkeit physisch auf Cluster verteilt sein.
- **Bekannte Implementierungen:** OpenDaylight, ONOS, Ryu und Cisco ACI.

4. Schnittstellen (APIs)



Die Kommunikation zwischen den Schichten erfolgt über definierte APIs, die Richtlinien nach unten und Statusinformationen nach oben transportieren.

- **Southbound APIs:** Verbinden Controller mit Datenebene (z. B. OpenFlow, P4, NETCONF).
- **Northbound APIs:** RESTful APIs zur Anbindung von Orchestrierungs- und Management-Software.
- **East/Westbound APIs:** Abstimmung und Synchronisation zwischen verteilten Controller-Instanzen.

5. OpenFlow-Protokoll



OpenFlow ist der Pionierstandard der Southbound-Kommunikation. Er definiert ein einheitliches Nachrichtenformat zur Flusssteuerung.

- **Verbindungssicherung:** TLS-verschlüsselte TCP-Sitzung zwischen Switch und Controller.
- **Match-Action-Prinzip:** Eingehende Headerfelder prüfen und definierte Aktionen anwenden.
- **Packet-In / Packet-Out:** Unbekannte Pakete werden zur Analyse an den Controller gesendet.

6. Flow Tables & Pipeline



OpenFlow-Switche verarbeiten Frames über tabellengestützte Pipelines. Jeder Tabelleneintrag enthält Header-Kriterien und Verrarbeitungsvorgaben.

- **Header-Felder:** Match auf Ingress-Port, MAC-Adressen, VLAN, IP-Adressen und Layer-4-Ports.
- **Counters:** Zähler für Pakete, Bytes und Flow-Dauer zur Verkehrsanalyse.
- **Instructions:** Aktionen wie Forwarding, Header-Modifikation, Drop oder Weiterleitung zur nächsten Tabelle.

7. Praxisablauf eines Flows



Paketbehandlung bei einem Cache-Miss (erstes Auftreten eines neuen Kommunikationsflusses):

1. Ein Frame trifft ohne Match in der Flow Table ein.
2. Switch sendet Paketkopf via Packet-In an den Controller.
3. Controller berechnet Route und sendet Flow-Mod zurück.
4. Switch schreibt Regel und leitet das Paket via Data Plane weiter.

1 Frame-Eingang → 2 Packet-In Nachricht → 3 Richtlinien-entscheidung → 4 Flow-Mod & Forwarding

8. Vorteile & Sicherheitsaspekte



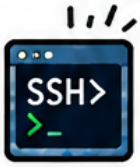
SDN vereinfacht Konfigurationen und beschleunigt Rollouts, verlagert jedoch auch Bedrohungsvektoren auf zentrale Steuerungspunkte.

- **Vorteile:** Automatisierte Mikrosegmentierung, zentrales QoS und herstellerunabhängige Hardware.
- **Single Point of Failure:** Fällt der Controller ungesichert aus, stagniert das Regel-Setup neuer Verbindungen.
- **Angriffsvektoren:** Controller-Hijacking, Man-in-the-Middle auf Southbound-Links und DoS gegen Flow-Tabellen.

PRAXIS-TIPP
Sichern Sie den Southbound-Kanal stets mit beidseitiger Zertifikatsvalidierung via mTLS ab, um gefälschte Controller oder Switche zu verhindern.

Netzwerkautomatisierung: Netmiko, Paramiko und CLI-Scraping

1. Paramiko Grundlagen



- SSHClient(): Initialisiert das Verbindungsobjekt im Skript
- AutoAddPolicy: Richtlinie zur automatischen Speicherung unbekannter Host-Keys (in Testumgebungen)
- exec_command(): Startet ein Kommando und liefert Streams (stdin, stdout, stderr)
- Low-Level-Kontrolle: Erfordert exaktes Einlesen von Stream-Puffern bis zum Verbindungsende

2. Netmiko – Treiberspezifische Abstraktion



- device_type: Bestimmt den Herstellertreiber (z. B. 'cisco_ios', 'arista_eos')
- ConnectHandler: Factory-Funktion zum Öffnen einer persistenten Terminal-Sitzung
- Automatische Paging-Deaktivierung: Sendet automatisch Befehle wie 'terminal length 0'
- Prompt-Synchronisation: Wartet eigenständig auf das Rückmeldezeichen (#, >)

3. Sichere Authentifizierung und Verbindungsmethoden



- Umgebungsvariablen: Speichern von Passwörtern und Token außerhalb des Quellcodes (os.environ)
- SSH-Key-Pairs: Public-Key-Authentifizierung (Ed25519 oder RSA-4096)
- Bastion- / Jump-Host: Weiterleitung von SSH-Sitzungen über Sicherheits-Gateways
- Session-Timeouts: Strikter Verbindungslimits zur Vermeidung blockierter VTY-Lines

Sicherheitshinweis für Zugangsdaten

Speichern Sie Passwörter niemals im Klartext im Skript. Nutzen Sie getpass für interaktive Eingaben oder dedizierte Secrets-Manager für Serverprozesse.

4. Statusabfragen mit send_command()



- send_command('show ip interface brief'): Liest Schnittstellenstatus aus
- Prompt-Detection: Erkennt dynamisch, wann der Befehl vollständig beendet ist
- strip_prompt & strip_command: Entfernt überflüssige Echo-Zeilen aus dem Ergebnis
- Read-Timeout: Abfangen langwieriger Befehle über anpassbare Verzögerungswerte

5. Konfigurationsausrollung mit send_config_set()



- Konfigurationsmodus: Automatischer Wechsel ('configure terminal') und Rückkehr ('end')
- Befehlslisten: Übergabe mehrerer Anweisungen als Python-Liste (List of Strings)
- Fehlererkennung: CLI-Fehlermeldungen wie '% Invalid input' im Rückgabetext prüfen
- Persistenz: Speichern der Konfiguration im NVRAM über 'save_config()' oder 'write memory'

6. Output-Parsing (TextFSM, TTP und Regex)



- **Reguläre Ausdrücke (re):** Selektive Filterung von IP-Adressen und Schnittstellennamen
- **TextFSM & ntc-templates:** Vordefinierte Tabellenvorlagen für Hunderte gängiger Netzwerkbefehle
- **use_textfsm=True:** Direkte Netmiko-Option zur Rückgabe strukturierter Dictionaries
- **TTP (Template Text Parser):** Deklaratives Parsing mit Jinja-ähnlicher Syntax für komplexe Tabellen

7. Fehlerbehandlung und robuste Verbindungsprüfung



- NetmikoTimeoutException: Tritt auf, wenn das Gerät per SSH nicht erreichbar ist
- NetmikoAuthenticationException: Signalisiert ungültige Benutzerdaten oder abgelehnte Schlüssel
- Try-Except-Blöcke: Protokollierung fehlerhafter Zielsysteme ohne Skriptabbruch
- **Logging:** Aktivierung des Netmiko-Loggers (logging.DEBUG) zur detaillierten Protokollanalyse

8. 6-Schritte Workflow & Entscheidungsmatrix



1. Geräteinventar und Parameter laden
2. Verbindung etablieren
3. Ist-Zustand prüfen (Pre-Check)
4. Konfiguration ausrollen
5. Soll-Zustand verifizieren (Post-Check)
6. Speichern und Session schließen



Zentraler Überblick: CLI-Scraping & SSH-Automatisierung



Die skriptbasierte Netzwerkautomatisierung ersetzt die fehleranfällige manuelle Befehlseingabe über administrative Terminals. Mithilfe von Python-Bibliotheken wie Paramiko und Netmiko werden SSH-Verbindungen zu Routern, Switches und Firewalls **aufgebaut, Konfigurationsbefehle standardisiert** ausgerollt und **Statusdaten automatisiert** ausgelesen.

- **SSH-Kanal:** Verschlüsselte Transportschicht (TCP-Port 22) als Sicherheitsbasis
- **Paramiko:** Low-Level-Implementierung des SSHv2-Protokolls für individuelle Verbindungslogik
- **Netmiko:** Abstraktionsschicht für herstellerspezifische CLI-Besonderheiten (Cisco, Juniper, Arista)
- **Regex & Parsing:** Strukturierung unformatierter Textausgaben (Show-Commands) in tabellarische Daten

Grundlagen-Tipp für Einsteiger

CLI-Scraping liest unstrukturierten Text aus. Verwenden Sie für operative Skripte stets Netmiko statt reinem Paramiko, da Netmiko CLI-Prompt-Erkennung, Paging ('--More--') und Timing-Probleme automatisch abfängt.

Praxis-Arbeitsblatt: Eigene Netzwerk-Automatisierung Protokollieren

Nutzen Sie dieses Protokollfeld zur strukturierten Erfassung von Verbindungsparametern, Zielbefehlen und Parsing-Mustern für Ihr nächstes Automatisierungsskript.

- Dokumentieren Sie die IP-Adresse und den device_type des Zielgeräts
- Notieren Sie die Testbefehle für Pre- und Post-Checks
- Halten Sie die erwarteten Regex-Muster für die Output-Validierung fest

Ziel-Host (IP / FQDN) & Gerätetyp (z.B. cisco_ios):

Pre-Check Befehle (z.B. show ip int brief):

Auszuführende Konfigurationsbefehle (send_config_set):

Erwartete Schlüsselbegriffe / Regex im Post-Check:

PROGRAMMIERBARE NETZWERK-APIS: RESTCONF & NETCONF



1. GRUNDPRINZIPIEN & ARCHITEKTUR

- Inhaltsschicht: Datenstruktur via YANG-Module.
- Operationsschicht: Standard-operationen für Abruf, Modifikation und Löschen von Knoten.
- Nachrichtenschicht: RPC-basierte Kapselung von Anfragen und Systemantworten.
- Transportschicht: Kryptografisch abgesicherte Punkt-zu-Punkt-Verbindungen.

2. NETCONF (RFC 6241)

- Transport: SSH (Port 830) oder TLS mit bidirektionalem XML-RPC-Framing.
- Datencodierung: Ausschlüöelich XML für Konfigurations- und Statusbäume.
- Sitzungskonzept: TCP/SSH-Verbindung mit persistenten Datenspeicher-Transaktionen.
- Sicherheitsmodell: Authentifizierung via SSH-Schlüssel oder Zertifikate.

3. RESTCONF (RFC 8040)

- Transport: HTTPS über Port 443 mit TLS-Verschlüsselung.
- Codierung: Unterstützt JSON und XML.
- Architektur: REST-basierte Ressourcenpfade (/restconf/data/...). zustandslos pro Anfrage.
- Integration: Ideal für Web-Frontends, Microservices und CI/CD-Pipelines.

4. DATENMODELLIERUNG MIT YANG

- Modelliert Konfigurationsdaten (rw) und Statuszustände (ro) hierarchisch.
- Validiert Datentypen, Wertebereiche, Schlüsselbegrenzungen und Abhänggikeiten.
- Unterstützt OpenConfig (Multi-Vendor) und IETF-Standards sowie herstellereigene Module.
- Ermöglicht automatische Schema-Prüfung vor dem eigentlichen Schreiben auf das Gerät.

5. OPERATIONEN & HTTP-VERBEN

- Daten abrufen: NETCONF nutzt <get-config> / <get>, RESTCONF verwendet GET.
- Ressource anlegen: NETCONF nutzt <edit-config> mit create, RESTCONF nutzt POST.
- Konfiguration ersetzen: NETCONF nutzt <edit-config> (replace), RESTCONF nutzt PUT.
- Feld modifizieren: NETCONF nutzt <edit-config> (merge), RESTCONF nutzt PATCH.
- Eintrag entfernen: NETCONF nutzt <edit-config> (delete), RESTCONF nutzt DELETE.

6. DATASTORES & TRANSAKTIONEN

- Running Datastore: Die aktuell aktive Konfiguration im laufenden Betrieb.
- Candidate Datastore: Arbeitsbereich für Tests vor der finalen Übernahme.
- Startup Datastore: Dauerhaft persistierte Konfiguration für Systemneustarts.
- Transaktionssicherheit: NETCONF unterstützt atomare <commit>- und <discard-changes>-Rollbacks.

7. PRAXISBEISPIEL & SICHERHEIT

- Python-Automatisierung: Nutzung von ncclient für NETCONF und requests für RESTCONF.
- Absicherung: Strikte rollenbasierte Zugriffskontrolle (NACM - RFC 8341).
- Ereignisüberwachung: Subskription von Telemetrie und Event-Streams (RFC 8639 / RFC 8640).
- Audit-Trail: Vollständige Nachvollziehbarkeit aller Schreiboperationen über Logs.

8. ENTSCHEIDUNGSMATRIX: NETCONF ODER RESTCONF?

- Wähle NETCONF, wenn atomare Multi-Device-Transaktionen und Candidate-Rollbacks zwingend sind.
- Wähle RESTCONF, wenn schlanke JSON-Payloads und Anbindung an Web-Tools im Fokus stehen.
- Kombinierter Einsatz: Beide Protokolle können parallel auf denselben YANG-Datenbestand zugreifen.

PRAXIS-TIPP

Für CI/CD-Pipelines mit Python oder Ansible bietet RESTCONF oft den schnelleren Einstieg, während NETCONF bei unternehmenskritischen Core-Netzen maximale Transaktionssicherheit garantiert.

RESTCONF und NETCONF im Überblick

Moderne Netzwerkgeräte werden zunehmend über automatisierte, standardisierte Programmierschnittstellen (APIs) anstelle manueller Befehlszeilen (CLI) konfiguriert. NETCONF (RFC 6241) und RESTCONF (RFC 8040) bilden das standardisierte Fundament für Model-Driven Programmability. Beide Protokolle greifen auf struktuierte Datenmodelle zurück, die in der Modellierungssprache YANG definiert sind, um Konfigurationen und Betriebszustände fehlerfrei zu verwalten.

RFC-Standardisierung

NETCONF ist in RFC 6241 spezifiziert und baut auf XML-RPCs auf. RESTCONF ist in RFC 8040 definiert und bietet eine REST-artige Schnittstelle für denselben YANG-Datenbestand via HTTPS.

- Ablösung fehleranfälliger textbasierter CLI-Skripte (Screen Scraping) durch deterministische APIs.
- Trennung von Konfigurationsdaten (Running, Startup, Candidate) und dynamischen Betriebsdaten.
- Verwendung herstellerneutraler oder nativer Datenmodelle über standardisiertes YANG.
- Sichere, authentifizierte Transportschichten über SSH oder TLS.

NETCONF (RFC 6241)	↔	RESTCONF (RFC 8040)
XML über SSH/830		JSON/XML über HTTPS/443

YANG-Datenmodellierung im Netzwerkmanagement

1. Was ist YANG?

YANG ist eine standardisierte, herstellerneutrale Datenmodellierungssprache für Netzwerkgeräte und -dienste.



- Definiert in RFC 6020 (YANG 1.0) und RFC 7950 (YANG 1.1)
- Modelliert Konfigurationsdaten, Statusdaten und Remote Procedure Calls (RPCs)
- Trennt Datenstruktur und Syntax von Transportprotokollen

Praxis-Tipp
Zur Syntaxprüfung und Strukturvisualisierung von YANG-Dateien das quelloffene Werkzeug pyang nutzen.

2. Anwendungsbereiche & Protokolle

YANG bildet das gemeinsame Datenfundament für moderne Automatisierungsprotokolle im programmierbaren Netzwerk.



- NETCONF: Transportiert XML-kodierte YANG-Daten über SSH (RFC 6241)
- RESTCONF: Bereitstellung von JSON/XML über HTTPS nach REST-Prinzipien (RFC 8040)
- gNMI: Streaming-Telemetrie und Konfiguration über HTTP/2 und Protobuf

3. Kernknotentypen

YANG organisiert Datenhierarchien über vier primäre Knotentypen mit klar abgegrenzten Eigenschaften.



- container: Gruppiert zusammengehörige Knoten ohne eigene Werte
- leaf: Speichert genau einen atomaren Wert (z. B. String, Integer, IP-Adresse)
- leaf-list: Sequenz gleichartiger atomarer Werte
- list: Mehrfache Container-Instanzen, identifiziert durch Schlüssel (key)

4. Typisierung & Constraints

Strikte Validierung auf Schema-Ebene sichert fehlerfreie Gerätekonfigurationen vor dem Deployment.



- Primitive Basistypen: string, boolean, enumeration, uint8 bis uint64
- Wiederverwendbare Typen: typedefs und abgeleitete Standardtypen (RFC 6991)
- Validierungsregeln: must, when und range/pattern schränken Gültigkeit ein

5. Standard- vs. Herstellermodelle

Im praktischen Netzwerkmanagement koexistieren offene Standards und modellspezifische Erweiterungen.



- IETF-Modelle: Grundlegende Schnittstellen- und Routing-Standards (z. B. ietf-interfaces)
- OpenConfig: Herstellerunabhängige Betreibermodelle für Multi-Vendor-Umgebungen
- Native Modelle: Herstellerspezifische YANG-Module für geräteeigene Spezialfunktionen

6. Workflow: Vom Modell zur Hardware

Typischer Ablauf einer softwaredefinierten Netzwerkkonfiguration via YANG:

1. **Modellauswahl**
   Passendes IETF- oder OpenConfig-YANG-Modul für die Zielaufgabe bestimmen.
2. **Validierung**
   Modul und Eingabedaten mit Werkzeugen wie pyang gegen Syntaxfehler prüfen.
3. **Payload-Erstellung**
   Strukturierte Konfigurationsdaten in XML oder JSON nach Schema generieren.
4. **Deployment**
   Übertragung an das Zielgerät per NETCONF edit-config oder RESTCONF PUT/POST.



YANG standardisiert das 'Was' der Daten, während NETCONF/RESTCONF das 'Wie' des Transports regeln.

7. Protokollwahl: NETCONF oder RESTCONF?

Entscheidungslogik für das geeignete Transportprotokoll bei der Übertragung von YANG-Modellen:



Welche Anforderungen hat die Automatisierungsumgebung an State-Handling und Datenaustausch?

- Zustandsbehaftete Session, Transaktionen, Candidate Datastore und Lock-Mechanismen zwingend erforderlich → NETCONF über SSH mit XML-Payload und standardisierten RPC-Operationen implementieren.
- Zustandslose Web-API-Integration, HTTPS-Toolchains und leichtgewichtiger JSON-Austausch priorisiert → RESTCONF über HTTPS mit standardisierten CRUD-Endpunkten einsetzen.

8. Zusammenfassung & Merkregel

YANG standardisiert das 'Was' der Daten, während NETCONF/RESTCONF das 'Wie' des Transports regeln.



- Verhindert manuelles Parsen von unstrukturierten CLI-Ausgaben
- Ermöglicht programmierbare, reproduzierbare Infrastruktur nach NetDevOps-Prinzipien
- Sichert herstellerübergreifende Portabilität von Netzwerkautomations-Skripten

NETZWERK-IAC: ANSIBLE & TERRAFORM

1. WAS IST NETZWERK-IAC?



Netzwerk-IaC beschreibt die automatisierte Bereitstellung, Verwaltung und Überwachung von Netzwerkressourcen durch Code.
Es ersetzt manuelle Konsoleneingaben durch standardisierte Pipelines.

- Vollständige Maschinenausführung ohne Ad-hoc-Konsoleneingriffe.
- Zentralisierte Definition von IP-Netzen, Routen, Schnittstellen und Firewall-Regelwerken.
- Automatisierte Validierung vor dem Rollout auf produktive Hardware.

2. ANSIBLE VS. TERRAFORM



Ansible und Terraform ergänzen sich im Netzwerkbetrieb optimal durch unterschiedliche Schwerpunkte bei Zustand und Verwaltungsmethode.

- Ansible: Agentenlos, primär zustandsgesteuertes Konfigurationsmanagement über SSH/NETCONF/ RESTCONF.
- Terraform: Stark zustandsbasiert (State File), deklarative Orchestierung von Schnittstellen und Cloud-Netzwerken.
- Zusammenspiel: Terraform baut Netzwerk-Gateways und Subnetze auf; Ansible konfiguriert Routing-Protokolle und BGP-Nachbarn.

3. DEKLARATIV VS. IMPERATIV



Das Paradigma bestimmt, wie Automatisierungs-anweisungen an Router und Switches formuliert werden.

- Imperativ: Skripte listen exakte CLI-Schritte auf ('interface GigabitEthernet0/1', 'ip address 10.0.0.1 255.255.255.0').
- Deklarativ: Die Codedatei beschreibt ausschließlich den Soll-Zustand ('vlan_id: 100, name: DMZ'); das Tool ermittelt die nötigen Diff-Schritte.
- Vorteil deklarativ: Verhindert doppelte Ausführungen und reduziert Seiteneffekte bei bestebenden Konfigurationen.

4. MULTI-VENDOR ABSTRAKTION



Heterogene Netzwerke erfordern einheitliche Schnittstellen zur herstellerübergreifenden Ansteuerung von Cisco, Arista, Juniper und Linux-Routern.

- Verwendung standardisierter Transportprotokolle wie NETCONF (RFC 6241) und RESTCONF (RFC 8040).
- Nutzung herstellerneutraler Datenmodelle mittels YANG zur Definition von Schnittstellen und BGP-Instanzen.
- Ansible-Collections (z. B. cisco.ios, arista.eos) kapseln herstellerspezifische Syntax abstrahiert ab.

5. PRAXIS-WORKFLOW: VOM CODE ZUM ROUTER



Strukturierter Ablauf zur fehlerfreien Implementierung einer Netzwerkänderung von der Definition bis zur Produktivschaltung.

1. **Branch erstellen & Konfiguration definieren**
   Neuen Git-Feature-Branch anlegen und den gewünschten Netzwerk-Sollzustand in YAML- oder NCL-Dateien formulieren.
2. **Syntax-Prüfung & Linting**
   Lokale Ausführung von `ansible-lint` oder `terraform validate` zur statischen Fehlererkennung.
3. **Plan- und Dry-Run-Phase**
   Ausführen von 'ansible-playbook --check' bzw. 'terraform plan', um das exakte Delta vor dem Anwenden zu prüfen.
4. **Peer Review & CI-Pipeline**
   Pull Requset öffnen, automatische Validierungstests durchlaufen lassen und Freigabe durch Netzwerkteam einholen.
5. **Automatisierter Rollout & Monitoring**
   Deployment über Pipeline mit automatischem Ping- und BGP-State-Check; automatischer Rollback bei Verbindungsabbruch.

6. SICHERHEIT & SECRET-MANAGEMENT



Kritische Zugangsdaten dürfen niemals unverschlüsselt in IaC-Repositorys gespeichert werden.

- **Ansible Vault:** AES-256-Verschlüsselung für Passwörter, SNMP-Community-Strings und Pre-Shared Keys.
- **Dynamic Secrets:** Nutzung von HashiCorp Vault oder Cloud-KMS für kurzlebige SSH-Zertifikate.
- **Least-Privilege-Service-Accounts:** Automatisierungsnutzer erhalten ausschließlich nötige Konfigurationsrechte statt generischer Root-/Enable-Rechte.

Zentraler Grundsatz
Niemals unverschlüsselte API-Tokens oder Enable-Secrets in Git-Repositories committen. GitGuardian oder Pre-Commit-Hooks zur Blockierung nutzen.

7. WICHTIGE BEFEHLE & TOOLS



Grundlegendes Rüstzeug für die tägliche Arbeit mit IaC auf Netzwerkebene.

- `ansible-playbook -i hosts site.yml --diff`: Führt Playbook aus und visualisiert exakte Zeilenänderungen.
- `terraform init && terraform plan`: Initialisiert Provider (z. B. AWS VPC, Cisco ACI) und kalkusiert Änderungen.
- `yamllint & tflint`: Statische Code-Analyse zur Sicherung von Syntax- und Typ-Standards.
- NetBox / Nautobot: Open-Source Source-of-Truth-Plattformen zur Bereitstellung dynamischer Inventare für Ansible.

8. ZUSAMMENFASSUNG & CHECKLISTE



Kompakte Orientierungshilfe zur Bewertung, wann welches Werkzeug eingesetzt wird.

- Verwende Terraform zur Provisionierung von virtuellen Routern, Cloud-VPCs, Subnetzen und Cloud-Gateways.
- Verwende Ansible für herstellerübergreifendes Konfigurationsmanagement, Firmware-Upgrades und Betriebsprüfungen.
- Pflege alle Parameter in zentralen Datenmodellen und dokumentiere jede Änderung über Git-Commits.

Welches Tool eignet sich für die anstehende Netzwerkaufgabe?

→ Bereitstellung neuer Netzwerkinfrastruktur, Cloud-Gateways oder Subnetze
Terraform verwenden:
Deklarative Verwaltung des Lebenszyklus und Tracking über State-File.

→ Konfiguration bestehender physischer Switches, ACL-Aktualisierung oder OS-Updates
Ansible verwenden:
Agentenlose SSH/NETCONF-Verbindung mit herstellerspezifischen Modulen.

ÜBERBLICK & ZENTRALES PRINZIP

Infrastructure as Code (IaC) überträgt die Prinzipien der Softwareentwicklung auf den Netzwerkbetrieb. Statt Router, Switches und Firewalls manuell per CLI oder Web-GUI zu konfigurieren, wird die gewünschte Netzwerktopologie deklarativ in maschinenlesbaren Konfigurationsdateien definiert. Dies ermöglicht automatisierte Tests, Versionskontrolle via Git und reproduzierbare Bereitstellungen über verschiedene Hersteller hinweg.

- **Eliminierung von Konfigurationsdrift** zwischen verschiedenen Netzwerkstandorten.
- Versionierbare Netzwerkänderungen mit nachvollziehbarer Commit-Historie.
- Verringerung menschlicher Tippfehler bei komplexen VLAN-, BGP- und ACL-Änderungen.

Zentraler Grundsatz
Konfigurationen werden niemals direkt auf Produktionsgeräten editiert. Die Git-Codebasis fungiert als alleinige verlässliche Quelle (Single Source of Truth).

CI/CD FÜR NETZWERK-PIPELINES

1. WAS IST NETZWERK-CI/CD





Continuous Integration (CI) und Continuous Delivery (Deployment, CD) übertragen moderne DevOps-Praktiken auf den Netzwerkbetrieb. Änderungen an Switch-, Router- und Firewall-Konfigurationen werden nicht mehr manuell per SSH oder Webschnittstelle eingepflegt, sondern als strukturierter Code in Repositories verwaltet, vorab automatisiert validiert und kontrolliert ausgerollt.

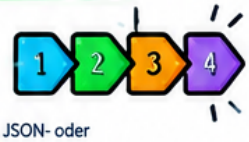
- **Network as Code (NaC):** Konfigurationen liegen versioniert in Git-Repositories.
- **Automatische Syntax- und Logikprüfungen** bei jedem Pull Request.
- **Reduzierung von menschlichen Fehlkonfigurationen** und Ausfallzeiten.
- **Vollständige Historie** und Nachvollziehbarkeit aller Netzwerkänderungen.



KERNEINSICHT
Durch Pipelines wird jede Netzwerkänderung wie Softwarecode behandelt: wiederholbar, testbar und auditierbar.

2. PIPELINE-STUFEN IM ÜBERBLICK

Eine typische Netzwerk-Pipeline durchläuft vier aufeinander aufbauende Phasen, um fehlerhafte oder inkonsistente Konfigurationen vor dem Produktionskontakt abzufangen.



1. **Linting & Syntax:** Überprüfung von YAML-, JSON- oder Jinja2-Dateien auf Formatfehler.
2. **Pre-Deployment Validation:** Simulation von Routing-Tabellen und ACL-Regeln.
3. **Deployment:** Automatisiertes Ausrollen auf Test- oder Produktionsgeräte via Netmiko, Ansible oder Nornir.
4. **Post-Deployment Testing:** Verifikation von Konnektivität, Latenz und Routenpräsenz.

3. TYPISCHE WERKZEUGE & ARCHITEKTUR

Die Toolchain kombiniert Versionskontrolle, CI-Runner, Netzwerkausrüter-Treiber und Test-Frameworks zu einem geschlossenen Workflow.



- **VCS & CI-Engine:** GitHub Actions, GitLab CI oder Gitea Runners.
- **Automatisierungs-Tools:** Ansible, Terraform, Nornir und Python-Skripte.
- **Test- & Simulationswerkzeuge:** Batfish, pyATS, Containerlab und Suzieq.
- **Monitoring-Feedback:** Prometheus, Zabbix oder Syslog-Alerting bei Schwellenwertüberschreitung.

4. AUTOMATISIERTE VALIDIERUNG & PRE-TESTS

Bevor eine Konfigurationsänderung an einen Router gesendet wird, analysiert Batfish oder pyATS die logischen Konsequenzen im virtuellen Modell.



- **ACL-Analyse:** Verifizieren, dass zulässiger Verkehr nicht versehentlich verworfen wird.
- **BGP/OSPF-Konflikterkennung:** Prüfung auf überlappende Subnetze und Routen-Leaks.
- **Konformitätsprüfungen:** Einhaltung von Passwort- und Verschlüsselungsstandards.
- **Präzise Fehlerberichte** direkt im Git-Merge-Request vor der Freigabe.



SICHERHEITSGEWINN
Pre-Deployment-Validierung fängt BGP-Hijacking und Fehlroutings bereits im Entwicklungsprozess ab.

5. BEREITSTELLUNG & ROLLBACK-STRATEGIEN

Die Bereitstellung erfordert robuste Mechanismen für den Fall, dass die Kommunikation abbricht oder unerwartete Fehler auftreten.



- **Canary Deployments:** Zuerst Rollout auf unkritischen Randgeräten oder Lab-Switches.
- **Atomic Commits:** Unterstützte Hardware sichert Änderungen erst nach Bestätigung dauerhaft.
- **Automatischer Rollback:** Automatischer Rückfall auf den vorherigen Zustand bei Ping-Verlust.
- **Idempotenz:** Wiederholte Ausführung der Pipeline verändert nur notwendige Differenzen.

6. SICHERHEIT IN DER PIPELINE (DEVSECOPS)

Die CI/CD-Infrastruktur besitzt privilegierten Zugriff auf kritische Netzwerkkomponenten und erfordert strenge Zugriffskontrollen.



- **Secret Management:** Vault oder geschützte CI-Variablen für SSH- und SNMP-Keys nutzen.
- **Vier-Augen-Prinzip:** Verpflichtende Genehmigung durch erfahrene Netzwerk-Engineers.
- **Least Privilege:** Pipeline-Service-Accounts erhalten nur zwingend benötigte Befehlsrechte.
- **Unveränderbare Logs:** Vollständige Audit-Protokolle aller Pipeline-Aktionen.



ACHTUNG
Niemals Klartext-Zugangsdaten in Git-Repositories committen; stets Secrets-Manager einbinden.

7. ANLEITUNG: ERSTE PIPELINE IMPLEMENTIEREN

In fünf klaren Schritten bauen Sie Ihre erste automatisierte CI/CD-Pipeline für Netzwerkkonfigurationen auf.



1. **Repository anlegen und Struktur definieren**
   Erstellen Sie ein Git-Repository mit getrennten Ordnern für Inventar (Hosts/IPs), Jinja2-Templates und Konfigurations-Playbooks.
2. **Linting- und Syntaxprüfungen einrichten**
   Konfigurieren Sie Pre-Commit-Hooks und CI-Runner, die YAML-, Jinja2- und Konfigurationsdateien automatisch auf Syntaxfehler prüfen.
3. **Validierungsstufe mit Batfish einbinden**
   Lassen Sie geplante Konfigurationsänderungen bei jedem Pull Request durch Batfish auf Erreichbarkeit und ACL-Sicherheit testen.
4. **Deployment-Stufe mit Bestätigung konfigurieren**
   Definieren Sie eine Pipeline-Stufe für das Ausrollen auf Testgeräten, gefolgt von einer manuellen Freigabe für Produktiv-Switches.
5. **Post-Deployment-Tests und Monitoring automatisieren**
   Führen Sie automatische ping- und route-lookup-Tests aus und verifizieren Sie den Status über Alerting-Systeme.

8. ENTSCHEIDUNGSMATRIX: PIPELINE-DESIGN

Wählen Sie anhand der Kritikalität und Infrastrukturgröße die passende Bereitstellungs- und Teststrategie aus.



Welcher Bereitstellungsansatz passt zu Ihrer Netzwerkinfrastruktur?

Kleines Netz (< 20 Geräte), Standard-Switches ohne API-Unterstützung	Mittelgroßes Enterprise-Netzwerk mit strukturierten VLANs und Routing	Rechenzentrumsnetz mit Cloud-Integration und SDN-Controllern
Verwenden Sie Git + Ansible mit SSH/CLI-Modulen, YAML-Linting und manueller Freigabestufe für Ausrollunger außerhalb der Arbeitszeiten.	Etablieren Sie Containerlab für virtuelle Integrationstests, Batfish für Vorabprüfungen und automatisches Rollback bei Verbindungsverlust.	Nutzen Sie vollständiges Network-as-Code via Terraform/Nornir mit Pre- und Post-Deployment pyATS-Testsuites, und automatischen Canary-Pipelines.

PROJEKT-ARBEITSBLATT: EIGENE PIPELINE PLANEN



Nutzen Sie dieses Formular, um die Eckdaten und Werkzeuge Ihrer geplanten Netzwerk-Automatisierung festzuhalten.

