Referenzmodelle Protokolle Netzelemente Normen Standards

Protokoll: Festlegung auf eine bestimmte Satz von Regel; Vereinbarung des Kommunikationsverhalten zwischen kommunizierenden Instanzen.

Zwei wichtigsten Referenzmodelle der heutigen Netzwerktechnik: OSI, TCP/IP

Anwendungsprogramm (z. B. WebBrowser, E-Mail-Client, VoIP-Telefon…)

Encapsulation (Datenkapselung)

Nr.	OSI-Layer	Protokolle	Adressen	PDU	Hardware	Aufgaben
7	Application	HTTP, HTTPS, SMTP, POP3, IMAP, DHCP, DNS, LDAP, NTP, SNMP, FTP, NFS, SMB, X.500		Data	Host, Server, Application-Layer-Gateway	Zusammenarbeit mit den Anwendungsprogrammen; diese Protokolle stellen den Anwendungen Netzwerkdienste zur Verfügung; Steuerung der untergeordneten Schichten;
6	Presentation	HTML, JPEG, MPEG, G.711, G.726, ZIP, GSM, ILBC, XDR, SSH, SDP, XML		Data		Hier werden die Daten ggf. kodiert, komprimiert, konvertiert und verschlüsselt, um sie in eine Form zu bringen, mit der der Nutzer etwas anfangen kann (Darstellung).
5	Session	SQL, RPC, RTP, RTCP, SIP, SDP, RSVP		Data		Auf- und Abbau von Kommunikationsbeziehungen (Sessions); Synchronisation und Steuerung des Dialogablaufs zwischen zwei Kommunikationsprozessen; Quality of Service;
4	Transport	TCP, UDP, TLS(SSL), SCTP	Ports	UDP: datagramms TCP: segments	Firewall (Paket-Filter)	Segmentierung der Daten; Port-Adressierung; Aufbau einer logischen Verbindung zwischen den Endsystemen; Erkennung von Transportfehlern und Flusssteuerung; (UDP-verbindungslos; TCP-verbindungsorientiert);
3	Network	IPv4, IPv6, ICMP, IGMP, IPX, AppleTalk, RIP, OSPF, EIGRP, BGP, GRE,	IP-Adr.	packets	Router, L3-Switch	Paktierung; logische Adressierung (IP-Adr.); Routing (Vermittlung); meist verbindungslos; Kommunikation zwischen den Endsystemen (Intenetworking); oft verbindungslos;
2	Data-Link	Ethernet (MAC), WLAN (MAC), HDLC, PPP, FrameRelay, ARP, LLDP	MAC-Adr.	frames	Switch, Bridge, NIC	Rahmenbildung; physikalische Adressierung (MAC); Fehlererkennung; Zugriffsverfahren (z.B. CSMA/CA); Kommunikation nur im gleichen LAN-Segment;
1	Physical	Ethernet (PHY), WLAN (PHY), xDSL, DOCSIS, SDH, OTN		Bits	Repeater, Hub	Festlegung der mechanischen und elektrischen Eigenschaften der Schnittstelle. Anpassung des Bitstroms an den Übertragungskanal (z.B. Modulation, Codierung..)

Decapsulation (Datenentkapselung)

Medium (Kupferkabel, Glasfaserkabel, Funk)

Hinweis: Die Anwendungsprogramme und die Medien sind nicht Bestandteil des OSI-Modells und somit keinem Layer zuzuordnen. Im OSI-Modell kann man nur **Protokolle** finden. Manchmal wird aber das Medium als ***Layer 0*** und die Anwendung bzw. der User als ***Layer 8*** bezeichnet.

PDU = Protocol Data Unit (Daten- und Verwaltungsinformation einer Schicht - Informationsbündel)

TCP/IP-Layer (OSI-Layer-Zahl): Network Access (1,2), Internet (3), Transport (4), Application (5, 6, 7)

PDU: Protocol Data Unit - komplette Satz Nutzdaten plus Verwaltungsinformationen einer Schicht, wird PDU dieser Schicht genannt.

Encapsulation: (Senderseite) Von oben nach unten durch die einzelnen Layer zusätzliche Informationen hinzufügen.

Jede Schicht N fügt den zu übertragenden Nutzdaten der Schicht (Service Data Unit), eigene Verwaltungs-informationen (PCI Header-/Trailer) hinzu. `PDU(N) = PCI(N) + SDU(N) + Footer(N)`

Decapsulation: Von unten (Medium) nach oben (Anwendung) Daten auspacken.

Segmentierung: Zu übertragende Datenmengen auf dem Transport-Layer in kleinere Teile zerlegen.

IETF Nummer: RFC (Request for Comments)

Standards LAN-Technologien: (IEEE 802): Ethernet (802.3), WLAN (802.11)

Internet: weltweiter Verbund von Rechnernetzen:

Intranet: Netz (im Gegensatz zum Internet) unabhängig vom öff. Netz nicht öffentlich zugänglich;

Extranet: Erweiterung des Intranets: Zugriff von Extern für festgelegte Gruppe

Physikalische Topologie: Aufbau bzw. Struktur des Netzwerks - Wie sind die Geräte durch Kabel verbunden?;

Logische Topologie: Datenfluss zwischen den Komponenten - Wie kommunizieren die Komponenten miteinander?

