Zusammenfassung

Computernetze 2

Michael Wieland

Hochschule für Technik Rapperswil

4. September 2016

Mitmachen
Falls Du an diesem Dokument mitarbeiten willst, kannst Du das Dokument auf GitHub unter `https://github.com/michiwieland/hsr-zusammenfassungen` forken.

Inhaltsverzeichnis

Akronyme

C | D | I | R

C

CP

Control Plane 6, 8, *Siehe:* Control Plane

D

DCE

Data Communication Equipment 6, 8, *Siehe:* Data Communication Equipment

DP

Data Plane / Forwarding Plane 6, 8, *Siehe:* Data Plane / Forwarding Plane

DSLAM

Digital Subscriber Line Access Multiplexer 6, 8, *Siehe:* Digital Subscriber Line Access Multiplexer

DTE

Data Terminal Equipment 6, 8, *Siehe:* Data Terminal Equipment

I

IANA

Internet Assigned Numbers Authority 6, 8, *Siehe:* Internet Assigned Numbers Authority

ICANN

Internet Corporation for Assigned Names and Numbers 6, 8, *Siehe:* Internet Corporation for Assigned Names and Numbers

R

RIPE

Réseaux IP Européens Network Coordination Centre 6, 8, *Siehe:* Réseaux IP Européens Network Coordination Centre

RIR

Regional Internet Registrar 6, 8, *Siehe:* Regional Internet Registrar

Glossar

C | D | I | R | V

C

Control Plane

Die Control Plane definiert die Logik wie der Verkehr weitergeleitet wird. Sie wird softwaremässig gesteuert (Protokolle, Virtuelle Switches, Virtuelle Router) 6, 8

D

Data Communication Equipment

Modem 6, 8

Data Plane / Forwarding Plane

Die Data Plane leitet die pakete anhand der Logik in der Control Plane weiter. Sie ist die Hardware (Switches, Router) 6, 8

Data Terminal Equipment

Client Router 6, 8

Digital Subscriber Line Access Multiplexer

Ist die Vermittlungsstelle zwischen mehrere Endkunden (DSL Anschlüsse) und dem Provider. 6, 8

I

Internet Assigned Numbers Authority

Eine Organisation die für die globale Koordination von IP-Adressen zuständig ist. Zudem registriert die IANA viele in Spezifikationen von Netzwerkprotokollen enthaltene Codecs (z.B Ports) 6, 8

Internet Corporation for Assigned Names and Numbers

Koordiniert die Vergabe von einmaligen Namen und Adressen im Internet (DNS) 6, 8

R

Regional Internet Registrar

Ist für die Verteilung von IP-Adressen innerhalb einer Region zuständig und erhält von der IANA einen definierten Adressrange. Für Europa ist die RIPE der RIR. 6, 8

Réseaux IP Européens Network Coordination Centre

Zuständig für die Vergabe von IP-Adressbereichen und AS-Nummern in Europa 6, 8

V

verbindungsloser Dienst

Ein verbindungsloser Dienst startet dagegen direkt mit der Übertragung von Daten. (z.B UDP, Ethernet) 8

verbindungsorientierter Dienst

Bei einem verbindungsorientierten Dienst wird im vorhinein eine Verbindung aufgebaut (z.B TCP, Frame Relay) Dabei werden immer die drei Phasen Verbindungsaufbau, Datenübertragung und Verbindungsabbau durchlaufen. 8

1. Grundlagen

1.1. OSI Headers

L1: Physical 12Byte Interframe Gap + 8Byte Start Frame Delmiter und Preamble

L2: Data Link 14 Byte Ethernet

L3: Network 20Byte IPv4 oder 40Byte IPv6

L4: Transport 20Byte TCP oder 8Byte UDP

L5: Application 12 Byte RTP

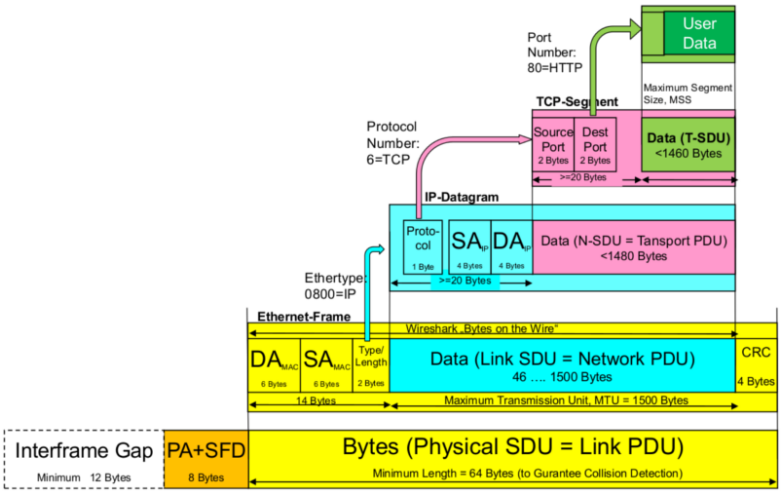


Abbildung 1: OSI Headers

1.2. Zahlensysteme

1.2.1. Dezimal in Hexadezimal

$$
\begin{aligned}
1278_D &\rightarrow Hexadezimal? \\
1278 : 16 = 79 \text{ Rest } 14 &\Rightarrow E \\
79 : 16 = 4 \text{ Rest } 15 &\Rightarrow F \\
4 : 16 = 0 \text{ Rest } 4 &\Rightarrow 4 \\
1278_D &\Rightarrow \underline{4FE}
\end{aligned}
\tag{1}
$$

1.2.2. Hexadezimal in Binär

$$
\begin{aligned}
4FE_H &\rightarrow Binär? \\
4 &= 4_D = 0100_B \\
F &= 15_D = 1111_B \\
E &= 14_D = 1110_B \\
4FE_H &\Rightarrow \underline{010011111110}
\end{aligned}
\tag{2}
$$

1.2.3. Hexadezimal in Dezimal

Möchte man eine IPv6 Adresse in IPv4 umwandlen, nimmt man immer 2 Hexzahlen und rechnet diese einzeln in dezimalZahlen um

$$
\begin{aligned}
0F : 2049 &\rightarrow Dezimal? \\
0_H &\Rightarrow 0_D \cdot 16^1 = 0 \\
F_H &\Rightarrow 15_D \cdot 16^0 = 15 \\
2_H &\Rightarrow 2_D \cdot 16^1 = 32 \\
0_H &\Rightarrow 0_D \cdot 16^0 = 0 \\
4_H &\Rightarrow 4_D \cdot 16^1 = 64 \\
9_H &\Rightarrow 9_D \cdot 16^0 = 9 \\
4FE_H &\Rightarrow (0+15).(32+0).(64+9) = \underline{xxx.15.32.73}
\end{aligned}
\tag{3}
$$

2. Subnetting

2.1. Classful

Bei Classfull Subnetting sind alle Subnetzmasken gleich. Die Subnetzmaske ist immer so gross, wie das grösste Subnetz.

Klasse	Binär Präfix	IP-Range	Netzmaske
A	0____.	0.0.0.0 - 127.255.255.255	255.0.0.0
B	10___.	128.0.0.0 - 191.255.255.255	255.255.0.0
C	110_.	192.0.0.0 - 223.255.255.255	255.255.255.0
D	1110.	224.0.0.0 - 239.255.255.255	Verwendung für Multicast
E	1111.	240.0.0.0 - 255.255.255.255	reserviert für zukünftige Zwecke

2.1.1. Private Adressbereiche

Klasse	Adressbereich	CIDR Prefix
A	10.0.0.0 bis 10.255.255.255	10.0.0.0/8
B	172.16.0.0 bis 172.31.255.255	172.16.0.0/12
C	192.168.0.0 bis 192.168.255.255	192.168.0.0/16

2.2. VLSM: Variable Length Subnetting /CIDR: Classless Inter-Domain Routing

Bei Classless können flexiblere Adressgrössen verwendet werden. Dabei müssen aber trotzdem Blöcke gemäss dem grössten Subnetz gemacht werden. Diese Blöcke können aber im Gegensatz zu Classful Subnetting in kleinere Netze unterteilt werden.

2.3. Vorgehen

Angenommen man bekommt Netz 172.16.0.0/16 (Class B) und muss dieses in mehrere Subnetze unterteilen. Es empfiehlt sich immer mit dem grössten Netz (mit den meisten Hosts) zu beginnen und dann immer kleinere Subnetze zu berechnen.

1. Man sucht sich das grösse Subnetz (angenommen 634 Hosts) und berechnet dessen Subnetzmaske: 624 Hosts $\Rightarrow 2^{10} = 1024$ verfügbare Hosts $\Rightarrow$ /22 = 255.255.252.0
2. Die Bits 16 - 22 können nun für die Subnetze genutzt werden

   11111111.11111111.|000000|00.00000000

   11111111.11111111.|000001|00.00000000

   11111111.11111111.|000010|00.00000000

   11111111.11111111.|000011|00.00000000
3. Im Subnetz Bereich werden nun die Bits binär hochgezählt (Startend bei 0000)
4. Die resultierenden Werte sind jeweils die Netzadressen
5. Das 0-er Netz wird meist für die Links verwendet (/30)
6. Beachte, dass immer zwei Adressen in jedem Subnetz für Broadcast und Netzadresse reserviert

2.3.1. Subnetzmasken

CIDR	Subnetzmaske
/30	255.255.255.252
/29	255.255.255.248
/28	255.255.255.240
/27	255.255.255.224
/26	255.255.255.192
/25	255.255.255.128
/24	255.255.255.0
/23	255.255.254.0
/22	255.255.252.0
/21	255.255.248.0
/20	255.255.240.0
/19	255.255.224.0
/18	255.255.192.0
/17	255.255.128.0
/16	255.255.0.0

2.3.2. IPv6

Empfohle werden fixe Netze von der Grösse /64

3. Cisco Command Line Interface (CLI)

3.1. Modes

Cisco Router sind in Berechtigungsschichten aufgeteilt. Jeder Modus erlaubt es unterschiedliche Aktionen auszuführen. Möchte man innerhalb des Konfigurationmodus ein show Befehl ausführen muss ein "do"vor gehängt werden.

Usermode Standmodus. In diesem Modus können "public"Router Einstellungen nur betrachtet werden

Priviledge Mode Mit 'enable' rsp. 'en' kann in den privilegierten Modus gewechselt werden. Dieser Modus erlaubt das betrachten von "privatenËinstellungen.

Configuration Mode Mit 'configure Terminal' rsp. 'conf t' kann in den konfigurations Modus gewechselt werden. Hier können Einstellungen im Memory konfiguriert werden.

Interface Configuration Mode Mit 'interface' kann ein Interface Konfiguriert werden

Router Configuration Mode Mit 'router' kann z.B das Routing Protokoll geändert werden.