Versionskontrollsystem & CI/CD-Runner (z. B. GitLab CI, GitHub Actions):

Zielgeräte & Betriebssysteme (z. B. Cisco IOS-XE, Arista EOS, Linux):

Geplante Pre-Deployment Validierungswerkzeuge (z. B. Batfish, Yamllint):

Sicherheits- & Freigabeprozess (Reviewer, Secrets-Speicher, Rollback-Strategie):

NETZWERKSIMULATION UND EMULATION: CONTAINERLAB, EVE-NG UND GNS3

1. GRUNDKONZEPT & ZWECK



Netzwerksimulation und -emulation ermöglichen das risikofreie Entwerfen, Konfigurieren und Testen von Multi-Vendor-Netzwerktopologien auf Standard-Hardware.

- **Simulation:** Abstrahierte Verhaltensmodelle von Protokollen ohne Original-Firmware.
- **Emulation:** Ausführung tatsächlicher Hersteller-Betriebssysteme (z. B. Arista cEOS, Cisco IOS-XE/XR, Nokia SR OS, FRRouting) in virtuellen Maschinen oder Containern.
- **Anwendungsfelder:** Validierung von Netzwerk-Upgrades, CI/CD-Pipelines für Infrastructure as Code (IaC) und Vorbereitung auf Zertifizierungen.

2. CONTAINERLAB (CLAB)



Ein leichtgewichtiges CLI-basiertes Orchestrierungswerkzeug, das Docker- und Podman-Container über virtuelle veth-Paare zu komplexen Topologien verknüpft.

- **Konfiguration:** Deklarative Topologiedefinition vollständig in lesbaren YAML-Dateien.
- **Ressourceneffizienz:** Geringer RAM- und CPU-Overhead durch native Linux-Container (z. B. FRR, cEOS, SRlinux).
- **Automatisierung:** Nahtlose Integration in Git-Workflows, CI/CD-Runner (GitHub Actions, GitLab CI) und automatisierte Tests.
- **Einschränkung:** Beschränkt auf Images mit Linux-/Container-Support; monolithische VM-Images erfordern zusätzliche Hilfstools wie vrnetlab.

3. EVE-NG PLATZIERUNG & ARCHITEKTUR



Eine browserbasierte Emulationsplattform auf Basis von Ubuntu Server und KVM, optimiert für gemischte Umgebungen und Laborbetrieb.

- **Hypervisor:** Nutzt QEMU/KVM für vollständige Hardware-Virtualisierung proprietärer Router- und Firewall-Images.
- **Multi-User & Multi-Vendor:** HTML5-Weboberfläche für kollaborativen Zugriff ohne zwingenden Client-Installationsaufwand.
- **Modell-Unterstützung:** Breite Kompatibilität mit Cisco vIOS, ASAv, Fortinet FortiGate, Juniper vSRX und Windows/Linux-Endpunkten.
- **Ressourcenbedarf:** Benötigt dedizierte Server-hardware mit ausreichend RAM für speicherhungrige VMs.

8. EIGENE LAB-PLANUNG & NOTIZEN

Dokumentieren Sie Ihre Ziel-Topologie, Schnittstellenzuordnungen und Adressschemata vor dem Start der Emulation.

- **Protokolle:** Routing- und Switching-Protokolle festlegen (z. B. OSPF Area 0, eBGP, VLANs).
- **Schnittstellen:** Port-Mapping der virtuellen Verbindungen vorab visualisieren.



Geplante Topologie & Zielsetzung (z. B. BGP Leaf-Spine Fabric): _____

Gewählte Plattform (Containerlab / EVE-NG / GNS3) & Begründung: _____

IP-Subnetz- & Schnittstellen-Zuordnungen: _____

NETZWERK-SIMULATION & EMULATION

4. GNS3 ARCHITEKTUR

Eine etablierte Open-Source-Plattform mit nativer Desktop-GUI, die lokale oder ausgelagerte Virtualisierungs-Server steuert.

- **Client-Server-Modell:** Lokale GUI verbindet sich mit einer dedizierten GNS3-VM (VMware ESXi, Workstation oder VirtualBox).
- **Megacy & KVM:** Unterstützt Dynamips für historische MIPS-Cisco-Images sowie moderne QEMU/KVM- und Docker-Nodes.
- **Packet Capture:** Direkte 1-Klick-Anbindüität an Wireshark auf jeder virtuellen Verbindung für Live-Traffic-Analysen.
- **Flexibilität:** Ideal für Einzelplatz-Workstations- und akademische Laborübungen.



7. PRAXISTIPPS FÜR DEN BETRIEB

Zentrale Eenpfehlungen für Performance und Stabilität virtueller Netzwerkumgebungen.

- **Nested Virtualization:** Für EVE-NG und GNS3-VMs muss Intel VT-x bzw. AMD-V im zugrundeliegenden Hypervisor aktiviert sein.
- **RAM-Dimensionierung:** Planen Sie mindestens 2 bis 4 GB RAM pro vollwertiger Hersteller-VM (z. B. Cisco CSR1000v oder Arista vEOS) ein.
- **Lizenzierung:** Verwenden und exportieren Sie ausschließlich offiziell autorisierte virtuelle Maschinendateien und Container-Images der jeweiligen Hersteller.

WICHTIGER PERFORMANCE-HINWEIS

Vermeiden Sie es, mehr als 15 KVM-basierte Router-VMs auf einem Desktop-Rechner mit weniger als 32 GB RAM auszuführen. Nutzen Sie für größere Topologien Containerlab mit leichtgewichtigen Container-Images.

6. PRAKTISCHER CLAB WORKFLOW

Schritt-für-Schritt-Ablauf zum Erstellen und Ausführen einer funktionierenden Routing-Topologie in Containerlab.

1. **Topologie-Datei verfassen**
   Erstellen Sie eine 'topo.yml', in der Nodes (z. B. zwei FRR-Router) und Links definiert werden, die eth1 von Node1 mit eth1 von Node2 verbinden.
2. **Labor bereitstellen**
   Führen Sie den Befehl 'containerlab deploy -t topo.yml' mit Root-Rechten aus. Containerlab startet die Container und richtet die Linux-Bridges bzw. veth-Paare ein.
3. **Knoten konfigurieren & validieren**
   Verbinden Sie sich per 'ssh' oder 'docker exec -it' auf die Router-Instanzen, weisen Sie IP-Adressen zu und prüfen Sie die OSPF-/BGP-Nachbarschaft.
4. **Labor abbauen**
   Mit 'containerlab destroy -t topo.yml' werden alle Netzwerk-Namespaces und Container rückstandslos und reproduzierbar entfernt.

5. PLATTFORM-VERGLEICH & ENTSCHEIDUNG

Wählen Sie das passende Emulationswerkzeug basierend auf Ihrem primären Einsatzszenario und der verfügbaren Hardware.

Welches Tool passt zu Ihrem Netzwerksimulations-Ziel?

Containerlab	EVE-NG	GNS3
Fokus auf Container, CI/CD, Infrastructure as Code und minimale Systemressourcen	Fokus auf vollständige Router-/Firewall-VMs, grafische Weboberfläche und Multi-User-Labore	Fokus auf Desktop-Labor mit direkter Wireshark-Sniffer-Integration für Lernzertifizierungen
Containerlab wählen: Deklarative YAML-Definitionen erstellen und direkt mit Linux-basierten Netzwerk-Containern starten.	**EVE-NG einsetzen:** Auf Bare-Metal-Server oder Typ-1-Hypervisor installieren, KVM-Images einbinden.	**GNS3 nutzen:** GNS3-VM lokal in VMware Workstation betreiben und per Desktop-GUI steuern.

Proaktive Netzwerk-Verifikation mit Batfish

1. Was ist es



Batfish ist ein quelloffenes Analysewerkzeug zur mathematischen Modellierung und formalen Verifikation von Netzwerkkonfigurationen. Es parst Konfigurationsdateien herstellerübergreifend und berechnet das resultierende Weiterleitungsverhalten rein softwarebasiert.

- Mathematische Modellierung der Routing- und Forwarding-Ebene
- Keine aktive Test-Hardware oder reale Geräteausführung erforderlich
- Herstellerunabhängiges Parsen von Konfigurationsdateien (Multi-Vendor)

2. Kernprinzip: Mathematische Analyse



Statt Pakete versuchsweise durch Testumgebungen zu senden, wandelt Batfish Konfigurationen in Datenflussmodelle um. Dadurch wird das Verhalten für jeden denkbaren Paketpfad deterministisch überprüfbar.

- Berechnung von Forwarding Information Bases (FIB) ohne Emulation
- Erimttlung aller erreichbaren Pfade für beliebige Header-Kombinationen
- Exakte Erkennung von Weiterleitungsschleifen und Routing-Sackgassen

3. Typische Einsatzszenarien



Verifikation eignet sich insbesondere für risikobehaftete Änderungen in komplexen Rechenzentrums- und Unternehmensnetzen vor deren Produktivschaltung.

- Pre-Commit-Validierung von ACL- und Firewall-Regeln
- Prüfung geplanter BGP- und OSPF-Routing-Änderungen
- Automatisierte Konformitätsprüfungen im Rahmen von CI/CD-Pipelines

4. Typischer Verifikations-Workflow



Der Verifikationsablauf folgt vier klaren Schritten: Konfigurationsexport, Snapshot-Erstellung, deklarative Abfrage und automatisierte Auswertung.

1. Snapshot zusammenstellen
2. Snapshot initialisierer
3. Verifikations-abfrage ausführen
4. Ergebnisse auswerten

5. Verifikations-Entscheidungsbaum



Kriterien zur Auswahl der passenden Prüfmethode vor einem Konfigurations-Rollout.

Welche Netzwerkeigenschaft soll primär verifiziert werden?

Ende-zu-Ende-Erreichbarkeit und ACL-Wirkung	Redundanz und Ausfallsicherheit (Link-/Node-Failure)	Konformität der Basiskonfiguration (NTP, DNS, ACL-Syntax)
Reachability-Query ausführen; Header-Space-Einschränkungen definieren und blockierte Flows prüfen.	Differential-Reachability-Snapshot mit deaktivierten Schnittstellen erzeugen und Pfadänderungen vergleichen.	Init-Issues und Config-Compliance-Queries aufrufen, um syntaktische Abweichungen zu isolieren.

6. Checkliste vor Rollout

Wesentliche Prüfpunkte, die vor der Freigabe eines Snapshots erfolgreich validiert sein müssen.

- [ ] Snapshot parst vollständig ohne kritische Syntax-Warnungen
- [ ] Keine Routing-Schleifen für standardmäßige Datenpfade ermittelt
- [ ] Subnetz-Isolationsregeln zwischen Mandanten oder Zonen bleiben aktiv
- [ ] Sicherheitsrelevante Ports (z. B. SSH/Telnet) sind von außen unzugänglich
- [ ] Ausfall eines redundanten Core-Links führt zu keinem Blackhole

Wichtiger Praxishinweis

Formale Verifikation analysiert die definierte Konfiguration. Laufzeitprobleme wie fehlerhafte Transceiver oder physische Kabelbrüche erfordern weiterhin separates Monitoring.

7. Praktisches Pybatfish-Beispiel



Beispielhafte Abfrage zur Erreichbarkeitsprüfung mit dem Python-Client Pybatfish.

```
bf.set_network('rechenzentrum_ost')
bf.init_snapshot('configs_v2',
    name='snapshot_v2', overwrite=True)
result = bf.q.reachability(
  pathConstraints=PathConstraints(
    startLocation='host1'),
  headers=HeaderConstraints(dstIps='10.20.0.5')
).answer().frame()
assert result.empty == False,
  'Verbindungsabbruch: Ziel 10.20.0.5
   nicht erreichbar!'
```

8. Arbeitsprotokoll



Protokollierungsfelder für den durchgeführten Validierungslauf im Change-Management.

Change-ID und betroffene Netzwerkknoten:

Ergebnis der Erreichbarkeitsanalyse (Reachability Query):

Festgestellte Anomalien oder blockierte Flows:

Freigabeentscheidung und Status für Deployment:

VRF & VLAN-MAPPING

1. GRUNDLAGEN VON VRF

Virtual Routing and Forwarding (VRF) ermöglicht es, mehrere unabhängige Routing-Tabellen auf einem einzigen physischen Router gleichzeitig zu betreiben. Dies trennt Netzsegmente auf Schicht 3 vollständig voneinander.



- Routing-Instanzen arbeiten strikt logisch isoliert
- Ermöglicht getrennte IP-Adressräume ohne gegenseitige Beeinflussung
- Typischer Einsatz in Multi-Tenant- und Provider-Umgebungen

2. VRF-LITE VS. MPLS-VRF

VRF-Lite implementiert isolierte Routing-Tabellen ohne MPLS-Signalisierung auf lokalen Routern. Im Gegensatz dazu nutzt MPLS-VRF Multiprotocol BGP und Label-Switching für providerweite Skalierbarkeit.



- VRF-Lite benötigt keine MPLS-Konfiguration auf Geräten
- MPLS-VRF nutzt Route-Distinguisher und BGP im Backbone
- VRF-Lite eignet sich ideal für Campus- und Firmennetze

3. LAYER-2 ZU LAYER-3 MAPPING

Die logische Verknüpfung erfolgt meist über Subinterfaces (z. B. GigabitEthernet0/0.10) oder Switch Virtual Interfaces (SVIs), die einem spezifischen VLAN zugeordnet und einer VRF-Instanz zugewiesen werden.



- Subinterfaces binden IEEE 802.1Q-Tags direkt an VRFs
- SVIs verbinden Layer-2-VLANs mit der Layer-3-Routing-Instanz
- Verhindert Datenlecks zwischen Mandanten auf Gateway-Ebene

4. ÜBERLAPPENDE IP-ADRESSRÄUME

Dank separater Routing- und Forwarding-Tabellen (FIB) können Mandanten identische IP-Bereiche (z. B. 192.168.1.0/24) nutzen, ohne dass Konflikte im Backbone-Routing auftreten.



- Identische Subnetze pro Mandant ohne Kollisionen
- Autonome Adressvergabe für externe Kundenstrukturen
- Saubere Kapselung aller Next-Hop-Informationen

5. ROUTING-PROZESSE

Dynamische Routing-Protokolle wie OSPF, EIGRP oder BGP können instanziert innerhalb individueller VRFs konfiguriert werden, wodurch Routeninformationen mandantenspezifisch getrennt bleiben.



- Eigene Protokoll-Instanzen je Kundenumgebung
- Keine Routenverbreitung in benachbarte VRFs
- Präzise Pfadauswahl pro Mandanten-Infrastruktur

6. INTER-VRF LEAKING

Müssen Mandanten auf gemeinsame Dienste zugreifen, können ausgewählte Präfixe über Route-Targets oder statische Routen gezielt zwischen VRF-Instanzen transferiert werden.



- Nutzung von BGP Extended Communities (Route-Targets)
- Statische Leaks für Gateway-Dienste oder zentrale DNS-Server
- Strenge Firewall-Prüfung an Leaking-Punkten erforderlich

7. SICHERHEITSVORTEILE

Die Layer-3-Isolation minimiert laterale Angriffspfade innerhalb physischer Infrastrukturen und schützt kritische Managementschnittstellen vor Standard-Netzwerkverkehr.



- Schutz vor unberechtigtem Hop-by-Hop-Traffic
- Isolation des internen Management-Netzes (Out-of-Band)
- Eindämmung von Spoofing- und Broadcast-Gefahren auf L3

8. DIAGNOSE & VERIFIKATION

Standardbefehlle müssen mit dem VRF-Kontext ausgeführt werden, da Routing-Lookups und Diagnose-Tools sonst nur in der Default-Tabelle ausgeführt werden.



- Befehl: show ip route vrf <NAME>
- Befehl: ping vrf <NAME> <ZIEL-IP>
- Befehl: traceroute vrf <NAME> <ZIEL-IP>



KONTEXT BEACHTEN
Wird bei Ping oder Traceroute die VRF ausgelassen, testet das Gerät fälschlicherweise die globale Standard-Tabelle.

TUNNELING-VERFAHREN (L3)

1. GRUNDPRINZIP DES TUNNELINGS

Tunneling kapselt vollständige Netzwerkpakete eines Protokolls (Payload-Paket) in die Nutzdaten eines Trägerprotokolls (Delivery-Header). Dadurch werden fremde, inkompatiblle oder ungeroutete Netzwerke durchquert, ohne dass Zwischenrouter den inneren Inhalt interpretieren müssen.



- Transittransport über autonome Systeme ohne native Routenunterstützung
- Kapselung auf Schicht 3 (Network Layer) durch Voranstellen eines äußeren IP-Headers
- Entkapselung am Tunnelendpunkt und Weiterleitung über die native Routingtabelle

KAPSELUNGS-OVERHEAD BEACHTEN
Zusätzliche Header verringern die effektive Maximum Transmission Unit (MTU). Ohne Anpassung (MSS Clamping) droht Paketfragmentierung oder Paketverlust durch gesetztes Don't-Fragment-Bit (DF).

2. IP-IN-IP (IP PROTOKOLL 4)

IP-in-IP (definiert in RFC 2003) stellt die einfachste Form des L3-Tunnelings dar. Ein IPv4-Paket wird unverändert in ein neues äußeres IPv4-Paket eingepackt.



- Protokollnummer im äußeren IPv4-Header: 4 (IPv4)
- Geringster Header-Overhead aller Tunnelverfahren (genau 20 Byte für IPv4)
- Unterstützt ausschließlich IPv4-Unicast, kein Multicast und kein IPv6
- Keine native Verschlüsselung oder Integritätsprüfung vorhanden

3. 6IN4 TRANSITIONSTUNNEL (IP PROTOKOLL 41)

6in4 (RFC 4213) kapselt native IPv6-Pakete direkt in IPv4-Pakete, um isolierte IPv6-Inseln über ein rein IPv4-basiertes Internet oder Weitverkehrsnetzwerk miteinander zu verbinden.



- Protokollnummer im äußeren IPv4-Header: 41 (IPv6-Encapsulation)
- Fester Kapselungs-Overhead: 20 Byte IPv4-Header vor 40 Byte IPv6-Basisheader
- Statisch konfigurierte Tunnelendpunkte (Point-to-Point)
- Häufig genutzt von Tunnel-Brokern zur IPv6-Migration ohne Provider-Unterstützung

4. GENERIC ROUTING ENCAPSULATION (GRE, PROTOKOLL 47)

GRE (RFC 2784, RFC 2890) ist ein flexibles Kapselungsprotokoll, das nahezu beliebige Layer-3-Nutzlasten über IPv4- IPv6-Netzwerke transportieren kann.



- Protokollnummer im Trägerheader: 47 (GRE)
- Unterstützt dynamische Routing-Protokolle (OSPF, EIGRP, BGP) via Multicast
- Zusätzlicher Header: Standardmäßig 4 Byte (bis zu 16 Byte mit Key/Checksum/Sequence)
- EtherType-Feld im GRE-Header kennzeichnet das transportierte Innenprotokoll

5. VERGLEICH DER VERFAHREN

Strukturierte Gegenüberstellung der Eigenschaften, Limits und Overhead-Kosten der drei Standard-L3-Tunnelmethoden.



Verfahren	Overhead	Protokolle / Typen	Besonderheiten
IP-in-IP	20 Byte	nur IPv4-Unicast	extrem ressourcen-schonend
6in4	20 Byte	nur IPv6-over-IPv4	kein dynamisches Multicast-Routing
GRE	24+ Byte	Multiprotokollfähig	Multicast- und Broadcast-fähig
Sicherheit	–	alle drei Verfahren sind unverschlüsselt	Klartext-Payload

KOMBINATION MIT IPsec
Für vertrauliche Unternehmensdaten über öffentliche Netze muss GRE oder IP-in-IP im IPsec-Transportmodus betrieben werden (GRE-over-IPsec).

6. ABLAUF DES PAKETTRANSPORTS

Chronologischer Pfad eines Datenpakets von der Einleitung in das virtuelle Tunnelinterface bis zur Auslieferung im Zielnetz.



1. **Routenentschieidung**
   Paket trifft auf Quellrouter ein, Routing-Tabelle verweist für das Zielnetzwerk auf die virtuelle Tunnelschnittstelle (z.B. `tun0`).
2. **Header-Kapselung**
   Router erzeugt äußeren IP-Header mit Quell- und Zieladresse der Tunnel-endpunkte und hängt den Kapselungs-Header an.
3. **Zwischentransport**
   Transit-Router im Zwischennetz leiten das Paket ausschließlich basierend auf den äußeren IP-Adressen weiter.
4. **Entkapselung & Zustellung**
   Ziel-Tunnelrouter entfernt äußeren Header, prüft den inneren Header und stellt das Originalpaket an das lokale Ziel zu.

7. AUSWAHL-LEITFADEN FÜR TUNNELVERFAHREN

Entscheidungsbaum zur Auswahl des optimalen Protokolls basierend auf Netzwerkanforderungen und Routing-Umgebung.



Welche Anforderungen stellt die Standortvernetzung an Protokolle und dynamisches Routing?

- Ausschließlich IPv4-Unicast-Verkehr ohne dynamische Routing-Protokolle gefordert → **IP-in-IP** (Protokoll 4) einsetzen, um minimalen Header-Overhead (20 Byte) und geringe CPU-Last sicherzustellen.
- Anbindung eines isolierten IPv6-Netzes über eine reine IPv4-Infrastruktur → **6in4** (Protokoll 41) verwenden; statiache Adressbindung und geringen Migrations-aufwand nutzen.
- Dynamische Routing-Protokolle (OSPF/EIGRP/BGP) oder Multiprotokoll-Payload nötig → **GRE** (Protokoll 47) wählen. Bei Vertraulichkeitsbedarf zwingend mit IPsec im Transportmodus kombinieren.

8. ZUSAMMENFASSUNG & CHECKLISTE

Wichtigste technische Parameter für Diagnose, Konfiguration und Betrieb von Point-to-Point L3-Tunneln.



- Firewall-Freigaben: IP-Protokolle 4, 41 und 47 (keine TCP/UDP-Ports) auf Zwischenstationen prüfen
- MTU-Kalkulation: MTU der Tunnelschnittstelle um Kapselungslänge reduzieren (z.B. 1476 bzw. 1400 Byte)
- MSS Clamping: TCP MSS auf Path-MTU minus Header-Größe setzen, um Paketverwerfung zu verhindern
- Sicherheits-Check: Reine Tunnelprotokolle bieten keinerlei Verschlüsselung gegen Sniffing

TRAFFIC ENGINEERING: RSVP-TE & SEGMENT ROUTING



1. WAS IST ES



Traffic Engineering (TE) beschreibt die gezielte Steuerung von Datenströmen über vorab definierte, explizite Pfade abseits des klassischen Shortest-Path-Routings (IGP).

- Ziel: Engpässe auf Standardpfaden proaktiv umgehen
- Optimale Auslastung paralleler Leitungen im Backbone
- Grundlage für garantierte Dienstgüten (Bandbreite, Latenz)

2. KERNKOMPONENTEN



Für die Pfadberechnung und Reservierung arbeiten IGP-Erweiterungen mit Signalisierungs- oder Label-Verfahren Hand in Hand.

- Link-State-Erweiterungen (OSPF-TE, IS-IS-TE) zur Topologie- und Bandbreitenerkennung
- Constraint-based Shortest Path First (CSPF) zur Pfadberechnung
- Label Switched Paths (LSPs) als Transporttunnel

3. RSVP-TE PRINZIP



Resource Reservation Protocol Traffic Engineering untzt zustandsbehaftete Signalisierung entlang jedes Zwischenknotens.

- Path- und Resv-Nachrichten etablieren feste Bandbreitenreservierungen
- Jeder Router im Pfad hält Statusinformationen (Soft States)
- Hoher Signalisierungsaufwand bei großen Netzen mit vielen Tunneln



Skalierungseinschränkung
RSVP-TE erfordert periodische Aktualisierungen aller Knoten; bei tausenden parallelen Tunneln führt dies zu hoher CPU- und Speicherlast.

4. SEGMENT ROUTING (SR)



Segment Routing (SR-MPLS / SRv6) nutzt Source Routing und verzichtet auf Statusverwaltung auf den Zwischenknoten.

- Der Ingress-Router kodiert den gesemten Pfad als Label-Stack im Paket-Header
- Transitknoten verarbeiten nur das oberste Label (Push, Swap, Pop)
- Zustandsloser Core sorgt für signifikant bessere Skalierbarkeit

5. VERGLEICH & TECHNOLOGIEWAHL



Die Wahl zwischen RSVP-TE und Segment Routing richtet sich nach Skalierungsanforderungen und bestehender Hardware-Unterstützung.

- RSVP-TE: Streng reservierte Ressourcen, aber zustandsbehaftet
- Segment Routing: Schlank, stateless, optimal mit SDN-Controllern kombinierbar

Welches TE-Verfahren ist für das Backbone-Szenario geeignet?

→ Große Netzwerktopologie mit >10.000 Tunneln und modernem SDN-Controller
Segment Routing (SR-MPLS/SRv6) mit zentrallogischer Pfadberechnung einsetzen.

→ Bestandsnetzwerk mit strikt reservierter Bandbreite ohne Controller-Infrastuktur
RSVP-TE mit lokalen CSPF-Berechnungen und Fast Reroute (FRR) beibehalten.

→ Große Netzwerktopologie mit >10.000 Tunneln und modernem SDN-Controller
Segment Routing (SR-MPLS/SRv6) mit zentrallogischer Pfadberechnung einsetzen.

→ Bestandsnetzwerk mit strikt reservierter Bandbreite ohne Controller-Infrastuktur
RSVP-TE mit lokalen CSPF-Berechnungen und Fast Reroute (FRR) beibehalten.

6. SCHUTZMECHANISMEN (FRR)

Fast Reroute (FRR) stellt den unterbrechungsfreien Betrieb bei Ausfall von Links oder Netzknoten im Millisekundenbereich sicher.

- RSVP-TE FRR: Facility Backup Tunnel oder One-to-One Backup
- SR TI-LFA (Topology-Independent Loop-Free Alternate): Deterministischer Schutzpfad in < 50 ms ohne Signalisierungsüberhang
- Vorabberechnete Alternativpfade direkt in der Hardware-FIB



7. IMPLEMENTIERUNGSSCHRITTE



Strukturierter Ablauf zur Einrichtung von Traffic Engineering im Carrier- oder Enterprise-Backbone.

- Vorbereitung der IGP-Metriken
- Aktivierung der Signalisierungsebenen
- Monitoring und Pfadvalidierung

1. **Schritt 1: Link-State TE aktivieren**
   In OSPF oder IS-IS die Traffic-Engineering-Erweiterungen (TE LSA / TLVs) auf allen Kern-Schnittstellen konfigurieren.
2. **Schritt 2: Signalisierungs- oder Segment-Verfahren wählen**
   RSVP auf Interfaces freischalten oder SRGB (Segment Routing Global Block) und Node/Adjacency SIDs definieren.
3. **Schritt 3: Explicit Path und Tunnel anlegen**
   Ingress-Tunnel mit expliziten Next-Hops oder CSPF-Bedingungen (maximale Latenz, Bandbreitenschwellen) definieren.
4. **Schritt 4: FRR-Schutzpfade absichern**
   Tie-Breaking und TI-LFA bzw. RSVP Backup-Tunnel aktivieren, um Sub-50ms Umschaltung im Fehlerfall zu testen.

8. ZUSAMMENFASSUNG & MERKBLATT



Kompakter Überblick über das gezielte Management von Verkehrsflüssen zur Vermeidung von Engpässen und zur Steuerung nach SLA-Kriterien.

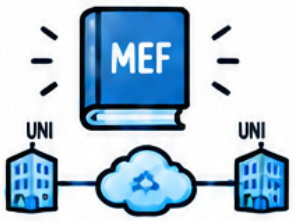
- Klassisches IGP nutzt nur den kürzesten Pfad; TE verteilt Last aktiv über alternative Wege
- RSVP-TE bindet Ressourcen statisch via Soft States
- Segment Routing verlagert Pfadentscheidungen komplett in den Paket-Header (Ingress-gesteuert)

CARRIER ETHERNET (MEF)

MEF-Standards für standardisierte Ethernet-Dienste über Weitverkehrsnetze mit serviceorientierten Leistungsmerkmalen.

1. DEFINITION & MEF-GRUNDLAGEN

Das Metro Ethernet Forum (MEF) definiert standardisierte Ethernet-Dienste über Weitverkehrsnetze (WAN/MAN). Carrier Ethernet kapselt Layer-2-Ethernet-Frames über Provider-Netzwerke (z. B. via MPLS, Segment Routing oder OTN) und garantiert serviceorientierte Leistungsmerkmale.



- **Standardisierte Schnittstelle:** User Network Interface (UNI) verbindet Kunden mit dem Netzbetreiber.
- **Dienstgrenze:** Klare Trennung zwischen Kunden-LAN und Netzbetreiber-Infrastruktur.
- **QoS & SLAs:** Fest zugesicherte Bandbreiten (CIR), Burst-Raten (EIR) und Latenzgrenzen.
- **Unabhängigkeit:** Transparente Übertragung von VLANs und Kunden-Protokollen.

MEF-Kernbegriff
Ein Ethernet Virtual Connection (EVC) definiert die logische Verknüpfung von zwei oder mehr UNIs über das Provider-Netzwerk.

2. E-LINE (ETHERNET LINE)

E-Line realisiert Punkt-zu-Punkt-Verbindungen zwischen exakt zwei UNIs. Sie dient primär als flexibler, bandbreitenstarker Ersatz für klassische Standleitungen (TDM/E1/T1) und verbindet Standorte direkt.



- Punkt-zu-Punkt-Topologie (PtP): Direkte Verbindung zweier Kundenendpunkte.
- EPL (Ethernet Private Line): Exklusive physische Port-Zuweisung, volles VLAN-Tunneling.
- EVPL (Ethernet Virtual Private Line): Multiplexing mehrerer virtueller Leitungen über ein einziges UNI (VLAN-Tag-basiert).
- Haupteinsatz: Standort-zu-Standort-Kopplung, Rechenzentrun-Spiegelung, Cloud-Direktanbindungen.

3. E-LAN (ETHERNET LAN)

E-LAN bietet eine Mehrpunkt-zu-Mehrpunkt-Topologie (Multipoint-to-Multipoint). Es serbindet drei oder mehr Kundenstandorte so, als wären alle Systeme an denselben physischen Switch angeschlossen.



- **Multipoint-to-Multipoint:** Beliebige Standorte kommunizieren direkt miteinander.
- **EP-LAN:** Vollständig dedizierte Schnittstellen mit uneingeschränkter Transparenz.
- **EVP-LAN:** Virtualisiertes Multiplexing via VLANs auf gemeinsamen Übergabepunkten.
- **Haupteinsatz:** Vernetzung dezentraler Firmenzentralen, Campus-Netze und verteilte Mesh-Standorte.

4. E-TREE (ETHERNET TREE)

E-Tree stellt eine gerichtete segmentierte Punkt-zu-Mehrpunkt-Architektur (Root-and-Leaf) bereit. Root-Knoten können mit allen Knoten kommunizieren, während Leaf-Knoten strikt voneinander isoliert bleiben.



- Rollenmodell: Definition von Root-Schnittstellen (Zentrale/Server) und Leaf-Schnittstellen (Filialen).
- Verkehrsfluss: Root-zu-Leaf und Root-zu-Root erlaubt; Leaf-zu-Leaf-Verkehr wird netzwerkseitig unterbunden.
- EP-Tree & EVP-Tree: Bereitstellung als dedizierter Port-Dienst oder VLAN-basiert gemultiplext.
- Haupteinsatz: Filialnetze, IP-Videoüberwachung, zentralisiertes Internet-Offloading und Point-of-Sale (PoS).

5. BANDBREITENPROFILE & QOS-PARAMETER

MEF-Dienste sichern Quality of Service (QoS) durch standardisierte Bandbreitenprofile ab. Diese Parameter bestimmen, wie Carrier-Netze eingehenden Kundenverkehr einstufen und drosseln.



- CIR (Committed Information Rate): Garantierte Mindestbandbreite ohne Paketverlust.
- CBS (Committed Burst Size): Erlaubtes kurzzeitiges Datenvolumen innerhalb der CIR.
- EIR (Excess Information Rate): Zusätzliche Bandbreite nach Best-Effort-Prinzip (wird bei Engpässen verworfen).
- EBS (Excess Burst Size): Maximales Übertragungskontingent für temporäre Bursts oberhalb der CIR.

Verkehrsfarben (Two-Rate Three-Color)
Grün = Innerhalb CIR (garantiert):
Gelb = Im EIR-Rahmen (nachrangig):
Rot = Übersteigt Grenzwerte (wird sofort verworfen).

6. WAN-SERVICEWAHL: E-LINE vs. E-LAN vs. E-TREE

Entscheidungsbaum zur Auswahl des passenden Carrier Ethernet Servicemodells basierend auf Standorttopologie und Sicherheitsanforderungen.

- Prüfen Sie vorab die Skalierungspläne und Vertraulichkeitsgrenzen zwischen den Standorten.

Welche Topologie und Kommunikationsbeziehung erfordert Ihr Weitverkehrsnetz?

Zwei Standorte müssen direkt und transparent gekoppelt werden	Alle Standorte müssen gleichberechtigt und direkt untereinander kommunizieren (Full-Mesh)	Zentrale Ressourcen müssen erreichbar sein, aber Filialen dürfen keinen Querverkehr austauschen
E-Line wählen (EPL für maximale Protokolltransparenz oder EVPL bei mehreren virtuellen Instanzen).	**E-LAN wählen** (EP-LAN oder EVP-LAN), um ein standortübergreifendes Layer-2-Broadcastnetzwerk bereitzustellen.	**E-Tree wählen** (Zentralstandorte als Root definieren, Filialen als Leaf kapseln).