QoS: Quality of Service - Priorisierung von bestimmten Traffic

Netzwerkkomponenten: End-Devices (alles mit NIC); Intermediate Devices (Hubs, Repeater, Switches, Router, Firewalls, Proxy-Server); Medien (passive Komponenten: Kabel, Dosen, Stecker, Patchfelder)

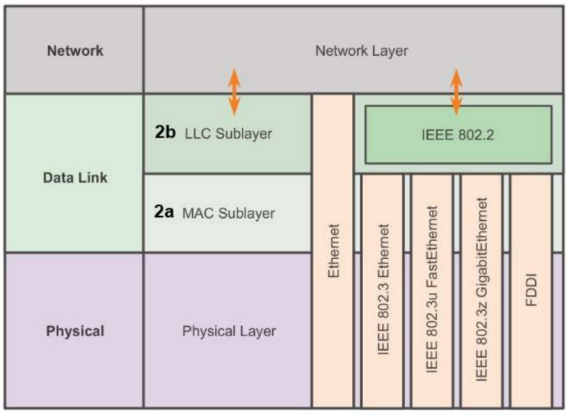
Standardisierungsgremien für die Hardware-nahen Protokolle im LAN und WAN: IEEE, IEC

Standardisierungsorganisationen: IEEE (Standardisierung von Technologien), IETF (Entwicklung von Protokollen), ICANN (Zuteilung von IP Adressen), IANA (Zuordnung von IP-Adressen zu Namen im Internet)

Client-Server
Ab kleinen Unternehmensnetzwerken
Pro: höhere Sicherheit, Zentrale Administration

Peer to Peer
Vernetzung weniger PCs und Drucker
Pro: Einfache Einrichtung, geringe Komplexität/Kosten

LAN-Technologien



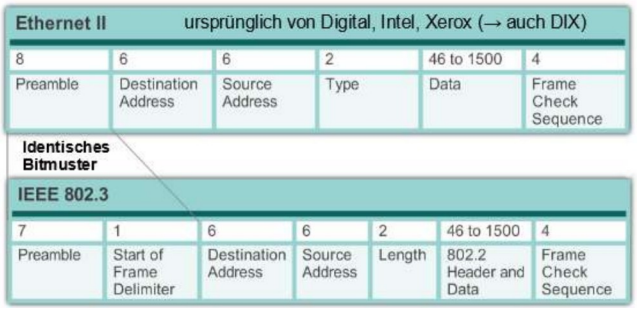
Layer der Ethernet-Technologie:

1. Physikalisches Layer: Bitübertragung
2. MAC-Sublayer: physikalische Adressierung
3. LLC (*logical link control*, IEEE 802.2)**:** Stellt Daten für die Auslieferung einer Layer-3-PDU (z. B. IP-Paket) zur Verfügung.

IEEE Standards, die für alle LAN, MAN Standards gültig sind:

- IEEE 802.1 (Authentifizierung in Rechnernetzen)
- IEEE 802.2 (definierte Schnittstelle zum Network-Layer
- (IPv4, IPv6,…)

Ethernet-Frame



- Preamble (& Delimiter): alternierenden Bitfolge `10101010…10101010`, folgend (SFD) mit `10101011`
- Frame Check Sequence: CRC

MAC-Sublayer: Layer 3 PDU (Frame) Encapsulation; Medienzugriff über CSMA/CD

Media Access Control: Grundsätzlich CSMA/CD bei Ethernet. Wegen logischer Multi-Access-Bus-Topologie eigentlich erforderlich. Bei Switch PC Verbindung (p2p) nicht erforderlich. *Zugriff auf „Shared Medium“.*

MAC-Adressen: Media-Access-Control-Address; Layer 2; Hardware-Adresse jedes einzelnen Netzadapters; eindeutiger Identifikator eines Geräts in einem Rechnernetz; Physischer Adresse, Geräteadresse.

MAC-Aufbau: 48 Bit in hexadezimal geschrieben, Bytes sind i. d .R. durch ein Doppelpunkt getrennt. Erste Hälfte: Organizationally Unique Identifier (fest durch die IEEE vorgegeben). Zweite Hälfte: Vom Hersteller einmal vergebene Nummer. *Die MAC-Adress ist rein statisch und kann nicht die Netzstruktur wiederspiegel.*

Jumbo-Frames: Protokoll-Overhead reduziert und die Effizienz verbessert –> Durchsatz erhöhen

MAC Adress Typen - Uni-, Multi- und Broad-Cast:

- Zielgerichtete Zustellung an einen Node: Über zugehörigen Ziel-MAC-Adresse *Unicast*
- Zielgerichtete Zustellung an eine bestimmte Gruppe von Nodes: Verwendung einer Multicast-MAC-Adresse beginnen immer mit `01:00:5E:xx:yy:zz` bei IPv4 → beginnen mit `33:33:ww:xx:yy:zz` bei IPv6
- „Rundmeldung“ an alle Nodes im eigenen LAN-Segment: MAC-Broadcast-Adresse `FF:FF:FF:FF:FF:FF`

Medien

Straight-Through-Patchkabel: beide Seiten nach 568A oder nach 568B aufgelegt: zwischen Hub/Switch und Routern/End-Devices

Crossover-Patchkabel: eine Seite nach 568A und die andere nach 568B aufgelegt: zwischen Hub/Switch - Hub/Switch & Router/End-Device - Router/End-Device

Grund für Crossover: Sendepaar von einem Gerät auf Empfangspaar des Gegenüber, Switches/Hubs haben interne Kreuzung

Auto-MDIX: Ab Gigabit-Ethernet (MDI = Medium Dependent Interface; X = Crossover)); auto Erkennung, ob Straight-Through- oder Cross-Over