3.2. Konfiguration anzeigen

Aktuelle Konfiguration filtern (Ganz Block anzeigen)	show run | section <my filter>
Aktuelle Konfiguration im RAM filtern (Zeile anzeigen)	show run | include <my filter>
Aktuelle Konfiguration im NVRAM anzeigen	show startup-config
Verbundene Geräte anzeigen	show cdp neighbor
Laufende Routing Protokolle anzeigen	show ip protocols
Routing Tabelle anzeigen	show ip route
Interface Übersicht anzeigen	show ip interface brief

3.3. Konsole konfigurieren

Konsole konfigurieren	line console 0
Session Timeout setzen (für die Konsole)	exec-timeout [min][sec]
Synchrones logging aktivieren	logging synchronous

3.4. Rooter konfigurieren

Hostname setzen	hostname name
Statischen Eintrag in die Hostname Tabelle einfügen	ip host <name>
Passwort setzen	enable secret <my secret>
DNS Lookup deaktivieren (Somit werden Falscheingaben nicht aufgelöst)	no ip domain-lookup
IP Route leeren	clear ip route *

3.5. NAT konfigurieren

NAT Tabelle eintragen	show ip nat translation
Statisches Port forwarding	ip nat inside source static tcp <local client> <port> interface <interface> <port>

3.5.1. RIP

RIP konfigurieren	router rip
Welche direkt angehängte Netzerke via RIP advertised werden sollen	network <net ip>
Verwendete RIP Version setzen	version 2
Automatisches Zusammenfassen von Netzen deaktivieren	no auto-summary
Mögliche Fehler der RIP Konfiguration anzeigen	debug ip rip

3.5.2. OSPF

OSPF konfigurieren. Prozess ID kann beliebig gewählt werden. Gilt Router lokal	router ospf <process-id [1-65535]>
Welche direkt angehängte Netzerke via OSPF advertised werden sollen	network <net ip> <inverse-subnet> area <area-id>
Wie oft der Shortest Path Algorithmus ausgeführt wurde. Zeigt auch das Link State Update Intervall	show ip ospf
Zeigt die OSPF Nachbarn	show ip ospf neighbor
Zeigt die Topologie Datenbank	show ip ospf database

3.5.3. BGP

BGP aktivieren	router bgp <as-number>
BGP Nachbarn eintragen	neighbor <ip-address> remote-as <as-number>
BGP Debuggen	debug condition interface <interface>
BGP Debuggen	debug ip packet detail
Alle BGP Infos anzeigen	show ip bgp
BGP Infos anzeigen	show ip bgp summary

3.6. Interface konfigurieren

Zu konfigurierendes Interface auswählen	interface [f/g]0/1
IP Konfiguration setzen	ip address <ip> <subnet mask>
Beschreibung setzen	Description <description>
Interface aktivieren	no shutdown
Serial-Clock-Speed einstellen	clock rate 128000

3.7. Konfiguration speichern

Routing Konfiguration speichern	copy running-config startup-config

3.8. Debugging

Debuging aktivieren	debug ip routing
Debuging deaktivieren	undebug all

3.9. Routing

Statische Route eintragen	ip route <target-net> <target-subnet> <next-hop> <path-cost>

4. Cisco Router Komponenten

DRAM: Dynamic RAM / RAM: Random Access Memory

- Routing Tabellen
- ARP Cache
- Fast Switching Cache
- Packet buffering
- Beinhaltet die Routing Konfiguration während der Router eingeschaltet ist
- Verliert den Inhalt sobald der Router neugestartet wird

NVRAM: Non Volatile Random Access Memory

- Beinhaltet die Startup und Backup Konfiguration des Routers
- Behält den Inhalt, auch wenn der Router abgeschalten oder neugestartet wird

Flash Speicher

- Beinhaltet das System Image
- Erlaubt das Updaten der Software ohne das der Chip auf dem Prozess ausgetauscht werden muss.
- Behält den Inhalt, auch wenn der Router abgeschalten oder neugestartet wird
- Kann mehrere IOS Software beinhalten

ROM: Read Only Memory

- Stellt Instruktionen für POST (power-on-self-test) Diagnosen zur Verfügung
- Speichert Bootstrap Programme und Grundlegende OS Software
- Benötigt ersetzbare, einsetzbare Chips für Software Updates

5. Telefonie

5.1. Vermittlungsarten

Leitungsvermittlung (circuit switched)
Bei der Leitungsvermittlung geht der komplette Traffic über eine reservierte Leitung. Dies hat den Vorteil, dass man garantierter QoS hat, dass man das Netzwerk für eine bestimmte Funktion optimieren kann und dass es sehr stabil ist. Nachteil ist ganz klar, dass die ungenutzte Übertragungskapazität nicht für andere Services genutzt werden. Ein klassisches Beispiel für die Leitungsvermittlung ist das Telefonienetz, wobei die Signalisierung heutzutage über SS7 läuft.

Paketvermittlung (packet switched)
Bei der Paketvermittlung wird der Weg anhand der Destination Adresse des Pakets entschieden. Dadurch kann es möglich sein, dass die Pakete unterschiedlich schnell beim Empfänger ankommen. Der Vorteil bei der Paketvermittlung ist, dass es flexibler ist und die Kosten pro Datenvolumen, rsp. FlatRate anfallen.

5.2. PSTN: Public Switched Telephone Network

PSTN (früher ein Synonym für POTS: Plain Old Telephone Service ⇒ analoges Netz) war das erste öffentliche Kommunikationssystem für die Telefonie. Es existierte eine physikalische Verbindung (Leitungsvermittlung) zwischen den Teilnehmer, wobei in der ersten Version eine Person die Verbindung manuell herstellte. In späteren Versionen wurde mittels Pulse Code Modulation das analoge Signal in ein Digitales umgewandelt.

5.3. ISDN: Integrated Service Digital Network = PSTN IV

ISDN lösste das analoge PSTN ab, da dieses stark limitiert war. ISDN unterstützt die Übertragung von Daten, Sprache und Video, wobei es mit einer Übertragungsrate von 64kbps für Sprachübertragung optimiert wurde.

5.3.1. Anschlüsse

Ein ISDN-Anschluss ist in zwei Varianten verfügbar

Basisanschuss: Es stehen zwei B-Kanäle (Nutzkanäle) zur Verfügung, die völlig unabhängig voneinander für Telefongespräche, Fax oder Datenübertragung genutzt werden können. Zusätzlich gibt es einen D-Kanal (Steuerinformationskanal)

Primärmultiplexanschluss: Es stehen 30 B-Kanäle und ein Steuerkanal, sowie einen weiteren Kanal für die Synchronisation und Wartung zur Verfügung.

5.4. IP-Telefonie

IP-Telefonie baut im Gegensatz zur herkömmlichen PSTN/ISDN Technologie (verbindungsoriertiert) auf ein verbindungsloses UDP Protokoll auf und sendet die einzelnen Pakete durch eine Wolke aus Switches und Router. IP-Telefonie hat dabei den klaren Vorteil, dass eine Verbindung für die Gesprächsdauer nicht fix reserviert wird und somit ungenutzte Übertragungskapazitäten für andere Teilnehmer zur Verfügung stehen.

5.5. SIP: Session Initiation Protocol

SIP eignet sich für den Aufbau, Betrieb und Abbau von Sprach- und Video-Verbindungen. Sowohl Punkt-zu-Punkt- als auch Multicast-Verbindungen lassen damit steuern. In der Grundversion werden die Informationen im Klartext übertragen. Da dies ein enormes Sicherheitsrisiko ist, sollte die SIPS verwendet werden.

- SIP ist ein textbasiertes Protokoll dass die Verbindung zwischen zwei Teilnehmer steuert.
- SIP beschreibt nur die Signalisierung. Alles Weitere wird über SDP ausgehandelt.
- Durch SIP wird eine verbindungsorientiert Kommunikation in einem paketvermittelnden Netz realisiert
- Es arbeitet auf Layer 5-7 und verwendet TCP und UDP auf Port 5060-5061
- Mit RTP (Real-Time Transport Protocol) werden die Medienströme in Echtzeit übertragen. Dies geschieht jedoch unverschlüsselt! Man sollte daher SRTP verwenden.
- Als Ersatz für die Telefonnummern wird ein Teilnehmer mit einer URI und DNS addressiert (sip:userid@domain)
- SIP verfügt über die User Location, Availability und Capabilities.

5.5.1. SIP Komponenten

Eine SIP Infrastruktur kann über folgende Komponenten verfügen, wobei nur die Uesr Agents pflichts sind und ein physisches Gerät die Funktionen mehrere logischen Komponenten übernehmen.

User Agent
Das Endgerät. Es wird zwischen User Agent Client (UAC) ⇒ Caller, Sender und User Agent Server (UAS) ⇒ Callee,Empfänger unterschieden.

Gateway
Übernimmt die Übersetzung von PSTN Geräten zum SIP Protokoll. Ein Gateway ist nur eine spezielle Variante eines User Agents

Registrar
Linked die SIP URI mit der Geräte IP Adresse. Nimmt SIP:Register Meldungen entgegen und beinhaltet alle aktuellen Standorte der UA innerhalb der Domäne.

Proxy Server
Routet und verbindet zwei Endgeräte. Nimmt UAC Request entgegen, fragt den Registrar nach der Adresse des UAS und leitet die Verbindung weiter. Ist die Adresse auserhalb seiner zuständingen Domäne, wird der Request an einen weiteren Proxy weitergeleitet. Ein Proxy kann ein Invite auch an mehrere Endgeräte senden und verbindet dann mit jedem, welches ein OK zurücksendet. Ein SIP Proxy kann entweder stateless oder stateful sein:

- Stateless: Leitet die SIP Pakete weiter ohne über den Status bescheid zu wissen.
- Statefull: Verwendet immer TCP und verwaltet den Status der Verbindung bis diese terminiert wird.

Redirect Server
Adressbuch, nimmt Anfragen entgegen und antwortet mit Adresse

5.5.2. SIP Meldungen

Das Protokoll unterscheidet zwischen Request und Responses:

Request: REGISTER (Registrier eine UA bei Registrar), INVITE, ACK, BYE, CANCEL, OPTIONS

Response:
HTTP Status Code

- 1xx = Informational
- 2xx = Success
- 3xx = Redirection
- 4xx = Client Error
- 5xx = Server Error
- 6xx = Global Error

5.5.3. Ablauf

1. Der Sender sendet dem Empfänger ein INVITE (kann auch über einen Proxy gehen)
2. Der Empfänger antwortet mit einem 100(Trying), 180 (Ringing) und Status Code 200 (OK)
3. Der Sender antwortet mit einem ACK und die Verbindung ist aufgebaut
4. Der UA der die Verbindung schliesst sendet ein BYE worauf die Gegenstelle mit einem Status Code 200 OK Antwortet

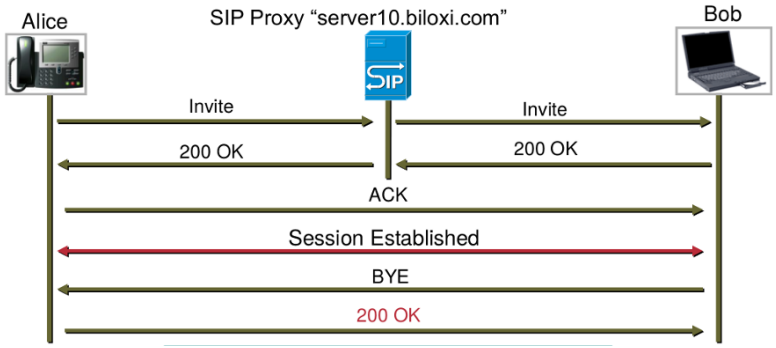


Abbildung 2: SIP Anruf Ablauf mit Proxy

5.5.4. SDP: Session Description Protocol

Mit SDP werden Medienbeschreibung (Video, Audio), Transportprotokoll(RTP, UDP, IP, H.320), Codec (H.261, MPEG), Ports und Senderichtung ausgetauscht. SDP wird z.B beim SIP Invite für das Aushandeln der Codecs verwendet. SDP ist textbasiert wobei die Reihenfolge der Eigenschaften eine Rolle spielt:

1. v = <protocol-version> (Pflicht)
2. o = <username> <session-id> <session-version> <nettype> <addrtype> <unicast-address> (Pflicht)
3. s = <session-name>
4. c = <nettyp> <addrtype> <connection-address> (Pflicht)
5. k = <encryption-keys>
6. t = <time the session is active> (Pflicht)
7. m = <media> <port> <protocol> <fmt (Link auf a Eintrag)> (Pflicht)
8. a = <media attribute lines> (Reihenfolge der a Einträge entsprechen deren Priorität)

5.6. ENUM: Telephone Number Mapping

ENUM mappt herrkömmliche PSTN Telefonnummern mit SIP Adressen. Dies erlaubt die Kommunikation zwischen PSTN und IP-Telefonie. Dabei wird eine DNS Anfrage vom Gateway mit der umgedrehten Telefonnummer gestellt. (0.1.0.2.2.9.3.4.4.1.4.e164.arpa) Der DNS Server antwortet mit der SIP Adresse.