7. PRÜF- UND ABNAHMESCHRITTE FÜR MEF-DIENSTE

Leitfaden zur systematischen Inbetriebnahme und Validierung von Carrier Ethernet Services am Kunden-Handover (UNI).

1. **Physische Signalisierung am UNI prüfen**
   Schnittstellenstatus (Port Speed, Duplex, Optikpegel) am Übergabepunkt mit Provider-Vorgaben abgleichen.
2. **VLAN-Mapping und Service-Typ validieren**
   Port-basiertes (All-to-One Bundling bei EPL/EP-LAN) oder Tag-basiertes (CE-VLAN zu EVC Mapping) konfigurieren.
3. **Durchsatz- und Latenztest (RFC 2544 / ITU-T Y.1564)**
   Messung von CIR/EIR, Frame Delay (Latenz), Inter-Frame Delay Variation (Jitter) und Frame Loss Ratio.
4. **Broadcast- und Multicast-Filterung schärfen**
   Storm Control und Control-Protocol-Tunneling (L2CP) konfigurieren, um Provider- und Kundennetze vor Loops zu schützen.

8. ARBEITSBLATT & EVC-KONFIGURATION

Dokumentieren Sie die Parameter der bereitzustellenden Carrier Ethernet Verbindung für die SLA-Überwachung und Netzdokumentation.

- Halten Sie alle relevanten Kenndaten fest, bevor Sie den Dienst produktiv schalten.

Servicetyp (E-Line / E-LAN / E-Tree): _____

UNI-Standort A (Knotenrolle: Single / Root / Leaf): _____

UNI-Standort B / Gegenstellen (Knotenrollen):

_____

_____

Kunden-VLAN IDs (CE-VLAN Mapping) & MTU-Größe:

_____

_____

SLA-Parameter (CIR / EIR / garantierte maximale Latenz):

_____

_____

OPTISCHE WEITVERKEHRSÜBERTRAGUNG: WDM, CWDM & DWDM



1. GRUNDPRINZIP WDM

Wavelength Division Multiplexing (WDM) bündelt mehrere unabhängige optische Datensignale mit unterschiedlichen Lichtwellenlängen auf einem einzigen Lichtwellenleiter. Dadurch vervielfacht sich die Übertragungskapazität bestehender Glasfaserstrecken ohne Neuverlegung von Erdkabeln.



- Farbmultiplexing: Jede Übertragung nutzt eine spezifische spektrale Trägerwellenlänge (Lambda).
- Bidirektionale oder unidirektionale Nutzung eines Glasfaserpaars (Tx/Rx) möglich.
- Transparenz: Datenraten und Protokolle (Ethernet, OTN, SDH) sind je Kanal flexibel mischbar.

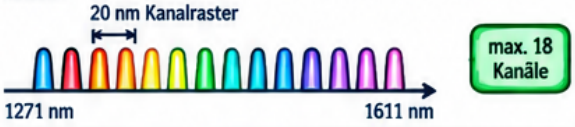
Physikalische Analogie

WDM funktioniert wie ein Prisma, das weißes Licht in Einzelfarben bricht: Am Eingang führt ein Multiplexer (Mux) viele Farbkanäle zusammen, am Ziel trennt ein Demultiplexer (Demux) diese sauber auf separate Empfänger.

2. CWDM – COARSE WAVELENGTH DIVISION MULTIPLEXING

CWDM nach ITU-T G.694.2 nutzt einen breiten Kanalabstand von 20 nm im Spektralbereich von 1271 nm bis 1611 nm. Es ist für städtische Netze (Metronetze) und Campus-Backbones bis etwa 40 bis 80 km konzipiert.

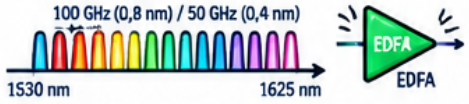
- Maximal 18 Kanäle bei 20 nm Kanalraster definiert.
- Ungekühlte DFB-Laser genügen durch das breite Toleranzfenster, was Investitionskosten senkt.
- Keine optischen Zwischenverstärker (EDFA) im Standard-Betrieb nutzbar.



3. DWDM – DENSE WAVELENGTH DIVISION MULTIPLEXING

DWDM nach ITU-T G.694.1 setzt auf ein extrem enges Frequenzraster (üblich 100 GHz bzw. 0,8 nm oder 50 GHz bzw. 0,4 nm) vor allem im optischen C-Band (1530–1565 nm) und L-Band (1565–1625 nm). Es bildet das Rückgrat weltweiter Weitverkehrsnetze.

- Hohe Kanaldichte: 40, 80 oder über 96 parallele Kanäle auf einer Glasfaser.
- Optische Verstärkung über EDFA (Erbium-Doped Fiber Amplifier) ohne elektro-optische Signalwandlung.
- Überbrückung von Hunderten bis Tausenden Kilometern im Weitverkehr (WAN).



4. VERGLEICH: CWDM VS. DWDM

Die Auswahl zwischen CWDM und DWDM orientiert sich an Reichweite, Investitionsbudget, Umweltbedingungen und dem Skalierungsbedarf über die Lebensdauer der Trasse.

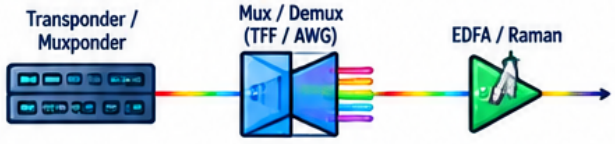
- Kanalabstand: CWDM 20 nm (grob) vs. DWDM 0,8 nm / 0,4 nm (dicht).
- Optische Verstärkung: CWDM ungeeignet für Standard-EDFA; DWDM nativ für EDFA-Verstärker optimiert.
- Laser-Kühlung: CWDM verwendet ungekühlte Laser; DWDM erfordert temperaturstabilisierte TEC-Laser.

Kriterium	CWDM	DWDM
Kanalabstand	20 nm	0,8 nm / 0,4 nm
EDFA (Standard)	nicht geeignet	geeignet
Laser-Kühlung	ungekühlt	TEC-stabilisiert

5. HARDWARE- UND INFRASTRUKTUR-BAUSTEINE

Ein optisches Transportnetz kombiniert passive Filterkomponenten mit aktiven optoelektronischen Transceivern und Verstärkereinheiten.

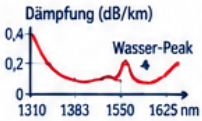
- Mux / Demux: Passive Dünnschichtfilter (TFF) oder Arrayed Waveguide Gratings (AWG) zur Kanalbündelung.
- Transponder / Muxponder: Wandeln Client-Signale (z. B. 10G/100G Ethernet Graulicht) in ITU-WDM-Wellenlängen.
- EDFA & Raman-Verstärker: Frischen Lichtsignale direkt im optischen Bereich auf langen Trassen auf.



6. OPTISCHE DÄMPFUNG UND DISPERSION

Die Übertragungsqualität und maximale Reichweite eines WDM-Signals werden primär durch Dämpfung und chromatische Dispersion auf der Glasfaser begrenzt.

- Dämpfungsbudget (dB): Summe aus Faserlänge (ca. 0,2 dB/km bei 1550 nm), Steckern und Spleißen.
- Chromatische Dispersion (CD): Unterschiedliche Frequenzen laufen unterschiedlich schnell; erfordert Kompensationsfasern (DCF) oder DSP.
- Optisches Signal-Rausch-Verhältnis (OSNR): Verschlechtert sich mit jeder optischen Verstärkerstufe.



Dämpfung bei Fasertypen

Standard-Singlemode-Fasern (ITU-T G.652) haben bei 1383 nm eine Dämpfungsspitze (Wasser-Peak). CWDM über alle 18 Kanäle erfordert Low-Water-Peak-Fasern (G.652.D).



Achtung bei Fasertypen

Standard-Singlemode-Fasern (ITU-T G.652) haben bei 1383 nm eine Dämpfungsspitze (Wasser-Peak). CWDM über alle 18 Kanäle erfordert Low-Water-Peak-Fasern (G.652.D).

7. ENTSCHEIDUNGSMATRIX: VERFAHRENSAUSWAHL

Wählen Sie anhand von Trassenlänge und Skalierungsbedarf das passende Multiplexing-Verfahren für Ihren Backbone-Entwurf.

Welche Trassenlänge und Kanalkapazität erfordert das Projekt?

Trasse unter 70 km, max. 8–16 Kanäle, begrenztes Budget	Trasse über 80 km oder mehr als 16 Kanäle mit Skalierung auf 400G+
Setzen Sie auf passives CWDM mit steckbaren SFP+/QSFP-Optiken ohne aktive Verstärker.	Planen Sie DWDM im C-Band mit EDFA-Verstärkern, Muxpondern und kohärenten Transceivern.

8. ZUSAMMENFASSUNG & PLANUNGS-CHECKLISTE

Führen Sie vor der Inbetriebnahme einer optischen WDM-Strecke die strukturierte Streckenprüfung durch.

- Streckendämpfung mittels OTDR-Messung einmessen und Dämpfungsbudget validieren.
- Wellenlängenplan (ITU-Grid) je Port am Multiplexer eindeutig beschriften und dokumentieren.
- Optische Eingangsleistung am Transceiver prüfen, um Übersteuerung des Empfängers zu verhindern.

1. **Schritt 1: Dämpfungsberechnung**
   Gesamtdämpfung berechnen: Faserlänge mal Dämpfungskoeffizient plus Schirmdämpfung der Patchfelder und Mux/Demux-Einfügedämpfung (typisch 2–4 dB pro Filter).
2. **Schritt 2: Transceiver-Abgleich**
   Sicherstellen, dass Sendeleistung (Tx) und Empfänger-Empfindlichkeit (Rx) zum berechneten Budget passen; ggf. optische Dämpfungsglieder (Attenuators) einsetzen.
3. **Schritt 3: Inbetriebnahme & Monitoring**
   Kanalweise Zuschaltung und Messung von Bitfehlerrate (BER) und OSNR vor Übergabe an die höheren Netzwerkschichten.

Gemessene Gesamtdämpfung der Trasse (dB): _____

Eingesetztes Verfahren (CWDM / DWDM / Grid-Abstand): _____

Dokumentierte Trägerwellenlängen (Lambdas je Kanal): _____

DATACENTER INTERCONNECT (DCI)

1. DEFINITION & DCI-ZWECK



Datacenter Interconnect (DCI) bezeichnet Technologien und Architekturen zur High-Speed-Vernetzung räumlich getrennter Rechenzentren für Workload-Mobilität, Georedundanz und Disaster Recovery.

- Kopplung über Stadtgebiete (Metro) oder Kontinente (WAN)
- Multi-Site-Clustering und aktive Redundanz
- Optimiert für niedrige Latenz und hohe Bandbreite

2. OPTISCHE ÜBERTRAGUNGSSCHICHT (LAYER 1)



Physikalische Verbindungen basieren auf Dark Fiber und optischem Wellenlängenmultiplex für maximalen Datendurchsatz.

- DWDM (Dense Wavelength Division Multiplexing) für Multi-Terabit
- CWDM für kostengünstige Kurzstrecken im Metro-Bereich
- Direkte optische Transceiver (z. B. QSFP-DD, ZR/ZR+)

3. LAYER-2-DCI-ERWEITERUNGEN



Ermöglicht das Dehnen gleicher Broadcast-Domänen und Subnetze über Standorte hinweg zur nahtlosen Servermigration.

- VXLAN mit EVPN-Control-Plane als moderner Industriestandard
- VPLS (Virtual Private LAN Service) über MPLS-Pfade
- OTV (Overlay Transport Virtualization) zur Isolation von Fehlern

4. LAYER-3-DCI & ROUTING



Standortkopplung auf Vermittlungsebene für hohe Fehlertoleranz ohne Risiken gestreckter Broadcast-Domänen.

- BGP (Border Gateway Protocol) für stabiles
- für stabiloe-Routing
- MPLS Layer-3 VPNs über Provider-Backbones
- Anycast-IP-Konzepte zur lokalen Lastverteilung

5. DCI-SICHERHEIT & VERSCHLÜSSELUNG



Da DCI-Strecken ungesicherte öffentliche Räume durchqueren, ist kryptografischer Schutz gegen Abhören und Manipulation obligatorisch.

- MACsec (802.1AE) für leitungsnahe Layer-2-Verschlüsselung mit Leitungsgeschwindigkeit
- IPsec für Layer-3-Tunneling über Fremdnetze
- Optische OTN-Layer-Verschlüsselung für minimale Zusatzlatenz

Kompensation von Broadcast-Stürmen

Bei Layer-2-DCI zwingend Broadcast/Multicast-Storm-Control und EVPN-ARP-Suppression aktivieren, um kaskadierende Ausfälle zu vermeiden.

6. REDUNDANZ & TOPOLOGIEN



Robuste Architekturen verhindern Single Points of Failure durch gezielte Diversität.

- Dual-Homed Edge-Router an jedem Standort
- Geografisch getrennte Glasfaser-Trassenführungen
- Aktive-Aktive Pfadnutzung via ECMP

7. DCI-ARCHITEKTURAUSWAHL



Entscheidungslogik zur Bestimmung des passenden Kopplungsansatzes anhand der Workload-Anforderungen.

- Prüfung: Erfordernis gleicher Subnetze vs. L3-Isolation
- Bewertung: Latenzbudget und maximale Umschaltzeiten

Müssen IP-Subnetze für nahtlose Live-Migration (z. B. vMotion) über Standorte hinweg identisch bleiben?

Ja
(Gleiche IPs an beiden Standorten nötig)

→ **Layer-2-Overlay einsetzen:** EVPN-VXLAN über DWDM/IP-Unterbau mit aktivierter ARP-Unterdrückung und MACsec.

Nein
(Unabhängige Subnetze pro RZ möglich)

→ **Layer-3-DCI via BGP/MPLS** Skalierbarkeit und vollständige Fehlerdomänen-Trennung.

8. BEREITSTELLUNGS-CHECKLISTE



Strukturierte Prüfschritte vor der Produktivschaltung einer DCI-Verbindung.

- Trassendiversität verifiziert
- Latenz- und Jitter-Budget gemessen
- MTU-Größe für Overlay-Header (mind. 1600 Byte) konfiguriert

Schritt-für-Schritt-Anwendung

1. **Schritt 1: Physik & Latenz messen**
   OTDR-Messung der Glasfaserstrecken durchführen und Round-Trip-Time (RTT) gegen SLA-Grenzen abgleichen.
2. **Schritt 2: MTU & Kapselung anpassen**
   Jumbo Frames auf allen Zwischenknoten aktivieren, um Paketfragmentierung durch EVPN/VXLAN-Header zu verhindern.
3. **Schritt 3: Verschlüsselung & Routing testen**
   MACsec- bzw. IPsec-Tunnel etablieren und Failover über getrennte Trassen unter Last simulieren.

Gemessene RTT (ms)	
Konfigurierte MTU-Größe (Byte)	
Freigegebener DCI-Technologietyp	

5G-Mobilfunknetzarchiktur: Radio Access Network und 5G Core

1. NG-RAN (gNodeB)



- **gNodeB (gNB):** Sendemast und Recheneinheit für die 5G-Funkschnittstelle (NR / New Radio).
- **CU/DU-Split:** Aufteilung in Central Unit (CU) und Distributed Unit (DU).
- **Massive MIMO & Beamforming:** Zielgerichtete Bündelung von Funkwellen auf einzelne Nutzer.

2. CUPS-PRINZIP



- **Control Plane (CP):** Regelt Verbindungsaufbau, Teilnehmerwechsel und Richtlinienverwaltung.
- **User Plane (UP):** Transportiert reine Nutzlastpakete (z. B. Videostreams, Webseitendaten).
- **Skalierungsvorteil:** Erweiterung von User-Plane-Knoten ohne Änderung der Steuerlogik.

8. NETWORK SLICING & QoS



- **eMBB:** Hohe Übertragungsgeschwindigkeiten und Medienstreaming.
- **uRLLC:** Zeitkritische Steuerungen in Industrie 4.0 und autonomem Fahren.
- **mMTC:** Millionen energiesparender IoT-Sensoren.

3. SERVICE-BASED ARCHITECTUR



- **RESTful APIs:** Funktionsaufrufe über HTTPS/JSON nach Webservices.
- **NRF:** Zentraler Katalog für alle Netzwerkfunktionen.
- **Cloud-native:** Virtualisierte Container in Rechenzentren und Edge-Standorten.

5G NETZWERKARCHITEKTUR (NG-RAN & 5GC)

7. AUSF & UDM (SICHERHEIT)



- **AUSF:** Überprüft Anmeldeanfragen und authentifiziert das Endgerät kryptografisch.
- **UDM:** Verwaltet Zugriffsrechte der Abonnenten.
- **SUPI/SUCI:** Schutz vor IMSI-Catchern durch Verschlüsselung der Identitätskennung.

4. AMF (MOBILITÄT)



- **Verbindungsverwaltung:** An- und Abmeldung von Geräten (Registration Management).
- **Mobilitätssteuerung:** Handover-Management zwischen Funkzellen.
- **NAS-Signalisierung:** Verschlüsselte Steuerbefehle zwischen Endgerät und Kernnetz.

6. UPF (NUTZDATEN)



- **Paketweiterleitung und Routing:** Transport der Nutzerdaten zwischen Funknetz und Internet.
- **Lokaler Datenanker:** Multi-Access Edge Computing für Latenzen im Millisekundenbereich.
- **Abrechnung und Messung:** Erfassung des genutzten Datenvolumens pro Sitzung.

5. SMF (SITZUNGEN)



- **PDU-Sitzungsverwaltung:** Zuweisung von IP-Adressen an Endgeräte.
- **UPF-Steuerung:** Konfiguration der Weiterleitungsregeln via N4-Schnittstelle.
- **QoS-Richtlinien:** Mindestbandbreiten und maximale Paketverzögerungen je Dienst.

Praxis-Prüfpfad: Verbindungsaufbau und Komponentenprüfung

Leitfaden zur systematischen Analyse und Fehlereingrenzung bei Verbindungsaufbau-Störungen in 5G-Netzwerken.

1 

Funkschnittstellen-Synchronisation

Verbindung zwischen UE und gNodeB über das NG-RAN verifizieren.

2 

NAS-Signalisierung und AMF-Erreichbarkeit

Registrierungsanfrage an die AMF; Absicherung über kryptografische Authentifizierung via AUSF/UDM prüfen.

3 

Sitzungsaufbau via SMF

Initiierung der PDU-Sitzung, IP-Adresse und Parameter für das Network Slicing.

4 

UPF-Tunnel-Aktivierung

Routingtabelle der UPF aktivieren und Durchsatz zum Data Network (DN) testen.

Prüfprotokoll

Geprüfter Slice / Dienst (z. B. eMBB, uRLLC, mMTC)

Festgestellte Latenz und Signalisierungsstatus

Entscheidungsfrage

Erfolgt der Verbindungsabrruch bereits während der Registrierung oder erst beim Datenfluss?

Abbruch vor IP-Vergabe

Funkverbindung zum gNB und Signalisierung zur AMF sowie Telinehmerrechte in UDM/AUSF prüfen.

Abbruch nach erfolgreicher Signalisierung

N4-Schnittstelle zwischen SMF und UPF sowie Routingregeln ins Ziel-Datennetz analysieren.

MOBILFUNK-KERNNETZE: 4G EPC vs. 5G SBA

Zentrales Konzept:
Vom Hardware-Knoten zum Cloud-Microservice

Das Mobilfunk-Kernnetz steuert Authentifizierung, Mobilität und Datenweiterleitung für Endgeräte. Während das 4G Evolved Packet Core (EPC) auf dedizierte Hardware-Knoten mit proprietären Punkt-zu-Punkt-Protokollen setzt, nutzt die 5G Service-Based Architecture (SBA) eine Cloud-native Microservice-Struktur, in der Netzwerkfunktionen modular über Webstandards (HTTP/2 und REST-APIs) kommunizieren.

- **4G EPC:** Statische Kopplung spezialisierter Funktionsblöcke (MME, SGW, PGW, HSS)
- **5G SBA:** Entkoppelte Network Functions (AMF, SMF, UPF, UDM, NRF) als Software-Container
- **Paradigmenwechsel:** Feste Schnittstellenkabel weichen flexiblen REST-API-Service-Bussen

1. 4G EPC ARCHITEKTUR & KERNKOMPONENTEN

- **MME (Mobility Management Entity):** Zentrale Signalisierungs- und Kontrollinstanz für Mobilitätsmanagement und Paging.
- **SGW (Serving Gateway):** Lokaler Routing-Anker bei Funkzellenwechneln und Puffer für Downlink-Pakete.
- **PGW (Packet Data Network Gateway):** Schnittstelle zum externen Internet, IP-Adressvergabe und Quality-of-Service-Durchsetzung.
- **HSS (Home Subscriber Server):** Zentrale Teilnehmerdatenbank mit Sicherheits- und Profildaten.



2. 4G PROTOKOLLSTAPEL & PUNKT-ZU-PUNKT-VERBINDUNGEN

- **GTP-C & GTP-U:** GPRS Tunnelling Protocol für Signalisierung (Control) und Nutzdaten (User Plane).
- **Diameter:** Authentifizierungs- und Autorisierungsprotokoll zwischen MME und HSS über Schnittstelle S6a.
- **SCTP / S1-MME:** Zuverlässiger Transport von Kontrollnachrichten zwischen Funkbasisstation (eNodeB) und MME.
- **Punkt-zu-Punkt-Abhängigkeit:** Jede Funktionserweiterung erfordert Anpassungen beider Endpunkte des Referenzpunkts.



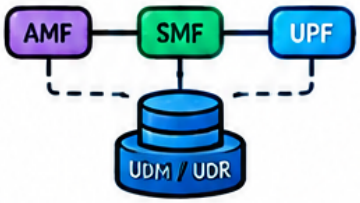
3. 5G SERVICE-BASED ARCHITECTURE (SBA) PRINZIPIEN

- **Service-orientiert:** Jede Funktion stellt über standardisierte Endpunkte Services (Producer) bereit oder konsumiert diese (Consumer).
- **Control & User Plane Separation (CUPS):** Radikale Trennung erlaubt die Platzierung von Datenpfaden nahe am Endanwender (Edge Computing).
- **Stateless Design:** Rechenlogik und Zustandsdaten werden getrennt, was elastisches Hoch- und Runterskalieren ermöglicht.
- **Cloud-Native:** Implementierung als zustandslose Container in Kubernetes-Umgebungen.



4. 5G KERNKOMPONENTEN & FUNKTIONALE ZUORDNUNG

- **AMF (Access and Mobility Management Function):** Übernimmt den verbindungs- und mobilitätsbezogenen Teil der ehemaligen 4G-MME.
- **SMF (Session Management Function):** Steuert IP-Sessions und Pfade (ehemalige Session-Aufgaben von MME und PGW-C).
- **UPF (User Plane Function):** Reiner Hochleistungs-Paketweiterleiter für Nutzdaten (ersetzt SGW-U und PGW-U).
- **UDM & UDR (Unified Data Management / Repository):** Trennt Telinehmerlogik von der eigentlichen Datenbank (ersetzt HSS).



5. SERVICE-SCHNITTSTELLEN: HTTP/2, REST & JSON

- **HTTP/2:** Transportprotokoll mit Multiplexing, Stream-Priorisierung und Header-Kompression über TLS.
- **RESTful APIs:** Ressourcenbasierte Architekturmuster (GET, POST, PUT, DELETE) zur Interaktion zwischen NFs.
- **JSON-Nutzlast:** Strukturierter, menschenlesbarer Datenaustausch für Profilabfragen und Session-Zustände.
- **NRF (Network Repository Function):** Zentraler Registrierungsdienst, bei dem sich NFs dynamisch anmelden und Services entdecken (Service Discovery).



6. DIREKTER ARCHITEKTURVERGLEICH: 4G EPC vs. 5G SBA

Gegenüberstellung der wesentlichen technischen Kenndaten beider Kernnetz-Generationen im schnellen Überblick.

- **Topologie:** 4G Punkt-zu-Punkt-Referenzpunkte vs. 5G Gemeinsamer Service-Bus / API-Mesh
- **Signalisierung:** 4G Diameter & GTP-C vs. 5G HTTP/2 REST APIs mit JSON
- **Skalierbarkeit:** 4G Vertikales Skalieren proprietärer Server vs. 5G Horizontales Auto-Scaling in Cloud-Clustern
- **Netzwerk-Slicing:** 4G Sehr eingeschränkt (DECOR/eDECOR) vs. 5G Voll integriertes End-to-End-Slicing per Software.



7. MIGRATIONSPFADE: NSA (OPTION 3x) vs. SA (OPTION 2)

- **Non-Standalone (NSA / Option 3x):** 5G-Funk (gNodeB) wird an das bestehende 4G-Kernnetz (EPC) angebunden. Schneller Rollout hoher Datenraten ohne neues Kernnetz.
- **Standalone (SA / Option 2):** Echtes 5G-Netz mit 5G-Funk direkt angebunden an die 5G SBA. Voraussetzung für Ultra-Low-Latency (URLLC) und echtes Slicing.
- **Koexistenz:** Dual-Connectivity-Geräte halten Verbindung zu LTE- und 5G-Zellen gleichzeitig.



8. ZUSAMMENFASSUNG & SICHERHEITSASPEKTE

- **Vorteile:** Schnellere Bereitstellung neuer Dienste, Edge-Fähigkeit und herstellerunabhängige Cloud-Infrastruktur.
- **Sicherheitsrisiken:** APIs bieten eine vergrößerte Angriffsfläche im Vergleich zu geschlossenen Telekommunikationsprotokollen.
- **Schutzkonzepte:** Transportverschlüsselung (TLS), API-Gateways (SEPP für Roaming) und strikte OAuth2-Token-Autorisierung.
- **Fazit:** 5G SBA transformiert das Mobilfunknetzwerk in eine verteilte, hochgradig programmierbare Softwareplattform.



PRAXIS-LEITFADEN: ARCHITEKTUR-AUSWAHL & ANALYSE-CHECKLISTE

ENTSCHEIDUNGSMATRIX: ARCHITEKTUR-AUSWAHL NACH EINSATZSZENARIO

Wählen Sie anhand der technischen Prioritäten die passende Kernnetz-Strategie.

Welche primäre Anforderung bestimmt die Einführung des Mobilfunk-Kernnetzes?

Fokus Breitband (NSA / Option 3x)

- Fokus auf schnellen Breitband-Rollout für Endverbraucher bei bestehender 4G-Infrastruktur.

Fokus URLLC & Slicing (SA / Option 2)

- Fokus auf Campusnetze, Industrie 4.0, ultra-geringe Latenz (URLLC) oder Network Slicing.

4G EPC HYBRID



- Einsatz von 5G Non-Standalone (NSA) mit 4G EPC. Nutzt vorhandene Core-Investitionen und liefert hohe Datenraten via 5G NR.

5G SBA



- Einsatz von 5G Standalone (SA) mit SBA. Ermöglicht lokale UPF-Instanzen am Edge und feingranulare API-Steuerung.

PRAXIS-CHECKLISTE: ANALYSE VON MOBILFUNK-KERNNETZKOMPONENTEN

Nutzen Sie diesen Leitfaden zur Bestandsaufnahme und Einordrung bestehender Mobilfunk-Netzarchitekturen.

PRAXIS-HINWEIS

Prüfen Sie bei der Umstellung auf 5G SBA besonders die Absicherung interner Service-Schnittstellen durch Mutual TLS (mTLS) und API-Firewalls.

1 SCHRITT 1: PROTOKOLLANALYSE DER KONTROLLSCHICHT

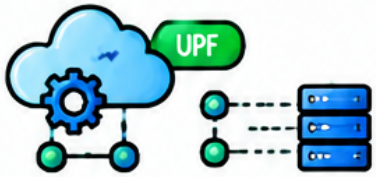
Identifizieren Sie die Signalisierungs-protokolle im Mitschnitt: Dominieren Diameter/GTP-C (4G EPC) oder HTTP/2-REST-Frames mit JSON-Struktur (5G SBA)?



- ○ Diameter / GTP-C (4G EPC)
- ○ HTTP/2 + JSON (5G SBA)

2 SCHRITT 2: TRENNUNG VON CONTROL UND USER PLANE ÜBERPRÜFEN

Prüfen Sie, ob Weiterleiitungselemente (UPF) autark am Netzwerk-Edge platziert sind oder mit Kontrollinstanzen gekoppelt bleiben.



3 SCHRITT 3: SERVICE-DISCOVERY UND SCHNITTSTELLENSICHERHEIT AUDITIEREN

Kontrollieren Sie das Vorhandensein der NRF sowie die Durchsetzung von TLS-Verschlüsselung und Authentifizierung zwischen den Microservices.



- ✓ NRF vorhanden
- ✓ TLS-Verschlüsselung
- ✓ Authentifizierung

Geprüfte Kernnetz-Topologie (4G EPC / 5G NSA / 5G SA):

Eingesetzte Sicherheitsmechanismen auf der Kontrollschicht (z. B. mTLS, OAuth2):

Notierte Latenz- und Edge-Anforderungen für UPF-Standorte:

5G NETWORK SLICING: END-TO-END QoS & ISOLATION



1. GRUNDPRINZIP & VIRTUALISIERUNG



- Network Slicing unterteilt eine gemeinsame physische 5G-Infrastruktur in mehrere logisch getrennte, virtuelle End-to-End-Netzwerke. Jeder Slice arbeitet als eigenständiges Netz mit maßgeschneiderten Leistungsmerkmalen.
- Basis: Network Functions Virtualization (NFV) und Software-Defined Networking (SDN)
- End-to-End-Abbeckung: Erstreckt sich über Funkzugang (RAN), Transportnetz und 5G Core
- Mandantenfähigkeit: Parallele Bereitstellung unterschiedlicher Anwendungsfälle ohne gegenseitige Störung

2. STANDARD-SLICING-TYPEN (3GPP SST)



- Die 3GPP definiert standardisierte Slice-Typen (Slice/Service Type, SST) zur Abdeckung der drei primären 5G-Nutzungsszenarien mit spezifischen Anforderungsprofilen.
- eMBB (Enhanced Mobile Broadband, SST 1): Hohe Datenübertragungsraten für Streaming und XR
- URLLC (Ultra-Reliable Low-Latency Communication, SST 2): Latenzen unter 1 ms für Robotik und autonomes Fahren
- mMTC (Massive Machine-Type Communications, SST 3): Hohe Verbindungsdichte bei geringem Energiebedarf für IoT

3. SLICING IM FUNKZUGANGSNETZ (RAN)



- Im Radio Access Network (gNodeB) werden die physischen Funkressourcen dynamisch oder statisch aufgeteilt, um die Anforderungen der jeweiligen Endgeräte zu bedienen.
- Dynamisches Radio Resource Management (RRM) priorisiert Frequenzblöcke
- Reservierung dedizierter Ressourcenblöcke (RB) für latenzkritischen Datenverkehr
- Verhinderung von Bandbreiten-Engpässen durch strenge Funkressourcen-Isolation

4. TRANSPORTNETZWERK & QoS



- Das Transportnetz verbindet Funkbasisstationen mit dem 5G-Kernnetz und garantiert garantierte Pfade und Übertragungsparameter über Metro- und Weitverkehrsstrecken.
- Segment Routing (SRv6/SR-MPLS) zur gezielten Pfadsteuerung einzelner Slices
- Garantierte Bandbreiten und minimale Jitter-Werte über DiffServ- und QoS-Mappings
- Einhaltung strikter Service Level Agreements (SLAs) für Ausfallsicherheit und Laufzeit

5. KERNNETZ (5G CORE) & FUNKTIONEN



- Im 5G Core (5GC) werden Steuerungsebene (Control Plane) und Nutzerebene (User Plane) modular aufgeteilt, um spezialisierte Rechenkapazitäten bereitzustellen.
- Dedizierte oder geteilte User Plane Functions (UPF) nahe am Endnutzer (Edge Computing)
- Slice Selection Function (NSSF) steuert die Zuweisung des Endgeräts zum passenden Slice
- Einsatz containerisierter Cloud-Native Network Functions (CNF) auf Basis von Kubernetes

6. ISOLATIONSEBENEN & SICHERHEIT



- Strikte Isolation stellt sicher, dass Fehler, Überlastungen oder Cyberangriffe innerhalb eines Slices keine Auswirkrungen auf parallele Netze haben.
- Performance-Isolation: Verkehrsspitzen in eMBB gefährden nicht die garantierten URLLC-Zeiten
- Sicherheits-Isolation: Eigene Sicherheitsrichtlinien, Verschlüsselungsschlüssel und Zugriffsfilter je Slice
- Management-Isolation: Getrennte Sichtbarkeit und Mandantenkonfiguration über Management-APIs

7. PRAXIS-WORKFLOW: SLICE-AUSWAHL

- Ablauf der Zuweisung eines 5G-Endgeräts (UE) zu einem spezifischen Network Slice beim Verbindungsaufbau.

1. **Schritt 1: Registrierungsanfrage**
   Das Endgerät sendet eine Registration Request mit der angeforderten NSSAI an die Basisstation (gNodeB).
2. **Schritt 2: Slice-Validierung**
   Die AMF (Access and Mobility Management Function) fragt die NSSF ab, um berechtigte Slices zu ermitteln.
3. **Schritt 3: Pfad- und UPF-Zuweisung**
   Die Session Management Function (SMF) bindet die passende UPF im gewählten Slice an und etabliert die QoS-Flüsse.

S-NSSAI Identifikator

- Jeder Slice wird eindeutig über Single Network Slice Selection Assistance Information (S-NSSAI) identifiziert, bestehend aus SST (Slice/Service Type) und optionalem SD (Slice Differentiator).