N Base-X: N = Übertragungsgeschwindigkeit; Base = Übertragung im Basisband → keine Modulation

X = *100 Gbase-SR10 = Short = Reach über 20 Multimode-Fasern (10*10GBit/s)*

- T: Twisted-Pair - Full Duplex, volle Bandbreite
- TX: Twisted-Pair - Zwei Adernpaare pro Richtung, schlechter als T
- SR”N”: Glasfaser Multimode - Short Reach, N Faserpaare, $2 \cdot N$ Glasfasern; SR = SR4
- LR”N”: Glasfaser Singlemode - Long Reach, N Wellenlängen, $N/2$ Glasfasern; LR = LR4
- FX: 2 Glasfaser Multimode für 100 BASE-FX *2*250 Mbit/s*

Adernbelegung Twisted-Pair**:** Fast-Ethernet: 4 Adern (2 Kupfer-Paare); Gigabit-Ethernet: 8 Adern (4 Kupfer-Paare)

Glasfaser/LWL Hardware-Module *(SC & LC sind Steckertypen)*

- GBIC = Gigabit Interface Card - 2 SC-Steckern (GBit Ethernet) *SC-Glasfaser-Buchsen*
- SFP = Small Form-factor Pluggable - 2 LC-Steckern (GBit Ethernet)
- SFP+ = kleinstes Format für 10 GBit-Ethernet - 2 LC-Steckern, aktualisiertes SFP
  Base = Übertragung im Basisband, also ohne Modulation, T= Kupfer Twisted Pair
- GBIC und SFP -> Gemeinsamkeit: Bitrate 1Gbits
- Unterschied: GBIC=Big Form Factor
- SFP=Small Form Factor
- SFP und SFP+ -> Gemeinsamkeit: gleicher small Form Faktor
  - Unterschied: SFP=Bitrate 1Gbits
  - *SFP+=Bitrate 10Gbits*

Zugangstechnologien

Vier wichtigsten Zugangstechnologien mit Netz: DSL (Digital Subscriber Line - Telefonnetz), DOCSIS (Kabelnetz), 2G GSM, 3G UMTS, 4G LTE (Mobilfunknetz), FTTH (Glasfasernetz)

FTT*x* (Fiber to the) : H (Home), B (Building), C (Curb = Bordsteinkante), P (Premises), D (Desk)

FTTC: Typisch für VDSL - Outdoor DSLAM (grauer Kasten) über Glasfaser angebunden, letzte Meter über Kupfer.

Symmetrisches und Asymmetrischen DSL Up 3Mbit/s 24Mbit/s Down

SDSL: Upstream = Downstream (symmetrisch) ADSL: Upstream ≠ Downstream (asymmetrisch)

Annex:

- Annex A („ADSL over POTS“, Plain Old Telephone Service) Größerer Frequenzbereich für DSL; darunter liegende Bereich (unter 25 kHz) ist noch ausreichend für analoge Telefonie aber nicht für ISDN. Hat Splitter;
- Annex B („ADSL over ISDN“) für digitale Telefonanschlüsse mit ISDN (Telefonie - Integrated Services Digital Network). Hat Splitter; Frequenzbereich von 0 – 120 kHz für ISDN reserviert
- Annex J: Modulationsverfahren für DSL-Anschlüsse, welches ohne DSL-Splitter aus kommt. Da es nur noch ein einziges Signal gibt. DSL-Endgeräte bekommen das DSL-Signal direkt von der Telefondose. Annex J nutzt das gesamte Frequenzband vom DSL-Anschluss und stellt so höhere Datenübertragungsraten zur Verfügung. All-IP-Anschluss

xDSL Verfahren für Aufteilung von Frequenzbereich in mehrere Teil-Träger: Discrete Multi Tone (DMT)

Bit-Allokation: (Anzahl der Bits je Träger): Automatische Anpassung an Qualität der Leitung.

VDSL (Very High Bitrate DSL): DSLAM in Nähe des Kunden, wird über Glasfaser an Vermittlungsstelle angebunden.

Vectoring 17a (VDSL2): 100MBit/s Down, 40MBit/s Up; Negativen Einflüsse von starkem Nebensprechen (zwischen Ader-Paaren) in einem Kabel mit Vectoring verringern. 0 bis 17 MHz

Super Vectoring 35b (VDSL2): 250MBit/s Down, 40MBit/s Up; 0 bis 35 MHz *„1&1“*

Reichweite 35b: *Bei 35b ist die Bandbreite also doppelt so groß, wodurch sich die maximal überbrückbare Kabellänge stark reduziert.*

G.fast: Straßenverteiler (FTTdp = Fiber to the Distribution Point); Kupferleitung verkürzen (< 250 m); bis zu 1Gbit/s

Gegenstück zum DSL-Modem beim Netzbetreiber: DSLAM

HFC: Hybrid Fiber Coax - Technologie für Übertragung von analogen/digitalen Signalen großer Datenraten. Zur Verteilung der Signale im Regionalbereich werden Glasfaserstrecken verwendet.

CMTS: Kabelnetzbetreibers hat CMTS = Cable Modem Termination System bedient Kunden der ein Kabel-Modem hat, welches an eine Multimediadose angeschlossen wird.

DOCSIS 3.0: 400 Mbit/s DOWN, 300 Mbit/s UP

AON (Active Optical Network) vs PON (Passive Optical Network) (meist FTTH / FTTC): Glasfasernetze, die im Gegensatz zu PONs auch „aktive“ Komponenten wie Switches, Repeater oder Router enthalten werden AON genannt. PONs arbeiten meistens mit optischen Splittern.