6. WLAN: Wireless LAN

SSID: Service Set Identifier

BSSID: Basic Service Set Identifier. Meistens die MAC Adresse des Access Points

BSS: Basic Service Set

ESS: Extended Service Set. Mehrere BSS mit gleicher SSID

RSSI: Received Signal Strength Indicator. Stellt einen Indikator für die Empfangsfeldstärke kabelloser Kommunikationsanwendungen dar.

CSMA/CA: Carrier Sense, Multiple Access, Collision Avoidance

SIFS: Short Interframe Gap. Dient dazu einen Sicherheitsabstand zwischen zwei Übertragungsblöcke einzubauen, damit sich diese nicht gegenseitig beeinflussen. SIFS hat die höchste Priorität; eine Station mit SIFS darf vor allen anderen Stationen senden. Typische SIFS-Intervalle betragen im 2,4-GHz-Frequenzband $10\mu s$ und im 5-GHz-Band $16\mu s$.

DIFS: Distributed Interframe Space. Er hat die längsten Wartezeiten mit etwa $50\mu s$ zuzüglich dem Backoff und die geringste Priorität.

EIFS: Extended Interframe Space. Das EIFS kommt immer dann zum Einsatz, wenn eine Station in einem Funknetz unvollständige oder fehlerhafte Datenpakete empfängt, oder wenn die Übertragung durch die Bitübertragungsschicht abgebrochen wurde.

ACK: Acknowledge

RTS: Requst to Send.

CTS: Clear to Send.

6.1. Passive Mode

- Access Points versenden Beacon Frames um den Clients ihre Möglichkeiten zu übermitteln. Diese werden in regelmässigen Intervallen versendet.

6.2. Active Mode

1. Die Clients hingegen senden Probe Requests an die Access Points um ihre Möglichkeiten bekannt zu machen
2. Der Acces Point antwortet mit Probe Response
3. Um die Rückwärtskompatibilität zu gewährleisten, wird nach einem erfolgreichen Probe Response ein Authentication Request und Response versendet.
4. Danach erfolgt das Verbinden mit genau einem Access Point mittels einem Association Request und Response.
5. Wechselt ein Client seinen Standort ist eine Reassoziierung von Nöten. (Handover) Es werden Reassociation Request und Responses versendet, falls sich der Client innerhalb eines ESS bewegt.

6.3. Datenrate

- Die maximal erreichbare Datenrate hängt von mehreren Kriterien ab
  1. Signal bzw. Kanalbandbreite
  2. Signal zu Geräusch Verhältnis
  3. Anzahl parallel nutzbare Ausbreitungswege (MIMO)

6.4. 2.4Ghz Band

- IEEE 802.11b/g/n
- Grössere Reichweite und Kompatibilität mit Legacy Geräten
- Kanalbandbreite von 22Mhz
  - 20Mhz: Von verfügbaren 13 Kanälen können 3 überlappungsfrei genutzt werden(meist 1, 6, 11)

6.5. 5hz Band

- IEEE 802.11a/n/ac
- Geringe Reichweite dafür weniger störungsanfällig und grössere Bandbreite
- Kanalbandbreite kann 20, 40Mhz sein
  - 20Mhz: 19 überlappungsfreie Kanäle (Kanal 36, 40, 44 .. 140)
  - 40Mhz: 9 überlappungsfreie Kanäle

6.6. Antennen

Es gibt viele WLAN-Antennen welche sich in deren Grösse und Form unterscheiden, wobei dies einen Einfluss auf das resultierende Signal hat. Bei höheren Frequenzen werden die Antennen kleiner, wie auch deren Reichweite.

Omnidirektionale Antennen Omnidirektionale Antennen haben eine donought-artige Abdeckung. Die Sendeleistung um die Antenne herum ist gut und sehr gleichmässig. Direkt über und unterhalb der Antenne ist die Sendeleistung am schwächsten.

Gerichtete Antennen Gerichtete Antennen haben konzentrieren ihre Abdeckung auf einen Punkt und sin deshalb für die Überbrückung von grösseren Distanzen geeignet.

6.7. Sendelesitung

6.7.1. TPC: Transmitted Power Control

Ist eine Regelung für die abgestrahlte Sendeleistung.

6.7.2. Einschränkungen

Einschränkungen werden vom BAKOM (Bundesamt für Kommunikation) vorgeschrieben und soll die Beeinträchtigung anderer Funksysteme wie die für militärische Radarsysteme oder die für die Satellitenkommunikation minimieren.

- 2.4GHz Frequenzband: max. 100mW
- Unteres 5Ghz Frequenzband(indoor): max 200mW ohne TPC Funktionalität, ansonsten 100mW
- Oberes 5Ghz Frequenzband (indoor/outdoor): max 1W (mit TPC) und 500mW (ohne TPC)

6.8. FHSS: Frequence Hopping Spread Spectrum

Bei FHSS wird alle paar Millisekunden die Frequenz innerhalb des Frequenzbereiches gewechselt. Dies hat den Vorteil, dass sich die Geräte weniger stören. Da während des Wechsels keine Daten übertragen werden können, leidet aber die Übertragungsrate. Es wird unter anderem bei Bluetooth eingesetzt.

6.8.1. EIRP

Die Equivalent Isotropically Radiated Power (EIRP) ist ein Mass für die maximale Signalstärke.

$$\underbrace{EIRP}_{Strahlenleistung} = \overbrace{P_T}^{EingespeisteLeistung} - \underbrace{L_c}_{\text{Verlust im Kabel}} + \overbrace{G_a}^{\text{Antennengewinn}}$$

Die EIRP wird in Decibel Miliwatt(dBm) ausgedrückt:

$$Power_{dBm} = 10 \cdot log_{10}(Power_{mW}/1mW)$$

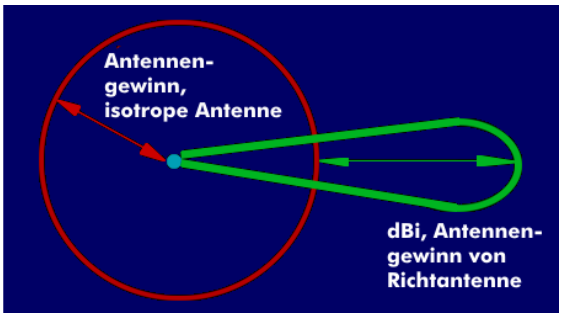


Abbildung 3: Effektive Isotrope Strahlungsleistung EIRP

6.9. Signal zu Rausch Verhältnis

Das Signal-Rausch-Verhältnis (SNR) ist das Verhältnis aus der Leistung des übertragenen Nutzsignals zur Leistung des Rauschsignals und ein Maß für die Reinheit eines Signals. Je größer das Signal-Rausch-Verhältnis ist, desto störungsfreier und weniger verrauscht ist das Nutzsignal.

$$SNR = 10 \cdot log_{10}(\frac{Nutzsignalleistung}{Rauschleistung})dB$$

6.10. Multipath

Unter eine Multipath versteht man die Ausbreitung von ungerichteten Funkfrequenzen. Solche ungerichtete Funkfrequenzen breiten sich beim Senden in verschiedene Richtungen aus und legen durch Beugung, Brechung, Fading und Reflexion unterschiedlich lange Wege zurück, bevor sie beim Empfänger mit unterschiedlichen Phasenlagen eintreffen. Die einzelnen Phasenlagen der Eingangsfrequenzen bilden sich am Empfängereingang als Interferenzen aus, die sich in starken Feldstärkeschwankungen bemerkbar machen.

6.11. MIMO: Multiple Input, Multiple Output

Das Grundkonzept von MIMO ist Raummultiplex mit einer Vervielfachung der Funkstrecken durch Mehrwegeausbreitung. Die einzelnen Funksignale, die von einem räumlich verteilten Antennen-Array abgestrahlt werden, haben die gleichen Frequenzen und werden als Spatial Streams (SS) bezeichnet.

- Unterstützt mehrere Sende- und Empfängerantennen um das Signal zu Rausch Verhältnis (SNR) zu verbessern
- Unterstützt das Senden mehrere Signalen zur gleichen Zeit

6.11.1. Multi User MIMO

Während in SU-MIMO nur ein Frame mit Zieladresse an einen einzelnen WLAN-Client übertragen werden kann, können in MU-MIMO gleichzeitig mehrere Frames mit unterschiedlichen Zieladressen an mehrere individuelle WLAN-Clients übertragen werden.

- Wird unterstützt ab 802.11ac

6.12. Channel Bonding

Channel Bonding beschreibt das Zusammenlegen mehrere Kanäle in einen grösseren um die Kanalbandbreite zu erhöhen.

6.13. Packet Aggregation

Bei Packet Aggregation werden mehrere Pakete in ein Frame verpackt, damit der Overhead minimiert werden kann.

6.14. Cisco Client Link

Diese Technologie dient zur Überbrückung der Abdeckungslücken von Access Points, die auf unterschiedliche Clients (802.11a/g/n und ac) zurückzuführen sind. Sie verbessert die Zugriffsleistung und Reichweite sowie die Benutzerfreundlichkeit des Wireless-Netzwerks.

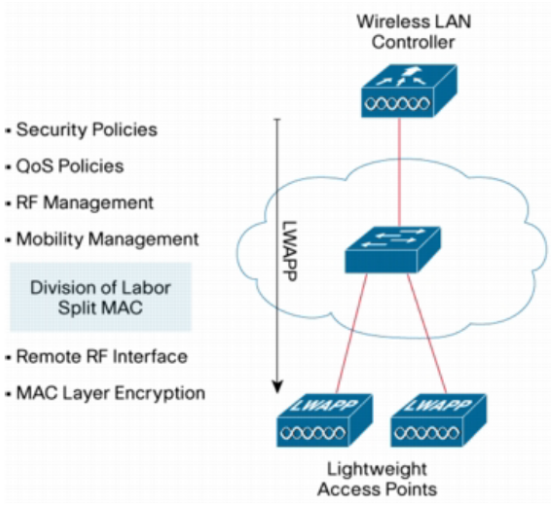


Abbildung 4: LWAPP

6.15. IAPP: Inter Access Point Protocol

Ist ein Protokoll zur herstellerübergreifenden Kommunikation zwischen Access Points. Die Kommunikation der Access Points erfolgt per Multicast.

6.16. LWAPP: Lightweight Access Point Protocol

Ist ein Protokoll welches es erlaubt, mehrere Access Points auf einmal zu konfigurieren. Dabei gibt es einen WLAN Controller der die Konfiguration Frames auf die anderen Access Points verteilt. Der Einsatz eines Controllers bietet zudem den Vorteil, dass sich alle Clients zuerst ihm Autorisieren und somit eine unterbrechungsfreies Roaming möglich ist.