8. ZUSAMMENFASSUNG & MERKMALE



- Network Slicing wandelt starre Telekommunikationsnetze in hochflexible Dienstplattformen um, die heterogene Branchenanforderungen simultan erfüllen.
- Maximale Ressourceneffizienz durch dynamische Bereitstellung auf geteilter Hardware
- Verlässliche Dienstgütegarantien (QoS) für geschäftskritische Industrie-4-0-Prozesse
- Wirtschaftliche Skalierbarkeit ohne Bau separater physischer Infrastrukturen

OPEN RAN (O-RAN) ARCHITEKTUR

Disaggregation des Funkzugangsnetzes

1. GRUNDPRINZIP DER DISAGGREGATION



Open RAN bricht traditionelle, proprietäre Mobilfunk-Basisstationen auf und teilt Hard- sowie Software in interoperable Module.

- Ablösung monolithischer Blackbox-Systeme klassischer Netzausrüster
- Nutzung standardisierter Commercial-off-the-Shelf (COTS) x86- oder ARM-Serverhardware
- Offene Schnittstellen ermöglichen herstellerübergreifenden Komponententausch

2. O-RU (OPEN RADIO UNIT)



Die O-RU ist für die physikalischen Funkfrequenzsignale direkt am Antennenmast zuständig.

- Verarbeitet analoge HF-Signale, Filterung und digitale Wandlung (ADC/DAC)
- Implementiert Lower-PHY-Schichtfunktionen (Beamforming, FFT/IFFT)
- Minimale Rechenkomplexität am Mast zur Reduktion von thermischer Last und Energieverbrauch

3. O-DU (OPEN DISTRIBUTED UNIT)



Die O-DU verarbeitet zeitkritische Protokollschichten in räumlicher Nähe zu den Funkstellen.

- Verantwortlich für High-PHY, MAC (Medium Access Control) und RLC (Radio Link Control)
- Erfordert deterministische Echtzeitverarbeitung und harte Latenzgrenzen (Sub-Millisekunden)
- Läuft virtualisiert (vDU) auf Edge-Servern oder dedizierten Beschleunigerkarten (FPGA/ASIC)

4. O-CU (OPEN CENTRALIZED UNIT)



Die O-CU übernimmt zentrale, nicht-echtzeitkritische Steuerungs- und Datenweiterleitungsaufgaben.

- Unterteilung in O-CU-CP (Control Plane mit RRC/PDCP-C) und O-CU-UP (User Plane mit PDCP-U/SDAP)
- Zentralisierbar in regionalen Rechenzentren oder Cloud-Infrastrukturen
- Steuert Verbindungsaufbau, Mobilitätsmanagement und Paketweiterleitung ins Core Network

5. SCHNITTSTELLEN & 7-2X SPLIT



Standardisierte Schnittstellen verbinden disaggregierte O-RAN-Knoten ohne Bindung an Einzellieferanten.

- Open Fronthaul (Split 7-2x): Verbindet O-RU und O-DU mit Ethernet über eCPRI / IEEE 1914.3
- F1-Schnittstelle: Koppelt O-DU und O-CU (getrennt nach F1-C Signalisierung und F1-U Nutzdaten)
- E1-Schnittstelle: Standardisiert die Trennung zwischen O-CU Control Plane und User Plane

6. RIC (RAN INTELLIGENT CONTROLLER)



Der RAN Intelligent Contreller ermöglicht softwaregesteuerte Funknetz-Optimierung durch KI und Apps.

- Near-Real-Time RIC (10ms bis 1s Latenz): Führt xApps für Funkressourcen- und Interferenzmanagement aus
- Non-Real-Time RIC (> 1s Latenz): Nutzt rApps für Modelltraining, Richtlinien und strategische Parameter
- E2-Schnittstelle bindet Netzknoten (O-CU/O-DU) direkt an den Near-RT RIC an

7. VORTEILE & SICHERHEITSHERAUSFORDERUNGEN



Die Öffnung des Zugangsnetzes bringt betriebliche Flexibilität, erweitert jedoch die Angriffsfläche.

- **Vorteile:** Herstellerunabhängigkeit, schnellere Feature-Bereitstellung, CAPEX- und OPEX-Senkung
- **Risiken:** Erhöhte Komplexität bei Multi-Vendor-Interoperabilität und Fehlersuche
- **Sicherheit:** Zusätzliche Schnittstellen (Fronthaul, E2) erfordern lückenlose Authentifizierung und mTLS

ARCHITEKTUR-HINWEIS

Im Fronthaul-Netzwerk ist eine präzise Zeitsynchronisation via PTP (IEEE 1588v2) zwingend notwendig, um Phasen- und Frequenzversatz zwischen verteilten Antenneneinheiten zu verhindern.

8. ZUSAMMENFASSUNG & EVOLUTION



Open RAN transformiert proprietäre Mobilfunkarchitekturen in modulare, programmierbare Cloud-Netzwerke.

- Klar definierte Trennung: Mast (O-RU), Edge (O-DU) und Cloud/Rechenzentrum (O-CU)
- O-RAN Alliance Standards definieren weltweit einheitliche Schnittstellen und Profile
- Grundlage für softwaredefinierte Campusnetze und adaptive 5G/6G-Infrastrukturen

Mindmap: Satelliten- und Nicht-Terrestrische Netzwerke (NTN)

SATELLITEN- & NTN-NETZWERKE

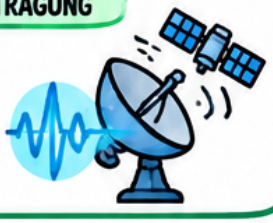
Orbits, Funkausbreitung und Routing zwischen Bodenstationen und Raumsegmenten.

1. ORBIT-KLASSEN (LEO, MEO, GEO)



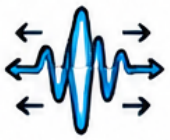
- LEO: 500–2.000 km, ca. 20–40 ms RTT.
- MEO: 2.000–35.786 km, ca. 100–180 ms RTT.
- GEO: 35.786 km, ca. 500–700 ms RTT.

2. DVB-S2X UND SATELLITEN-ÜBERTRAGUNG



- DVB-S2X: bis zu 256-APSK.
- ACM: Anpassung an Wetterbedingungen.
- GSE: IPv4/IPv6 direkt auf Satelliten-Frames.

3. DOPPLER-EFFEKT UND FREQUENZ-KOMPENSATION



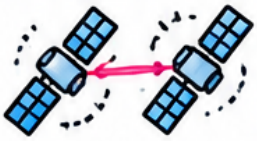
- **Frequenzdrift:** Annäherung ↑, Entfernen ↓.
- **Pre-Compensation:** Korrektur mit Ephemeridendaten.
- **Carrier Recovery:** PLL zur Nachführung der Frequenz.

4. LEO-MEGAKONSTELLATIONEN



- **Orbital Planes:** Hunderte bis Tausende Satelliten.
- **Frequent Handovers:** nahtloser Wechsel alle wenigen Minuten.
- **Space Debris Management:** Ausweichmanöver & Deorbiting.

5. ROUTING IM RAUM: ISL VS. BENT-PIPE



- **Bent-Pipe:** Satellit als Reflektor, leitet sofort weiter.
- **ISL:** Laser-Querverbindungen im Mesh-Netzwerk.
- **Dynamisches IP-Routing:** unterstützt wechselnde Topologien.

6. BODENSTATIONEN & GATEWAYS



- **Tracking-Antennen:** Phased-Array oder motorisierte Spiegel.
- **PoP:** Glasfaseranbindung an IXPs.
- **Feeder Links:** Q/V- oder Ka-Band mit hoher Bandbreite.

7. TRANSPORTPROTOKOLLE & TCP-HERAUSFORDERUNGEN



- **BDP:** große Empfangsfenster für GEO (TCP Window Scaling).
- **PEP:** Gateways splitten TCP auf.
- **QUIC & BBR:** robuster bei Verlusten und Jitter.

8. ZUSAMMENFASSUNG & NTN-ZUKUNFT



- 3GPP NTN Integration: Direct-to-Cell ab Release 17.
- Hybrid-Ökosystem: nahtloser Wechsel.
- Redundanz-Standard: Schutz kritischer Infrastrukturen.

ENTSCHEIDUNGSBAUM: AUSWAHL DES SATELLITEN-UPLINKS

Ermitteln Sie die passende Satelliten-Netzwerkarchiteiktur anhand der geforderten Anwendungslatenz und infrastrukturellen Gegebenheiten vor Ort.

- Vergleichen Sie die Anwendungsanforderung an Latenz und Datenvolumen.
- Wählen Sie die wirtschaftlich und technisch optimale Orbit-Klasse.

Welche Anforderungen stellt die Anwendung an die Ende-zu-Ende-Latenz und Ausfallsicherheit?

Echtzeitanwendung (Voice over IP, Gaming, Videokonferenzen mit (RTT unter 60 ms gefrodert)	Broadcast-Verteilung (TV/Radio) oder unkritisches Bulk-Data-Backup ohne Latenzrelevanz	Schiff- oder Luftfahrt mit globalem Roaming und mittlerem Latenzbedarf (100–150 ms)
LEO-Konstellation mit Phased-Array-Terminal wählen; Paketverluste bei Satelliten-Handovers einkalkulieren.	Klassischen GEO-Transponder mit stationärer Parabolantenne einsetzen; kostengünstig und dauerhaft stabil ausgerichtet.	MEO-Netzwerk oder hybride LEO/GEO-Flottenlösung mit automatisiert nachführenden Antennen evaluieren.

SCHRITT-FÜR-SCHRITT: NTN-VERBINDUNGSANALYSE DURCHFÜHREN

Gehen Sie diese Schritte durch, wenn Sie eine Verbindung über ein nicht-terrestrisches Netz prüfen oder debuggen.

- Strukturierte Überprüfung von Sichtfeld, Latenz und TCP-Optimierung.

1. **Sichtfeld & Elevation prüfen**
   Stellen Sie sicher, dass die Antenne freie Sicht zum Himmel hat (keine Abschattung durch Gebäude oder Bäume bei flachen Winkeln < 25°).
2. **Ping- und RTT-Messung ausführen**
   Prüfen Sie mit ICMP-Echos die Umlaufzeit: Typisch 30–50 ms bei LEO, rund 120 ms bei MEO und über 550 ms bei GEO.
3. **Jitter während Handover monitoren**
   Beobachten Sie Pings über 15 Minuten. Latenzspitzen oder Paketverluste deuten auf den Wechsel zwischen zwei LEO-Satelliten hin.
4. **TCP-Buffer & Window-Scale validieren**
   Überprüfen Sie am Endgerät, ob TCP Window Scaling akitiviert ist, um das Bandbreiten-Verzögerungs-Produkt voll auszuschöpfen.

Gemessene Basis-RTT (ms):	
Verwendetes Protokoll / Orbit-Typ (LEO / MEO / GEO):	
Beobachteter Paketverlust während Handover (%):	

Notizen zur TCP-Durchsatzmessung:

TIME-SENSITIVE NETWORKING (TSN)

1. GRUNDLAGEN & ECHTZEIT-BEDARF

- Klassisches Standard-Ethernet (IEEE 802.3) arbeitet nach dem Best-Effort-Prinzip mit unvorhersehbaren Latenzen und Jitter durch Queuing in Switches. Time-Sensitive Networking (TSN) erweitert Etherent auf Schicht 2 (Data Link Layer) um deterministische Garantien mit garantierten maximalen Latenzen und Null-Paketverlust durch Überlastung.
- **Problem:** Konkurrierender Datenverkehr verzögert zeitkritische Steuerdaten unkalkulierbar
- **Einsatzgebiete:** Industrielle Automatisierung (OT), Automotive (Fahrassistenz, Drive-by-Wire) und Avionik
- **OSI-Einordnung:** Reines Layer-2-Verfahren; kompatibel mit IP- und TCP/UDP-Stacks auf höheren Schichten

UNTERSCHIED ZU LEGACY-SYSTEMEN
TSN ersetzt proprietäre Feldbusse durch standardisiertes, interoperables IEEE-802-Ethernet bei voller Beibehaltung harter Echtzeitfähigkeit.

2. ZEITSYNCHRONISATION (IEEE 802.1AS)

- Fundament aller deterministischen Mechanismen ist eine gemiensane hochpräzise Zeitbasis. Das Profil IEEE 802.1AS nutzt das Precision Time Protocol (PTP) zur Synchronisation aller TSN-Endgeräte und Switches (Bridges) im Sub-Mikrosekundenbereich.
- **Grandmaster Clock:** Eine zentrale, hochgenaue Referenzuhr synchronisiert die Netzwerkknoten
- **Laufzeitkorrektur:** Kontinuierliche Messung von Leitungsverzögerungen (Propagation Delays)
- **Notwendigkeit:** Zeitgesteuerte Schalter (Gates) benötigen phasenstarre Synchronität

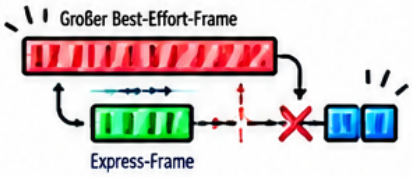
3. TIME-AWARE SHAPER (IEEE 802.1Qbv)

- IEEE 802.1Qbv realisiert zeitgesteuertes Multiplexen (TDMA). Für jede Ausgangs-Warteschlange (Queue) eines Switches schaltet ein Gate Control List (GCL) Zeitfenster exklusiv für hochpriore Klassen frei.
- **Gate Control List (GCL):** Zyklische Zeittabellen öffnen und schließen spezifische Queues
- **Geschützte Zeitfenster:** Niederpriorer Datenverkehr wird blockiert, wenn geplante Frames anstehen
- **Garantie:** Feste Obergrezene für Jitter und Übertragungsverzögerung



4. FRAME PREEMPTION (IEEE 802.1Qbu & 802.3br)

- Frame Preemption erlaubt es, die Übertragung eines bereits begonnenen größen Best-Effort-Frames auf dem physischen Link zu unterbrechen, um einen zeitkritischen Express-Frame ohne Wartezeit einzuschleusen.
- **Express vs. Preemptible:** Unterscheidung in unverzügliche Express- und unterbrechbare Datenströme
- **Fragmentierung:** Große Ethernet-Frames werden in minimale Fragmente geteilt und danach wieder zusammengesetzt
- **Bandbreitenschonung:** Verringert Guard-Bands vor 802.1Qbv-Fenstern erheblich



5. REDUNDANZ & VERLÄSSLICHKEIT (IEEE 802.1CB)

- IEEE 802.1CB (Frame Replication and Elimination for Reliablity / FRER) sichert geschäftskritische Kommunikationsflüsse gegen Hardware- und Kabelausfälle ohne Rekonfigurationsverzögerung ab.
- **Replikation:** Sendeknoten oder Ingress-Bridges duplizieren zeitkritische Ethernet-Frames
- **Disjunkte Pfade:** Duplikate laufen über getrennte Netzwerktrassen simultan zum Ziel
- **Eliminierung:** Die Egress-Bridge oder der Empfänger verwirft doppelt eintreffende Sequenznummern nahtlos



6. TRAFFIC POLICING: IEEE 802.1Qci & 802.1Qch

- Um die Einhaltung des deterministischen Plans sicherzustellen, überwachen und glätten auzätzliche TSN-Standards die Datenströme direkt an den Netzwerkports.
- 802.1Qci (PSFP): Per-Stream Filtering and Policing blockiert fehlerfafte oder böswillige Überlast (Babbling Idiots)
- 802.1Qch (CSFP): Cyclic Queuing and Forwarding synchronisiert zyklische Pufferung über Switches hineg
- Schutzwirkung: Gewährleistet Netzintegrität und Determinierung auch bei Komponentendefekten



7. PRAXISLEITFADEN: TSN-KONFIGURATION

Vorgehensweise zur Planung und Ihbetriebnahme deterministischer Netzwerkflüsse mittels zentraler Konfigurationsmodelle (CNC/CUC).

- Stream-Anforderungen erheben (Latenzbudget, Paketgröße, Zykluszeit)
- GCL-Berechnung durch den Centralized Network Configurator (CNC)
- Bereitstellung und Verifikation der Schedule-Tabellen

1. Bedarfsanalyse (Traffic Streams)
2. Topologie- & Latenz-Mapping
3. GCL & Preemption Berechnung
4. FRER-Pfad-definition

Welche TSN-Komponente löst primär Ihr Latenz- oder Zuverlässigkeitsproblem?

Große Best-Effort-Frames blockieren unvorhersehbar zeitkritische Steuersignale	Feste Zykluszeiten mit garantierten Mikrosekunden-Latenzschranken erforderlich	Verbindungsausfall führt zu sofortigem Fertigungsstopp oder Sicherheitsrisiko
↓	↓	↓
Aktivieren Sie IEEE 802.1Qbu Frame Premeption zusammen mit 802.3br an den Switchports.	Konfigurieren Sie IEEE 802.1Qbv Time-Aware Shaper mit synchronisierter Gate Control List.	Implementieren Sie IEEE 802.1CB (FRER) zur redundanten Paket-übertragung über disjunkte Pfade.

8. SYSTEMÜBERSICHT & PRÜFPROTOKOLL

- Arbeitsblatt zur Validierung eines neu parametrisierten TSN-Netzwerksegments vor der Freigabe im Produktivbetrieb.
- Dokumentation der Kernparameter
- Sicherstellung der deterministischen Schranken
- Bestätigung von Redundanz und Taktsynchronität

MESSPROTOKOLL BEREITSTELLEN
Hardwaregestützte Latenzanalysatoren verwenden, um Jittergrenzen im Dauerbetrieb unter Volllast empirisch nachzuweisen.

Netzwerk-Segment ID & Maschinenlinie: _____

IEEE 802.1AS Grandmaster Clock Quelle & Abweichung (ns): _____

GCL-Zykluszeit (µs) & reserviertes Zeitfenster (Qbv): _____

802.1CB Disjunkte Pfade (Interface Primär / Sekundär): _____ / _____

Gemessene maximale Latenz unter Worst-Case-Volllast (µs):

INDUSTRIELLE ETHERNET-FELDBUSSE

1. GRUNDPRINZIP: STANDARD-ETHERNET VS. ECHTZEIT-FELDBUSSE



Klassisches Standard-Ethernet (IEEE 802.3) arbeitet mit CSMA/CD oder Switch-basiertem Best-Effort-Verkehr. Dies reicht für Büro-kommunikation aus, erzeugt jedoch unvorhersehbare Latenzen (Jitter). Industrielle Feldbusse verlangen strikten Determinismus mit garantierten Zykluszeiten im Sub-Millisekundenbereich.

- Best-Effort vs. Determinismus: Büro-Netzwerke tolerieren Verzögerungen, Steuerkreise (Motion Control) führen bei Millisekunden-Jitter zur Notabschaltung.
- Zykluszeiten: Industrielle Prozesse fordern deterministische Wiederholraten typischerweise zwischen 250 µs und 10 ms.
- Lösungsansatz: Umgehung oder Erweiterung des Standard-TCP/IP-Stacks für direkte Hardware- oder Schicht-2-Kommunikation.

ECHTZEIT-KLASSEN

Industrielle Anforderungen unterteilen sich in weiche Echtzeit (z. B. HMI-Visualisierung, ca. 100 ms) und harte Echtzeit (Synchronisation von Antriebsachsen, < 1 ms mit Jitter < 1 µs).

2. PROTOKOLLARCHITEKTUR IM ISO/OSI-MODELL



Industrielle Ethernet-Protokolle verlagern zeitkritische Nutzdaten auf optimierte Pfade innerhalb des Schichtenmodells, um den Verarbeitungs-Overhead höherer Protokollschichten zu eliminieren.

- Schicht 7 (Anwendung): Bereitstellung von Objekt- und Gerätemodellen (z. B. CIP bei Ethernet/IP).
- Schichten 3 & 4 (IP/TCP/UDP): Reserviert für unkritische Parametrierung, Diagnose und IT-Anbindung.
- Schicht 2 (Sicherungsschicht): Direkte Frame-Einspeisung über dedizierte EtherTypes (z. B. Profinet RT/IRT oder EtherCAT) zur Minimierung von Protokoll-Overhead.

3. PROFINET: VON RT BIS IRT



Profinet unterscheidet drei Leistungsklassen je nach Echtzeit-Anforderung und Hardware-Unterstützung im Automatisierungsnetzwerk.

- Profinet Standard (NRT): Nutzt unverändertes TCP/IP für Konfiguration, Diagnose und Übertragung von Webdiensten.
- Profinet RT (Real-Time): Umgeht Schichten 3 und 4; Datenframes nutzen Schicht-2-Priorisierung nach IEEE 802.1Q (Zykluszeit: ca. 1-10 ms).
- Profinet IRT (Isochronous Real-Time): Verlangt spezielle Switch-Hardware (ASIC/FPGA) mit zeitgesteuertem TDMA-Verfahren für taktsynchrone Motion-Control-Vorgänge (< 1 ms, Jitter < 1 µs).

4. ETHERCAT: ON-THE-FLY-VERARBEITUNG



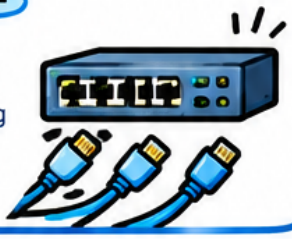
EtherCAT (Ethernet for Control Automation Technology) optimiert den Schicht-2-Durchsatz durch ein innovatives Durchlauf-Rahmenverfahren.

- Prinzip "Processing-on-the-fly": Ein Master sendet einen Standard-Ethernet-Frame durch alle Slaves. Jeder Slave entnimmt Eingangsdaten und fügt Ausgangsdaten direkt beim Durchlauf der Bits ein.
- Topologie: Physikalisch Linie oder Ring, logisch ein strukturierter Ring über Hin- und Rückleiter im selben Kabel.
- Effizienz: Ein einziger Frame bedient hunderte Ein-/Ausgangs-knoten; extrem geringe Telegrammlaufzeiten und Hardware-Latenzen.

HARDWARE-VORAUSSETZUNG

EtherCAT-Slaves benötigen zwingend dedizierte Hardware-bausteine (EtherCAT Slave Controller, ESC), während für den Master handelsübliche Standard-Ethernet-Schnittstellen genügen.

5. NETZWERK-TOPOLOGIE



Industrielle Feldbusse setzen auf eine hierarchische Struktur mit Switches und stern- oder linienförmiger Verkabelung für hohe Verfügbarkeit und einfache Erweiterbarkeit.

6. PRAXISBEISPIEL



Eine Verpackungsmaschine nutzt Profinet RT für die Antriebssteuerung und IRT für die synchronisierten Achsen. Das Ergebnis: kurze Zykluszeiten, hohe Präzision und stabile Produktion.

7. BEST PRACTICES



- Netzwerksegmentierung nutzen.
- Prioritäten und QoS konfigurieren.
- Kritische Geräte redundant auslegen.
- Überwachung und Diagnose kontinuierlich durchführen.

8. KURZE ZUSAMMENFASSUNG



Industrielle Ethernet-Feldbusse ermöglichen deterministische Kommunikation, reduzieren Protokoll-Overhead und nutzen optimierte Schicht-2-Pfade. Dadurch werden kurze Zykluszeiten, hohe Netzwerkeffizienz und zuverlässige Echtzeitprozesse realisiert.

PROTOKOLLVERGLEICH, ENTSCHEIDUNGSMATRIX UND PRAXIS-ARBEITSBLATT

5. ETHERNET/IP: COMMON INDUSTRIAL PROTOCOL (CIP)

Ethernet/IP integriert das etablierte **Common Industrial Protocol (CIP)** auf Basis standardisierter Internet- und Transportprotokolle.

- **Protokollbasis:** Nutzt reguläre TCP/IP-Stacks (TCP Port 44818 für explizite Nachrichten, UDP Port 2222 für zyklische I/O-Echtzeitdaten).
- **QoS & Priorisierung:** Stützt sich auf Differentiated Services Code Point (DSCP) nach IEEE 802.1p für I/O-Verkehr.
- **CIP Sync:** Implementiert IEEE 1588 (PTP) für verteilte Uhrensynchronisation in Antriebsapplikationen.
- **Netzwerkhardware:** Funktioniert mit handelsüblichen Commercial-off-the-Shelf (COTS) Switches, erfordert aber striktes IGMP-Snooping.

6. PROTOKOLL-ENTSCHEIDUNGSMATRIX

Wählen Sie das passende industrielle Ethernet-Protokoll basierend auf den Steuerungsanforderungen und Hardwarevorgaben aus.

Welche primären Steuerungs- und Zyklusanforderungen stellt die industrielle Anlage?

EtherCAT	PROFINET	EtherNet/IP
Hochgradig taktsynchrone Achssynchronisation mit minimalem Jitter (< 1 µs) und hardwarebasierter Linientopologie.	Siemens-kompatible Automatisierungsumgebung mit flexibler Skalierung von NRT über RT bis IRT.	Rockwell/Allen-Bradley-Ökosystem mit Standard-Switch-Infrastruktur und CIP-Objektmodell.
EtherCAT einsetzen (Master mit Standard-NIC, Slaves mit dedizierten ESC-Chipsätzen für On-the-Fly-Verarbeitung).	**Profinet wählen** (IRT mit ASIC-Switches für Motion Control, RT für Standard-SPS-zu-Peripherie-Verbindungen).	**Ethernet/IP implementieren** (Managed Switches mit IGMP-Snooping und QoS-Unterstützung konfigurieren).

7. INBETRIEBNAHME & DIAGNOSE-CHECKLISTE

Systematische Prüfung industrieller Ethernet-Installationen zur Vermeidung deterministischer Signalstörungen.

- **Verkabelung:** Geschirmte Industrial-Ethernet-Kabel (z. B. Cat 5e/6 M12 oder geschirmtes RJ45) verifizert und EMV-getrennt verlegt.
- **Switch-Konfiguration:** Bei Ethernet/IP Multicast-Filterung (IGMP Snooping) und DSCP-Priorisierung aktiv.
- **Topologie-Vorgaben:** Bei EtherCAT geschlosssne Ringverbindung oder Linienabschluss geprüft; keine Fremdswitches zwischen Slaves.
- **Zykluszeit-Budget:** Sendetakt und Aktualisierungszeit im Steuerungskonfigurator auf maximale Schirmung/Leitungslänge abgestimmt.

Drei Schritte zur Diagnose

1 Schritt 1: Physikalische Signal- und Schirmprüfung
Verbindungen mit industriellem Kabeltester durchmessen, Schirmbeidseitigkeit auf Potentialausgleich prüfen.



2 Schritt 2: Adress- und Namensvergabe
Gerätenamen (DCP bei Profinet) vergeben oder eindeutige IP-Zuweisung vornehmen; MAC-Adress-Kollisionen ausschließen.



3 Schritt 3: Zykluszeit- und Telegrammanalyse
Netzwerkanalysator (TAP-basiert) vorschalten und Jitter sowie Cyclic-Redundancy-Check (CRC)-Fehler unter Volllast aufzeichnen.



8. ARBEITSBLATT: FELDBUS-KONFIGURATIONSPROTOKOLL

Dokumentieren Sie die Eckdaten des industriellen Segments für Wartung, Audit und Fehlerdiagnose.

Dokumentationspflicht
Präzise Aufzeichnungen über Knotennummern, Soll-Zykluszeiten und Switch-Ports beschleunigen die Fehlerbebebung bei unerwartetem Busausfall drastisch.

Anlagensegment / Maschinen-ID:

Eingesetztes Protokoll (Profinet RT/IRT, EtherCAT, Ethernet/IP):

Projektierte Zykluszeit (µs / ms) & Master-Schnittstelle:

Slaves / Feldgeräte (Bezeichnung, EtherCAT-Adresse / IP / DCP-Name):

Gemessener Jitter und Switch-Konfigurationsnotizen (QoS / IGMP):

EDGE COMPUTING & LOCAL BREAKOUT (MEC)

1. GRUNDPRINZIP EDGE & MEC

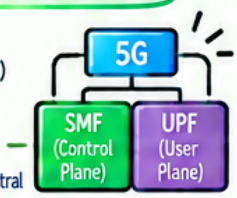
Multi-Access Edge Computing verlagert Cloud- und Rechenressourcen direkt an den Rand des Zugangsnetzes (Radio Access Network / Mobilfunkmast), um Datenwege radikal zu verkürzen.



- Verarbeitung nah an Endgeräten und Sensoren
- Dramatische Reduktion der Round-Trip-Time (RTT)
- Entlastung des zentralen Mobilfunk- und WAN-Backbones
- Ermöglicht deterministische Reaktionszeiten für zeitkritische Prozesse

2. ARCHITEKTUR & 3GPP-INTEGRATION

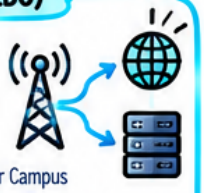
Im 5G-Kernnetz (5GC) wird die Steuerebene (Control Plane) von der Nutzerebene (User Plane) strikt entkoppelt (CUPS-Prinzip).



- SMF steuert Session-Management und Datenpfade zentral
- UPF transportiert den eigentlichen Nutzdatenverkehr
- Edge-Knoten beherbergen lokale Virtualisierungsinfrastruktur
- Offene APIs ermöglichen Third-Party-Edge-Anwendungen

3. LOCAL BREAKOUT (LBO)

Local Breakout leitet anwenderspezifischen IP-Verkehr direkt vor Ort aus dem Mobilfunknetz aus, anstatt ihn über das zentrale Core-Netzwerk zu routen.



- Auskopplung direkt am Edge-Standort oder Campus
- Vermeidung des Backhaul-Umwegs zum zentralen Rechenzentrum
- Lokaler Internet- oder Enterprise-LAN-Zugang
- Granulare Filterung nach Ziel-IP, FQDN oder APN/DNN

4. UPF-PLATZIERUNGSMODELLE

Die physische und logische Position der User Plane Function bestimmt Latenz, Betriebskosten und Hochverfügbarkeit der Gesamtlösung.



- On-Premises UPF: Kürzeste Latenz (< 5 ms) direkt auf dem Campusgelände
- Regional/Edge UPF: Zusammenfassung mehrerer Funkzellen an Verteilerknoten
- Central UPF: Traditionelles Modell mit hoher Latenz im Kern-Rechenzentrum
- Kaskadierte UPFs: Lokaler Branching Point leitet nur Edge-Traffic lokal ab

5. SCHRITT-FÜR-SCHRITT TRAFFIC FLOW

Der standardisierte Ablauf eines lokal ausgekoppelten Datenpakets vom Endgerät zur Edge-Anwendung:



1. **PDU-Session-Aufbau**
   Das Endgerät baut via gNodeB eine PDU-Sitzung auf; SMF wählt anhand DNN/NSSAI die passende UPF am Edge-Standort.
2. **Klassifikation am Branching Point**
   Die lokale UPF prüft Datenpakete per Uplink Classifier (UL CL) auf Übereinstimmung mit lokalen Edge-Routen.
3. **Lokales Routing & NAT**
   Passende Pakete verlassen das GTP-U-Tunnelnetzwerk und werden nativ ins lokale Edge-Subnetz weitergeleitet.
4. **Verarbeitung & Direkte Antwort**
   Edge-Container berechnen Antworten mit minimaler RTT und senden Pakete direkt über den lokalen Pfad zurück.

6. SICHERHEIT & ISOLATION

Die Verteilung von Rechenkapazitäten und Netzauskopplung an dezentrale Standorte erfordert angepasste Sicherheitszonen.



- Absicherung der Schnittstellen N3 (GTP-U) und N6 (Edge-LAN)
- Zero-Trust-Segmentierung zwischen Mobilfunknetz und Edge-Workloads
- Verschlüsselung sensibler Telemetriedaten am Edge-Knoten
- Physischer Schutz unbewachter dezentraler Edge-Racks

Sicherheitshinweis N6-Interface
Da der Datenverkehr beim LBO die geschützte Mobilfunk-Tunnelung verlässt, muss am N6-Interface zwingend eine Firewall-Inspektion erfolgen.

7. ENTSCHEIDUNGSMATRIX: EDGE-DESIGN

Wegweiser zur optimalen Platzierung von UPF und Edge-Ressourcen basierend auf Latenz- und Sicherheitsanforderungen:

Welche primäre Anforderung bestimmt den Anwendungsfall?

Ultra-Low-Latency (< 5 ms) oder strenge On-Premises-Datensouveränität (z. B. Robotik, Industrie 4.0)	Regionale Aggregation (10–25 ms) mit ausgewogenen Kosten (z. B. Smart-City, Flottenmanagement)	Klassische Weitverkehrs-anwendungen ohne Echtzeitanspruch (> 50 ms)
Dedizierte UPF und MEC-Server direkt auf dem Firmengelände platzieren (On-Premises Local Breakout).	Gemeinsame Edge-UPF am regionalen PoP/Zentralamt des Mobilfunkanbieters mit geteilten Server-Clustern nutzen.	Standard-Zentralisierung beibehalten: Zentrales Core-Rechenzentrum mit regulärem WAN-Routing.