PON: PASSIV optical Network -> keine aktiven Komponten zwischen OLT und ONT.
AON: Aktive Optical Network-> active Komponenten zwischen OLT und ONT
Vorteil (bei PONs) von Punkt-zu-Punkt gegenüber Punkt-zu-Mehrpunkt Topologie: kein shared Medium

- Punkt zu Punkt: Jeder Kunde hat seine eigene Glasfaser.
- Punkt-zu-Mehrpunkt: Splitter in der Leitung → Kunden müssen sich Bitrate teilen

Mobilfunk Faktoren Bitrate: Mobilfunk-Generation, Firmware-Version Endgerät & Basis-Station, Anzahl der Nutzer in der Funkzelle, Entfernung Basisstation, Gelände, Störsignale

Mobilfunk Frequenzen & Reichweite: niedrigeren Frequenzen → Reichweite größer → größere Funkzellen

Switching

- Weiterleitung von Frames (Ethernet, WLAN) anhand der Ziel-MAC-Adresse und den vorhandenen Informationen in der MAC-Adress-Tabelle des Switches.
- Wenn eine Ziel-MAC-Adresse keinen Eintrag in der MAC-Adress-Tabelle hat, wird der Frame zu allen aktiven Interfaces weitergeleitet → Flooding.
- Die MAC-Adress-Tabelle des Switches ist nach einem Neustart leer. Der Switch lernt die MAC-Adressen, wenn ein Frame über ihn weitergeleitet wird. Zuordnung der Quell-MAC-Adresse zu einem Interface→ Learning.

Die drei Ebenen eines geswitchten LAN-Netzwerks: Sogenannte „Tiers“: ➢ Core ➢ Distribution ➢ Access

- Core Layer: „High-Speed-Backbone“. Verbindet andere Layer des Campus-Netzes mit anderen Blöcken der Netz-Architektur. Isoliert fehlerhafte Bereiche
- Distribution-Layer: Intelligentes Routing und Switching inklusive Regeln „von wo nach wo“ Zugriff erlaubt ist. Grenze für OSI-Layer 2 Broadcasts und Routing zwischen Netzen.
- Access Layer: Ein/Ausgang des eigentlichen User-Datenverkehrs. Anschluss der Anwender.

Auswahlkriterien für Switches: Kosten, Port-Dichte & Geschwindigkeit, Power over Ethernet, redundante Netzteile, Zuverlässigkeit, Pufferspeicher für Frames, Skalierbarkeit

Backplane (Switch Fabric): „interne Pfade“ verbindet Ports des Switches; limitiert die Datenübertragung, z. B. wenn alle Ports Switches im Voll-Duplex Modus ausgelastet werden.

Switch-Modi:

- Store & Forward: speichert Frame →prüft CRC-Prüfsumme → leitet erst dann weiter
- Cut-Through: leitet ohne Prüfung weiter, bei (Fast Forward) direkt nach Erhalt der Destination-MAC

PoE-Modi:

- Midspan: Leistung in das Kabel über einen Power-Injector eingeschleift → Switches können unverändert bleiben
- Endspan: PoE-fähige Switches→ übernehmen Aufgabe Stromversorgung

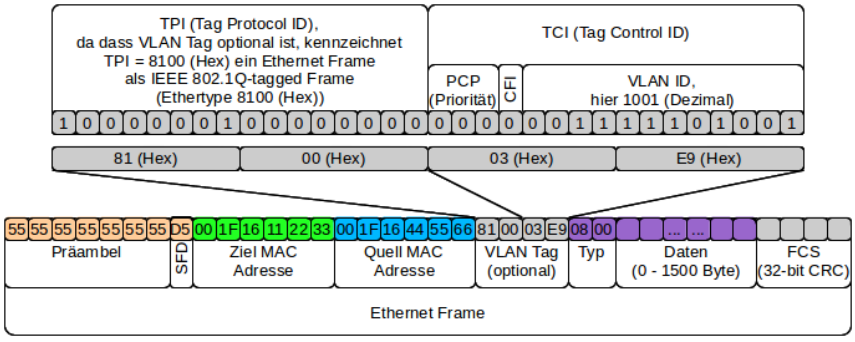
Switch-IP-Adresse: Einem Switch wird meist eine IP zugewiesen, obwohl er ein Layer 2 Gerät ist →Die IP wird für den Zugriff auf den Switch gebraucht z. B. zum konfigurieren.

VLAN (Virtual Local Area Network)

- Eigenständige Netzwerke: logisches Teilnetz innerhalb eines gesamten physischen Netzwerks. (Ausdehnung über mehrere Switches möglich). VLAN-fähige Switches leiten Frames eines VLANs nicht in ein anderes VLAN weiterleiten.
- VLAN bildet dabei eine eigene Broadcast-Domain.
- Pro VLAN wird ein eigenes IP-Netz benötigt!
- Traffic zwischen VLANs ist nur über einen Router möglich!