7. Switching

7.1. Spanning Tree Protokolle (STP, RSTP)

- Wird eingesetzt um Broadcast Storms zu unterbinden. Layer 2 Loops werden aufgelöst.
- Unter RSTP werden im Gegensatz zu STP nicht nur BPDU versendet wenn solche auf dem Root Port empfangen werden, sondern alle n-Sekunden gemäss der Hello-Time. (default 2s)
- Werden unter RSTP 3 BPDU nicht mehr empfangen, wird die gegenüberliegende Bridge als offline betrachtet.
- RSTP ist rückwärtskompatibel

7.1.1. Begriffe

STP Spanning Tree Protocol

RSTP Rapid Spanning Tree Protocol

BPDU
Bridge Protocol Data Unit

Root Port
Der Port mit dem kürzesten Weg zur Root Bridge. Die Root Bridge selbst besitzt keine Root Ports ist jedoch zuständig für die angeschlossenen Segmente und versendet daher die BPDU für die angeschlossenen Segmente.

Designated Port
Der zuständige Port für ein Segment

Bridge ID
8 Oktett = 2 Oktett Priorität + 6 Oktett MAC-Adresse

7.1.2. Ablauf

Spanning Trees werden immer pro VLAN aufgebaut. Grundlegend geschieht dies jedoch gemäss folgendem Ablauf:

1. Auswahl einer Root-Bridge (kleinste Bridge ID)
   a) jede Bridge hat alle Port im Blocking Mode
   b) jede Bridge geht davon aus selber Root Bridge zu sein
   c) versendete Configurations-BPDU mit Root-Path Kosten = 0
2. Kürzesten Weg zur Root Bridge berechnen
   a) Aufsummieren der Path Costs in Richtung Root Bridge
   b) Kosten sind in der Regel von der Interface Geschwindigkeit abhängig
3. Für jedes Segment wird die Designated Bridge ausgewählt
   a) Die Designated Bridge ist die Bridge mit den geringeren Kosten zur Root Bridge
4. Root Ports werden gesetzt
   a) Port mit kürzestem Weg zur Root Bridge sind Root Ports
5. Alle anderen Ports gehen in den Blocking Mode

7.2. Virtual LAN (VLAN)

7.2.1. Begriffe

Trunk Port
Leitet den Verkehr mehrerer VLAN durch (tagged)

Access Port
Leitet den Verkehr von genau einem VLAN durch (untagged)

Native VLAN
Frames ohne Tag werden standardmässig über das Nativ VLAN übertragen. Dieses ist per default das VLAN1

- Logische Workgroups innerhalb eines Netzes, auch wenn die Teilnehmer nicht physisch am gleichen Netz angeschlossen sind.
- VLAN ID's werden in der VLAN Datenbank abgelegt (show vlan)
  - 1 - 1005: Normal Range
  - 1005+ = Extended Range

7.3. VLAN Trunking Protocol (VTP)

- Arbeitet auf Layer 2
- Überwacht die VLAN Konsistenz
- Managed das Hinzufügen, Löschen und Umbenennen von VLAN innerhalb eines Netzwerks.
- Erkennt Misskonfigurationen
- Änderungen an einem Switch werden an alle anderen propagiert. (ACHTUNG: Switch mit höchster Configuration Revision Number gilt als Master Konfiguration. Hat der neue Switch die höchste Nummer, wird dessen default Config an alle anderen Switches verteilt)

8. Routing

8.1. Grundlagen

- Routing kann allgemein als den Prozess des Weiterleitens eines Pakets bezeichnet werden. Router schauen dabei nur auf den Netzteil einer IP-Adresse.
- Für die Kommunikation zwischen zwei autonomen Systemen (AS) werden Routing Protokolle wie BGP eingesetzt. (Internet ⇒ EGP: Exterior Gateway Protocols)
- Für die Kommunikation innerhalb eines autonomen Systems (AS) werden Routing Protokolle wie OSPF, EIGRP, IS-IS und älteren Netzen RIP, IGRP eingesetzt (Intranet ⇒ IGP: Interior Gateway Protocols)
- Ein Routing Protokoll muss stehts über die Erreichbarkeit andere Router informiert sein. Zudem soll es den optimalen Weg zu einem Netzwerk finden und Änderungen im Netzwerk erkennen und die nötigen Anpassungen vornehmen.

8.2. Routing Tabellen

Pakete die an unbekannte Netzte gerichtet sind, werden per default einfach verworfen. Deshalb wird meistens als letzter Eintrag eine Default Route (0.0.0.0/0) eingetragen. Liegen mehrere Netze hinter einem Router werden diese meist in einem generischen Eintrag zusammengefasst. Ebenfalls können zwei Routen zum selben Ziel mit den gleichen Kosten eingetragen werden, um die Last auf den beiden physikalischen Verbindungen zu verteilen.

```
1 R     172.16.8.0  [100/118654] via 172.16.7.9, 00:00:23, Serial0
```

1. Wie wurde der Eintrag gelernt (Statisch, Routing Protokoll)
2. Zielnetz
3. administrative Distanz / metrische Distanz
4. Next Hop
5. Alter des Eintrages (Stunden:Minuten:Sekunden)
6. Interface auf welchem das Paket raus soll

8.3. Static Routing

Eine statische Route wird auf einem Cisco Router wie folgt eingetragen.

```
1 ip route <net address> <subnetmask> <next hop> [<costs>]
```

8.3.1. Vorteile

- Keine unnötigen Routing Updates die das Netz belasten
- Sicherer, da Pakete on the Wire nicht geändert werden können

8.3.2. Nachteile

- Statische Tabellen können sehr zeitintensiv beim Installieren / Warten sein
- Topologieänderungen müssen manuell umgesetzt werden. Somit kann es passieren, dass bei eienm Netzausfall solange kein Traffic fliesst, bis jemand manuell eine neue Route eingetragen hat.

8.3.3. Default Routen

Damit nicht zu viele Routen eingetragen werden müssen, macht man insbesondere auf Router die am Rande eines Netzwerkes stehen, sogenannte Default Routen

```
1 ip    route 0.0.0.0 0.0.0.0 192.168.98.1
```

8.3.4. Summary Routes

Mit Summary Routen können mehrere Routen mit einer grösseren Subnetzmaske zusammengefasst werden.

```
1 ip route 192.168.10.0 255.255.255.128 10.10.10.1
2 ip route 192.168.10.128 255.255.255.128 10.10.10.1
3
4 ip route 192.168.10.0 255.255.255.0 10.10.10.1
```

8.3.5. Alternative Routen

Alternative Routen werdne als Backup verwendet, falls eine Verbindung ausfällt. Dazu erstellt man eine alternative Route mit erhöhten Kosten, welche im normalfall nicht gewählt wird.

```
1 ip route 10.1.9.0 255.255.255.0 192.168.128.33
2 ip route 10.1.9.0 255.255.255.0 192.168.96.1  50
```

8.3.6. Load Sharing

Um einen Lastausgleich für eine Verbindung zwischen zwei Router zu erziehlen, werden zwei Routen mit den gleichen Kosten eingetragen. Der Unterschied liegt beim Next Hop.

```
1 ip route 10.1.5.0 255.255.255.0 10.1.6.2
2 ip route 10.1.5.0 255.255.255.0 10.1.7.2
```

8.4. Dynamic Routing Protokolle

8.4.1. Grundlegendes

- Dynamisches Routing basiert darauf, dass jeder Router seine eigene Routing-Tabelle verwaltet und in regelmässigen Abständen sein Wissen an andere Router übermittelt. Natürlich muss ein Router auch auf Informationen von anderen Geräten reagieren können. Das Routing-Protokoll berechnet dabei überall den besten Weg zu einem anderen Netzwerk.
- Zuerst erkennt ein Router seine lokal angeschlossenen Netze. Diese trägt er in seine Routing-Tabelle ein und übermittelt sein Wissen anschliessend an die anderen Geräte. Währenddessen erhält er Informationen von den anderen Router und trägt diese ebenfalls in seine Routing Tabelle ein.

- Die Kosten werden in Hops, virtuelle Kosten, Bandbreite oder Delay gemessen

8.4.2. Distance Vector Protocol

- Ein Distance Routing Protokoll berechnet den schnellsten Weg anhand von Informationen, welch ihm seine direkten Nachbarn mitgeteilt haben. Ein Router weiss wie weit ein anderer Router entfernt ist. Generell lässt sich ein Distance Vector Protokoll mit einem Wegweiser vergleichen. Der Router kennt immer nur den nächsten Schritt/Router, ohne jedoch das Ganze, die Karte/Topologie, zu sehen.
- Routing by Rumor: Ein Router muss sich auf die empfangen Information verlassen und kann diese nicht auf ihre Korrektheit prüfen.
- Gibt es eine Änderung im Netzwerk, wird die gesamte Routing Tabelle an alle Nachbarn verteilt. (RIPv1)

Nachteile

- Router versenden ihre komplette Distanztabelle alle 10-90 Sekunden. Dies verursächt einen beachtlichen Netzwerktraffic in grossen Netzwerken.

8.4.3. RIP: Routing Information Protocol

- Ist ein Routing Protokoll für das Intranet. RIP gehört zu den Interior Gateway Protocols (IGP) und ist technisch von OSPF abgelöst worden. Trotzdem wird RIP noch heute eingesetzt.
- RIPv1 unterstütz nur Classfull Routing. Erst ab RIPv2 wurde Classless Routing eingeführt
- RIP berechnet seine den besten Weg über die Hop Counts.

Berechnung / Distanz Vector Algorithmus

$D^X(Y, Z)$ = Distanz von X nach Y via Z

1. Mittels obiger Formel rechnet jeder Router eine Distanztabelle zu allen anderen Router aus
2. Anhand der Distanztabelle wird dann die Routing Tabelle abgeleitet. Dabei wird einfach der Weg mit den geringsten Kosten genommen.

Üblicher Ablauf

1. Beim Starten eines Routers kennt dieser nur seine direkt angeschlossenen Netzwerke.
2. Der Router trägt die Kosten zu den direkt angeschlossenen Router in seine Distanztabelle ein.
3. Die Kosten zu einem Router der über einen anderen erreichbar ist, wird vorerst als Infinity eingetragen.
4. Der Router erzeugt aus der Distanztabelle seine Routing Tabelle und sendet diese an seine Nachbarn.

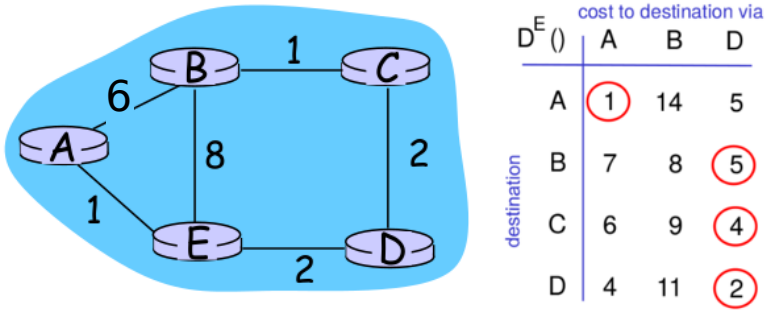


Abbildung 5: RIP Distanz Tabelle

5. Mit den erhaltenen Informationen erweitert er seine Distanztabelle und errechnet damit eine neue Routing Tabelle.
6. Ändern sich die minimalen Kosten, zu denen ein Router erreicht werden kann, wird wieder Schritt 2 ausgeführt.
7. Schlussendlich hat dann jeder die selbe Routing Tabelle.

Probleme

Count-To-Infinity

Ist das Problem unendlichen hochzählens der Pfadkosten. Folgendes Beispiel sollte das Problem näher erklären.