8. CHECKLISTE: EDGE-DEPLOYMENT

Praxisleitfäden zur Validierung und Inbetriebnahme einer Edge- und LBO-Netzwerkarchitektur:



- [ ] GTP-U Kapselung und Uplink-Classifier-Filterregeln validiert
- [ ] Latenzmessung: Gemessene Round-Trip-Time (RTT) zum lokalen Edge-Knoten in ms
- [ ] Sicherheits- und Firewallregeln für ausgehende N6-Übergänge eingerichtet
- [ ] DNS-Konfiguration für lokale Hostauflösung im Breakout-Subnetz geprüft

MULTI-CLOUD-NETZWERKKONNEKTIVITÄT: DIRECT CONNECT, EXPRESSROUTE & INTERCONNECT

1. WAS IST ES



- Dedizierte private Cloud-Direktverbindungen umgehen das öffentliche Internet vollständig. Sie verbinden Unternehmensrechenzentren (On-Premises) über Layer-2- oder Layer-3-Leitungen direkt mit den Backbones von Cloud-Service-Providern (AWS Direct Connect, Azure ExpressRoute, Google Cloud Interconnect).
- Physische oder virtuelle Standleitung statt IPsec-Tunnel über das ungesicherte Internet
- Ermöglicht deterministische Latenzzeiten und garantierte Bandbreitenkontingente (1 Gbps bis 100 Gbps)
- Dient als infrastrukturelles Fundament für hybride Cloud- und Multi-Cloud-Topologien

2. ARCHITEKTUR & EBENEN

Die physische und logische Bereitstellung stützt sich auf standardisierte Netzwerkebenen nach dem OSI- und Internet-Schichtenmodell.



- **Layer 1 (Physical):** Glasfaser-Cross-Connects in Colocation-Rechenzentren (Meet-Me-Rooms)
- **Layer 2 (Data Link):** 802.1Q-VLAN-Tags (Virtual Interfaces/VIFs) zur logischen Trennung mehrerer Netze über einen Link
- **Layer 3 (Network):** IP-Routing mittels Border Gateway Protocol (BGP, RFC 4271) für dynamischen Routenaustausch

3. DIE HYPERSCALER-VARIANTEN

Jeder größe Cloud-Anbieter nutzt spezifische Gateways und Terminierungslogiken für den privaten Datenverkehr.



- AWS Direct Connect: Anbindung via Direct Connect Gateway (DXGW) an Transit Gateways oder VPC-VIFs
- Azure ExpressRoute: Kopplung über ExpressRoute-Gateways an Virtual WAN oder Virtual Networks (VNets)
- Google Cloud Interconnect: Dedicated oder Partner Interconnect mit Anbindung an Cloud Router via VLAN-Attachments

MULTI-CLOUD DIRECT CONNECT



4. VERBINDUNGSWEGE (CROSS-CONNECT)

Zwei primäre Bezugsmodelle stehen für die Kopplung des eigenen Routers mit der Cloud zur Verfügung.



- **Dedicated Connection:** Direkte 10/100-Gbps-Glasfaserports in Colocation-Standorten direkt am Switch des Providers
- **Hosted Connection / Partner Model:** Cloud-Exchange-Provider (z. B. Equinix, Megaport) bündeln VLANs über geteilte Trunks (50 Mbps bis 10 Gbps)

5. BGP-ROUTING-DYNAMIK

Der Border Gateway Protocol-Standard (BGP) steuert das Routing und sorgt für Ausfallsicherheit über autonome Systeme (AS).



- eBGP-Peering: Austausch privater oder öffentlicher IPv4/IPv6-Präfixe zwischen Kunden-AS und Hyperscaler-AS
- BFD (Bidirectional Forwarding Detection): Sub-Sekunden-Erkennung von Leitungsabbrüchen für sofortiges Failover
- Routenfilterung: Absicherung gegen BGP-Route-Hijacking durch strikte Prefix-Listen und AS-Path-Filter

7. PRAXIS: BEREITSTELLUNG EINER HYBRID-VERBINDUNG

Folgen Sie diesen Schritten zur Einrichtung einer ausfallsicheren Hybrid-Cloud-Verbindung:

1. **Verbindung buchen & LOA-CFA abrufen**
   Port beim Hyperscaler oder Partner beauftragen; Letter of Authorization (LOA-CFA) an den Rechenzentrumsbetreiber zur physischen Verkabelung übergeben.
2. **VLAN & IP-Subnetze konfigurieren**
   802.1Q-VLAN-Tagging auf dem Kundenrouter (CPE) und Cloud-seitig einrichten. Transfer-Subnetze (/30 oder /31 IPv4) bzw. /126 IPv6) zuweisen.
3. **eBGP-Peering & Authentifizierung etablieren**
   BGP-Session mit Kunden-ASN und Cloud-ASN initiieren; MDS-Passwortschutz und Prefix-Listen aktivieren.
4. **Redundanz & Failover validieren**
   Zweiten unabhängigen Pfad testen; Primärverbindung testweise deaktivieren und BFD-Failover-Umschaltzeiten protokollieren.



8. ENTSCHEIDUNGSMATRIX: VERBINDUNGSTYP WÄHLEN

Wählen Sie die passende Verbindungsmethode abhängig von Sicherheitsvorgaben, Bandbreitenbedarf und Budget.

Welche Anforderungen hat Ihre Hybrid-Cloud-Workload an Bandbreite und Latenz?

Niedrige Bandbreite (< 1 Gbps), variable Latenz akzeptabel, Budget limitiert	Site-to-Site IPsec-VPN über das öffentliche Internet einrichten.
Mittlere Bandbreite (50 Mbps - 10 Gbps), feste SLAs, mehrere Cloud-Anbieter parallel	Partner Interconnect / Hosted Connection über Cloud-Exchange-Provider buchen.
Sehr hohe Bandbreite (10 Gbps - 100 Gbps), minimale Latenz, strenge Compliance	Dedizierte Direct Connect / ExpressRoute / Dedicated Interconnect Glasfaserverbindung mit MACsec buchen.



9. KURZE ZUSAMMENFASSUNG

AWS Direct Connect, Azure ExpressRoute und Google Cloud Interconnect bieten unternehmensweite, hochperformante Bypass-Konnektivität abseits des Internets.

- Vorteile: Vorhersehbare Latenz, keine Internet-Jitter, 802.1Qete Daten-Egress-Kosten bei hohen Transfervolumina
- Wichtige Protokolle: IEEE 802.1Q (VLAN), BGP (RFC 4271), BFD für Sub-Sekunden-Routing-Umschaltung
- Best Practice: Stets redundante Leitungen über getrennte Carrier und Rechenzentrumswege für Hochverfügbarkeit vorsehen



THEMENKARTE: CLOUD VIRTUAL PRIVATE CLOUDS (VPC)

1. GRUNDKONZEPT & ARCHITEKTUR

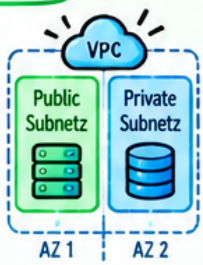
Eine Virtual Private Cloud (VPC) ist ein isoliertes, software-definiertes Netzwerk innerhalb einer Public-Cloud-Umgebung.



- Definiert einen logisch getrennten IPv4/IPv6-Adressbereich (z. B. 10.0.0.0/16) für eigene Resscurcen.
- Volle Mandantentrennung auf Hypervisor- und SDN-Ebene ohne physische Hardware-Bindung.
- Ermöglicht granulare Zonenaufteilung und direkte Kontrolle über Datenströme.

2. ÖFFENTLICHE & PRIVATE SUBNETZE

Subnetze unterteilen den Adressbereich einer VPC in logische und funktionale Segmente.



- Öffentliches Subnetz: Besitzt direkte Route zu einem Internet Gateway für Webserver und Proxys.
- Privates Subnetz: Keine direkte öffentliche Route; beherbergt Datenbanken und interne Logik.
- Verteilung über mehrere Verfügbarkeitszonen hinweg sichert Redundanz und Ausfallsicherheit.

3. ROUTING-TABELLEN & VERKEHRSFLUSS

Routing-Tabellen definieren Regeln, über die Netzwerkpakete ihr Ziel innerhalb oder außerhalb der VPC finden.

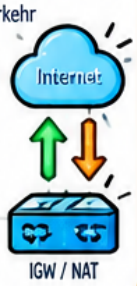


- Lokale Standardroute (Local Route) verbindet alle Subnetze innerhalb derselben VPC automatisch.
- Standardroute 0.0.0.0/0 legt das Standard-Gateway für ausgehenden Internetverkehr fest.
- Jedes Subnetz ist fest mit genau einer Routing-Tabelle verknüpft.

Routing-Tabelle	
10.0.0.0/16	local
0.0.0.0/0	igw
10.0.1.0/24	nat

4. INTERNET & NAT GATEWAYS

Gateways regulieren den Ein- und Ausgangsverkehr an den Perimetern des virtuellen Netzwerks.



- Internet Gateway (IGW): Ermöglicht zustandslose bidirektionale Kommunikation mit dem Internet.
- NAT Gateway: Erlaubt Instanzen in privaten Subnetzen ausgehende Updates, blockiert aber eingehende Verbindungen.
- NAT Gateways müssen in einem öffentlichen Subnetz mit statischer Public-IP platziert werden.

5. VPC PEERING TOPOLOGIEN

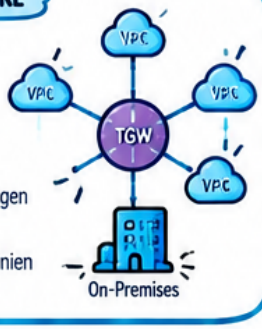
VPC Peering schaltet direkte Layer-3-Verbindungen zwischen zwei getrennten VPCs.



- Pakete verbleiben vollständig auf dem privaten Cloud-Backbone ohne öffentliches Internet-Transit.
- Kein transitiver Datenfluss: Verbindung VPC-A zu VPC-B und VPC-B zu VPC-C verbindet A und C nicht.
- Voraussetzung: IP-Adressbereiche (CIDR-Blöcke) dürfen sich keinesfalls überschneiden.

6. TRANSIT GATEWAY & HUB-AND-SPOKE

Ein zentraler Netzwerk-Hub vereinfacht komplexe Multi-VPC- und Hybrid-Cloud-Verbindungen.



- Hub-and-Spoke-Modell: VPCs und On-Premises-Netze verbinden sich sternförmig mit dem Gateway.
- Beseitigt den Verwaltungsaufwand von Vollvermaschungen (Full-Mesh-Peering) bei vielen VPCs.
- Zentraler Kontrollpunkt für firmenweite Routing-Richtlinien und Firewall-Inspektionen.

7. SECURITY GROUPS VS. NETWORK ACLS

Zweistufige Firewall-Schutzschichten sichern Datenströme auf Instanz- und Subnetzebene ab.



- Security Groups: Zustandshaft (Stateful), wirken direkt an der virtuellen Netzwerkschnittstelle.
- Network ACLs: Zustandslose (Stateless) Paketfilter auf Subnetzebene mit expliziten Allow/Deny-Regeln.
- Defense-in-Depth: Beide Mechanismen greifen komplementär für maximale Zugriffskontrolle.

Praxis-Merksatz

Security Groups lassen Antwortverkehr automatisch zurückfließen; Stateless NACLs verlangen explizite Freigaben für Hin- und Rückweg.

8. ZUSAMMENFASSUNG & PLANUNGSSCHRITTE

Strukturierter Leitfaden zur sicheren Dimensionierung und Bereitstellung einer neuen Cloud-VPC.



1. CIDR-Bereich krisenfest wählen und Überschneidungen mit On-Premises strikt vermeiden.
2. Subnetze symmetrisch über mindestens zwei Verfügbarkeitszonen auftellen.
3. Routing-Tabellen strikt nach Schutzbedarf trennen (Public vs. Private).
4. Sicherheitsregeln nach dem Prinzip der geringsten Berechtigung (Least Privilege) definieren.

Planungsschritte

1. Adressraum definieren
2. Subnetze partitionieren
3. Gateways zuordnen
4. Filterregeln schärfen

Entscheidung: Direkter Internetzugriff?

Benötigt die im Subnetz gehostete Ressource direkten Zugriff aus dem öffentlichen Internet?

- **Ja (z. B. Ingress Web-Loadbalancer)** → In öffentlichem Subnetz mit Route zum Internet Gateway platzieren und Security Group auf Port 80/443 beschränken.
- **Nein (z. B. Datenbank, Backend-Dienst)** → In privatem Subnetz isolieren; ausgehende Verbindungen nur über ein NAT Gateway leiten.

CLOUD VPC & NETZWERK-ARCHITEKTUR

Kubernetes-Netzwerkmodell: Pod-to-Pod-Kommunikation und CNI

1. GRUNDPRINZIP: FLACHES NETZWERK

Jeder Pod erhält eine eigene, clusterweit eindeutige IP-Adresse. Container innerhalb desselben Pods teilen sich den Netzwerk-Namespace und kommunizieren direkt über localhost. Zwischen Pods erfolgt die Adressierung direkt ohne Port-NAT (Network Address Translation).

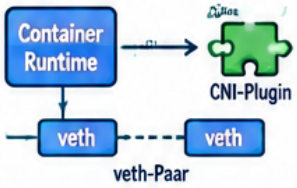
- Jeder Pod besitzt eine eindeutige IP im Cluster-IP-Bereich
- Pod-zu-Pod-Verbindung funktioniert standardmäßig ohne NAT
- Agents auf dem Node (z. B. Kubelet) erreichen alle lokalen Pods direkt



2. CONTAINER NETWORK INTERFACE (CNI)

Das CNI ist ein standardisiertes Plugin-Framework zur Netzwerkanbindung von Containern. Bei der Pod-Erstellung ruft die Container Runtime das CNI-Plugin auf, welches veth-Paare anlegt und die IP-Konfiguration vornimmt.

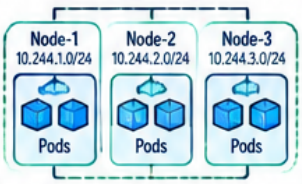
- Standardisierte Schnittstelle zwischen Runtime und Netzwerk-Treiber
- Erzeugt virtuelle Netzwerkadapter (veth-Paare) für den Pod
- Bindet das Pod-Interface an die Bridge oder Routing-Tabelle des Nodes



3. IPAM (IP ADDRESS MANAGEMENT)

Das CNI steuert die IP-Adressverwaltung im Cluster über dedizierte IPAM-Module wie host-local oder etcd-basierte Zuweisungen. Jedem Kubernetes-Node wird ein Subnetz-Block zugewiesen, aus dem Pod-IPs dynamisch bezogen werden.

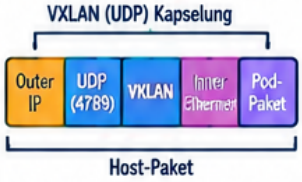
- CIDR-Block-Zuweisung pro Node (z. B. Node-1: 10.244.1.0/24)
- Verhindert IP-Kollisionen über verteilte Adresspools
- Automatische Freigabe bei Beendigung oder Verschiebung von Pods



4. OVERLAY-NETZWERKE (Z. B. FLANNEL)

Overlay-Netzwerke kapseln den ursprünglichen Pod-Verkehr in reguläre Host-Pakete (z. B. VXLAN oder Geneve). Dies ermöglicht Pod-Routing über physische Netze hinweg, ohne dass der physische Switch Pod-Subnetze lernen muss.

- VXLAN-Kapselung: Pod-Paket wird in UDP-Datagramm verpackt
- Funktioniert unabhängig von der zugrunde liegenden Switch-Topologie
- Geringfügiger Kapselungs-Overhead (MTU-Reduktion beachten)



KUBERNETES NETZWERKMODELL: POD-TO-POD & CNI



5. UNDERLAY- & DIRECT-ROUTING (Z. B. CALICO)

Underlay-Lösungen routen Pod-Pakete direkt über das physische Netzwerk ohne Paketkapselung. Calico nutzt dafür typischerweise BGP (Border Gateway Protocol) oder Linux-Routingtabellen für maximale Übertragungsgeschwindigkeit.

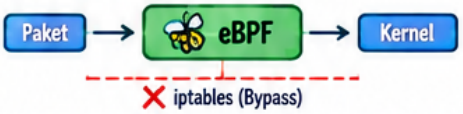
- Keine VXLAN-Kapselung: Volle Leitungsgeschwindigkeit und geringe Latenz
- Node agiert als virtueller Router und verteilt Routen via BGP
- Erfordert Netzwerk-Infrastruktur, die Pod-IP-Routen akzeptiert



6. eBPF-ARCHITEKTUR (Z. B. CILIUM)

Moderne CNI-Plugins wie Cilium nutzen eBPF (Extended Berkeley Packet Filter) direkt im Linux-Kernel. Netzwerkpakete und Sicherheitsrichtlinien werden ohne Umweg über iptables oder Kube-Proxy verarbeitet.

- Paketverarbeitung direkt auf Socket- und TC-Ebene im Kernel
- Ersetzt aufwändige iptables-Ketten durch hocheffiziente BPF-Maps
- Bietet integrierte Transparenz, L7-Filterung und Service-Routing



7. PRAXIS: POD-ROUTING VERIFIZIEREN

Schritte zur manuellen Prüfung der Pod-Netzwerkkonfiguration auf einem Kubernetes-Worker-Node.

1	2	3	4
Pod-IP und Node ermitteln	veth-Schnittstelle inspizieren	Node-Routingtabelle prüfen	Konnektivität und Tunnel testen
kubectl get pods -o wide	ip link oder crictl inspectp	ip route show	ping + tcpdump
Befehl ausführen, um Ziel-IP und Host-Node zu prüfen.	Das zugehörige virtuelle Interface identifizieren.	Pod-Subnetz auf das CNI-Interface oder Gateway prüfen.	Kapselung oder Direct Routing auf vxlan oder eth0 prüfen.

8. CNI-AUSWAHL ENTSCHEIDUNGSMATRIX

Wegweiser zur Wahl des passenden Netzwerk-Treibers basierend auf den Infrastruktur- und Sicherheitsanforderungen.

Welche Netzwerkanforderung dominiert Ihre Cluster-Umgebung?

Einfaches Test-Setup oder keine Kontrolle über Switches	Fokus auf strikte Network Policies und BGP-Routing	Hohe Durchsatzraten, Service-Mesh und Kernel-Sicherheit
Flannel mit VXLAN-Overlay wählen; minimale Konfiguration erforderlich.	**Calico** im Direct-Routing- oder Overlay-Modus einsetzen.	**Cilium** mit eBPF-Unterstützung aktivieren.

ZUSAMMENFASSUNG & ARCHITEKTUR-KERN

Das Kubernetes-Netzwerkmodell garantiert ein flaches Adressierungsmodell, bei dem jeder Pod wie eine vollwertige VM im Netzwerk erreichbar ist. Das CNI-Plugin setzt diese Abstraktion in die Praxis um: Overlay-Plugins (Flannel) kapseln Pakete via VXLAN für maximale Portabilität, Underlay-Systeme (Calico) routen direkt via BGP für maximale Performance, und eBPF-Engines (Cilium) optimieren den Datenpfad direkt im Betriebssystemkern.

- Flaches Modell vermeidet Port-Kollisionen auf Host-Ebene
- Wahl des CNI-Plugins bestimmt Latenz, CPU-Overhead und Policy-Features
- IPAM steuert die Zuweisung kollisionsfreier Adressbereiche je Node

Praxis-Hinweis

Netzwerkrichtlinien (NetworkPolicies) werden erst durch ein geeignetes CNI wie Calico oder Cilium durchgesetzt. Flannel allein unterstützt standardmäßig keine Richtlinien.

KUBERNETES SERVICE-NETZWERKE UND INGRESS-CONTROLLER

1. GRUNDLAGEN & SERVICE-ABSTRAKTION



Pods in Kubernetes sind ephemer: Sie werden dynamisch erstellt, zerstört und neu geplant, wodurch sich ihre IP-Adressen ständig ändern. Ein Kubernetes-Service stellt eine stabile IP-Adresse und einen beständigen DNS-Namen als Abstraktionsschicht bereit.

- Löst das Problem dynamischer Pod-IP-Adressen durch virtuelle Endpunkte.
- Labels und Selektoren steuern die dynamische Zuordnung aktiver Ziel-Pods.
- Erzeugt automatisch Endpoints- bzw. EndpointSlice-Objekte zur Zielverfolgung.

2. CLUSTERIP: INTERNE KOMMUNIKATION



ClusterIP ist der Standard-Servicetyp in Kubernetes. Er vergibt eine interne, nur innerhalb des Clusters erreichbare IP-Adresse aus dem dedizierten Service-CIDR-Adressbereich.

- Verhindert direkten unautorisierten Datenverkehr aus externen Netzwerken.
- Dient vorrangig für Microservices, Datenbanken und Backend-APIs.
- Pakete werden clusterintern direkt zum Pod-Netzwerk geroutet.

3. NODEPORT: STATISCHER HOST-ZUGANG



NodePort öffnet einen identischen Port (Standardbereich: 30000-32767) auf jedem einzelnen Node des Clusters. Eingehender Datenverkehr wird automatisch an die zugehörigen Backend-Pods weitergeleitet.

- Baut transparent auf dem darunterliegenden ClusterIP-Service auf.
- Erlaubt externen Zugriff ohne dedizierte Cloud-Load-Balancer-Infrastruktur.
- Risiko ungelicher Lastverteilung bei direktem Ansprechen einzelner Nodes.

4. LOADBALANCER: CLOUD-INTEGRATION



Der Service-Typ LoadBalancer provisioniert über die jeweilige Cloud-Controller-Schnittstelle (z. B. AWS NLB, GCP Load Balancer) eine externe, öffentlich erreichbare IP-Adresse.

- Schaltet automatisch NodePort- und ClusterIP-Routingebenen vor.
- Verteilt externe Netzwerkverbindungen auf alle Worker-Nodes des Clusters.
- Verursacht je nach Cloud-Anbieter separate laufende Infrastrukturkosten.

5. KUBE-PROXY: IPTABLES VS. IPVS



Kube-Proxy läuft als Daemon auf jedem Node und setzt den virtuellen Paketfluss um. Er konfiguriert Kernel-Paketfilter, um Service-IPs auf Pod-IPs umzuschreiben.

- iptables-Modus: O(n)-Suchkomplexität; sequenzielle Regellisten werden bei vielen Services träge.
- IPVS-Modus: O(1)-Hashing-Tabellen: optimiert für Tausende Services und bietet Load-Balancing-Algorithmen (Round Robin, Least Connection).
- Wendet DNAT (Destination NAT) an, um virtuelle Service-IPs in Pod-IPs zu transformieren.

SNAT vs. DNAT

Kube-Proxy nutzt DNAT zur Umleitung an den Pod. Verlässt das Antwortpaket die Node, sorgt SNAT dafür, dass die Rückroute symmetrisch bleibt.

6. INGRESS-CONTROLLER & L7-ROUTING

Während Services auf Transportebene (Layer 4) arbeiten, fungiert ein Ingress-Controller als HTTP/HTTPS-Reverse-Proxy (Layer 7) für domain- und pfadbasiertes Routing.

- Zentralisiert SSL/TLS-Terminierung und Zertifikatsverwaltung an einer Stelle.
- Ermöglicht Host-Routing (api.domain.tld) und Pfad-Routing (/shop, /user).
- Gängige Implementierungen: NGINX Ingress, Traefik, HAProxy, Envoy.



7. ANWENDUNG & FEHLERSUCHE



Schrittweises Vorgehen bei der Diagnose von Netzwerkproblemen zwischen Client, Service-Abstraktion und Backend-Pods.

1. Pod-Endpoints prüfen
   Kontrollieren, ob der Service aktive Pods selektiert: kubectl get endpoints <service-name>.
2. Cluster-DNS verifizieren
   Namensauflösung im Cluster via CoreDNS testen: nslookup <service>.<namespace>.svc.cluster.local.
3. Kube-Proxy-Regeln prüfen
   Sicherstellen, dass iptables- bzw. ipvs-Tabellen auf den Nodes synchrone DNAT-Regeln aufweisen.
4. Ingress-Routing validieren
   HTTP-Antworten und Header direkt am Ingress-Controller abfragen: curl -vkH 'Host: api.beispiel.de' <ingress-ip>.

8. ZUSAMMENFASSUNG & ENTSCHEIDUNGSWEG

Wahl des passenden Bereitstellungsmechanismus basierend auf Anwendungszweck, Netzwerkschicht und Sicherheitsgrenzen.

- ClusterIP: Nur interne Cluster-Dienste ohne direkten externen Pfad.
- NodePort: Entweiklungs- und Testcluster oder On-Premise ohne externen Load Balancer.
- LoadBalancer: Einzelne Nicht-HTTP-Dienste oder Legacy-Protokolle mit externer IP.
- Ingress (L7): Moderne Webanwendungen, APIs und TLS-terminierte HTTP-Microservices.



Welche Routing-Komponente passt für Ihre Arbeitslast?

Interner Mikrodienst oder Datenbank ohne externen Zugriff	→ ClusterIP-Service mit interner DNS-Adressierung konfigurieren.
Öffentliche Webanwendung mit mehreren URLs und HTTPS-Terminierung	→ Ingress-Ressource mit L7-Reverse-Proxy und ClusterIP-Backends bereitstellen.
Extern erreichbarer Raw-TCP/UDP-Dienst in der Cloud	→ Service-Typ LoadBalancer zur Zuweisung einer externen Cloud-IP wählen.



eBPF IM NETZWERK-STACK

1. GRUNDLAGEN & ARCHITEKTUR

eBPF (Extended Berkeley Packet Filter) erlaubt das sichere Ausführen von Sandboxed-Code direkt im Linux-Kernel, ohne den Kernel neu kompilieren oder Module laden zu müssen.

- Ausführung im Kernel-Space ohne Userspace-Kontextwechsel
- Sicherheitsprüfung zur Ladezeit durch den internen In-Kernel-Verifier
- JIT-Kompilierung in nativen Maschinencode für maximale Ausführungsgeschwindigkeit
- Kommunikation und Zustandsspeicherung über eBPF-Maps (Key-Value-Stores)

2. XDP (EXPRESS DATA PATH)

XDP ist ein eBPF-basiertes Framework-Pfad, der Netzwerkpakete auf der untersten Treiberebene verarbeitet, noch bevor Kernelspeicher-Strukturen (sk_buff) allokiert werden.

- Paketverarbeitung direkt im Treiber oder hardwarenah auf der SmartNIC
- Minimale Latenz und Durchsatz im Bereich von mehreren Millionen Paketen pro Sekunde
- Aktionen pro Paket: XDP_DROP, XDP_TX, XDP_REDIRECT, XDP_PASS
- Optimaler Hebel gegen volumetrische DoS- und DDoS-Angriffswellen

3. KERNEL-BYPASS IM VERGLEICH

Traditioneller Kernel-Bypass (wie DPDK) umgeht den Linux-Kernel vollständig, eBPF bietet eine kontrollierte Alternative innerhalb des Kernels.

- DPDK: Treibt Netzwerkkarte im Userspace via Polling-Modus, bindet volle CPU-Kerne
- eBPF/XDP: Nutzt weiterhin Kernel-Sicherheit, Treiber und Hardware-Abstraktion
- Kein Verlust von Standard-Linux-Tools und Schnittstellen bei eBPF
- Geringerer Integrations- und Wartungsaufwand im laufenden Rechenzentrumsbetrieb

4. L4-LOAD-BALANCING & NAT

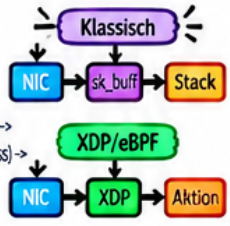
eBPF ersetzt klassische iptables/IPVS-Architekturen durch hochperformantes Layer-4-Load-Balancing auf Paketebene.

- Direkte Manipulation von Quell- und Ziel-IP/Port via eBPF-Maps
- Direct Server Return (DSR): Rückverkehr umgeht den Load Balancer vollständig
- Konstanter O(1)-Lookup-Aufwand unabhängig von der Anzahl der Routing-Regeln
- Einsatz in Cloud-Plattformen (z. B. Katran bei Meta oder Cilium in Kubernetes)

5. VERARBEITUNGSPFAD IM VERGLEICH

Der Lebenszyklus eines eingehenden Pakets entscheidet über Rechenaufwand, Latenz und CPU-Auslastung im Netzwerkstack.

- Klassisch: NIC Interrupt -> Ring Buffer -> sk_buff-Allokation -> iptables/Netfilter -> TCP/IP-Stack -> Socket
- XDP/eBPF: NIC Empfang -> XDP-Treiber-Hook -> eBPF-Programmentscheidung (Drop/Redirect/Pass) -> Direkte Aktion



6. OBSERVABILITY & TRACING

eBPF bietet tiefen, programmatischen Einblick in Netzwerkmetriken und Latenzen auf Socket- und Kernel-Ebene ohne Overhead.

- Anheften an Kernel-Probes (kprobes), Tracepoints und Socket-Filter
- Messung von TCP-Handshake-Latenz, Retransmissions und RTT in Echtzeit
- Transparente Protokollerfassung ohne Neuverkabelung oder Port-Spiegelung
- Grundlage moderner Cloud-Native-Sicherheits- und Observability-Lösungen

7. PRAXIS: XDP-FILTER ABLEGEN

Typischer Ablauf zur Erstellung, Überprüfung und Verankerung eines eBPF/XDP-Paketfilters.

1. C-Code verfassen: Paket-Header parsen und Entscheidungslogik definieren
2. Mit Clang/LLVM in eBPF-Bytecode (.o) kompilieren
3. Bytecode via 'ip link set dev eth0 xdpgeneric obj filter.o' an das Interface binden
4. Verifier prüft Speicherzugriffe und Terminationssicherheit vor Aktivierung

VERIFIER-REGEL

Der Kernel-Verifier verwirft Programme mit unbeschränkten Schleifen oder ungesicherten Zeigerzugriffen sofort. Jeder Header-Zugriff muss explizit auf Paketgrenzen geprüft werden.

8. ENTSCHEIDUNGSMATRIX: NETZWERKPFAD

Wann lohnt sich der Einsatz von eBPF/XDP im Vergleich zum Standard-Stack oder reinem Userspace-Bypass?

Welche Netzwerkanforderung steht im Vordergrund?

Standard-Routing & kleine Bandbreite (< 1 Gbit/s)	DDoS-Mitigation & L4-Load-Balancing im Terabit-Bereich	Exklusive proprietäre Protokolle mit festen CPU-Kernen
Klassischer Linux-Stack mit nftables/iptables reicht aus; kein Zusatzaufwand nötig.	XDP mit eBPF direkt im Treiber oder auf SmartNIC einsetzen, um Kernel-Overhead zu eliminieren.	Userspace-Kernel-Bypass (z. B. DPDK) prüfen, falls Linux-Treiberkompatibilität entbehrlich ist.

SERVICE MESH: ENVOY & ISTIO



1. WAS IST ES

- Ein Service Mesh stellt eine transparente Infrastrukturschicht für die Ausführung von Mikrodiensten dar. Es trennt den eigentlichen Anwendungscode strikt von Netzwerkaufgaben wie Ausfallsicherheit, Verschlüsselung und Telemetrie.
- **Data Plane:** Ausführung von Envoy-Proxys direkt neben jedem Container (Sidecar-Muster).
- **Control Plane:** Istio koordiniert Konfiguration, Zertifikatsvergabe und Richtlinienverwaltung.
- **Transparenz:** Applikationscontainer kommunizieren nur noch über das lokale Loopback mit Envoy.

Netzwerkisolierung
Entwickler müssen keine TLS-Bibliotheken oder Wiederholungslogik mehr in Geschäftslogik-Services einbauen: Envoy übernimnnt den gesamten Ingress- und Egress-Verkehr.

2. DATA PLANE: ENVOY ALS SIDECAR-PROXY

Envoy läuft als eigenständiger Prozess im selben Nextwerk-Namespace (Pod) wie die Zielanwendung. Durch iptables-Regeln wird sämtlicher Datenverkehr über diesen Proxy geleitet.

- Extrem geringer Speicher- und CPU-Overhead bei hohem Durchsatz (in C++ implementiert).
- Dynamisches Abrufen von Upstream-Endpunkten und Listener-Definitionen.
- Echtes Schicht-7-Verständnis für HTTP/1.1, HTTP/2 und gRRC.

3. CONTROL PLANE: ISTIO ARCHITEKTUR & ISTIOD

Istiod bündelt frühere Teildienste (Pilot, Citadel, Galley) in einen monolithischen Kontrollcontroller. Er übersetzt Deklarationen in hardwere- und clusterspezifische xDS-Konfigurationen.

- Verteilung von Endpunktdaten (Service Discovery) in Echtzeit an alle Envoy-Instanzen.
- Zentrale Zertifizierungsstelle (CA) zur Generierung ephemerer SPIFFE-Zertifikate.
- Validierung von CRDs (Custom Resource Defintions) vor der Verteilung.

4. MTLS: GEGENSEITIGE AUTHENTIFIZIERUNG

Zero-Trust-Netzwerkkommunikation wird durch automatiache mTLS-Tunnel (Mutual Transport Layer Security) zwischen Quell- und Ziel-Sidecars gewährleistet.

- Verifizierung kryptografischer Identitäten mittels SPIFFE ID im X.509-Subject-Alternative-Nane.
- Automatische Zertifikatsrotation ohne Verbindungsabbruch oder Neustarts.
- Erzwingung strikter Verschlüsselung (STRICT) oder Migration über PERMISSIVE-Modus.

5. L7-TRAFFIC-MANAGEMENT: ROUTING & POLICIES

Feingranulare Steuerung des Netzwerkflusses auf Basis von Anwendungsheadern, Methoden und URL-Pfaden über Istio VirtualServices und DestinationRules.

- Canary-Releases: Prozentuale Lastverteilung (z. B. 90 % v1, 10 % v2).
- A/B-Testing: Routing basierend auf HTTP-Headern. (z. B. User-Agent oder End-User-ID).
- Ausfallsicherheit: Automatische Timeouts, Retries und Circuit Breaking (Leitungsschutz).