Portbasierte VLANs: Unterteilen eines einzelnen physischen Switch auf mehrere logische Switche. Immer ein Kabel pro VLAN notwendig für Verbindung zu anderem Switch →Lösung: Tagged VLAN

Tagging: Hinzufügen eines Tags zum Standard-Ethernet-Fram um Zugehörigkeit zu einem VLAN zu anzuzeigen. IEEE 802.1Q



Type kennzeichnet VLAN-tagged-Frame
Pri = Für Class-of-Service-Abbildungen
CFI = heute DEI (Drop Eligible Indicator)
VID = VLAN-Identifier / VLAN-Nummer

Switchport-Modi

- *Trunk-Verbindung überträgt die getaggten Frames aller VLANs.*
  ->Bei VoIP-> Da sowohl das Daten-VLAN als auch das VoIP-VLAN über die gleiche physikalische Verbindung gesendet werden müssen, muss der Switchport Mode Trunk gewählt werden.(Weil mehrere VLANs)
- *Access Port: Port für normale Endgeräte das untagged im VLAN hängt. Endgeräte kennen keine Tags. Der Tag*

wird bei diesem Modus entfernt. Feste Zuordnung von Interfaces zu einem VLAN.
-> Was passiert mit Ethernet-Frame?->Der vom Endgerät ankommende ungetaggte Ethernet-Frame bekommt am Switch-Interface einen VLAN-Tag hinzugefügt und bei allen Frames in Richtung Endgeräte wird der VLAN-Tag wieder entfernt.

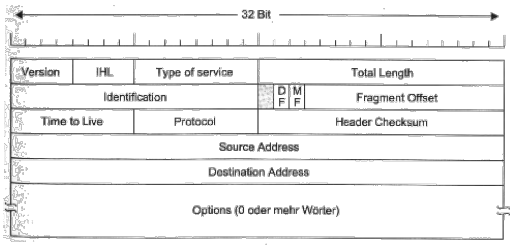
Internet-Layer

- Adressierung von Endgeräten / Hosts → über eindeutige Adressen, IP-Adressen
- Encapsulation zu versendender Daten des „Transport Layers“ → PDU = Paket; Voranstellen eines IP-Headers, u.a. mit Quell- und Ziel-IP-Adresse *mit physikalischer Addressierung mit MAC-Adressen*
- Routing des Pakets durch Layer-3-Geräte (Router) – auf Basis der Ziel-IP-Adresse im IP-Header
- Decapsulation des Pakets auf Ziel-Host und Weitergabe der enthaltenen Daten an Layer 4

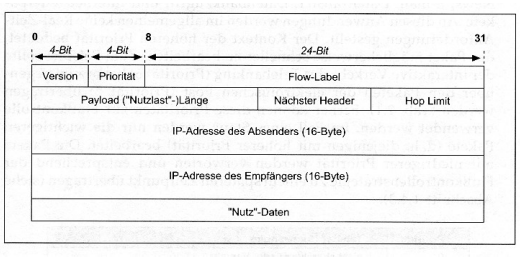
Grundeigenschaften

- Verbindungslos → Vor dem Versand eines Pakets wird keine Verbindung zum Ziel aufgebaut, das Paket geht einfach so auf die Reise → keine Garantien für die zuverlässige Übertragung.
- „Stets bemüht“ / Best Effort (unreliable) → Paket-Auslieferung wird nicht gewährleistet bzw. garantiert.
- Unabhängig vom Medium / Media Independent → Betrieb bzw. Verhalten von IP ist unabhängig vom Netztyp / Netzmedium das die Daten transportiert

Geroutete Protokolle: IPv4 und IPv6



IPv4-Header



IPv6-Header

TTL: Time To Live, wird bei jedem Router Hop um 1 reduziert.

Default Gateway: Ziel *(meist Router)* für Pakete, mit IP-Adresse aus einem anderen IP-Netz.

ARP (Address Resolution Protocol): Lookup MAC für IP → MAC-Broadcast ARP-Request ins Netz → Unicas ARP-Reply vom “richtigen” Ziel. *Quell-PC ARP-Tabelle, Es wird die zugehörige IP-Adresse eingetragen*

ICMP: Internet Control Message Protocol *Hilfprotokoll zu IPv4 &IPv6*

Routing

Routing bezeichnet die Weiterleitung von IP*-Paketen (Layer 3) anhand der Ziel-IP-Adresse und den vorhandenen Routing-Informationen in der Routing-Tabelle.

Routing-Tabelle Codes: C: Directly Connected Network; S: manuell; D: über EIGRP erlernt; O: über OSPF erlernt

Direkte Routen (C): Netz über ein Interface direkt erreichbar.

Remote Routen: können auto. erlernt werden gehen über andere Router

Default Route: `0.0.0.0/0` - Eintrag in einer Routing-Tabelle an die alle Pakete weitergeleitet (an anderen Router) werden, für die kein expliziter Eintrag in der Tabelle existiert. Ist eine statische Route

Metrik: „Kosten“ der Route

Administrative Distanz (AD): Routen Vertrauenswürdigkeit. Kleiner ist besser. Wichtig bei mehreren Routen für ein Ziel.

Link Local Route: IP des Routers im Netz.

Statisches Routing
*Sollten wenige Gateways zu konfigurieren sein, können statische Routing-Tabellen eingesetzt werden. Der Nachteil dieser **Konfiguration** ist klar, die **statische Routing**-Tabelle passt sich nicht automatisch an die Netzwerkumgebung an. Nur die Routen, die konfiguriert wurden, werden auch erkannt.*
Dynamisches Routing
*Ein Netzwerk, dass über viele mögliche Routen verfügt, sollte das **dynamische Routing** benutzten. Bei diesem Verfahren werden Protokolle, wie das RIP (Routing Information Protocol) und das OSPF (Open Shortest Path First) eingesetzt. Die Routing-Tabelle wird mittels dieser Protokolle gepflegt und passt sich den Veränderungen im Netzwerk an.*
Diagnose über die Hilfsprogramme: `PING & TRACEROUTE(ICMP)`

IGMP (Internet Group Management Protocol): Organisation von Multicast-Gruppen. Fester Bestandteil von IPv4 auf allen Hosts, die IPv4-Multicast unterstützen.