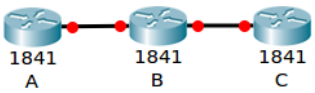


Abbildung 6: Counting-To-Infinity

- In einem Netzwerk mit den Routern A-B-C
- C geht offline
- B markiert C als Offline in seiner Routing Tabelle
- A versendet seine Routing Tabelle mit der Information, dass es C über B erreichen werden kann.
- B updated seine Routing Tabelle mit dieser Information und weiss dabei nicht, dass der Pfad über sich selber geht
- B veröffentlicht nun, dass er einen neue Weg nach C gefunden hat.
- Mit der neuen Information von B updated A seine Kosten nach C mit den Kosten die er von B erfahren hat. Diese beinhalten aber bereits eine Loop
- Die neuen Kosten propagiert A dann wieder nach B
- Der Prozess wiederholt sich bis ins Unendliche.

Lösungen

Split Horizon
Eine Pfadinformation darf nicht über dasselbe Interface veröffentlicht werden, worüber sie empfangen wurde.

Poison Reverse
Wenn der Router A eine neue Route von Router B gelernt hat, veröffentlicht er die Route zurück zu B mit einer Metrik von 16. Damit bekommt Router B nie den Eindruck, dass Router A eine bessere Route zu C kennt.

Triggered Updates
Wenn ein Router eine Änderung in seiner Routing Tabelle detektiert, sendet er sofort (ohne das Update Intervall abzuwarten) ein "Triggered Update". Triggered Updates sind eine Möglichkeit zum ein Count-To-Infinity zu vermeiden.

Holddown Timers
Die Routen werden nicht direkt gelöscht, wenn eine Route als nicht erreichbar detektiert wird. Die Route wird vorerst mit den Kosten von 16 veröffentlicht. Dies führt dazu, dass die Nachbarn über Trigged Updates direkt über den potentiell unerreichbaren Router informiert werden. Damit werden kurze Netzausfälle überbrückt und zu grosser Routing Traffic vermieden. Nach Ablauf des Holddown Timers wird die neue Information übernommen. Neue Informationen werden angenommen und gewartet ob sich die Information bestätigt. (Default 3x30s = 90s) Der Timer wird nur bei schlechten Informationen gestartet. (grössere Kosten) Kommt währende dem Ablauf des Timers eine gute Nachricht, wird der Timer gelöscht.

Request Message
Erlaubt einem neuen Router schnell an die Routing Tabellen seiner Nachbarn zu gelangen.

8.4.4. Link State Protocols

- Beim Link State Protokollen weiss ein Router über die ganze Topoligie des Netzes bescheid.
- Link State Protokolle sind zuverlässiger, einfacher zu debuggen und benutzen weniger Bandbreite als Distance Vector Protokolle. Dafür brauchen Link State Protokolle mehr Speicherplatz (Topologie Datenbank und Routing Tabelle) und CPU Leistung. ACHTUNG: Initial belasten LSP das Netzwerk mehr wie DVP. (Flooding von LSA)
- LSA = Link State Advertisement werden benötigt um Änderungen an der Topology an alle anderen Router zu propagieren.
- Link State Protokolle verteilen im Gegensatz zu Distance Vector Protokollen nie die ganze Routing Tabelle, sondern immer nur einzelne Einträge, die sich geändert haben.

Hello Protocol
Im ersten Schritt lernen alle Router nur ihre Nachbargeräte kennen. Über Keep-Alive Nachrichten (alle 10s) wird sichergestellt, dass der Nachbar noch eingeschaltet ist. Antwortet eine Gegenstelle für 30-40s nicht mehr, wird sie als Down markiert. Für alle diese Funktion wird das Hello Protocol verwendet. Zusätzlich ist das Hello Protocol für die Parameter Aushandlung sowie für die Wahl eines Designated Routers und Backup Designated Router zuständig.

LSA: Link State Advertisements
Bei Änderungen in der Topologie informiert ein Router alle seine Nachbarn über diese Änderungen mittels LSA, welche als Trippel aus [Router_ID, Neighbor_ID, Kosten] bestehen. Jedes erhaltene LSA wird dabei auf allen ausgehenden Interfaces weitergeleitet und in der eigenen Datenbank abgelegt. Ein eingehendes LSA wird nie auf dem gleichen Interface veröffentlich, auf dem es reingekommen ist. Damit das Flooden nicht unendlich lange dauert, gibt es Sequenznummern innerhalb des LSA. Bereits erhaltene LSA werden nicht mehr weiter geleitet. Eine Sequenznummer ist 32Bit gross. Wird ein Router neu gestartet sendet er LSA mit der Sequenznummer 0, worauf die benachbarten Router ein LSA mit seiner letzten Sequenznummer senden.

Topologie Datenbank
Alle gesammelten Informationen aus den LSA werden in der Topologie Datenbank abgespeichert. Die Topologie Datenbank beinhaltet alle Routen zu eine Ziel, wohingegen die Routing Table nur die "besten"Routen zum Ziel speichert.

Kürzesten Pfad berechnen
Nachdem alle Tabellen verteilt wurden können die Kosten auf jedem Router berechnet werden. Dazu wird mittels Dijkstras Algorithmus ein Baum mit minimaler Länge berechnet.

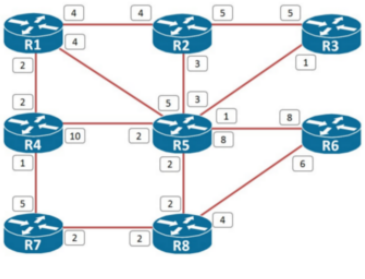
8.4.5. Dijkstras Algorithmus / Shortest Path First

1. Alle Router initialisieren sich selber als Root und fügt sich mit den Kosten 0 in den Tree ein.
2. Von dem Router, welcher zuletzt dem Tree hinzugefügt wurde, werden alle direkten Nachbarn mit den jeweiligen Kosten in Form eines Trippels <FROM_ROUTER>, <TO_ROUTER>, <COST> in die Kandidatenliste geschrieben

   Ist das Ziel eines Kandidaten bereits im Baum oder ist gibt einen anderen Kandidaten mit gleichem Ziel, aber geringeren Kosten, wird der Kandidat gestrichen.
3. Danach werden die Kosten kumuliert, von der Root aus berechnet.
4. Die kürzeste Variante der berechneten Kosten wird dem Tree hinzugefügt. Achtung: Die Kosten im Tree entsprechen nicht den kumulierten Kosten sondern den Kosten von Router A nach Router B.
5. Alle übrigen Kandidaten werden für die nächste Iteration übernommen.
6. Zu guter Letzt wird wieder bei Schritt 2 begonnen, jedoch ist der Zielrouter der zuletzt zum Tree hinzugefügten Variante der neue Ursprung. Es werden nun alle Kandidaten für diesen Router aufgelistet.
7. Ist nur noch ein Kandidat übrig, wird dieser ebenfalls noch dem Tree hinzugefügt

8.4.6. OSPF: Open Shortest Path First

- OSPF nutzt als Metrik die Bandbreite und das Delay (RIP: Hop Counts)
- Gibt es eine Änderung im Netzwerk, werden nur die Änderungen an die Nachbarn verteilt.
- Ist ein Routing Protokoll für das Intranet



Kandidaten	Kosten von der Wurzel bis zum Kandidaten	Definitiver Baum
		R1, 0
R1, R2, 4 R1, R4, 2 R1, R5, 4	4 2 4	R1, 0
R1, R2, 4 R1, R5, 4 ~~R4, R5, 10~~ R4, R7, 1	4 4 ~~12~~ 3	R1, 0 R1, R4, 2

Abbildung 7: Dijkstras Tree von R1

- Implementiert das Hello Protocol, LSA und Dijkstra
- OSPF Pakete haben die IP Adresse 224.0.0.5 und MAC: 01-00-5e-00-00-05 (ACHTUNG: Multicast Overlapping)
- Bündelt Netze in sogenannte Areas damit das Verteilen einer Topologieänderung nicht zu lange dauert. Das Aufteilen in Areas hat den Vorteil dass die Routing Tabellen kleiner werden und der Rechenaufwand für den SPF Algorithmus geringer wird.

  Ein Router innerhalb der Area kennt nur die Router in seiner Area

  Ein Area Border Router (ABR) kennt die Router beider Areas zwischen welchen er routet und hat zwei Topologie Datenbanken (eine pro Area)
- Area 0 ist die Backbone Area
- Ein Netz kann mit CLI mittels folgendem Command publiziert werden: (ACHTUNG: Inverse Subnetzmaske verwenden)

```
1 Router# network <Netzadresse> <Inverse Subnetz-Maske> area <Area-Nummer>
```

8.5. BGP: Border Gateway Protocol

Das Internet besteht aus autonomen Systemem (AS). Innerhalb eines AS kann jeder Betreiber seine eigenen Routing Regeln umsetzen. Jedes AS besitzt eine eigene Nummer zwischen 1 und 65535. Die oberen Nummern sind dabei für den privaten Gebrauch bestimmt. (64512-65535) Die einzelnen AS sind über BGP verbunden.

Grundlagen

- TCP Port 179
- Path Vector Protocol mit inkrementellen Updates darüber in welchem AS eine IP-Adresse gefunden werden kann.
- Es gibt zwei verschiedenen Tabellen
  1. In der BGP Tabelle sind alle Pfade gespeichert (show ip bgp)
  2. In der Routing Tabelle werden die besten Pfade gespeichert
- Seit BGP4 wird CIDR unterstützt

- Es gibt vier verschiedene Nachrichtentypen
  1. OPEN MESSAGE: Verbindungsaufbau. Neue BGP Session wird geöffent
  2. KEEPALIVE: Session erhalten, wenn keine Updates kommen
  3. UPDATES: Beinhaltet das Routing Update. Initial wird die ganze BGP Tabelle versendet, danach nur noch inkrementelle Updates.
  4. NOTIFICATION: Fehlermeldungen werden hiermit verbreitet.
- Standardverhalten
  1. Interne Netzwerke werden an andere AS nach aussen propagiert
  2. Netzwerke die von anderen AS kommen, werden gelernt und weitergegeben. Dabei wird die eigene AS Nummer dem AS Pfad angehängt.

8.5.1. AS: Autonomes System

Ist ein unabhängiges Netzwerk, welches von einer einzigen Organisation verwaltet wird. Dies kann eine grosse Firma oder ein ISP sein. Innerhalb eines AS wird ein einheitliches Routing Protokoll eingesetzt, welches von der Organisation bestimmt wird. Damit Informationen zwischen zwei AS ausgetauscht werden können, muss ein EGP (Exterior Gateway Protocol) wie BGP eingesetzt werden. Um BGP einzusetzen benötigt ein Unternehmen eine AS Nummer.

8.5.2. Single Homed AS / Ein Standort

Um einen Standort mit dem Internet zu verbinden gibt es drei Varianten:

1. Die einfachste Variante ist die Verbindung zwischen Standort und ISP mittels statischen Routen zu verbinden
2. Eine weitere Variante ist es, dass ein Standort seine interne Netzstruktur via OSPF dem ISP bekannt macht
3. Eine letzte Variante ist es, dem Standort eine private AS-Nummer zu vergeben.

8.5.3. Multi Homed AS / Mehrere Standorte

Hierzu erfolgt die Anbindung ans Internet über mindestens zwei ISP's. Fällt einer der Internetprovider aus, so schaltet der Router automatisch alle Routen, die bisher über diesen liefen, auf die anderen Provider um.

8.5.4. AS-Pfad

Der AS Pfad besteht aus den AS Nummern welche von AS_1 zu AS_n durchlaufen werden. Wird eine Loop detektiert wird das Update ignoriert.

IP Prefix Der IP Prefix wird dem AS Pfad vorgehängt.