6. TELEMETRIE: OBSERVABILITY & TRACING

Envoy generiert strukturierte Messdaten für jeden Ein- und Ausgangsvektor, ohne dass Code instrumentiert werden muss.

- Metriken: Export der goldenen Signale (Latenz, Fehlerrate, Sättigung, Durchsatz) an Prometheus.
- Distributed Tracing: Weiterleitung von B3-/W3C-Trace-Headern für Jaeger oder Zipkin.
- Access Logs: Detaillierte Protokollierung von HTTP-Statuscodes und Antwortzeiten.

7. INGRESSE & EGRESS: NETZWERKGRENZEN

Der Datenverkehr, der das Mesh verlässt oder betritt, wird über spezialisierte Envoy-Gateways isoliert und geregelt.

- Ingress-Gateway: Sicherer Einstiegspunkt für externen Datenverkehr mit TLS-Terminierung.
- Egress-Gateway: Kontrollierter Austritt für Auditierung und Beschränkung externer APIs.
- Verhinderung von Datenabfluss durch strenge Egress-Whitelists.

8. DIAGNOSE & FEHLERBEHEBUNG

Systematischer Prüfablauf bei Verbindungsfehlern zwischen Mikrodiensten im Mesh.

- Synchronisationsstatus zwischen Istiod und Envoy mit 'istioctl proxy-status' prüfen.
- Konfigurationszustand des Envoy-Proxys abrufen: 'istioctl proxy-config endpoints <pod-name>'.
- mTLS-Handshake-Fehler über die Access-Logs der Ziel-Sidecars analysieren.

SCHRITT-FÜR-SCHRITT-ANALYSE

1. **Proxy-Synchronisation prüfen**
   'istioctl proxy-status' ausführen.
2. **Zertifikatsgültigkeit analysieren**
   'istioctl proxy-config secret <pod-name>' nutzen.
3. **Routing-Regeln testen**
   Mit 'curl' HTTP-Header manipulieren.

FELDER

Betroffener Service / Pod-Name

Istiod Sync Status (SYNCED / STALE / NOT SENT)

Fehlercode in Envoy Access-Logs (z. B. 503 UC, 404 NR)

Welcher Fehlercode erscheint im Envoy Access-Log bei Verbindungsabbruch?

- **503 UC** → Überprüfen, ob der Zielcontainer abstürzt oder mTLS STRICT aktiviert ist, während der Client Klartext sendet.
- **404 NR** → VirtualService und Service-Port-Präfixe prüfen (z. B. 'name: http-web'), da Envoy den Datenverkehr sonst als reines TCP behandelt.

VoIP & Echtzeitkommunikation: SIP, SDP, RTP & RTCP

VOIP & ECHTZEITPROTOKOLLE

1. GRUNDPRINZIPIEN & ARCHITEKTUR



Voice over IP trennt Verbindungssteuerung und Medientransport strikt voneinander.

- Signalisierung steuert Rufaufbau, Halten, Weiterleiten und Terminierung.
- Medienstrom überträgt digitalisierte Sprachdaten direkt zwischen Endgeräten.
- Verzögerungsempfindlicher Transport nutzt UDP anstelle von verbindungsorientiertem TCP.

2. SIP (SESSION INITIATION PROTOCOL)



Textbasiertes Signalisierungsprotokoll nach RFC 3261 auf Schicht 7 für Sitzungsmanagement.

- Nutzt typischerweise UDP oder TCP auf Standard-Port 5060 (verschlüsselt TLS auf 5061).
- Kernmethoden: INVITE zum Rufaufbau, ACK zur Bestätigung, BYE zum Beenden.
- Status-Codes ähneln HTTP: 100 Trying, 180 Ringing, 200 OK, 404 Not Found.

3. SDP (SESSION DESCRIPTION PROTOCOL)



Deklaratives Format nach RFC 4566, das in SIP-Nachrichten zur Parameterabsprache transportiert wird.

- Handelt Medienformate (Audio, Video), Portnummern und IP-Adressen aus.
- Definiert unterstützte Codecs (z. B. G.711a/u, G.729, Opus) im Offer-Answer-Verfahren.
- Enthält Zeitstempel, Bandbreitenparameter und Verbindungsattribute.

4. RTP (REAL-TIME TRANSPORT PROTOCOL)



Ende-zu-Ende-Transportprotokoll nach RFC 3550 für zeitkritische Audiodatenströme.

- Arbeitet über UDP mit dynamischen, meist geraden Portnummern (z. B. 16384–32766).
- Header enthält 16-Bit-Sequenznummern zur Erkennung von Paketverlust und Vertauschung.
- Zeitstempel steuern die synchrone und kontinuierliche Audiowiedergabe beim Empfänger.

5. RTCP (RTP CONTROL PROTOCOL)



Kontroll- und Diagnoseprotokoll, das parallel zum Nutzdatenstrom auf ungeraden Ports läuft.

- Versendet periodisch Sender Reports (SR) und Receiver Reports (RR).
- Überwacht Übertragungsqualität anhand von Paketverlustrate, Round-Trip-Time und Jitter.
- Erlaubt dynamische Anpassung von Senderaten oder adaptive Codec-Umschaltung.

6. LATENZ, JITTER & JITTER-BUFFER



Netzwerkanomalien erfordern gezielte Pufferung und strenge Grenzwerte im IP-Netz.

- One-Way-Delay solite für natürliche Konversation unter 150 ms blebien (ITU-T G.114).
- Jitter bezeichnet statistische Schwankungen der Paketlaufzeit im Routingpfad.
- Jitter-Buffer puffert eingehende Pakete temporär, um gleichmäßige Tonausgabe zu sichern.

7. PRAXIS: SIP-CALL-FLOW ANALYSIEREN



Standardisierter Signal- und Medienablauf zur Diagnose in Netzwerk-Traces wie Wireshark.

1. **INVITE mit SDP-Offer**
   Endgerät A sendet INVITE an SIP-Proxy oder Endgerät B mit gewünschten Audio-Codecs und eigenem RTP-Empfangsport.
2. **Provisorische Antworten & Ringing**
   Empfänger bestätigt Empfang (100 Trying) und signalisiert Rufzustand (180 Ringing) an den Initiator.
3. **200 OK mit SDP-Answer**
   Endgerät B nimmt das Gespräch an und sendet 200 OK mit ausgewähltem Codec und Ziel-RTP-Port zurück.
4. **ACK & RTP-Medienstrom**
   Endgerät A bestätigt mit ACK, Sprachübertragung fließt bidirektional via UDP/RTP direkt zwischen beiden Peers.
5. **Gesprächsende via BYE & 200 OK**
   Aufleger sendet BYE-Anforderung: Gegenstelle quittiert mit 200 OK, woraufhin die RTP-Ports geschlossen werden.

8. ENTSCHEIDUNGSBAUM & FEHLERDIAGNOSE



Strukturierte Ursachenanalyse bei typischen Störungen in VoIP-Netzwerkumgebungen.

VoIP-Praxishinweis
Einseitiges Audio deutet fast immer auf asymmetrische NAT- oder Firewall-Blockaden des RTP-Rückkanals hin, während SIP korekt verhandelt wurde.

Welches Fehlerbild tritt bei der VoIP-Verbindung auf?

- **Kein Verbindungsaufbau / SIP-Timeout**
  Prüfe Erreichbarkeit von Port 5060 (UDP/TCP), DNS-SRV-Einträge und SIP-Registrierungsstatus am PBX-Server.
- **One-Way Audio (Nur eine Seite hört Ton)**
  Überprüfe SDP-Verbindungs-IP (c=) auf private Adressen hinter NAT sowie Freigabe der dynamischen RTP-UDP-Ports in der Firewall.
- **Verzerrter Klang oder Aussetzer**
  Analysiere RTCP-Paketverluste und Jitter-Werte; vergrößere adaptiven Jitter-Buffer oder priorisiere RTP mittels DSCP/QoS EF (Expedited Forwarding).

NAT-TRAVERSAL (STUN, TURN und ICE)

1. DAS NAT-PROBLEM BEI PEER-TO-PEER



Network Address Translation (NAT) maskiert private IPv4-Adressen hinter einer gemeinsamen öffentlichen IP. Eingehende Verbindungen von außen scheitern ohne vorherigen ausgehenden Datenstrom, da der Router keine Zielzuordnung im lokalen Netz kennt.

- Private IP-Bereiche (RFC 1918) sind im öffentlichen Internet nicht direkt erreichbar.
- Symmetrische und asymmetrische NAT-Router verhalten sich unterschiedlich bei Portzuweisungen.
- VoIP, WebRTC und P2P-Gaming benötigen direkte End-zu-End-Kommunikation ohne feste Serverweiterleitung.

HERAUSFORDERUNG
Zwei Clients hinter restriktiven Firewalls/NATs können ohne Vermittlungstechnologien keine direkte Verbindung aufbauen.

2. STUN: ERKENNUNG ÖFFENTLICHER ENDPUNKTE

Session Traversal Utilities for NAT (STUN) ermöglicht einem internen Client, seine eigene vom Router vergebene öffentliche IP-Adresse und den externen UDP/TCP-Port zu ermitteln.



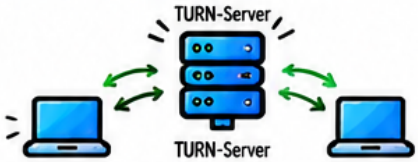
- Client sendet Binding Request an öffentlichen STUN-Server.
- Server antwortet mit der reflektierten IP und Portnummer (XOR-MAPPED-ADDRESS).
- Funktioniert zuverlässig bei Full Cone, Restricted Cone und Port Restricted Cone NAT.

GRENZE VON STUN
STUN versagt bei symmetrischem NAT, da für jedes neue Ziel ein anderer externer Port dynamisch generiert wird.

3. TURN: DATENRELAIS BEI RESTRIKTIVEN ROUTERN

Traversal Using Relays around NAT (TURN) stellt einen Relay-Server im Internet bereit, über den der gesamte Medien- oder Datenverkefir geleitet wird, wenn keine Direktverbindung möglich ist.

- Funktioniert auch bei strikten symmetrischen NATs und restriktiven Unternehmens-Firewalls.
- Erfrodert Authentifizierung und Bandbreitenressourcen auf dem Relay-Server.
- Erhöht Latenz im Vergleich zu P2P, garantiert jedoch Verbindungsaufbau als Fallback.



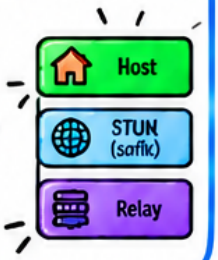
4. ICE: DER VERBINDENDE KONTROLLRAHMEN

Interactive Connectivity Establishment (ICE) kombiniert STUN und TURN zu einem systematischen Verfahren, um den schnellsten und stabilsten Pfad zwischen zwei Peers zu ermittelen.

- Sammelt alle verfügbaren Kandidatenadressen beider Endpunkte.
- Führt strukturierte Verbindungstests (Connectivity Checks) über UDP und TCP durch.
- Wählt automatissch die qualitativ beste Route aus (bevorzugt direkte P2P-Wege vor Relays).

5. ICE-KANDIDATENTYPEN IM DETAIL

Während des ICE-Prozesses generiert jeder Endpunkt drei spezifische Kategorien von Netzwerkkandidaten für den Verbindungsaufbau.



- Host Candidate: Lokale IP-Adresse und lokaler Port des Netzwerkadapters (für LAN-Kommunikation).
- Server Reflexive (srflx): Vom STUN-Server ermittelte öffentliche IP und Port des NAT-Routers.
- Relay Candidate: Auf einem TURN-Server allozierte Relay-Adresse als Ausfallsicherung.

6. SCHRITTWEISER ABLAUF DER PFADFINDUNG

Der ICE-Prozess folgt einem verbindlichen Ablaufprotokoll zwischen den beiden kommunitierenden Peers.

1. **Kandidatensammllung**
   Client erfasst lokale Schnittstellen und kontaktiert STUN/TURN-Server zur Adressermittlung.
2. **Signalisierungsaustausch**
   Peers tauschen ihre Kandidatenlisten via SDP (Session Description Protocol) über einen Signalweg aus.
3. **Paarbildung & Connectivity Checks**
   Kandidatenpaare werden nach Priorität geordnet und durch STUN-Binding-Requests gegenseitig geprüft.
4. **Pfadauswahl & Start des Datenstroms**
   Das schnellste esfiogreiche Paar wird fixiert; Mediendaten fließen direkt oder über das Relay.

7. ENTSCHEIDUNGSLOGIK FÜR DEN NAT-TRAVERSAL-FFAD

Bestimmen Sie anhand der Netzwerksituation, welcher Traversal-Modus im System aktiv wird.

Liegt mindestens auf einer Seite ein symmetrisches NAT vor oder blockiert die Firewall direkte UDP-Pakete?

- **Nein** (Beide Seiten nutzen Cone-NAT oder öffentliche IPs) → Nutzung von Host- oder STUN-Kandidaten für eine direkte Peer-to-Peer-Verbindung ohne Relay-Kosten.
- **Ja** (Symmetrisches NAT auf beiden Seiten oder strenge Paketfilter) → Aktivierung des TURN-Relays (Relayed Candidate), um den Datenverkefr transparent weiterzuleiten.

8. SCHNELLREFERENZ & FEHLERANALYSE

Typische Fehlerquellen und Kenndaten zur Diagnose von Verbindungsabbrüchen in Echtzeitsystemen.

- Hohe Latenz oder Audioaussetzer weisen oft auf ungewollten Fallback auf überlastete TURN-Relays hin.
- Firewall blockiert UDP: ICE weicht auf TCP oder TLS (TURN über Port 443) aus.
- Keep-Alive-Pakete (z. B. STUN-Refresh) verhindern den Timeout von NAT-Routingtabellen.

HRAXIS-TIPP
In WebRTC-Browsern gibt chrome://webrtc-internals Aufschluss über die gewählten ICE-Kandidatenpaare.

Geprüfter STUN-Server (FQDN / Port): _____

Ermittelter NAT-Typ (z. B. Cone / Symmetrisch): _____

Verwendeter Verbindungspfad (Host / STUN / TURN): _____

WEBRTC NETZWERKARCHITEKTUR

1. WAS IST WEBRTC?

WebRTC (Web Real-Time Communication) ermöglicht direkte Audio-, Video- und Datenübertragung im Browser ohne zusätzliche Plugins.



- Echtzeitkommunikation über UDP-Transport
- Signalisierung separat über HTTPS oder WebSockets
- Geringe Latenzzeiten für Konferenzen und Streaming

2. VERBINDUNGSAUFBAU MIT ICE

Interactive Connectivity Establishment (ICE) ermittelt den optimalen Netzwerkpfad zwischen zwei Gegenstellen durch NAT- und Firewall-Systeme.



- Sammelt lokale Host-Adressen und reflexive Kandidaten
- Testet Verbindungspaare systematisch auf Erreichbarkeit
- Wählt den direktesten funktionsfähigen Übertragungspfad

3. NAT-TRAVERSAL: STUN & TURN

STUN und TURN überwinden Adressübersetzungen und strikte Firewall-Regeln in komplexen Heim- oder Firmennetzwerken.



- STUN ermittelt öffentliche IP-Adressen und Port-Zuordnungen
- Funktioniert bei symmetrischem NAT oft nicht vollständig
- TURN leitet Datenpakete als Relay-Server verbindlich weiter

Praxis-Hinweis
TURN-Server verursachen kontinuierliche Bandbreitenkosten, da der gesamte Medienverkehr über den Relay läuft.

4. SICHERHEIT: DTLS & SRTP

WebRTC erzwingt standardmässig eine durchgehende Verschlüsselung für sämtliche Medien- und Steuerdaten.



- DTLS handelt Schlüsselmaterial über UDP sicher aus
- SRTP verschlüsselt und authentifiziert Audio- und Videodaten
- SCTP kapselt zuverlässige Datenkanäle über DTLS

5. P2P-MESH TOPOLOGIE

Im Full-Mesh sendet jeder Teilnehmer seinen Medienstream direkt an jeden anderen Teilnehmer der Sitzung.



- Keine zentrale Medienserver-Infrastruktur erforderlich
- Minimale Serverkosten und minimale Zwischenlatenz
- Upload-Bandbreite skaliert quadratisch mit N*(N-1) Kanälen

6. SFU (SELECTIVE FORWARDING UNIT)

Eine SFU empfängt Streams einmalig vom Sender und leitet diese selektiv unverändert an andere Teilnehmer weiter.



- Client sendet stets nur einen einzigen Uplink-Stream
- Server dekodiert Medien nicht und schont Rechenleistung
- Unterstützt Simulcast für flexible Auflösungsstufen

7. MCU (MULTIPOINT CONFERENCING UNIT)

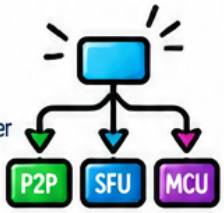
Eine MCU dekodiert sämtliche eingehenden Videoströme, mischt sie zu einem Gesamtbild zusammen und kodiert neu.



- Empfänger benötigen minimale Bandbreite und CPU-Last
- Hohe Server-Rechenlast durch kontinuierliches Transkodieren
- Zusätzliche Verzögerung durch Dekodier- und Kodierschritte

8. TOPOLOGIE-ENTSCHEIDUNGSMATRIX

Wählen Sie die Architektur basierend auf Teilnehmerzahl, Endgeräte-Leistung und zulässiger Server-Bandbreite.



- P2P-Mesh ideal für 2 bis maximal 4 Teilnehmer
- SFU optimal für Konferenzen mit 5 bis 100 aktiven Nutzern
- MCU für Legacy-Geräte oder feste Kombi-Videostreams

IoT-WEITVERKEHRSNETZE: LoRaWAN und NB-IoT

1. DEFINITION & LPWAN-GRUNDLAGEN

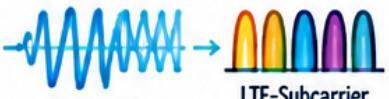
Low-Power Wide-Area Networks (LPWAN) verbinden energiearme Sensoren über Distanzen von mehreren Kilometern bei minimalem Stromverbrauch und geringer Datenrate.

- Ziel: Mehrjährige Batterielaufzeit für verteilte Sensorik
- Hohe Gebäudedurchdringung und Reichweiten bis über 10 km
- Nutzlasten typischerweise im Bereich von 10 bis 200 Bytes pro Paket

2. PHYSIKALISCHE SCHICHT & MODULATION

LoRa nutzt Chirp Spread Spectrum (CSS) zur robusten Übertragung, während NB-IoT auf zellularen Schmalband-Standards der 3GPP basiert.

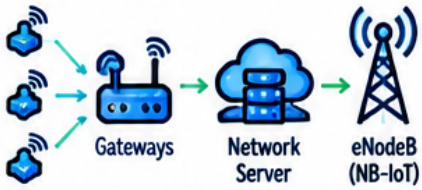
- LoRa: Frequenzgespreizte Chirps trotzen Störungen und Rauschen
- LoRa Spreading Factor (SF7 bis SF12): Abwägung zwischen Reichweite und Datenrate
- NB-IoT: OFDMA/SC-FDMA auf 180-kHz-LTE-Trägerbändern



3. GATEWAY- & NETZWERK-TOPOLOGIEN

Architekturunterschied zwischen privater Gateway-Infrastruktur und Anbindung an bestehende Mobilfunkmasten.

- LoRaWAN: Stern-von-Sternen-Topologie (Nodes -> Gateways -> Network Server)
- LoRaWAN-Gateways leiten Rohpakete transparent über IP weiter
- NB-IoT: Direkte Verbindung zu lizenzierten LTE-Basisstationen (eNodeB)



4. FREQUENZBÄNDER & LIZENZMODELLE

Die Betriebsfrequenzen bestimmen Kostenstruktur, Netzhoheit und regulatorische Auflagen.

- LoRaWAN: Unlizenzierte ISM-Bänder (868 MHz EU, 915 MHz US)
- NB-IoT: Lizenziertes Spektrum (Mobilfunk-Provider mit SIM-Karte)
- Eigenes LoRaWAN-Netz ohne laufende Provider-Gebühren aufbaubar



5. DUTY-CYCLE & BANDREITEN-REGULIERUNG

Gesetzliche Sendezeitbeschränkungen im ISM-Band verlangen striktes Timing bei LoRaWAN.

- Duty-Cycle im 868-MHz-Band meist maximal 1 % (36 s Sendezeit pro Stunde)
- Keine Dauerübertragung: Downlinks blockieren Gateway-Kapazitäten
- NB-IoT: Kein fester ISM-Duty-Cycle, aber Abrechnung nach Datenvolumen

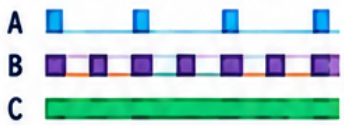
Achtung bei LoRa-Acknowledge

Bestätigte Uplinks belasten den Duty-Cycle der Gateways stark. Für Sensorwerte unbestätigte Nachrichten bevorzugen.

6. LORAWAN ENDGERÄTE-KLASSEN

Drei definierte Geräteklassen balancieren Energiebedarf und Empfangsbereitschaft aus.

- Klasse A (Standard): Empfangsfenster nur kurz nach eigenem Sendevorgang (höchste Sparsamkeit)
- Klasse B: Zusätzliche periodische Empfangsfenster synchronisiert über Beacons
- Klasse C: Kontinuierlicher Empfang bei dauerhafter Stromversorgung



7. PROTOKOLLAUSWAHL FÜR EIN IoT-PROJEKT

Strukturierter Entscheidungsbaum zur Wahl des passenden LPWAN-Standards nach Projektkriterien.

Soll das Projekt ohne Mobilfunkvertrag und mit eigener Gateway-Hoheit betrieben werden?

- Ja, autarke Infrastruktur oder isoliertes Areal → LoRaWAN mit eigenen Gateways, lokalem Network Server und unlizenziertem 868-MHz-Band einsetzen.
- Nein, flächendeckende Netzaddeckung über Mobilfunk nötig → NB-IoT mit SIM-Karten der Provider wählen; geringerer eigener Wartungsaufwand bei Mobilfunk-Zellenabdeckung.

8. INBETRIEBNAHME & KONFIGURATIONS-WORKFLOW

Schrittfolge zur Vorbereitung und Übertragung des ersten Messwerts eines IoT-Sensorknotens.

1. **Schlüssel & Parameter registrieren**
   DevEUI, JoinEUI und AppKey im Nettwerk-Server hinterlegen und auf dem Sensor kenfigurieren.
2. **Join-Request durchführen**
   OTA-Aktivierung (Over The Air Activation) starten und Session-Keys dynamisch aushandeln.
3. **Nutzlast übertragen und decodieren**
   Messwert komprimiert als Byte-Array absenden und im Payload-Formatter des Servers parsen.

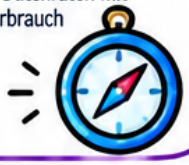
Verwendeter Standard (LoRaWAN / NB-IoT)	
Übertragungsintervall & geplante Byte-Größe	

IoT-Kurzstrecken- und Mesh-Netzwerke

1. Was ist es

Kurzstrecken- und Mesh-Technologien verbinden ressourcenbeschränkte Geräte über drahtlose Punkt-zu-Punkt- und vermaschte Topologien zur Gebäude- und Sensorautomation.

- Direkte Gerätekopplung ohne zwingende sternförmige Verkabelung
- Einsatzgebiete: Gebäudeautomation, Smart Metering, Sensornetzwerke
- Betrieb auf niedrigen Datenraten mit minimalem Energieverbrauch



2. IEEE 802.15.4 Funkgrundlagen

Physische Schicht (PHY) und Medienzugriffskontrolle (MAC) bilden das industrielle Fundament für energieeffiziente Funkübertragung über kurze Distanzen.

- Frequenzbänder: Weltweites 2,4-GHz-ISM-Band sowie Sub-GHz (868 MHz / 915 MHz)
- Niedrige maximale Datenrate von 250 kbps bei 2,4 GHz
- CSMA/CA-Kanalzugriff und Paketgrößenbeschränkung auf 127 Bytes MTU



3. Mesh-Topologien & Selbstheilung

Vermaschte Netze leiten Daten über mehrere Zwischenknoten (Multi-Hop) weiter und kompensieren Ausfälle einzelner Stationen dynamisch.

- Knotenrollen: Coordinator (Zentralsteuerung), Router (Weiterleitung), End Device (Schlafmodus)
- Selbstheilung: Automatische Neuberechnung alternativer Routen bei Verbindungsausfall
- Reichweitenerweiterung durch Multi-Hop-Routing ohne höhere Sendeleistung



4. Protokollvergleich: Zigbee & Z-Wave

Zigbee und Z-Wave sind bewährte Smart-Home-Standards mit unterschiedlichen Funkspektren und Zugangsmodellen.

- Zigbee: Basiert auf IEEE 802.15.4, offener Standard, vorwiegend 2,4 GHz, bis zu 65.000 Knoten
- Z-Wave: Proprietäres Protokoll der Z-Wave Alliance, Sub-GHz (z. B. 868 MHz in Europa), minimales Interferenzrisiko mit WLAN
- Beide Standards benötigen dedizierte Gateways zur Anbindung an IP-basierte Heimnetzwerke



5. Thread & 6LoWPAN-Kapselung

Thread verzichtet auf anwendungsspezifische Gateways und bringt IPv6 direkt auf ressourcenarme Sensorknoten.

- 6LoWPAN (RFC 4944 / 6282): Komprimierung von IPv6- und UDP-Headern auf wenige Bytes
- Paket-Fragmentierung: Einbettung von 1280-Byte-IPv6-Paketen in 127-Byte-Funkframes
- Ende-zu-Ende-Adressierung: Jeder Thread-Knoten besitzt eine eigene IPv6-Adresse

Header-Kompression

6LoWPAN reduziert 40 Byte IPv6-Header durch stateless und stateful Kompression auf bis zu 2 Byte Nutzlast-Overhead.

6. Bluetooth Low Energy (BLE) Mesh

BLE Mesh erweitert Punkt-zu-Punkt-BLE um ein vermaschtes Netzwerk auf Basis kontrollierter Paketüberflutung (Managed Flooding).

- Keine Routing-Tabellen: Nachrichten werden über Advertising-Kanäle an benachbarte Knoten gestreut
- Time-to-Live (TTL) und Message Cache verhindern Endlosschleifen und Netzüberlastung
- Zweischichtige Sicherheit: Getrennte Schlüssel für Netzwerkzugehörigkeit und Anwendungsdaten



7. Auswahl-Entscheidung & Absicherung

Entscheidungsbaum und Sicherheitsmechanismen zur Protokollauswahl im Gebäudeentwurf.

- Zigbee/Thread: AES-128-Verschlüsselung auf Sicherungs- und Vermittlungsschicht
- Thread: DTLS-Authentifizierung und nahtlose Integration in Matter-Architekturen
- BLE Mesh: Rollenbasierte Verschlüsselung für Beleuchtungs- und Beacon-Szenarien



8. Zusammenfassung & Planungsprotokoll

Kompakte Rekapitulation der Kernparameter und Arbeitsfeld für das Systemdesign.

- 802.15.4 bietet robuste Low-Power-Grundlagen mit 250 kbps Bandbreite
- Selbstheilende Topologien sichern Verfügbarkeit bei Sensorausfällen
- 6LoWPAN schlägt die Brücke zwischen IP-Welt und Nahbereichs-Mesh

Geplantes Protokoll & Frequenz (z. B. Thread 2,4 GHz, Z-Wave 868 MHz)

Anzahl Routing-Knoten vs. schlafende Endgeräte (Sleepy End Devices)

Gateway- / Border-Router-Strategie zur IPv6-Netzwerkanbindung

IoT-Applikationsschichtprotokolle: MQTT, CoAP und AMQP

1. GRUNDPRINZIPIEN & ARCHITEKTUR

Eingebettete Systeme und Sensoren benötigen schlanke Protokolle mit minimalem Overhead. Während das klassische Web auf HTTP und synchrone Verbindungen setzt, nutzen IoT-Netzwerke ereignisgesteuerte oder hochoptimierte Datentransfers.



- **Ressourcenschonung:** Geringe Bandbreitennutzung, optimierter Speicherbedarf und sparsamer Energieverbrauch bei batteriebetriebenen Knoten.
- **Kommunikationsparadigmen:** Publish/Subscribe (Entkopplung von Sender und Empfänger) und zustandsloses Request/Response.
- **Netzwerkebene:** Anwendungsschicht (OSI 7), aufbauend auf TCP oder UDP.

ARCHITEKTUR-HINWEIS
Publish/Subscribe-Broker entkoppeln Endgeräte räumlich und zeitlich, verlangen jedoch einen zentralen Vermittlungspunkt im Netzwerk.

2. MQTT (MESSAGE QUEUE TELEMETRY TRANSPORT)

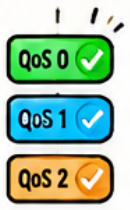
MQTT ist ein offener Standard für das Publish/Subscribe-Modell über TCP, optimiert für unzuverlässige Netzwerke und Telemetriedaten mit minimalem Protokoll-Header.



- **Verbindungsmodell:** Permanente TCP-Verbindung zu einem zentralen Broker (z. B. Mosquitto); Port 1883 (Klartext) oder Port 8883 (TLS).
- **Hierarchische Topics:** Pfadstrukturen mit Wildcards ('+' für Einzelebenen, '#' für Mehrebenen).
- **Paket-Overhead:** Extrem kompakter fester Header von nur 2 Bytes.
- **Keep-Alive:** Automatische Heartbeat-Pings zur frühzeitigen Erkennung unterbrochener Verbindungen.

3. MQTT QUALITY OF SERVICE (QOS)

Drei definierte Dienstgütestufen steuern die Verlässlichkeit der Paketzustellung gegen Netzwerk-Overhead.



- **QoS 0 (At most once):** Einmaliges Senden ohne Empfangsbestätigung, Nachrichten können verloren gehen.
- **QoS 1 (At least once):** Senden mit PUBACK-Bestätigung; Garantiert Zustellung, kann Duplikate erzeugen.
- **QoS 2 (Exactly once):** Vier-Wege-Handshake (PUBLISH, PUBREC, PURREL, PUBCOMP); garantiert die exakt einmalige Zustellung ohne Duplikate.

4. COAP (CONSTRAINED APPLICATION PROTOCOL)

CoAP ist ein für ressourcenbeschränkte Knoten (z. B. 8-Bit-Mikrocontroller) konzipiertes Webprotokoll, das RESTful-Mechanismen über UDP abbildet.



- **Transportbasis:** UDP-Datagramme auf Port 5683 bzw. 5684 (DTLS) für minimale Latenz.
- **Binärer Header:** Kompakter 4-Byte-Basisheader; deutlich geringerer Verarbeitungsaufwand.
- **Nachrichtentypen:** CON (ACK/RST) und NON bilden optionale Zuverlässigkeit auf UDP ab.
- **REST-Mapping:** GET, POST, PUT und DELETE in CoAP-Codes mit Proxy-Kompatibilität zu HTTP.

5. AMQP (ADVANCED MESSAGE QUEUING PROTOCOL)

AMQP ist ein interoperables Protokoll für unternehmensweites Messaging und IoT-Gateways mit strengen Garantien und flexiblen Routing-Mechanismen.



- **Transport & Standard:** TCP auf Port 5671 (TLS) bzw. 5672; standardisiert nach OASIS/ISO/IEC 19464.
- **Erweitertes Routing:** Exchange, Bindings, Queues (Fanout-, Direct- und Topic-Routing).
- **Zuverlässigkeit:** Transaktionssicherheit, Persistenz und Bestätigungen für IoT-Backends.
- **Ressourceneinsatz:** Höherer Speicher- und Rechenbedarf; primär auf Gateways, Industrie-Controllern und Servern.

6. PROTOKOLLVERGLEICH & METRIKEN

Direkter technischer Vergleich der Eigenschaften für die Protokollauswahl im Netzwerkentwurf:



- **MQTT:** TCP/TLS, Publish/Subscribe, Headergröße ab 2 Bytes, Sensordaten & Status.
- **CoAP:** UDP/DTLS, Request/Response (REST), Headergröße 4 Bytes, Kleinstgeräte.
- **AMQP:** TCP/TLS, Publish/Subscribe & Queues, variabler Header, Backend-Integration.

ENTSCHEIDUNGSREGEL
Wählen Sie CoAP bei strenger UDP/Batterie-Restriktion, MQTT für viele Abonnenten und AMQP für geschäftskritische Gateway-Verarbeitung.

7. SICHERHEIT & VERSCHLÜSSELUNG

Schutzmaßnahmen zur Absicherung von IoT-Verbindungen gegen Abhören, Manipulation und unberechtigten Zugriff.



- **Transportverschlüsselung:** TLS für MQTT/AMQP; DTLS ab 2 Bytes, Sensordaten & Status.
- **CoAP:** UDP/DTLS, Request/Response (REST), Header 4 Bytes, Kleinstgeräte.
- **AMQP:** TCP/TLS, Publish/Subscribe & Queues, variabler Header, Backend-Integration.

SICHERHEITSWARNUNG
Welches IoT-Protokoll passt zu Ihrer Netzwerkanforderung? auf Port 1883 ohne Passwortabfrage. Niemals ungesichert in Produktivnetzen betreiben.

8. ZUSAMMENFASSUNG & AUSWAHLMATRIX

Entscheidungshilfe zur Bestimmung des passenden Anwendungsprotokolls nach Systemanforderung Zugriff.