Routing Protokolle

- Interior Gateway Protocols

  Distance Vector Protocols: *(für kleine Netzen mit Verbindungen zwischen Routern die gleich schnell sind)* Routen sind als Vektoren mit Richtung und Distanz (Metrik) dargestellt. Router teilen ihren Nachbarroutern die Routen mit, die sie selbst kennt. Jeder Router pflegt seine eigene Routingtabelle! Die Router kennen nicht die Topologie des Gesamt-Netzes!

  - RIP: Routing Information Protocol - Classful; RIPv2 - Classless
  - IGRP: Interior Gateway Routing Protocol - Classful
  - EIGRP: Enhanced Interior Gateway Routing Protocol - Classless

  - **Link-State Protocols** *(für größere Netze mit Verbindungen zwischen Routern unterschiedliche schnell)*: Jeder Router ermittelt als Wurzel einen Shortest-path-first-Baum (Dijkstra), aus einer DB mit der ganzen Netztopologie. Bandbreite wird berücksichtigt.

    - OSPF: Open Shortest Path First - Classless
    - IS-IS = Intermediate System to Intermediate System Protocol - Classless
- Exterior Gateway Protocols (Verbindung von autonomen Systemen)
  - BGP = Border Gateway Protocol - Classless

Autonomes System / Routing Domains: Netze die von einer Organisation verwaltet werden. Das Internet ist ein Verbund von autonomen Systemen.

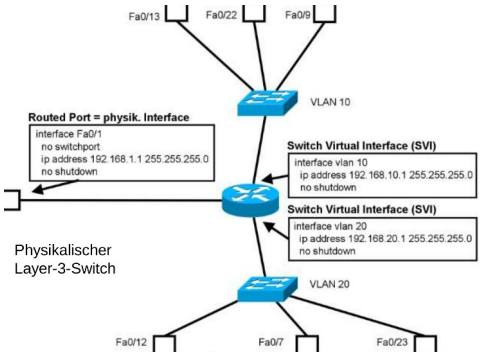
Classful Routing: Feste Längen der Subnetzmaske definiert (Class A → /8, B → /16, C →/24). Die Klassen haben bestimmte Adressbereiche → Subnetzmaske wird aus IP bestimmt.

Classless Routing: VLSM (Variable Length of Subnet Mask) möglich → Subnetzmaske muss explizit mitgeteilt werden.

Inter-VLAN Routing: Datenverkehr zwischen mehreren VLANs

Layer-3 Switch:

- Routed Ports: mit physikalischen Ports von reinen Routern vergleichbar → Adressierbar
- Switched Virtual Interfaces (SVI): virtuelle VLAN-Schnittstellen für Inter-VLAN Routing
  - Ersatzdarstellung →



IP & Subnetting

IPv4

IP Adressarten: Unicast: Ein Empfänger, Multicast: Gruppe von Empfängern, Anycast: nächstgelegener Empfänger)

Broadcast: höchste Adresse

Netz-ID: niedrigste Adresse

Gateway: meistens am Ende der Host-Range

IP-Adressen-Anzahl: $2^{(32 - \text{Notation})}$

Netz-Anzahl: 2^{Notation}

Host-Range: Netz-ID – Broadcast

LAN1 – Anzahl(30) der Hosts+GW+NA+BC = 33Adr. → 64er-Netz /26

Router – 2IP Adr.+NA+BC = 4Adr → 4er-Netz/30

NA = muss gerade sein / muss durch Netzgröße gerade teilbar sein

Bereich	Prefix	Anwendung
Unicast	0.0.0.0-223.255.255.255	von einem zu einem anderen Host
Broadcast	255.255.255.255	Directed Broadcast-> an alle Hosts im Netz. Router blockieren normalerweise Weiterleitung. Typische Verwendung:ARP+DHCP-Requests
Multicast	224.0.0.0-239.255.255.255	von einem Host an ausgewählte Menge anderer Hosts, über ein Packet

Loopbackadresse	127.0.0.1	Genau genommen für Localhost reserviert.
Link Local	169.254.0.0-169.254.255.255	Für Automatische Adressvergabe durch OS kein Routing dieser Adressen
Für Lehre	192.0.2.0-192.0.2.255	Oft mit Domain example.com/.net
Ip-Forschungszweck	240.0.0.0-255.255.255.254	Für Forschungszwecke reserviert.

Ipv6

Grund für IPv6: *zu wenig IPv4 Adressen; Routing-Tabellen auf den Backbone-Routern wurden zu groß, durch NAT keine IPv4 Ende-zu-Ende-Verbindung möglich, einfachere IP-Header*

Aufbau IPv6: 48 Bit (Global Routing Prefix), 16 Bit Subnet ID, 64 Bit Interface ID = 128 Bit

Notation: 8 Blöcke zu jeweils 4 Hexadezimalstellen; durch Doppelpunkte getrennt; Ein Block hat 16 Bit; 0 Blöcke, dürfen aufeinander folgende Doppelpunkte notiert werden: `2001:db8:0:0:0:0:1428:57ab` = `2001:db8::1428:57ab`

Subnetting: immer /64, Im Netzadressenteil beliebig hochzählen

Wichtige Bereiche:

Bereich	Prefix	Anwendung
Link-Local Unicast	fe80::/64	Nur im lokalen LAN-Segment gültig. (Nicht gültig über Router hinweg) Bildung Link-Local Unicast Müssen nur im jeweiligen Link-Segment (LAN eindeutig sein)
Loopback	::1/128	Der eigene Rechner
Unique Local Unicast /Unique Local Addresses	fc00::/7 - fdff::/7	Werden im Internet nicht geroutet nur gültig in lokalen Netzwerken. (Bspw. Firmen Intranets)
Multicast	ff00::/8 - ffff::/8	Siehe Multicast **Broadcast ist auch Teil von Multicast !!! (All Nodes Multicast Gruppe)**
Global Unicast	2000::/3 - 3fff::/3	Weltweit gültige Adressen.