8.5.5. Upstream und Downstream AS

Upstream AS sind Netzte welche ein AS mit dem Rest der Welt verbinden. (Provider) Downstream AS sind AS welche an ein AS angeschlossen sind. (Kunden)

8.5.6. Peering und Transit

Unter Peering versteht man den Zusammenschluss, bzw. Weiterleitung von Daten zwischen verschieden Provider. Diese Verbindung werden mittels Verträge geregelt. In der Schweiz ist der grösste "Peering Point"das TIX in Zürich. Ein Peering Point ist ein Ort wo der Datenverkehr direkt von einem AS an ein andere übergeben wird, damit der Verkehr nicht über einen teureren upstream Provider gesendet werden muss.

Transit Transit ist spezielle eine Art von Peering. Dabei bietet ein meist sehr grosser Provider eine Verbindung zu mehreren Zielorten. Dieser Dienst ist Kostenpflichtig

8.5.7. HSRP: Hot Standby Router Protocol

Mehrere pyhsische Router werden zu einer logischen Gruppe zusammen gefasst. Die Gruppe von Router präsentiert sich im Netzwerk dann als ein logischer Router. HSRP wird zur Steigerung der Verfügbarkeit eingesetzt.

8.5.8. Redistribution

Man versteht unter Redistribution der Austausch von Routing Tabellen zwischen einem Interior und einem Exterior Routing Protokoll.

8.6. NAT: Network Address Translation

NAT wird verwendet um lokale Netzwerke mit dem Internet zu verbinden. Lokale IP-Adressen haben keine Gültigkeit im Internet. Der Einsatz von NAT resultierte aus der Adressknappheit von IPv4 Adressen. Der Router schreibt bei ausgehenden Verbindungen seine öffentliche Adresse in den IP Header und merkt sich welche TCP Verbindung zu welchem Client gehört, damit er die Antwortpakete wieder dem richtigen Client zuordnen kann.

DNAT: Destination NAT Mit DNAT können mehrere Dienste unter einer IP angeboten werden (Port Forwarding)

PAT: Port Address Translation Zusätzlich zur IP-Adresse wird auch der Port in die Tabelle geschrieben.

8.6.1. Adresstypen

Inside Local Address Private IP-Adresse die dem Client zugeordnet ist

Inside Global Address Öffentliche IP-Adresse des Routers

Outside Local Address Die IP Adresse eines öffentlichen Hosts wie er im inneren Netz erscheint. Kann gleich wie die Outside Global Adresse sein, muss es aber nicht, da diese beim Router noch umgesetzt werden kann.

Outside Global Address Die IP Adresse eines öffentlichen Hosts wie er spätestens nach dem Router erscheint. (zB. Google 8.8.8.8)

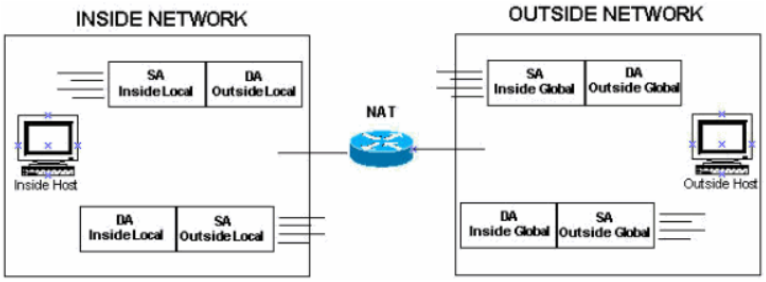


Abbildung 8: NAT Local und Global Adressen

9. Multicasting

Multicasting ist, wenn genau ein Sender IP Datagramme an eine Gruppe von Empfänger versendet. (immer via UDP) Multicast kann im Gegensatz zu Unicast Überlastungen im Netz dadurch reduzieren, dass die IP-Datenpakete nicht einzeln zwischen dem Absender und vielen Empfängern verschickt werden, sondern nur einmal zielgerichtet an alle Teilnehmer gehen. Im Gegensatz zu Unicast ist die Destination Adresse nicht die Adresse des Empfängers sonder einer ganzen Multicast Gruppe.

9.1. Multicast Szenarien

One-to-May Video/Audio Broadcasts, Stocks, Software Verteilung

Man-to-May Multicast Konferenzen, Chat Gruppen

Many-to-One Auktionen, Abstimmungen/Wahlen

9.2. Adressierung

- IPv4: 224.0.0.0 bis zu 239.255.255.255 (Klasse D, Begin mit 1110)
  - Privater Bereich (Link Local): 224.0.0.0 - 224.0.0.255
  - Globaler Bereich: 224.0.1.0 - 238.255.255.255
  - Administrativer Bereich: 239.0.0.0 - 239.255.255.255
- IPv6: FF00::/8
- Pseudo MAC (PMAC): 01-00-5e-00-00-00 bis 01-00-5e-7f-ff-ff
  - Die letzten 23 Bits der IP Multicast Adresse wird für die letzten drei Blöcke der MAC Adresse verwendet (01-00-5e-xx-xx-xx)
  - ACHTUNG: Die ersten 5Bit der IP Multicast Adresse werden nicht beachtet, was dazu führt, dass mehrere IP Adressen ($2^5 = 32$) auf die gleiche MAC Adresse führen.
  - Die MAC Adresse verfügt über 48Bits. Dabei sind 25 fix und die restlichen 23 kommen von der IP Adresse

9.3. IGMP: Internet Group Management Protocol

Mittels IGMP, welches auf Layer 2 angesiedelt ist, kann sich ein Client für eine Multicast Gruppe bei seinem Default Gateway anmelden. Der Router sendet dann regelmässig Anfragen an 224.0.0.1 (Broadcast) ob die Mitglieder einer Gruppe immer noch Mitglieder sein wollen. Seit v2 muss sich ein Client aktiv von einer Gruppe abmelden. (Leave). Stehen mehrere Multicast Gruppen zur Verfügung kann ein Client seit v3 sich explizit für eine Gruppe abmelden (exclude). IGMP kommt (da L2) nur zwischen den Hosts und dem ersten Multicast Router zum Einsatz.

IGMP Snooping Switches merken sich dne IGMP Verkehr

9.4. PIM: Protocol Independent Multicast

PIM ist auf Layer 3 angesiedelt. PIM ist zuständig für die Kommunikation zwischen mehreren Multicast Router. (IGMP meldet Host an Gruppe an und PIM Routet diese Information über mehrere Router) Es ist vollkommen unabhängig von dem darunterliegenden Routing Protokoll. Das PIM-Protokoll stellt zwei Modi zur Verfügung. Welche der beiden Modi verwendet wird, hängt von der verfügbaren Bandbreite und der Aufteilung der Endstationen im Netzwerk ab. Es gibt den Dense-Mode (PIM-DM) mit Flooding-Algorithmus und den Sparse-Mode (PIM-SM), der auf Rendezvous-Punkten basiert.

Dense Mode / PIM-DM Im Dense-Mode sendet die Multicast-Quelle ihren Inhalt an jedes Ziel, bis es sich explizit bei der Gruppe abmeldet. In einer ersten Phase wird das komplette Netz geflooded. Anschliessend wird der kürzeste Pfad genommen und den anderen Router mitgeteilt, dass auf den anderen Pfaden keinen Multicast Verkehr mehr angenommen wird (prune). Diese Betriebsart eignet sich für Multicast-Netze, bei denen das Verhältnis zwischen Teilnehmern und Netzsträngen ausgewogen ist. PIM Dense Mode verwendet den Source Base Tree Ansatz, weil der Tree mittels RPF direkt zum Source Multicast Host aufgebaut wird.

Sparse Mode / PIM-SM Im Sparse Mode wird der Traffic nur an bestimmte Clients gesendet, die auch effektiv in der Gruppe sein wollen. Hierzu baut der Empfänger und der Sender zuerst eine Verbindung mit einem sogenannten Rendezvous Point auf. Der Rendezvous Point stellt dann eine Verbindung als Source Tree zum Sender und eine Verbindung als Shared Tree zum Receiver her.

9.5. Verteilungsbäume

Im lokalen Netz werden Multicast Gruppen mittels IGMP verwaltet. IGMP arbeitet nur zwischen den Hosts und dem ersten Multicast Router. Im WAN sind die Router dafür zuständig, dass sich ein Client einer Multicast Gruppe anschliessen kann. (PIM/DVMRP) Dazu bauen sich die Router Trees auf. Man unterscheidet zwischen einem ”Source Path Tree” und dem ”Shared Tree”. Ersterer benötigt mehr Speicherplatz auf dem Router, erzielt aber optimale Pfade von der Quelle zu allen Empfängern. Bei der zweiten Variante wird weniger Speicherplatz benötigt, allerdings können suboptimale Pfade entstehen.

9.6. RPF: Reverse Path Forward

RPF ist die Technik zur Weiterleitung von Multicast-Datagrammen. Bei dem RPF-Verfahren merkt sich der Router, der die Datenpakete empfängt, die Datenquelle und die Schnittstelle, über die die Daten empfangen wurden. Falls die Schnittstelle den kürzesten Pfad zur Datenquelle besitzt, werden die Pakete an alle anderen Schnittstellen des Routers weitergeleitet. Dabei werden keine bestimmten Multicast-Routing-Informationen benötigt. Es wird also der beste Weg von der Destination zur Source gesucht. Existieren zwei Pfade mit äquivalententen Pfadkosten wird die höhere Next Hop IP Adresse gewählt.

1. Basierend auf der Source Adresse wissen die Router den besten Pfad zum Sender. Sind die Kosten gleich, wird die höhere Next-Hop Adresse gewählt.
2. Es werden Joins zwischen den Router gesendet um den Multicast Tree aufzubauen
3. Ist der Tree aufgebaut können die Multicast Datagramme vom Sender an die Empfänger gesendet werden

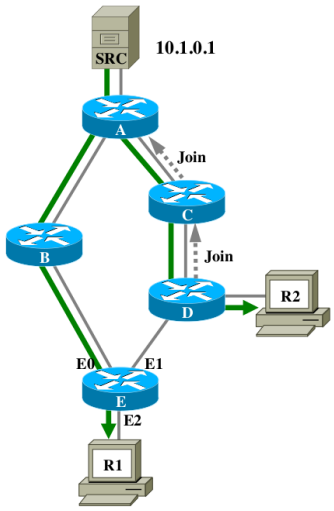


Abbildung 9: Reverse Path Forwarding

10. WAN: Wide Area Networks

Ein WAN verbindet zwei Standorte über einen Service Provider. Wichtig sind dabei folgende Punkte

1. Bandbreite / Delay
2. Sicherheit / Wer hat Zugriff auf das Netz
3. Verfügbarkeit. Sollte mittels SLA festgehalten werden
4. Kosten

Im WAN Bereich wird auf den verschiedenen OSI Layern unterschiedliche Technologien eingesetzt:

- Layer 1:
  - kurze Distanz: DSL
  - weite Distanz: TDM, SDH
- Layer 2:
  - bis 2005: Frame Relay, ATM
  - seit 2005: Ethernet
- Layer 3:
  - seit 2000: IP-Sec / SSL-VPN
  - seit 2002: MPLS-VPN

10.1. Vergleich zum LAN

Bereich	LAN	WAN
Bandbreite	10/100/1000Mbps	64kbps - 20Mbps
Topologien	Extended Star Topology (Mehrer Router miteinander verbunden)	Point-to-Point, Point-to-Multipoint, Any-To-Any
Verfügbarkeit / Redundanz	Normalerweise sehr hoch	Kosten und Nutzen: Wird meist über SLA definiert
Verwaltbarkeit	Sehr gut, alles unter der eigenen Kontrolle	Komplett abhängig vom Service Provider
Kosten per Mbps	100CHF pro Gigabit Port	50-100CHF pro Mbps im Monat
Technologien	Ethernet	Mietleitung (Seriell), Frame Relay, DSL, ATM, SDH, MPLS

10.2. Vergleich Overlay Modell und Peering Modell

Bereich	Overlay Modell (P2P, Frame-Relay)	Peering Modell (MPLS)
Verbindungstyp	Logische End-to-End Verbindung	Any-to-Any IP Routing
Adressierungschema	DLCI	IP Adressen
Kosten	P2P auf L2, Kosten pro Verbindung basierend auf Bandbreite	L2 oder L3 any-to-any wobei Kosten für Zugang zum MPLS Netz basierend auf Bandbreite
QoS	Traffic Shapping	MPLS Traffic Engineering (Header Feld)

10.3. Serial Lines / Mietleitungen

Serial Lines sind gemietete Leitungen welche eine synchrone Übertragung erlauben. Hierbei stellt der Provider meist ein Modem (CPE) zu Verfügung welches mit dem Router (DTE) des Kunden verbunden wird. Dies ermöglicht eine Punkt zu Punkt Verbindung zwischen zwei Standorten. Der Nachteil einer Mietleitung ist, dass sie auch gebraucht wird, wenn keinen Daten übertragen werden. Serial Lines werden mit PPP vermittelt.