- **Transportverschlüsselung:** TLS für MQTT/AMQP; DTLS für CoAP über UDP.
- **Authentifizierung:** Client-Zertifikate (mTLS), OAuth/SASL oder benutzerbezogene Anmeldedaten.
- **Härtung:** Offene Broker-Ports schließen, ACLs und Ratenbegrenzung gegen DoS.

ENTSCHEIDUNGSMATRIX
Standardinstallationen von Brokern lauschen oft unverschlüsselt auf Port 1883 ohne Passwortabfrage. Niemals ungesichert in Produktivnetzen betreiben.

IOT-APPLIKATIONS-SCHICHT: PROTOKOLLE

PRÜFUNG & SYSTEMKONFIGURATION

Schritte zur Inbetriebnahme und Sicherheitsvalidierung eines MQTT/CoAP-Netzwerksegments.

1 Protokoll und Transport festlegen



Entscheiden Sie zwischen TCP/TLS (MQTT/AMQP) oder UDP/DTLS (CoAP) anhand der Latenz- und Energiespezifikation des Endgeräts.

2 Broker-/Server-Authentifizierung aktivieren



Standard-Portschutt konfigurieren, anonymen Zugriff unterbinden und mTLS-Zertifikate für Knoten ausrollen.

3 Dienstgütestufe und Timeouts kalibrieren



QoS-Stufe für MQTT (0, 1 oder 2) bzw. CON/NON-Nachrichtentypen für CoAP definieren, um Netzüberlastung zu vermeiden.

4 Netzwerk-Monitoring und Filterregeln schärfen



Firewall-Ports (1883/8883, 5683/5684, 5671/5672) reglementieren und unverschlüsselten Klartextverkehr unterbinden.

Protokoll-Audit (Checkliste)

Verwendetes Protokoll & Port (z. B. MQTT/TLS 8883)

Konfigurierte QoS-Stufe / Nachrichtentyp

Sicherheits-Audit (TLS/DTLS & Authentifizierung geprüft)

SCADA- UND LEITTECHNIK-NETZWERKE

1. MODBUS TCP FRAME-STRUKTUR



Modbus TCP kapselt traditionelle serielle Modbus-RTU-Nachrichten ohne Prüfsumme (CRC) direkt in TCP-Paketen über den Standardport 502. Der Rhamen wird um einen 7 Byte langen MBAP-Header (Modbus Application Protocol Header) ergänzt.

- Transaktions-ID (2 Bytes): Eindeutige Zuordnung von Anfrage und Antwort
- Protokoll-ID (2 Bytes): 0 für Standard-Modbus-Protokoll
- Längenfeld (2 Bytes): Anzahl der verbleibenden Bytes inklusive Unit-ID und PDU
- Unit-ID (1 Byte): Adressierung serieller Slaves hinter einem Gateway
- Funktionscode & Daten: Enthalten Steuerbefehle (z. B. Read Coils 0x01, Write Single Register 0x06)

2. DNP3 ÜBER TCP UND UDP



DNP3 (Distributed Network Protocol) ist im nordamerikanischen Energiesektor und Wasserbau Standard. Es arbeitet standardmäßig auf Port 20000 und unterstützt fragmentierte Datenübertragungen sowie Zeitstempelung auf Feldebene.

- Verbindungsorientiert über TCP oder verbindungslos über UDP für schlanke Funkanbindungen
- Schichtenarchitektur nach EPA (Enhanced Performance Architecture) mit Pseudo-Transportschicht
- Priorisierte Ereignisklassen (Class 1, 2, 3) für kritische Statusmeldungen
- Integrierte Sequenznummern zur Erkennung doppelter oder verlorener Telemetriedaten

3. IEC 60870-5-104 PROTOKOLLSTAPEL



IEC 60870-5-104 („104") adaptiert die europäische Fernwirktechnik IEC 60870-5-101 für TCP/IP-Netzwerke unter Nutzung von Standardport 2404. Es strukturiert Telegramme in klar definierte Steuerungs- und Dateneinheiten.

- APCI (Application Protocol Control Information): Steuerung des Verbindungszustands
- ASDU (Application Service Data Unit): Eigentliche Nutzdaten wie Messwerte und Schaltbefehle
- I-Frames (Information): Nummerierte Übertragung von Prozesswerten mit Sendequittung
- S-Frames (Supervisory): Quittierung empfangener I-Frames bei ausbleibendem Rückverkehr
- U-Frames (Unnumbered): Steuerfunktionen wie Start/Stop des Datenverkehrs und Test-Frames

4. SERIELLE-ZU-ETHERNET-GATEWAYS



Zur Migration alter Bestandsanlagen (Brownfield) binden Gateways serielle Feldbusse (RS-232/RS-485) an moderne Ethernet-basierte Leitsysteme an.

- Kapselung: Wandelt serielle Modbus RTU / DNP3 seriell in TCP/IP-Pakete um
- Baudraten- und Latenzanpassung: Pufferung unvollständiger serieller Zeichenströme
- Adress-Mapping: Zuweisung von IP-Adressen und Ports zu seriellen Slave-IDs
- Schwachstelle: Gateways besitzen oft ungesicherte Webschnittstellen und verarbeiten keine TLS-Zertifikate-Schutz bei Leitstellen-Ausfallen

5. SEGMENTIERUNG NACH ISA/IEC 62443



Industrienetzwerke werden nicht flach betrieben, sondern nach ISA/IEC 62443 in logische Sicherheitszonen und überwachte Kommunikationskanäle (Conduits) unterteilt.

- Zonen: Gruppierung von Assets mit identischen Sicherheitsanforderungen (z. B. SPS, HMI)
- Conduits: Kommunikationspfade zwischen Zonen mit strikter Paket- und Flusskontrolle
- Purdue-Modell-Zuordnung: Strikte Trennung von IT (Level 4/5) und OT (Level 0–3) über eine DMZ (Level 3.5)
- Industrielle Deep Packet Inspection (DPI) Firewalls sperren unberechtigte Funktionscodes

6. TELEMETRIE: POLLING VS. UNSOLICITED



Die Leittechnik nutzt zwei primäre Übertragungsmuster, um Sensordaten abzufragen und Netzwerklast zu steuern.

- Cyclic Polling: Leitstation fragt Slaves zyklisch ab; deterministische Latenz, hohe Bandbreitenaulastung
- Unsolicited Responses: Feldgerät sendet spontan Daten bei Statusänderung oder Grenzwertüberschreitung
- DNP3 & 104 unterstützen spontane Telegramme, Modbus TCP arbeitet überwiegend im Master-Polling-Modus
- Netzwerkeinfluss: Spontane Ereignisse erfordern Buffer-Overflow-Schutz bei Leitstellen-Ausfällen

7. PROTOKOLLSICHERHEITSLÜCKEN



Klassische SCADA-Protokolle wurden für isolierte physikalische Leitungen konzipiert und verfügen standardmäßig über keinerlei native Sicherheitsmechanismen.

- Klartextübertragung: Keine Verschlüsselung, alle Messdaten und Schaltbefehle sind mit Sniffern lesbar
- Fehlende Authentifizierung: Jede Komponente im Netz darf Steuerbefehle wie Motorenstopp absetzen
- Keine Integritätsprüfung: Man-in-the-Middle-Angreifer können Sensorwerte manipulieren (Replay/Injection)
- Anfällig für DoS: Verbindungsabbrüche führen zu NOT-HALT oder Blindflug des Leitpersonals

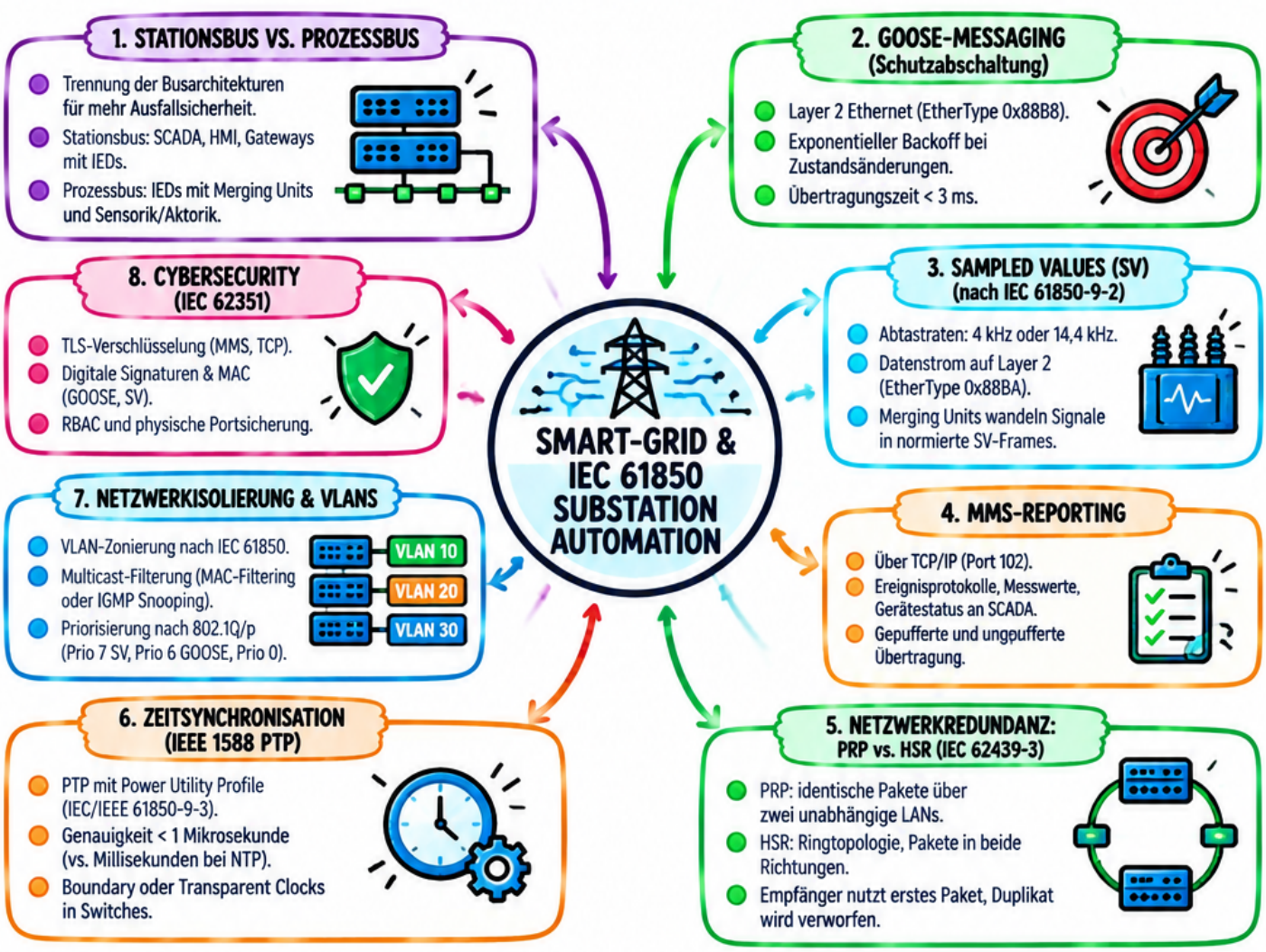
Achtung bei Legacy-Protokollen
Wegen fehlender Authentifizierung in klassischem Modbus TCP und DNP3 darf kein OT-Netzwerk direkt mit Büro- oder Firmennetzen ohne zwischengeschaltete OT-DMZ verbunden werden.

8. SECURE SCADA ERWEITERUNGEN



Moderne Standards rüsten kryptografische Absicherungen nach, um Integrität, Authentizität und Vertraulichkeit in kritischen Infrastrukturen zu garantieren.

- Modbus TCP Security (Port 802): Verwendet TLS 1.2/1.3 mit X.509-Zertifikaten zur gegenseitigen Authentifizierung
- DNP3 SAv5 (Secure Authentication v5): Kryptografische Challange-Response-Verfahren und HMAC
- IEC 62351: Umfassende Sicherheitsnorm für Energieprotokolle inklusive IEC 60870-5-104 Absicherung
- IPsec-Tunnel & MACsec: Netzwerkseitige Absicherung auf Layer 2 und Layer 3 bei Legacy-Geräten



Smart-Grid-Netzwerke & IEC 61850 Substation Automation

1. IEC 61850 Stationsarchitektur im Überblick

Die Normenreihe IEC 61850 definiert die digitale Kommunikation in modernen Umspannwerken und Energieverteilnetzen. Die physikalische Trennung in logische Busebenen ermöglicht deterministische Reaktionszeiten für den Netzschutz.

- Ersatz herkömmlicher Kupfer-Punkt-zu-Punkt-Verdrahtung durch echtzeitfähiges Industrial Ethernet
- Aufteilung der Netzwerkinfrastruktur in Stationsbus (Leitebene) und Prozessbus (Primärtechnik)
- Schnittstelle zwischen IEDs, Merging Units und Leitwartensoftware

Echtzeitanforderung im Netzschutz
Schutzabschaltungen müssen Latenzen unter 4 Millisekunden einhalten, weshalb zeitkritische Protokolle TCP/IP umgehen und direkt auf Ethernet-Ebene operieren.

1. Stationsbus vs. Prozessbus

Generischer Objekt Orientierte Busarchitekturen gewährleistet Ausfallsicherheit und schützt geschäftskritische Messdaten vor Überlastung durch administrative IT-Kommunikation.

- Stationsbus verbindet Stationsleitebene (SCADA, HMI, Gateways) mit Feldleit- und Schutzgeräten (IEDs)
- Prozessbus verbindet IEDs mit den Merging Units (MU) und Sensorik/Aktorik an Wandlern und Schaltern
- Vermeidung von Datenkollisionen durch physikalisch oder per VLAN isolierte Netzwerksegmente

2. GOOSE-Messaging (Schutzabschaltung)

Object Oriented Substation Events (GOOSE) übertragen kritische Steuersignale für Verriegelungen und Schutzauslösungen mit minimaler Verzögerung.

- Direkte Kapselung in Layer 2 Ethernet-Frames (EtherType 0x88B8) zur Umgehung von IP/TCP-Latenzen
- Zyklische Wiederholung mit exponentiellem Backoff bei Zustandsänderungen für maximale Zuverlässigkeit
- Erreicht Übertragungszeiten von unter 3 ms zur selektiven Schnellabschaltung bei Kurzschlüssen.

3. Sampled Values (SV nach IEC 61850-9-2)

Sampled Values digitalisieren analoge Strom- und Spannungsmesswerte direkt am Wandler im Prozessbus.

- Abtastraten typisch 4 kHz (80 Samples/Periode bei 50 Hz) oder 14,4 kHz (288 Samples/Periode für Power Quality)
- Konstanter, ununterbrochener Datenstrom direkt auf Layer 2 (EtherType 0x88BA)
- Merging Units wandeln analoge Strom-/Spannungssignale in normierte SV-Frames.

4. MMS-Client-Server-Reporting

Manufacturing Message Specification (MMS nach ISO 9506) dient der Parametrierung, Protokollierung und Steuerung auf der Stationsleitebene.

- Arbeitet über den vollen TCP/IP-Stack (TCP-Port 102) mit gesicherter Punkt-zu-Punkt-Verbindung
- Übertragung von Ereignisprotokollen, Messwert-Tabellen und Gerätestatus an SCADA-Systeme
- Unterstützt gepufferte (Buffered Report Control Blocks) und ungepufferte Übertragung bei Leitungsverlust

5. Netzwerkredundanz: PRP vs. HSR (IEC 62439-3)

Um bei Leitungsunterbrechungen Null-Umschaltzeit (Zero-Recovery-Time) zu garantieren, setzen moderne Umspannwerke auf redundante Übertragung.

- PRP (Parallel Redundancy Protocol): Knoten senden identische Pakete parallel über zwei unabhängige LANs (LAN A / LAN B)
- HSR (High-availability Seamless Redundancy): Ringtopologie, in der Pakete dupliziert in beide Ringrichtungen laufen
- Empfänger verarbeitet jeweils das erste eintreffende Paket und verwirft das Duplikat anhand des Redundanz-Trailers.

6. Zeitsynchronisation: IEEE 1588 PTP

Die phasengenaue Verrechnung von Sampled Values und korrekte Ereignisabfolge erfordern Sub-Mikrosekunden-Präzision im gesamten Schaltanlagennetz.

- Precision Time Protocol (PTP) mit Power Utility Profile (IEC/IEEE 61850-9-3)
- Erreicht Genauigkeiten unter 1 Mikrosekunde (vs. Millisekundenbereich bei herkömmlichem NTP)
- Einsatz von Boundary Clocks oder Transparent Clocks in Switches zur Kompensation von Frame-Jitter.

8. Cybersecurity nach IEC 62351

IEC 62351 definiert die Sicherheitsstandards für die Kommunikationsprotokolle der IEC 61850 zur Abwehr von Manipulation und Spionage.

- IEC 62351-3: TLS-Verschlüsselung und Authentifizierung für TCP-basierte MMS-Sitzungen
- IEC 62351-6: Digitale Signaturen und MAC für GOOSE und Sampled Values
- Role-Based Access Control (RBAC) nach IEC 62351-8 und strenge physikalische Portsicherung an den Schutzgeräten.

Performanz-Zielkonflikt bei L2-Verschlüsselung
Da GOOSE Latenzen < 3 ms fordert, wird statt ressourcenintensiver Vollverschlüsselung primär auf HMAC-Signaturen und dedizierte VLAN-Isolierung gesetzt.

OPTISCHE CORE-NETZWERKE: OTN (ITU-T G.709)

1. OTN-SCHICHTENARCHITEKTUR (OTH, ODUk, OTUk, OCh)



Die OTN-Hierarchie (Optical Transport Hierarchy) trennt Client-Anpassung, logisches Management und die optische Wellenlänge in klar definierte Sub-Schichten.

- OPUk: Ratenanpassung und Kapselung des nativen Client-Signals
- ODUk: Überwachung, TCM und Switching
- OTUk: Rahmensynchronisation, Overhead und FEC
- OCh: Optischer Kanal auf dedizierter Wellenlänge

2. VORWÄRTSFEHLERKORREKTUR (FEC)



FEC ermöglicht die mathematische Korrektur von Bitfehlern auf der Empfängerseite ohne Neuübertragung, was die optische Reichweite signifikant vergrößert.

- Standard-FEC (GFEC nach G.709): RS(255,239) mit ca. 6 dB NCG
- Enhanced FEC (E-FEC) / Soft-Decision: über 11 dB Coding Gain
- Betrieblicher Nutzen: Kompensiert OSNR-Degradation und senkt die BER

3. MULTIPLEXHIERARCHIEN: 10G BIS 800G



OTN ermöglicht zeitmultiplexierte Verschachtelung niedrigerer Datenströme in übergeordnete Transportbehälter für maximale Faserauslastung.

- Basisstufen: OTU1 (2,5G), OTU2 (10G), OTU3 (40G), OTU4 (100G)
- ODUflex: 1,25G-Schritte (Tributary Slots)
- B100G & Terabit-Klassen: OTUCn und 400G/800G-Schnittstellen

4. KAPSELUNG VON CLIENT-SIGNALEN



OTN verarbeitet unterschiedlichste Übertragungsprotokolle vollständig protokolltransparent ohne Paketverlust oder Timing-Verfälschung.

- Ethernet: 1GE, 10GE, 40GE, 100GE, 400GE
- Legacy & Storage: SONET/SDH (STM-N/OC-N) und Fibre Channel (FC-8G bis FC-32G)
- Mapping: BMP, Byte-synchron und GFP-T/F

5. OPTISCHES SWITCHING & ROADM-ARCHITEKTUR



ROADM erlauben das dynamische Schalten von Wellenlängen im photonischen Pfad ohne elektro-optische Konversion.

- Funktionsprinzip: Drop, Add oder Express
- CDC-Eigenschaften: Colorless, Directionless, Contentionless
- Latenzvorteil: Reines optisches Bypass-Routing reduziert Signalverzögerungen und Kosten

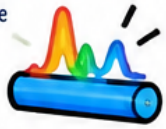
6. WAVELENGTH SELECTIVE SWITCHES (WSS)



WSS sind die zentralen mikro-optischen Komponenten im Herzen moderner ROADM-Knoten.

- Technologie: LCoS oder MEMS-Spiegel-Arrays
- Flex-Grid-Unterstützung: 12,5-GHz-Granularität nach ITU-T G.694.1
- Leistungsanpassung: Dämpfungsregelung pro Wellenlänge

7. STRECKENDÄMPFUNGS- UND DISPERSIONSMANAGEMENT



Lange Glasfasergeografisch erfordern präzise physikalische Kompensation von Signal-verzerrungen und Dämpfungsverlusten.

- Optische Verstärkung: EDFA und Raman
- Chromatische Dispersion (CD): digital im DSP
- Polarisationsmodendispersion (PMD): über adaptive Equalizer

8. DCI & CORE-TRANSPORT



DCI verbindet geografisch verteillte Hyperscale-Rechenzentren über optische Hochleistungs-Backbones mit extremen Bandbreitenanforderungen.

- Formfaktoren & Standards: 400ZR / OpenZR+ und OpenROADM
- Modulationsformate: DP-QPSK, DP-16QAM
- Sicherheit im Backbone: Layer-1 OTN-Verschlüsselung

ZUSAMMENFASSUNG CORE-TRANSPORT

OTN fungiert als universelles Bindeglied zwischen DWDM-Wellenlänge und digitalen IP/Ethernet-Diensten für maximale Effizienz und Stabilität.

HPC INTERCONNECTS

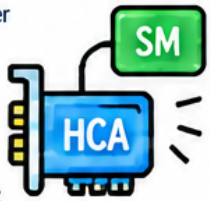
1. RDMA-GRUNDPRINZIPIEN



Remote Direct Memory Access (RDMA) ermöglicht den direkten Speicherzugriff von Server zu Server ohne Beteiligung des Host-Betriebssystems.

- **Kernel-Bypass:** Direkter Datentransfer zwischen User-Space-Anwendung und Netzwerkkarte reduziert CPU-Overhead drastisch.
- **Zero-Copy:** Daten werden ohne Zwischenspeicherung in Betriebssystem-Puffern direkt in den Ziel-Arbeitsspeicher geschrieben.
- **Extrem geringe Latenz:** Übertragungszeiten im Sub-Mikrosekundenbereich für latenzkritische Berechnungen.

2. INFINIBAND ARCHITEKTUR & KOMPONENTEN



InfiniBand ist ein eigenständiger, kabelgebundener Switching-Fabric-Standard mit nativer verlustfreier Hardware-Flusskontrolle.

- **Host Channel Adapter (HCA):** Spezialisierte Netzwerkschnittstelle mit integrierter RDMA-Beschleunigungslogik.
- **Subnet Manager (SM):** Zentrale Kontrollinstanz für Pfadfindung, Zuweisung lokaler Bezeichner (LIDS) und Fabric-Topologie.
- **Kreditbasierte Flusskontrolle:** Verhindert Pufferüberläufe auf Link-Ebene durch explizite Sendefreigaben vor Paketübertragung.

3. HPC-TOPOLOGIEN: FAT-TREE & DRAGONFLY

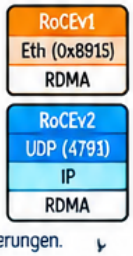


Große KI- und Rechencluster setzen auf optimierte Switching-Architekturen zur Minimierung von Hop-Counts und Bisektionsbandbreiten.

- **Fat-Tree:** Mehrstufige hierarchische Topologie mit blockierungsfreier (non-blocking) Gesamtbandbreite zwischen Leaf- und Spine-Ebenen.
- **Dragonfly:** Gruppierte Mesh-Architektur zur Minimierung langer optischer Verbindungen bei maximal 3 Switchen Durchmesser.
- **Adaptives Routing:** Dynamisches Ausweichen auf alternative Pfade bei lokaler Verbindungsüberlastung.

4. ROCEV1 VS. ROCEV2

RDMA over Converged Ethernet portiert InfiniBand-Verkehr auf Ethernet-Frames, unterscheidet sich jedoch stark je Versionsstand.



- **RoCEv1:** Kapselung direkt in Layer-2-Ethernet (Ethertrpe 0x8915); strikt beschränkt auf eine einzelne Broadcast-Domäne.
- **RoCEv2:** Gekapselt in UDP/IP (Zielport 4791); ermöglicht Layer-3-Routing über Subnetzgrenzen hinweg im Rechenzentrum.
- **Infrastrukturvoraussetzung:** Verlangt verlustfreie Ethernet-Switches (Lossless Fabric) via RoCE-Erweiterungen.

5. iWARP ÜBER TCP/IP

iWARP implementiert RDMA direkt über Standard-TCP/IP und nutzt dessen integrierte Fehler- und Überlastkontrolle.



- **Protokoll-Stack:** Basiert auf DDP (Direct Data Placement) und MPA (Marker PDU Aligned Framing) aufgesetzt auf TCP.
- **Loss-Toleranz:** Funktioniert auf herkömmlichen Standard-Ethernet-Switches, da TCP Paketverluste eigenständig ausgleicht.
- **Einschränkungen:** Höhere Protokoll-Komplexität und leicht erhöhte Latenz gegenüber purem RoCEv2 oder InfiniBand.

6. VERLUSTFREIES ETHERNET: PFC & ECN



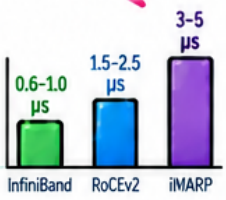
Um Ethernet für RoCE verlustfrei zu betreiben, arbeiten zwei zentrale Kontrollmechanismen Hand in Hand.

- **Priority Flow Control (PFC, IEEE 802.1Qbb):** Pausiert gezielt einzelne CoS-Verkehrsklassen bei Pufferstau ohne Beeinflussung anderer Flows.
- **PFC-Deadlock-Gefahr:** Zyklische Pufferblockaden erfordern strikte Watchdog-Mechanismen und sauberes VLAN-Design.
- **Explicit Congestion Notification (ECN/DCQCN):** Markiert IP-Header bei beginnender Switch-Überlastung, damit Sender die Rate drosseln.

Verlustfreies Fabric
PFC verhindert Paketverluste im Puffer, während ECN dauerhaften Durchsatzstau abbaut, bevor PFC aktiv werden muss.

7. LATENZ- & DURCHSATZMETRIKEN FÜR KI

Moderne Distributed-AI-Workloads wie Large Language Model Training stellen spezifische Anforderungen an die Netzwerkleistung.



- **AllReduce-Kommunikation:** Kollektive Operationen für Modellgewicht-Synchronisation erfordern deterministische Leitungszeiten.
- **Latenzvergleich:** InfiniBand (~0.6-1.0 µs) bietet minimale Latenz; RoCEv2 liegt bei ~1.5-2.5 µs; iWARP bei ~3-5 µs.
- **Throughput-Skalierung:** Moderne H100/B200-Cluster nutzen 400G bis 800G pro Port zur Vermeidung von GPU-Compute-Starvation.

8. PROTOKOLLAUSWAHL IM CLUSTER-DESIGN



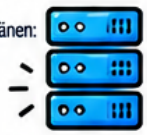
Entscheidungsbaum zur Auswahl der passenden Interconnect-Technologie basierend auf Fabric-Anforderungen und Hardwarebestand.

- **Pure HPC & homogene Großcluster:** InfiniBand ist der Referenzstandard für maximale Performance.
- **Ethernet-Konvergenz:** RoCEv2 untzt bestehende Datacenter-Switches bei adäquater PFC/ECN-Konfiguration.
- **Unzuverlässige/Heterogene Netze:** iWARP vermeidet Deadlock-Risiken auf Kosten minimaler Latenzvorteile.

NETZWERK-VIRTUALISIERUNG: NFV & VNF/CNF-MANAGEMENT

1. ETSI-NFV-ARCHITEKTUR

Das ETSI-Referenzmodell gliedert die Virtualisierung in drei Hauptdomänen: NFVI, VNFs und das Management-Framework MANO.



- NFVI (NFV Infrastructure): Physische Hardware (Compute, Storage, Network) plus Virtualisierungsschicht
- VNF (Virtual Network Function): Die virtualisierte Software-Netzwerkfunktion
- MANO (Management & Orchestration): Übergeordnete Steuerungs- und Lebenszyklus-Ebene
- Standardisierte Schnittstellen (Or-Vnfm, Vi-Vnfm, Vnf-Vnfm) sichern Interoperabilität

2. MANO: NFVO, VNFM UND VIM

Das MANO-Framework steuert Bereitstellung, Ressourcenallokation und Instanziierung über klar getrennte Funktionsebenen.



- NFVO (NFV Orchestrator): Erstellt End-to-End-Netzwerkdienste und koordiniert NFVI-Ressourcen
- VNFM (VNF Manager): Verwaltet den Lebenszyklus (Start, Stop, Scale, Update) einzelner VNFs
- VIM (Virtualized Infrastructure Manager): Kontrolliert physische und virtuelle Ressourcen (z. B. OpenStack)
- Zusammenspiel garantiert zustandsabhängige Skalierung bei wechselnder Last

3. VNF vs. CNF

Netzwerkfunktionen können als klassische virtuelle Maschinen (VNF) oder containerisiert (CNF) betrieben werden.



- VNF: KVM- oder VMware-basierte VMs mit eigenem Gast-Betriebssystem und fest zugewiesenem RAM
- CNF (Cloud-Native Network Function): Microservices in Containern (Docker/Kubernetes)
- CNF-Vorteile: Startzeiten im Millisekundenbereich, schlanke Images, feinere Skalierbarkeit
- VNF-Vorteile: Strikte Kernel-Isolation und ausgereifter Support für Legacy-Netzwerk-Stacks

4. BESCHLEUNIGUNGSTECHNOLOGIEN

Virtualisierte Software benötigt hardwarenahe Beschleunigung, um Carrier-Grade-Durchsatz und minimale Latenz zu erreichen.



- SR-IOV (Single Root I/O Virtualization): PCIe-Aufteilung in Virtual Functions für direkten Hardwarezugriff
- DPDK (Data Plane Development Kit): Kernel-Bypass und Polling-Mode-Treiber im User-Space
- vHost-user: Effiziente Inter-Process-Kommunikation für paketorientierte VM-Anbindungen
- Reduziert CPU-Interrupts und Overhead des Standard-Linux-Netzwerkstacks signifikant

5. SERVICE FUNCTION CHAINING (SFC)

SFC verknüpft einzelne Netzwerkfunktionen zu einer definierten Bearbeitungskette für den Datenverkehr.



- Verkettung: Traffic durchläuft sequentiell Router, Firewall, DPI und NAT
- NSH (Network Service Header): Kapselt Service-Pfad-Metadaten direkt im Paket
- Klassifikator (Classifier) analysiert Ingress-Pakete und weist den Service-Pfad zu
- Dynamische Pfadänderungen möglich, ohne physische Verkabelungen umzukonfigurieren

6. SKALIERUNGSSTRATEGIEN

NFV ermöglicht elastische Anpassung an Lastspitzen über automatisierte Skalierungsmechanismen.



- Scale-Out (horizontal): Hinzufügen weiterer VNF/CNF-Instanzen hinter einem Lastverteiler
- Scale-Up (vertikal): Zuweisung zusätzlicher vCPUs oder RAM an bestehende Instanzen
- Metrikbasierte Trigger: Automatisches Auslösen bei Schwellenwerten für CPU, Bandbreite oder Session-Counts
- MANO-gesteuerte Drainage stellt unterbrechungsfreie Verbindungen beim Scale-In sicher

7. HOCHVERFÜGBARKEIT (HA)

Virtualisierte Firewalls und Router erfordern Ausfallsicherheit auf Software- und Knotenebene.



- Aktiv/Standby- und Aktiv/Aktiv-Clusterpaare mit synchronisiertem Verbindungsstatus
- VRRP / dynamisches Routing sorgt für unterbrechungsfreie Pfadumschaltung
- Anti-Affinity-Regeln erzwingen (RBAC) für redundante VNFs auf getrennten physischen Hosts
- Zustandssynchronisation schützt aktive TCP-Sitzungen vor Verbindungsabbrüchen

8. MULTI-TENANCY & ISOLATION

Sichere Mandantentrennung auf gemeinsamen physischen Virtualisierungsressourcen.



- Netzwerk-Isolation via VXLAN-VNIs, Geneve oder VLAN-Tags pro Mandant
- Compute- und Memory-Quotas verhindern Noisy-Neighbor-Effekte
- Rollenbasierte Zugriffssteuerung (RBAC) für MANO-Schnittstellen
- Einhaltung strikter Sicherheits-zonen innerhalb derselben Hardware-Infrastruktur

ENTSCHEIDUNGSMATRIX: VIRTUALISIERUNGSMODELL FÜR NETZWERKFUNKTIONEN

Wegweiser zur Wahl zwischen traditioneller VNF auf Hypervisor-Basis und containerisierter CNF.



Welche primären Anforderungen stellt die bereitzustellende Netzwerkfunktion?



Monolithisches System, strikte Kernel-Isolation oder proprietäre Firmware

→ Einsatz von VNF in KVM/VMware mit festen virtuellen Ressourcen und SR-IOV-Durchleitung.



Cloud-native Microservice-Architektur mit extrem kurzen Skalierungszyklen

→ Einsatz von CNF auf Kubernetes mit DPDK-fähigen CNI-Plugins.

INTENT-BASED NETWORKING & KI-BETRIEB

Moderne Unternehmensnetze verlagern den Schwerpunkt von manueller CLI-Konfiguration auf deklarative Geschäftsabsichten (Intent) und geschlossene Regelkreise mit Machine Learning.