Autoconfiguration:

- SLAAC (Stateless Address Autoconfiguration): Endgeräte konfigurieren sich selbst über Link-Local Adressen. Router Präfixe werden über Router Advertisements verteilt.
- DHCPv6: DHCPv6 Server verteilt IP Adressen
- DHCPv6 + SLAAC: Kombination aus beiden Technologien. Es werden zusätzliche IP Optionen über DHCP verteilt. Beispielsweise eine 2. IPv6 Adresse.

EUI-64: Interface ID wird aus MAC-Adresse gebildet. Zwischen Bit 24 und Bit 40 wird die Bitfolge “FFFE” eingefügt.

Privacy Extensions: Definiert in RFC

Übergangsmechanismen IPv4 zu IPv6

- **Dual-Stack:** Endgerät kann über IPv4 und IPv6 gleichzeitig kommunizieren.
- **Dual Stack Lite:** Router kommuniziert nur über IPv6. Im lokalen LAN werden jedoch auch private IPv4 Adressen verwendet, die vom Router in IPv6 Paketen gekapselt werden. Der Provider übersetzt das gekapselte Paket dann in eine öffentliche IPv4 Adresse. (Carrier Grade NAT) CGN
- **Tunnel:** 6to4
- **Übersetzungsverfahren:** NAT64: Übersetzt IPv6 Adressen in IPv4 Adressen

Temporäre IPv6 Adresse: Enthält anstelle der MAC Adresse der Schnittstelle eine zufällig erzeugte 64Bit Zahl als Schnittstellen-ID

SSH: Verschlüsselter Zugriff auf ein Remote-Gerät über dessen IP-Adresse.Was braucht PC, um im Netz zu kommunizieren? ->Ip-Adresse, Subnetzmaske, Standartgateway, DNS-Server(Namensauflösung)

IPv6 Multicast Adressen ☾ FF00::/8: [13]
• **Assigned Multicast-Adressen**, sind vorab definiert. Geräte sind je nach Funktion Mitglied in betreffenden Gruppen – z.B. o FF02::1 All-nodes multicast group
☾ Ersetzt die IPv4-Broadcast-Adresse
o FF02::2 All-routers multicast group (nur Router!)
• **Solicited-Node Multicast**
☾ wird beim Neighbor Discovery benötigt bzw. verwendet.
o IPv4 verwendet ARP-Requests/-Replies um notwendige Layer-2-Adresse zu erfragen
o IPv6 verwendet dafür ICMPv6 Neighbor Solicitation (NS)

& Neighbor Advertisment (NA)

Switche Konfigurieren(Labor 2)

1. Privilleged execution mode
Switch> enable
Switch#
2. Konfiguration anzeigen
Switch# show running-config
3. Konfigurieren
Switch# configure terminal
Switch(config)# hostname S1
S1(config)# exit

S1#

Sitzung VTY)

S1(config)# line vty 0 15 //für alle ports von 0 bis 15
S1(config-line)# password letmein
S1(config-line)# login
S1(config-line)# end
7. Zugriff über die Konsole
C:\> telnet 10.10.10.11
8. Ssh auf Switch (erst domain-name und rsa-schlüssel konfigurieren)
S1(config)# ip domain-name hhs.de
S1(config)# crypto key generate rsa
S1(config)# ip ssh version 2
S1(config)# username admin secret 1234

9. SSH auf VTY-Lines konfigurieren
S1(config)# line vty 0 15
S1(config-line)# transport input ssh
S1(config-line)# login local
S1(config-line)# end

Wie viele FastEthernet-Interfaces hat der Switch? 24

• Wie viele GigabitEthernet-Interfaces hat der Switch? 2
• Wie viele vty-lines kann man konfigurieren? 16 (0 15)
• Welcher Befehl zeigt den Inhalt des NVRAM (non-volatile-RAM) an?

show startup-config

• Wieso antwortet der Switch mit „startup-config is not present“?

Weil bisher noch keine running-config aus dem RAM auf die startupconfig im NVRAM gespeichert wurde.