10.4. ISDN: Integrated Service Digital Network

ISDN lösste das analoge Public Switched Telephone Network (PSTN) ab, da dieses stark limitiert war. ISDN unterstützt die Übertragung von Daten, Sprache und Video, wobei es mit einer Übertragungsrate von 64kbps für Sprachübertragung optimiert wurde.

10.5. DSL: Digital Subscriber Line

DLS nutzt das bestehende Telefonkabel zur Datenübertragung. Für DSL hat man die Bandbreitenbeschränkung von 3.1kHz, wie sie im analogen Telefonanschlüssen üblich ist, aufgehoben damit die gesamte Bandbreite des Kupfers zur Verfügung steht.

Symmetrical DSL Upload und Download Geschwindigkeiten sind gleich

Asymmetrical DSL Upload und Download Geschwindigkeiten sind unterschiedlich, wobei die Download Geschwindigkeit meist grösser ist.

Tiefpassfilter Signalanteile mit Frequenzen unterhalb der Grenzfrequenz gehen durch, Anteile mit höheren Frequenzen werden gedämpft.

10.5.1. ADSL / VDSL / VDSL2 Vectoring

ADSL: Asymmetric DSL
ADSL und ADSL2 benutzten den Frequenzbereich zwischen 138 kHz und 1,104 MHz, der in den Upstreambereich zwischen 138 kHz und 276 kHz und den Bereich für den Downstream von 276 kHz bis 1,104 MHz unterteilt ist

VDSL: Very High Speed DSL
Die VDSL-Technik wurde speziell für den Einsatz in hybriden Glasfaser-/Kupferkabelnetzen in Zugangsnetzen entwickelt. VDSL arbeitet im Frequenzbereich zwischen 138 kHz und

12 MHz mit Quadraturamplitudenmodulation (QAM). Der Frequenzbereich ist in zwei Upstream- und zwei Downstream-Bereiche unterteilt.

VDSL 2 Vectoring
Ziel von Vectoring ist das Übersprechen in Kupferkabel zu verringern und zu kompensieren um somit höhere Datenraten zu erreichen.

ADSL und VSDL arbeiten auf unterschiedlichen Frequenzbereichen wobei noch zwischen Up und Downstream unterschieden wird. VSDL bietet im Gegensatz zu ADSL zwar einen höheren Durchsatz, ist dafür in seiner Reichweite begrenzt.

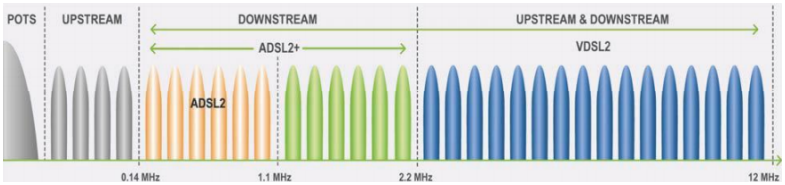


Abbildung 10: Frequenzen POTS/ADSL/VDSL

10.5.2. SDH: Synchronous Digital Hierarchy

SDH moduliert die Daten in Envelopes bestehend aus Reihen und Spalten. Ein SDH Netzwerk ist meistens ringförmig aufgebaut. Es gibt zwischen zwei Nodes in jede Richtung jeweils 2 Fibers (ergo Total 4). Pro Richtung wir jedoch nur eine verwendet. Die zweite Fiber dient einzig der Aufallsicherheit. git

10.6. DOCSIS: Data over Cable Service Interface Specification

DOCSIS ist ein Standard für die Datenübertragung mit Kabelmodems im TV-Kabelnetz, wie es in der Schweiz die Cablecom nutzt. Für Europa existiert ein abgeänderter Standard (EuroDOCSIS) mit einer Bandbreite von 8 MHz im Downstream-Kanal, gegenüber 6 MHz im amerikanischen DOCSIS. Seit DOCSIS 3.0 sind Dantenraten von 100MBit/s möglich. Der Nachteil dieser Technologie ist, dass auf die Bandbreite auf der letzten Meile geshared ist.

10.7. FTTH: Fiber to the Home

Bei FTTH wird anstatt Kupfer optische Glasfaserkabel für die Datenübertragung verwendet. Es existieren zwei FTTH Varianten:

10.7.1. Layer 1

Bei dieser einfacheren, jedoch teureren Variante bekommt jeder Haushalt/Organisation ein eigenes Glasfaserkabel in das Gebäude gezogen.

10.7.2. Layer 2

Hierbei wird eine Haushalt/Organisation an einen Switch in der Verteilzentrale angeschlossen und die Dienste des Service Providers über VLANs getrennt. Ein Provider benötigt maximal 3 VLAN (Data, Video, Voice)

10.8. PPP: Point to Point Protocol

PPP hat die Aufgabe, Punkt-zu-Punkt-Verbindungen zu initialisieren, aufrecht zu erhalten und auch wieder zu beenden. PPP ist für die Authentifizierung, die Aushandlung der Paketgröße, die Vergabe von IP-Adressen und die Verschlüsselung der Daten zuständig. PPP arbeitet auf Layer 2. PPP überträgt verschiedenste L3 Protokolle und ist von diesen unabhängig. Typische Punkt-zu-Punkt-Verbindungen sind Verbindungen in leitungsvermittelnde Netze:

- Wählverbindungen über das analoge Telefonnetz (mit analog-Modem)
- Wählverbindungen über GSM (Mobilfunk)
- Wähl- oder Festverbindungen über ISDN
- serielle Verbindungen
- ATM-Verbindungen (PPP over Ethernet bei DSL)

LCP: Link Control Protocol PPP nutzt LCP zum Aufbau, Konfiguration und Testen einer Datenverbindung

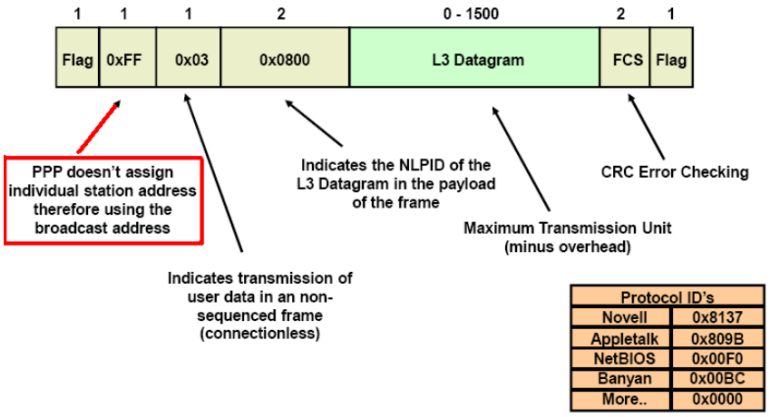


Abbildung 11: PPP Frame

10.8.1. PAP: Password Authentication Protocol

PAP ist ein Protokoll für die Authentifizierung über PPP mittels Benutzername und Passwort. Die Daten werden unter PAP unverschlüsselt übertragen. Ebenfalls gibt es kein Maximum bei den Authentifizierungsversuchen, womit Brutforce Attacken möglich sind.

10.8.2. CHAP: Challenge Handshake Authentication Protocol

CHAP ist wie PAP ein Protokoll für die Authentifizierung über PPP, wobei die Sicherheitslücken von PAP zu verringern.

1. Hat sich der Client eingewählt wird er vom Server zur Authentifizierung aufgefordert. Der Server schickt dazu eine zufällige Zahl (Challenge) an den Client.

2. Der Client bildet aus der Zufallszahl und dem Passwort einen Hashwert (z. B. mit MD5) und überträgt ihn an den Server (Response).

3. Der Server bildet ebenfalls aus der Zufallszahl und dem hinterlegten Passwort einen Hashwert. Stimmt der Hashwert des Clients mit dem des Servers überein wird die Authentifizierung akzeptiert (Accept). Wenn nicht, wird sie abgelehnt (Reject).

10.8.3. PPPoE: Point to Point Protocol over Ethernet

PPPoE ist ein Netzwerkprotokoll, dass PPP Frames in Ethernet Frames verpackt. Es wird für ADSL/VDSL und FTTH verwendet.

10.9. RADIUS: Remote Authentication Dial-In User Service

Radius ist ein Client-Server-basiertes Sicherheitsprotokoll zur Authentifizierung, Authorisierung und zum Accounting (AAA) von Benutzern in einem Netzwerk. Radius arbeitet mit dem Challenge-Response-Verfahren und unterstützt die zentrale Administration von Benutzerdaten. RADIUS arbeitet mit UDP. Möchte ein Client sich im Netzwerk authentifizieren, sendet er einen Request an den RADIUS Server mit Benutzernamen und Passwort. Der RADIUS Server überprüft und Daten und gibt ein Accept (Ip-Adresse und weitere Konfigurationparameter) oder Reject zurück.

10.10. Framerelay

Im Gegensatz zu Ethernet, welches die Daten an alle Teilnehmer Broadcasted erstellt Framerelay eine virtualisierte Punkt zu Punkt Verbindung. Das heisst Frame Realy ist im Vergleich zu Ethernet verbindungsorientiert. FR ist der Versuch Ethernet im WAN zu simulieren. Framerelay arbeitet auf L2 und ist Paket geswitched. Framerelay unterstützt im Gegensatz zu Ethernet QoS. Man unterscheidet zwischen zwei Verbindungstypen:

PVC: Permanent Virtual Circuits Permanente Verbindung bei welcher kein Verbindungsaufbau nötig ist. Dies wird insbesondere in kleineren Netzwerken benutzt

SVC: Switched Virtual Circuits Temporäre Verbindung mit Sessions. Hierbei wird nur bei Bedarf die Leitung genutzt. Sie hat einen Verbindungsaufbau, Transfer und Abbauphase. Dies findet insbesondere in grossen Netzwerken anwendung.

DLCI: Data Link Connection Identifier

- Pro physichen Link kann es mehrere virtuelle Links geben
- Ein DLCI ist die Adresse des virtuellen Interfaces innerhalb des physischen Kabel. Es kann maximal 1024 DLCI pro physisches Kabel geben, da im FrameRelay Header 10Bits für DLCI Informationen vorhanden sind.
- DLCI's haben lokale Signifikanz (zwischen zwei L2 Switches)
- Ist auf einem Switch Port bereits ein DLCI eingetragen, wird für die neue Verbindung einfach die nächst höhere genommen.