- Vom zustandsorientierten Scripting zum deklarativen Intent-Modell
- AIOps kombiniert Streaming-Telemetrie mit algorithmischer Ursachenanalyse
- Closed-Loop-Architekturen validieren Konfigurationszustände kontinuierlich gegen die Soll-Vorgabe



MERKSATZ

Der Administrator definiert das 'Was' (z. B. SLA-Garantien, Isolationszonen), während der Netzwerkcontroller automatisch das 'Wie' über alle Fabric-Komponenten hinweg umsetzt.

1. INTENT FORMULATION & ÜBERSETZUNG



Der Intent beschreibt die geschäftliche Anforderung in deklarativer Form (z. B. über APIs, GUI oder NLP), entkoppelt von Hardwarespezifika.

- **Deklaration:** Anforderung wird als Soll-Zustand modelliert (z. B. 'Entwicklungsnetz darf nicht auf Produktionsdatenbank zugreifen').
- **Parsing:** Zerlegung der High-Level-Absicht in logische Sicherheits- und Routing-Richtlinien
- **Abstraktion:** Unabhängig von Switch-Modellen, Firmware-Versionen oder herstellerspezifischen Befehlssätzen

2. AUTOMATISIERTE POLICY-GENERIERUNG



Der Controller übersetzt den abstrahierten Intent in herstellerspezifische Konfigurationsanweisungen für alle beteiligten Netzwerkgeräte.

- **Synthese:** Erzeugung von ACLs, VLAN/VXLAN-Zuordnungen, VRFs und QoS-Parametern
- **Konfliktprüfung:** Mathematische Verifikation gegen bestehende Regeln vor dem Rollout
- **Zero-Touch Deployment:** Automatisierte Verteilung via NETCONF, RESTCONF oder gNMI

3. KONTINUIERLICHE VALIDIERUNG (CLOSED-LOOP)



Closed-Loop Automation prüft fortlaufend, ob das reale Netzwerkverhalten exakt dem formulierten Intent entspricht.

- **State Verification:** Abgleich des Ist-Zustands der Routingtabellen und Forwarding Information Bases (FIB) mit dem Soll-Modell
- **Drift Detection:** Sofortige Alarmierung bei manuellen Eingriffen oder unerwünschten Divergenzen
- **Formale Verifikation:** Mathematische Beweisbarkeit von Datenflüssen und Isolationsgrenzen

4. STREAMING TELEMETRIE VS. SNMP



AIOps erfordert hochfrequente, strukturierte Datenströme, die das klassische Pull-basierte Polling ablösen.

- **SNMP Polling:** Periodisches Abfragen (Pull) belastet Switch-CPUs und liefert zeitlich gemittelte Daten mit Lücken
- **Push-Telemetrie:** Netzwerkgeräte senden Zustandsänderungen und Zähler fortlaufend in Subsekunden-Intervallen
- **Modellgetrieben:** Daten werden strukturiert via gPRC/Protobuf basierend auf YANG-Modellen

5. ANOMALIEERKENNUNG MIT MACHINE LEARNING



Statistische Modelle und Machine Learning identifizieren Musterabweichungen in Datenströmen und Übertragungszeiten.

- **Dynamische Baselines:** Automatische Anpassung an tageszeitliche Lastschwankungen ohne starre Schwellenwerte
- **Clustering & Klassifikation:** Gruppierung gleichartiger Flow-Anomalien zur Früherkennung von DDoS oder Fehlkonfigurationen
- **Rauschunterdrückung:** Reduktion redundanter Fehlermeldungen (Alert Fatigue) auf relevante Sicherheits- und Performance-Ereignisse

6. PREDICTIVE MAINTENANCE VON NETZWERKPFADEN



Vorausschauende Wartung analysiert physikalische und logische Metriken, um Ausfälle vor Beeinträchtigung der Nutzer abzuwenden.

- **Hardware-Trends:** Erkennung degradierender optischer Signalpegel an SFP-Transceivern und zunehmender CRC-Fehler
- **Kapazitätsprognose:** Zeitreihenanalyse warnt vor drohenden Link-Engpässen und Pufferüberläufen
- **Proaktives Umleiten:** Frühzeitige Neuberechnung von Pfaden vor tatsächlichem Paketverlust

7. ROOT CAUSE ANALYSIS (RCA)



Korrelations-Engines isolieren die eigentliche Ursache komplexer verteilter Netzstörungen in Millisekunden.

- **Topologie-Abgleich:** Verknüpfung von Log-Meldungen entlang des gesamten Forwarding-Pfads
- **Kausalitätsgraphen:** Trennung von primären Auslösern (z. B. Flapping Link) und sekundären Folgefehlern (z. B. BGP Session Drops)
- **Geführte Diagnose:** Ausgabe präziser Handlungsanweisungen für Netzwerker und SecOps-Teams

8. CLOSED-LOOP REMEDIATION



Selbstheilende Netzwerke führen vordefinierte Korrekturmaßnahmen autonom oder nach expliziter Freigabe durch.

- **Autonome Korrektur:** Automatische Isolierung kompromittierter Endgeräte oder Umgehung defekter Trunks
- **Rollback-Sicherheit:** Automatisches Rücksetzen auf den letzten verifizierten Gut-Zustand bei fehlgeschlagenen Änderungen
- **Schnittstellenintegration:** Nahtloses Eröffnen und Aktualisieren von Incident-Tickets im ITSM-System



PRÜFPFAD: IBN-INTERVENTION & AUTOMATISIERUNGSGRAD



Entscheidungslogik zur Festlegung, wann ein Intent-basiertes System autonom konfigurieren darf und wann menschliche Validierung erforderlich ist.



PRODUKTIONSHINWEIS

In kritischen Infrastrukturen empfiehlt sich zu Beginn der Modus 'Human-in-the-Loop', bis die False-Positive-Rate statistisch stabil unter dem geforderten Schwellenwert liegt.

Welche Risikoklasse weist die erkannte Drift bzw. Netzwerkanomalie auf?

Geringe Kritikalität
(z. B. Interface CRC-Fehler auf redundanter Teilstrecke oder isoliertes Test-VLAN)

→ **Vollautonome Closed-Loop Remediation** ausführen (Link drainen, Datenverkehr über Backup-Pfad routen, Ticket protokollieren).

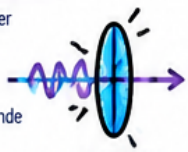
Hohe Kritikalität
(z. B. Core-BGP-Peer Flapping, Re-Routing von Produktivdatenströmen mit SLA-Relevanz)

→ **Semi-automatisierter Modus (Human-in-the-Loop):** RCA-Bericht und Korrekturvorschlag generieren, Genehmigung durch Administrator anfordern.

QUANTUM KEY DISTRIBUTION & PQC NETZWERKVERSCHLÜSSELUNG

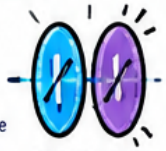
1. PHOTONISCHE GRUNDLAGEN

- Einzelphotonen-Quellen oder stark abgeschwächte kohärente Laserpulse.
- No-Cloning-Theorem: Unbekannte Quantenzustände können nicht fehlerfrei kopiert werden.
- Heisenbergsche Unschärferelation: Jeder Abhörversuch verändert den Zustand messbar.



2. PROTOKOLLE: BB84 UND E91

- BB84: Verwendung zweier nicht-orthogonaler Basen (z. B. linear und diagonal). Basenabgleich über klassischen Kanal.
- E91: Verschränkte Photonenpaare und Überprüfung der Bellschen Ungleichung.
- Sifting & Error Correction: Verwerfen nicht-übereinstimmender Basen und Berechnung der QBER.



3. QUANTUM RNG (QRNG)

- Hardwarebasierte Nutzung fundamentaler quantenphysikalischer Prozesse (Photonen-Strahlteiler, Phasenrauschen).
- Echte, beweisbare Unvorhersehbarkeit im Gegensatz zu deterministischen PRNG.
- Erzeugung robuster Seed-Werte für TLS-Sitzungen und Schlüsselvereinbarungen.



4. DISTANZ & TRUSTED NODES

- Klassische optische Verstärker (EDFA) zerstören den Quantenzustand.
- Trusted Nodes: Zwischenstationen entschlüsseln Schlüssel im geschützten Speicher und verschlüsseln sie neu.
- Zukunftstechnologie Quantenrepeater: Noch in Forschung, erfordert Quantenspeicher und Verschränkungsaustausch.



5. HYBRIDE ARCHITEKTUREN

- Zwei-Schichten-Modell: Mathematische Härte von PQC kombiniert wit physikalischer Sicherheit von QKD.
- Kombination der Sitzungsschlüssel über HKDF: $K_{final} = HKDF(K_{pqc} || K_{qkd})$.
- Kompensation von Implementierungsschwachstellen: Sollte ein Algorithmus brechen, schützt die zweite Schicht weiterhin.



6. KYBER & DILITHIUM INTEGRATION (IPsec / TLS)

- **ML-KEM (Kyber):** Gitterbasiertes Key Encapsulation Mechanism für TLS 1.3 Handshake und IPsec IKEv2.
- **ML-DSA (Dilithium):** Quantenresistente digitale Signaturen zur X.509-Zertifikatsauthentifizierung.
- Herausforderung: Größere Schlüssel- und Signaturpakete erfordern Anpassung vnd Fragmentierung und MTU-Werten.



7. ETSI-QKD-SCHNITTSTELLENSTANDARDS

- ETSI GS QKD 014: Protokoll zur Anforderung und Auslieferung symmetrischer Schlüssel an Endanwendungen via REST/JSON-API.
- ETSI GS QKD 004: Anwendungsschnittstelle zwischen Schlüsselmanagement-Schicht und QKD-Modulen.
- Herstellerunabhängige Integration in VPN-Gateways, SD-WAN-Controller und Router.



8. ROUTING & KEY MANAGEMENT

- **Key Management Layer (KMS):** Verwaltet Schlüsselpools und synchronisiert Schlüssellager entlang des Routing-Pfads.
- **QKD-Routing:** Ermittlung des optimalen Pfads unter Berücksichtigung von Knoten-Sicherheitsniveau und Schlüsselrate.
- **Multiplexing:** Parallele Übertragung von Quanten- und klassischem Servicedatenkanal über separate Fasern oder DWDM-Wellenlängen.



ZENTRALES KONZEPT: QKD & POST-QUANTEN-NETZWERKVERSCHLÜSSELUNG

Die Quanteninformatik stellt bestehende asymmetrische Public-Key-Verfahren (RSA, ECC) vor fundamentale Herausforderungen durch den Shor-Algorithmus. Dieses Lernblatt visualisiert die zwei komplementären Sicherheitsansätze moderner Netzwerke: Physikbasierter Schlüsselaustausch via QKD und mathematisch quantensichere Kryptographie (PQC).

- Shor-Algorithmus bricht klasssiche asymmetrische Kryptographie.
- QKD liefert informationstheoretische Sicherheit durch Quantenmechanik.
- PQC schützt bestehende Datennetze über gitterbasierte Verfahren.
- Kombination beider Ansätze garantiert zukunftssichere Netzwerkinfrastrukturen.

KLASSIFIKATION

QKD transportiert keine Nutzlastdaten, sondern erzeugt und verteilt ausschließlich symmetrische Sitzungsschlüssel über physikalische Quantenkanäle.

PRAKTISCHER WORKFLOW: HYBRIDE VPN-MIGRATION

Schrittfolge zur Vorbereitung eines Unternehmensnetzwerks auf Quantensicherheit.

- Inventarisierung bestehender Kryptobibliotheken und Algorithmen.
- Proof-of-Concept mit hybriden TLS/IPsec-Tunneln (PQC).
- Anbindung kritischer RZ-Kopplungen an QKD-Infrastruktur.

PRODUKTIONSHINWEIS

Store-Now-Decrypt-Later: Angreifer zeichnen heute verschlüsselten Datenverkehr auf, um ihn später mit Quantenrechnern zu entschlüsseln. Kritische Netze müssen zeitnah migriert werden.

1. **Krypto-Agilität auditieren**
   Überprüfen aller Netzwerkkomponenten auf modulare Austauschbarkeit von Chiffrensuiten und Zertifikaten.
2. **PQC-Hybridmodus aktivieren**
   Bereitstellung von X22519 fombiniert mit ML-KEM in IKEv2/IPsec-Tunneln für Standortverbindungen.
3. **ETSI-API anbinden**
   Konfiguration des VPN-Gateways für den periodischen Abruf symmetrischer Schlüssel via ETSI GS QKD 014.

ENTSCHEIDUNGSLOGIK

Welche Verschlüsselungsarchitektur ist für den spezifischen Netzwerklink erforderlich?

- **Faserstrecke unter 100 km, höchste Vertraulichkeitsstufe (kritische Infrastruktur)**
  → Einsatz von QKD mit direkter Glasfaseranbindung in Kombination mit PQC-authentifiziertem IPsec-Tunnel.
- **Weitverkehrsnetz (WAN/Internet) ohne dedizierte Glasfaserhoheit**
  → Implementierung rein gitterbasierter PQC (ML-KEM / Kyber) mit vergrößerten MTU-Puffern in TLS 1.3 / IPsec.

IN-BAND NETWORK TELEMETRY (INT) UND PROGRAMMIERBARE DATENPFADE MIT P4

1. P4-SPRACHGRUNDLAGEN & PIPELINE



P4 (Programming Protocol-independent Packet Processors) definiert die Verarbeitung von Datenpaketen direkt in programmierbaren Netzwerkchips. Der Ablauf folgt einer festen Struktur: Ein Parser zerlegt eingehende Byte-Ströme in definierte Header-Felder. Die Match-Action-Pipeline vergleicht diese Felder mit Routing- sowie Filtertabellen und führt zugewiesene Aktionen aus. Abschließend fügt der Deparser modifizierte oder neue Header wieder zu einem gültigen Paket zusammen.

- **Parser:** Dekodiert protokollunabhängig Header-Strukturen
- **Match-Action:** Tabellenbasierte Regelausführung auf Chipebene
- **Deparser:** Serialisiert Header vor der Ausgabe auf den Port

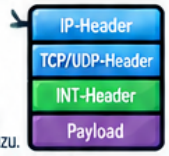
2. TRENNUNG VON DATENEBENE & P4RUNTIME



Die Netzwerkarchitektur trennt strikt zwischen der schnellen Paketweiterleitung (Datenebene) und der administrativen Logik (Kontrollebene). P4Runtime dient als standardisiertes API-Framework basierend auf gRRC und Protocol Buffers. Die Kontrollebene kann Tabelleneinträge, Zähler und Portkonfigurationen zur Laufzeit manipulieren, ohne den P4-Code auf den Switches neu kompilieren oder die Hardware neu starten zu müssen.

- **Datenebene:** Weiterleitung von Terabits/s in Hardware
- **Kontrollebene:** Zentrale SDN-Logik und Routingentscheidungen
- **P4Runtime:** Silizuim-unabhängige Schnittstelle via gRPC

3. INT-HEADER & TELEMETRIE-EINFÜGUNG



In-Band Network Telemetry (INT) bettet Diagnoseinformationen direkt in normale Produktionsdatenpakete ein. Am Quell-Switch (INT-Ingress) wird ein INT-Header hinter den Transport-Headern eingefügt. Entlang des Pfades fügt jeder teilnehmende Switch eigene Messdaten hinzu. Am letzten Switch (INT-Egress) werden diese Telemetriedaten extrahiert, der ursprüngliche Paketkopf wiederhergestellt und die Metadaten an ein Analysesystem gesendet.

- Ingress-Knoten: Fügt INT-Anweisungsheader und Switch-ID ein
- Hop-Knoten: Hängen hardwaregenerierte Metadaten-Shims an
- Egress-Knoten: Entfernt INT-Header vor Zustellung an das Ziel

4. HOP-BY-HOP LATENZMESSUNG



Klassische Werkzeuge wie Ping oder SNMP liefern nur aggregierte oder ungenaue Schätzungen. INT nutzt Hardware-Timestamps mit Nanosekunden-Genauigkeit, die direkt beim Enitritt (Ingress) und Austritt (Egress) an jedem Switch im P4-Datenpfad in den Header geschrieben werden. Dadurch lässt sich die Verweildauer (Hop Latency) exakt für jeden einzelnen Netzwerkknoten isolieren.

- **Nanosekunden-Genauigkeit:** Echte Hardware-Zeitstempel im ASIC
- **Hop Latency:** Exakte Berechnung der Verweildauer pro Switch
- **Pfadverfolgung:** Rekonstruktion des exakten Routenverlaufs

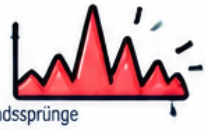
5. SWITCH-WARTESCHLANGEN (QUEUE OCCUPANCY)



Überlastungen entstehen primär in den Pufferspeichern der Switch-Ports. Programmierbare Datenpfade erlauben es, den aktuellen Füllstand der Pufferwarteschlange (Queue Depth) in Echtzeit auszulesen und im Paket zu protokollieren. Administratoren erkennen Überläufe sofort, noch bevor Puffer vollaufen und Frames verworfen werden.

- **Queue Depth:** Anzahl gepufferter Bytes zum Weiterleitungszeitpunkt
- **Buffer Monitoring:** Frühwarnung vor drohendem Pufferüberlauf
- **Fairness-Analyse:** Erkennung von Bandbreiten-Monopolisierern

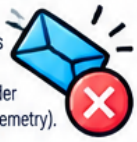
6. MICROBURST-DETEKTION



Microbursts sind extrem kurze Lastspitzen im Millisekundenbereich, die von herkömmlichem Monitoring (z. B. 10-Sekunden-SNMP-Polling) übersehen werden, aber massive Latenzausreißer verursachen. INT registriert schlagartige Queue-Füllstandssprünge auf Paketebene und triggert sofortige Alarmierungen oder automatisches Traffic Engineering.

- **Transiente Spikes:** Sichtbarkeit von Millisekunden-Staus
- **Kein Polling-Verlust:** Erfassung auf Paketebene statt Durchschnitt
- **Automatisierte Reaktion:** Auslöser für dynamisches Umrouting

7. PAKET-DROP-LOKALISIERUNG IN ECHTZEIT



Wenn ein Paket im Netzwerk verworfen wird, schlägt die End-to-End-Zustellung fehl, ohne dass der fehlerhafte Hop unmittelbar ersichtlich ist. Mithilfe programmierbarer Datenpfade erzeugt der verwerfende Switch einen Drop-Report (Drop Telemetry). Dieser enthält den Drop-Grund (z. B. Puffer voll, ACL-Verletzung, TTL abgelaufen) sowie die Paket-Header und sendet ihn direkt an den Telemetrie-Server.

- **Root-Cause-Erkennung:** Ursache (z. B. Tail Drop vs. Filterregel)
- **Punktgenaue Lokalisierung:** Exakte Identifikation des fehlerhaften Ports
- **Kein "Silent Loss":** Unbemerkter Paketverlust wird ausgeschlossen

Netzwerkpraxis
Drop-Reports erzeugen bei massiven Staus zusätzlichen Datenverkehr. Richten Sie Ratenbegrenzungen (Rate-Limiting) für generierte Telemetrie-Berichte ein.

8. INTEGRATION IN TELEMETRIE-KOLLEKTOREN



Die an den Egress-Switches extrahierten INT-Metadaten werden via UDP an hochperformante Kollektoren (z. B. Apache Kafka, InfluxDB, Prometheus) gestreamt. Analyse-Engines aggregieren die Hop-Daten, visualisieren Topologie-Hotspots in Dashboards und leiten Alarme bei SLA-Überschreitungen an das Betriebsteam weiter.

- **Pipeline:** Switch-Export -> Message Queue -> Time-Series DB
- **Visualisierung:** Hop-by-Hop-Latenzen auf Grafana-Karten
- **Regelkreis:** Übergabe an SDN-Controller für Lastverschiebung



IN-BAND NETWORK TELEMETRY (INT) & P4

NETZWERK-TROUBLESHOOTING & END-TO-END-FEHLERANALYSE

Strukturierte Diagnosepfade & End-to-End-Isolationsmethodik

1. SCHICHTENMODELLE



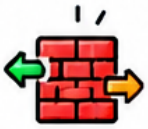
- Wähle das passende Diagnose-Modell je nach Fehlersymptom, um den Suchbereich gezielt einzugrenzen.
- Top-Down: Start bei Applikation (L7) bei isolierten Softwareproblemen.
- Bottom-Up: Start bei Verkabelung und Link-Status (L1) bei totalem Ausfall.
- Divide-and-Conquer: Start auf L3/L4 mittels ICMP-Ping oder Traceroute.

2. MTU- & MSS-FEHLKONFIGURATION (BLACK HOLE DETECTION)



- Symptom: Kleine Ping-Pakete gehen durch, SSH friert ein, Webseiten laden unvollständig.
- Ursache: Blockierte ICMP Type 3 Code 4 (Fragmentation Needed) durch restriktive Firewalls.
- Diagnose: Ping mit gesetztem Don't-Fragment-Flag (z.B. ping -M do -s 1472 <Ziel>).
- Lösung: TCP MSS Clamping auf Routern/Tunnel-Gateways aktivieren.

3. ASYMMETRISCHES ROUTING & STATE-DESYNCHRONISATION



- Stateful Firewalls blockieren Antwortpakete ohne gespeicherten Verbindungszustand (State Table Miss).
- Ursachen: Fehlkonfigurierte statische Routen, ungleiche BGP-Metriken oder Multi-Homing.
- Erkennung: Paketmitschnitte an beiden Netzübergängen vergleichen.
- Abhilfe: Policy-based Routing (PBR) oder synchrone Session-Cluster einrichten.

4. TCP-PROBLEMANALYSE (ZERO WINDOW, RETRANSMISSIONS)



- TCP Zero Window: Empfangspuffer des Endgeräts ist voll; Sender stoppt Übertragung.
- Retransmissions & Out-of-Order: Paketverlust auf Übertragungswegen oder instabile LACP-Trunks.
- Wireshark-Filter: 'tcp.analysis.flags' zur schnellen Detektion fehlerhafter Segmente.
- Prüfziel: CPU-Auslastung und Socket-Puffergrößen der Endpunkte kontrollieren.

5. DUPLEX & SPEED MISMATCH AUF L1/L2



- Problem: Ein Port steht fest auf 100/Full, die Gegenseite auf Auto-Negotiation (fällt auf Half zurück).
- Symptome: Extreme Latenz bei hoher Last, hohe Anzahl an Late Collisions und CRC-Fehlern.
- Diagnose: Schnittstellenstatistiken prüfen (z.B. 'show interfaces' oder 'ethtool').
- Standard: Durchgängige Auto-Negotiation auf beiden Seiten erzwingen.

6. ROUTING-FLAPPING & ROUTE DAMPENING



- Flapping: Ständiger Wechsel zwischen Up und Down triggert permanante SPF-/BGP-Neuberechnungen.
- Hohe CPU-Last auf Routern führt zu sporadischen Paketverlusten im gesamten Transitverkehr.
- Dampening: Temporäres Unterdrücken instabiler Routen zur Beruhigung des Netzes.
- Ursachenbehebung: Schadhafte Transceiver, Wackelkontakte oder instabile WAN-Leitungen austauschen.

7. DNS-LATENZEN & NAMENSAUFLÖSUNG



- Timeouts durch nicht erreichbare primäre Nameserver in '/etc/resolv.conf' oder DHCP-Optionen.
- Fehlendes Caching oder defekte Split-Brain-DNS-Konfigurationen in VPN-Umgebungen.
- Diagnose-Werkzeuge: 'dig +trace <Domain>', 'nslookup' oder 'systemd-resolve --status'.
- Verifikation: Direkte Abfrage gegen lokale Gateways versus öffentliche Upstream-Resolver.

8. CHANGE-TRACKING & BASELINE-VERGLEICHE



- Untersuchung: Welche Router-, Switch- oder Firewall-Änderung ging der Störung voraus?
- Vergleich aktueller Interface-Counter und Flussraten mit der historiechen Baseline.
- Konfigurationsversionierung mittels Git, Syslog-Audits und Change-Management-Tickets.
- Standardisierung: Regelmäßige automatisierte Backups und Diff-Prüfungen durchführen.

STRUKTURIERTER ARBEITSABLAUF BEI STÖRUNGEN

Folge diesen Schritten zur gezielten Ursachenfindung bei unklaren Netzwerkproblemen:

1. **Fehlerbereich eingrenzen**
   Nutze Divide-and-Conquer per Ping und Traceroute, um festzustellen, ab welchem Hop der Datenverkehr abbricht.
2. **L1/L2 Hardware & Link prüfen**
   Interface-Counter auf CRC-Fehler, Collisions und Duplex-Diskrepanzen an den betroffenen Ports analysieren.
3. **Paketfluss & MTU analysieren**
   DF-Pings zur Überprüfung der MTU-Kette durchführen und Paketmitschnitte auf Retransmissions prüfen.
4. **Veränderungen abgleichen**
   Audit-Logs der letzten Änderungen an Routing, ACLs und Firewalls mit dem Zeitpunkt des Fehlereintritts vergleichen.

ENTSCHEIDUNGSBAUM

Ist das Zielsystem per ICMP-Ping erreichbar, aber HTTP/SSH-Verbindungen hängen?

- **Ja, Ping funktioniert, Datenübertragungen frieren ein** → Prüfe auf PMTU-Blackhole (ICMP Type 3 Code 4) Filterung) oder Duplex-Mismatch; teste mit großen DF-Pings.
- **Nein, überhaupt keine IP-Erreichbarkeit** → Wechsle zu Bottom-Up: Link-Status (L1), ARP-Einträge (L2), Subnetz/Routing-Tabelle und Gateway-Status (L3) prüfen.

TROUBLESHOOTING-EINSATZPROTOKOLL

Dokumentation für den Vor-Ort- oder Remote-Einsatz bei akuten Netzwerkstörungen.

- [ ] Betroffenes System / Hostname / IP
- [ ] Erster fehlerhafter Hop (Traceroute)
- [ ] Gemessene PMTU / Paketverlustrate
- [ ] Identifizierte Ursache & getroffene Maßnahme

NETZWERKDOKUMENTATION & TOPOLOGIE-MAPPING

1. TOPOLOGIE-MAPPING (L1 BIS L3)

Strukturierte Mehrschichten-Dokumentation von physischer Verkabelung bis zur logischen Routing-Topologie.



- **L1 Physisch:** Patchfelder, Switch-Ports, Glasfaser-/Kupferstrecken und Gebäudeübergänge exakt erfassen.
- **L2 Logisch:** VLAN-Zuweisungen (802.1Q), Trunk-Ports, STP-Wurzelbrücken und Link Aggregations (LACP).
- **L3 Routing:** IP-Subnetze, Gateway-Schnittstellen, VRFs und dynamische Routing-Nachbarschaften.

Schichten-Trennung
L1-, L2- und L3-Pläne niemals in einer unübersichtlichen Gesamtgrafik vermischen, sondern als getrennte Diagrammlayer pflegen.

2. IP-ADRESSMANAGEMENT (IPAM)

Aufbau einer verlässlichen Single Source of Truth für alle IPv4- und IPv6-Netzwerkbereiche.

- **Zentrale Verwaltung:** Nutzung dedizierter IPAM-Systeme (z. B. NetBox) statt dezentraler Tabellenkalkulationen.
- **Subnetz-Hierarchie:** Dokumentation von Supernets, Transfer-Netzen (/30 bzw. /31) und Loopback-Adressen.
- **Statusverfolgung:** Klare Kennzeichnung von reservierten, aktiven und veralteten IP-Pools inklusive DHCP-Ranges.



3. KABEL- UND RACK-MANAGEMENT

Physische Nachvollziehbarkeit im Serverraum durch normierte Kennzeichnung und Höhenbelegung.

- **Höheneinheiten (HE):** Präzise Erfassung von Einbaupositionen, Netzteilen und Luftstromrichtungen (Front/Rear).
- **Port-Mapping:** 1:1-Zuordnunge vom Switchport über Rangierfeld und Datendose bis zum Endgerät.
- **Kabelbeschriftung:** Eindeutige Quell- und Ziel-Kennzeichnung an beiden Enden jedes Patchkabels nach TIA-606-Norm.



4. ASSET-INVENTARISIERUNG

Vollständige Erfassung aller aktiven Netzwerkkomponenten und ihrer Lebenszyklusdaten.

- **Hardware-Metadaten:** Modell, Seriennummer, MAC-Adressen und physischer Aufstellungsort je Gerät.
- **Software-Stände:** Installierte Firmware- und Betriebssystemversionen zur schnellen Schwachstellenidentifikation.
- **Support-Status:** Erfassung von Garantielaufzeiten, End-of-Sale (EoS) und End-of-Life (EoL) Meilensteinen.



5. KONFIGURATIONS-BACKUP & VERSIONIERUNG

Automatisierte Sicherung und revisionssichere Nachverfolgung aller Gerätekonfigurationen nach GitOps-Prinzipien.

- **Tägliche Extraktion:** Automatisierter Abzug der Running-Config via SSH/API über Tools wie Oxidized oder RANCID.
- **Versionskontrolle:** Speicherung in Git-Repositories mit automatischem Diff-Vergleich bei Modifikationen.
- **Verschlüsselte Ablage:** Sichere Verwahrung von Konfigurationsständen inklusive getrennt verwalteter Secrets.



Passwort-Hygiene
Sicherstellen, dass Klartext-Passwörter und pre-shared keys in Git-Commits automatisch maskiert oder ausgelagert werden.

6. COMPLIANCE- UND SICHERHEITSAUDITS

Regelmäßige Soll-Ist-Abgleiche gegen etablierte Härtungsstandards und Richtlinien.

- **Benchmark-Prüfung:** Automatisierte Überprüfung von Konfigurationen gegen CIS-Benchmarks oder BSI-Grundschutz.
- **Zugriffsprüfung:** Verifikation deaktivierter unsicherer Protokolle (z. B. Telnet, HTTP, SNMPv1/v2c) zugunsten von SSH/HTTPS/SNMPv3.
- **Port-Sicherheit:** Deaktivierung ungenutzter Switchports und strikte Durchsetzung von 802.1X-Zugangskontrollen.



7. DISASTER RECOVERY & NOTFALLPLÄNE

Dokumentierte Notfallkonzepte für Hardwareausfälle, Fehlkonfigurationen und Totalausfälle.

- **Cold-Standby-Provisioning:** Definierte Wiederherstellungsschritte auf Ersatzhardware (Zero-Touch / Re-Imaging).
- **Out-of-Band-Management (OOB):** Vollständig dokumentierter Notfallzugang über LTE/Konsolenserver bei Netzwerkausfall.
- **Rollback-Pfade:** Verbindlich formulierte Rückrollpläne für jede anstehende Konfigurations- oder Firmware-Änderung.



8. RUNBOOKS & SCHNITTSTELLENÜBERSICHTEN

Praxisorientierte Betriebshandbücher für Routineaufgaben und externe Verbindungspunkte.

- **Standard-Betriebsabläufe (SOP):** Schritt-für-Schritt-Anleitungen für VLAN-Anpassungen, Portfreischaltungen und Firmware-Upgrades.
- **Übergabepunkte (Demarcation):** Dokumentation aller WAN-Carrier, ISP-Übergabepunkte und Circuit-IDs mit Provider-Hotlines.
- **Dienstabhängigkeiten:** Zuordnung kritischer IT-Dienste zu den zugrundeliegenden Netzwerkpfaden und Switch-Stacks.



Praxis-Leitfaden & Audit-Arbeitsblatt

PRAXIS-LEITFADEN: TOPOLOGIE-AUDIT DURCHFÜHREN

Strukturierter Arbeitsablauf zur Erfassung und Validierung des aktuellen Netzwerkstatus.

1 Schritt 1: Bestandsaufnahme und LLDP/CDP-Discovery

Abfrage der Nachbarschaftsbeziehungen auf allen Core- und Distribution-Switches zur Rekonstruktion der L2/L3-Pfade.



2 Schritt 2: IPAM- und Routing-Validierung

Abgleich der Routing-Tabellen und statischen Zuweisungen mit der zentralen IPAM-Dokumentation (z. B. NetBox).



3 Schritt 3: Backup- und Git-Diff-Prüfung

Verifikation der nächtlichen Konfigurations-Backups auf Unstimmigkeiten zwischen Startup- und Running-Config.



4 Schritt 4: Härtungscheck und Berichterstellung

Prüfung der aktiven Dienste gegen Härtungsvorgaben (SSH-Version, SNMP-Communities) und Protokollierung von Abweichungen.



ENTSCHEIDUNGSWEGWEISER: REVISIONSABWEICHUNGEN

Handlungsschema bei Feststellung von Konfigurations- oder Topologieabweichungen im Netzwerk.

Welche Art von Abweichung wurde während des Audits identifiziert?

Undokumentierte physische Verbindung oder unbekannte MAC	Diff zwischen Running-Config und Git-Repository	Veralteter Firmware-Stand mit Sicherheitswarnung
		
Port sofort isolieren, physische Verbindung am Rack prüfen und Asset-Eigentümer ermitteln.	Änderungsprotokoll (Syslog/TACACS+) prüfen, Freigabe nachfordern oder Konfiguration per GitOps zurückrollen.	Patch-Fenster im Change Management eröffnen, Konfigurations-Backup ziehen und Wartungsupdate einplanen.

AUDIT-DOKUMENTATIONSBOGEN

Formular zur standardisierten Dokumentation des monatlichen Topologie- und Konfigurations-Audits.

Geprüfter Netzwerkbereich / Standort:

_____

Audit-Verantwortlicher / Datum:

_____

Identifizierte Abweichungen (Topologie / IPAM / Config):

_____

_____

_____

Eingeleitete Korrekturmaßnahmen und Change-Ticket-ID:

_____

_____