Router-Switch-PCs (Labor 2)

1. Welcher Zusammenhang besteht zwischen /24 und der 255.255.255.0 und wie bezeichnet man die Schreibweise /24 noch? Das Prefix /24 (Prefix- oder CIDR-Schreibweise) gibt an, dass die Subnetzmaske von links beginnend 24 „1“-Bits hat. Somit entspricht dies der Subnetzmaske von 255.255.255.0 (Dotted-Decimal#Schreibweise). CIDR = Classless-Inter-Domain-Routing

2. Welche Adresssen dürfen nicht vergeben werden?

Netzadresse alle Host-ID-Bits sind „0“ • Broadcastadresse alle Host-ID-Bits sind „1

3. Welche Funktion hat das Default-Gateway und warum muss es auf jedem Host konfiguriert werden?

Das Default- oder Standard-Gateway oder auch nur Gateway wird vom Host für alle IP-Pakete benötigt, die eine Ziel-IP-Adresse aus einem fremden Netz haben. Für die Kommunikation zu Ziel-IP-Adressen im eigenen IP-Netz wird das Default-Gateway nicht benötigt

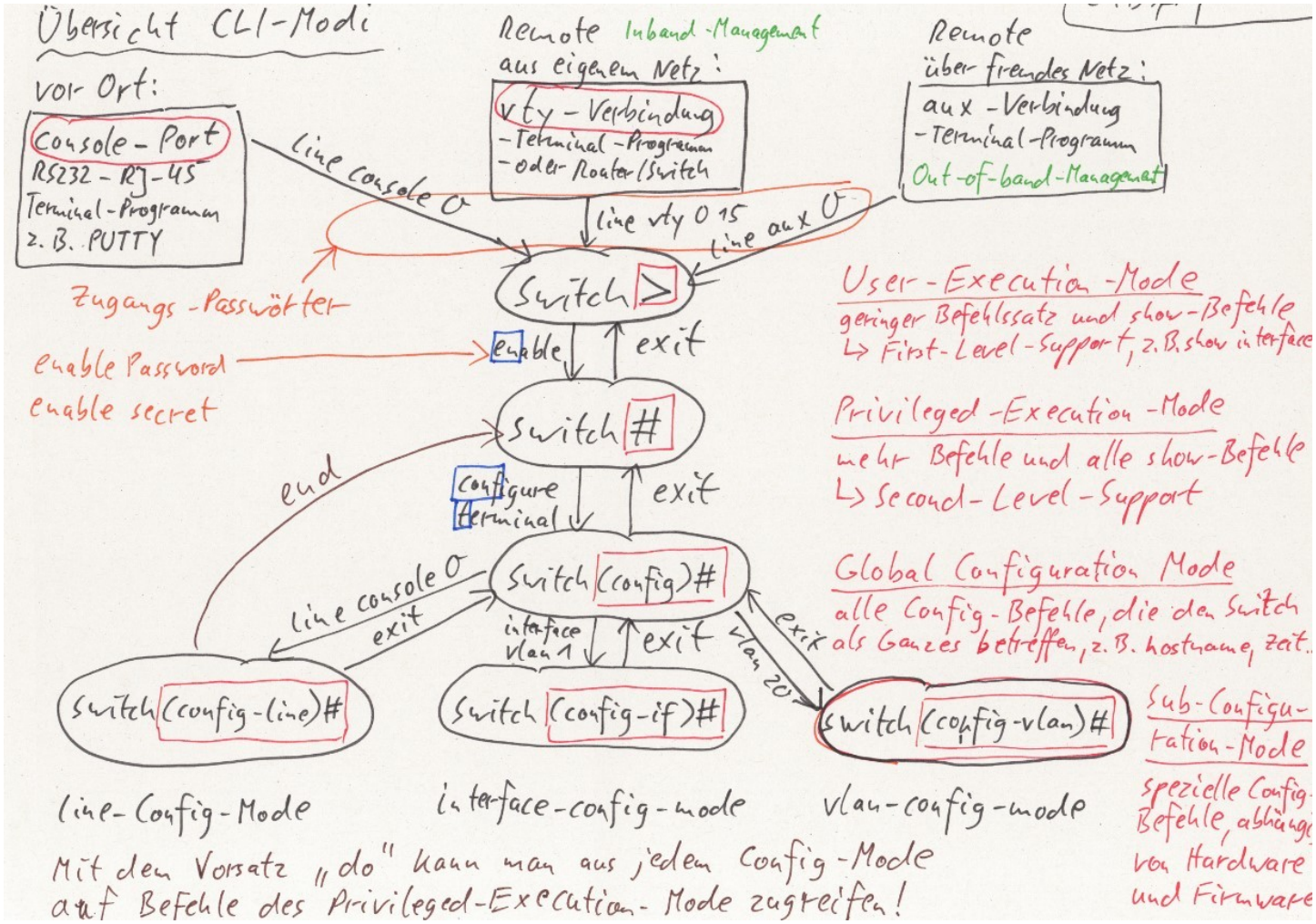
4. Wie leitet der HUB das Paket weiter?

Der Hub leitet das Paket immer bitweise vom Eingangs- auf alle aktiven Ausgangs-Interfaces weiter. Reines Layer-1-Gerät ohne jegliche Adress-Auswertung

5. Definieren Sie nun ein Paket von PC0 zu PC1. Wie verhält sich der SWITCH im Vergleich zum HUB bei der Weiterleitung des Paketes? Der Switch leitet im Gegensatz zum Hub das Paket vom Eingangs-Interface gezielt auf das Ausgangs-Interface weiter, an das der Ziel-PC1 angeschlossen ist. Dazu pflegt der Switch eine MAC-Adress-Tabelle in der die Zuordnung MAC#Adresse zu Switch-Interface eingetragen ist

6. Nach Neustartenund ping Befehl, welche Anfrage führt der PC aus?

Es wird zuerst ein ARP-Request zum PC1 durchgeführt, weil der PC0 keinen Eintrag zur MAC-Adresse für PC1 in seiner ARP-Tabelle hat. ARP = Address Resolution Protocol



Welche Ziel bei einem neuen Mobilfunk-Standard verfolgt? Höhere Übertragungsrate und Energiesparender