10.10.1. Traffic Control (QoS)

Frame Relay hat im Gegensatz zu Mietleitungen eine grössere physikalische Bandbreite. Bei der Mietleitung muss zu viel Traffic gepuffert und zeitversetzt versendet werden. Bei FrameRelay hat es beim Eingang einen sogenannten Shaper. Dieser prüft dass der Kunde sich an die abgemachten Geschwindigkeiten gemäss dem Vertrag (SLA) hält. Falls die Bandbreite überschritten wird, werden die übrigen Daten gepuffert.

CIR: Commited Information Rate
Ist die garantierte Bandbreite innerhalb eines Virtual Circuit unter normalen Bedingungen. Wird diese Schranke übertreten, wird die Pakete mit dem DE Bit (Discard Eligibility) markiert.

EIR: Extended Information Rate
Wird diese Schranke übertreten, werden die Pakete gedropt.

AR: Access Rate
Die effektive physische Bandbreite

BECN: Backward Explicit Congestion
Ist eine Meldung in Richtung Sender, dass ein Frame Relay Knoten überlastet ist. Der Shaper reduziert daraufhin den Traffic. BECN ist Teil von QoS

FECN: Forward Explicit Congestion Notification
Ist eine Meldung in Richtung Empfänger, dass ein Frame Relay Knoten überlastet ist. Der Shaper reduziert daraufhin den Traffic. FECN ist Teil von QoS

10.11. ATM: Asynchronous Transfer Mode

- ATM arbeitet mit Zellen in der Grösse von 53 Bytes
- Wurde für UMTS, ADSL genutzt
- Skalliert schlechter wie MPLS
- Cell-Switching kann aufgrund der fixen Zellgrösse in Hardware umgesetzt werden. Dies ist brachte früher einen grossen Geschwindigkeitsgewinn. Aktuelle Ethernet Software Switches erreichen aber heutzutage gleiche Geschwindigkeiten.
- VPI: Virtual Path Identifier = Identifiziert einen Pfad innerhalb eines ATM Netzwerkes zwischen zwei Knoten und hat wie die DLCI nur lokal signifikanz.
- VCI: Virtual Channel Identifier = Wird für das Multiplexing benögt und erlaub das Unterscheiden mehrere Datenströme. Ist eine Zahl die hochgezählt wird, sobald bereits eine Verbindung besteht.
- VCC: Virtual Channel Connection = Ein VCC ist eine einzelne Verbindung zwischen zwei ATM Endsystemem.
- VPC: Virtual Path Connection = Bündeln mehrere VCI in einem physischen Medium

10.12. MPLS: Multiprotocol Label Switching

- Nutzt das Beste aus Layer 2 (effizient, Traffic Engineering über FEC (Forwarding Equivalence Class)) und Layer 3 (Flexibel, skalierbar) und wird deshalb auch Layer 2.5 Protokoll genannt
- Leitet Pakete aufgrund von Labels weiter (Label Switching). IP Adressen werden innerhalb eines MPLS Netzwerkes nicht nötig
- Wie bei die DLCI bei Frame Relay sind die Labels nur lokal signifikant. Sie können also während dem Transport zwischen Router und Router wechseln.
- MPLS wird von ISP angeboten
- MPLS nutzt BGP um die verschiedenen Router zu synchronisieren

10.12.1. MPLS Router

LSR: Label Switch Router
LSR = Router innerhalb der MPLS Wolke. Wird vom Provider betrieben.

P: Provider Router
Switched Pakete mit Labels im MPLS Netzwerk und ändern allenfalls die Labels (Label Swap)

PE: Provider Edge Router
Setzt (Label push) und entfernt (Label pop) die Labels

CE: Customer Edge Router
Verbindet das Kundennetzwerk mit dem MPLS Netzwerk

Route Target
Pro Kunde ein eindeutiger Identifier

Route Distinguisher
Pro VPN Route wird ein eindeutiger Identifier gesetzt. Normalerweise wird die AS Nummer genommen.

VRF: Virtual Routing and Forwarding
Erlaubt mehrere Routing Tabellen auf einem physischen Router. Dies erlaubt überlappende IP-Netze (Overlapping Networks). Das VRF ist das Label für ein VPN. Zusätzlich kommt auf L3 ein IGP Label hinzu (lokal signifikant)

10.12.2. Ablauf

Bei der Kommunikation von einer Niederlassung zur einer zweiten über MPLS werden folgende Stationen durchschritten:

1. CE Router der ersten Nierlassung leitet den Verkehr an PE Router weiter
2. Der PE Router fügt ein VPN Label hinzu (falls MPLS VPN verwendet wird). Ebenfalls wird anhand der IP-Zieladresse des Pakets ein Destination Label angehängt. Danach leitet der PE das Paket dem LSR weiter.

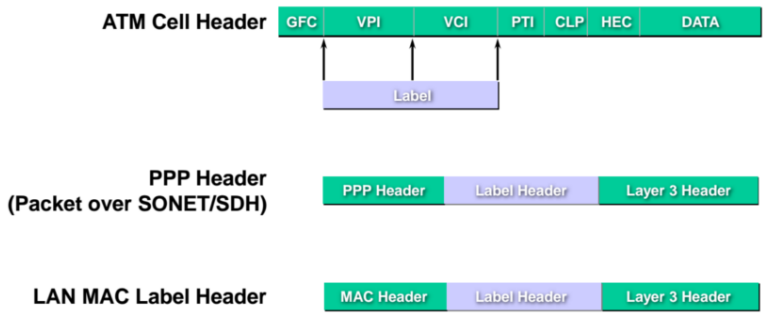


Abbildung 12: MPLS Label für L2 Protokolle

3. Der LSR leitet die Pakete anhand seiner Destination Labels weiter. Sie ändern diese höchstens, da die Labels nur lokal signifikant sind.

4. Beim zweiten PE Router angekommen, wird das Destination Label entfernt und gemäss Destination IP zum CPE geroutet.

10.12.3. LDP: Label Distribution Protocol

Ist verantwortlich über den Austausch der Labels. Es gibt zwei Varianten der Verteilung:

1. Control Driven: Die Labelinformationen werden von Routern bekannt gegeben. Dieses Methode ist schnell, verursacht jedoch Overhead, da sämtliche Routen verteilt werden.

2. Data Driven: Der Pfad wird erst dann aufgelöst wenn wirklich ein Paket mit Label anliegt.

Ein LDP Rooter findet seine Nachbarn mittels dem HELLO Protokoll. Er versendet dabei periodisch UDP Multicast Nachrichten um neue Nachbarn zu erkennen.

Label Distribution Vorgang

1. Traditionelle IP Routing Protokolle bilden Routing Tables

2. Jeder LSR (Label Switch Router) weist unabhängig von anderen LSR's allen Destinations in seiner Routing Tabelle ein Out-Label zu.

3. LSR's geben die zugewiesenen Label Informationen an andere LSR mittels LDP weiter.

4. jeder LSR bildet seine Label Information Base (LIB) anhand der erhaltenen Informationen. Ein Eintrag in der LIB wird FEC (Forwarding Equivalence Class) genannt.

Label Stacking Es ist möglich mehrere Labels einem Paket anzuhängen um so mehrere MPLS Verbindungen in einander zu verschachteln.

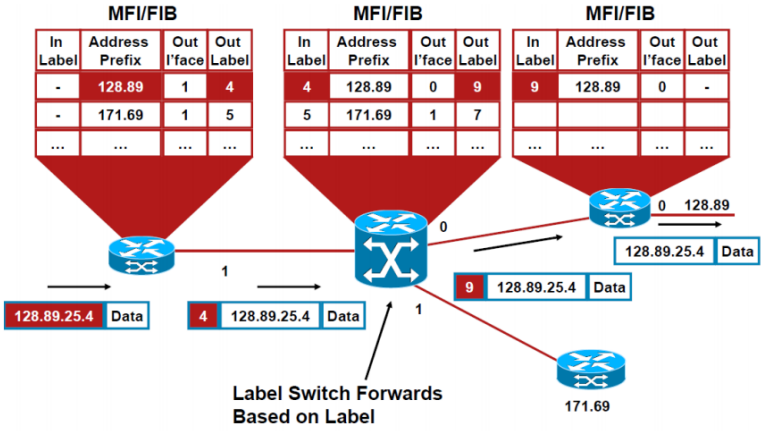


Abbildung 13: MPLS Label für L2 Protokolle

10.13. MPLS VPN

- Im Gegensatz zum klassischen VPN (nur L3) geht eine MPLS Verbindung nicht über das Internet sondern nur über einen einzigen ISP.
- Unterstützt QoS (Quality of Service)
- Ein VPN wird eindeutig mittels Label und VPN-ID identifiziert (VRF)

10.13.1. Layer 2 VPN

Es gibt drei Typen von L2 VPN. Alle benutzen Pseudo Wires mit VC Labels.

1. VPWS: Virtual Private Wire Service (Point to Point)
   a) Layer 2 Tunneling Protocol (L2TP): L2 VPN über IP (Internet)
   b) Any Transport over MPLS (AToM): L2 VPN über MPLS
2. VPLS: Virtual Private LAN Service (Point to Multipoint)
   a) Benötigt MPLS
   b) Nutzt Split Horizon um Loops zu unterbinden

10.14. MPLS QoS

- QoS wird auf Layer 3 in dem Feld DSCP definiert
- Will man QoS auf MPLS machen, muss das DSCP Feld von IP auf das EXP Feld von MPLS gemapt werden.
- Bei Routing Protokollen besteht das Problem, dass immer der beste Pfad genommen wird. Um trotzdem QoS einzusetzen wird als next Hop ein Tunnel angegeben.

10.15. Multiplexing

SDM: Space Division Multiplex
Übertragung von mehreren Signalen über mehrere Übertragungswege

FDM: Frequency Division Multiplex
Gleichzeitiges Übertragen auf unterschiedlichen Frequenzen innerhalb eines Frequenzbandes

TDM: Time Division Multiplex
Die komplette Bandbreite steht einem Kanal für ein bestimmtes Zeitfenster zur Verfügung.

WDM: Wavelenght Division Multiplex
Ist ähnlich wie FDM, wobei das Signal einer speziellen Lichtwellenlänge zugeordnet wird.

OFDM: Orthogonal Frequency Division Multiplex
Bandbreitegewinn durch überlappen der Signale. Jedes Nachbar Signal startet exakt in der Mitte des vorherigen Signals

CDM: Code Division Multiplex
Die Signale werden mit einer unterschiedlichen Codierung übertragen.

11. IPv6

IPv6 ist die Antwort auf die grosse Adressknappheit die unter IPv4 existiert und mittels NAT gelindert aber nicht gelöst wurde. Aktuell sind ca. 10-15% des gesamten Internetverkehrs IPv6.

11.1. IPv4 Transition

Dualstack Hierbei hat ein Client zwei Protokoll Stacks. Einerseits einen IPv4-, und anderseits einen IPv6-Stack. Es wird anhand der der Destination Address entschieden, welcher Stack verwendet wird. Falls beide Protokolle verfügbar sind, wird IPv6 bevorzugt. Der Fallback auf IPv4 bis zu 30 Sekunden dauern kann, wurde der Happy Eyeballs Algorithmus entwickelt. Dieser erlaubt das öffnen von zwei parallel laufenden Verbindungen (1x IPv4 und 1x IPv6). Der Fallback kann somit verkürtzt werden, falls die Webseite kein IPv6 anbietet.

6in4 (Overlay Tunnels) Hierbei wird IPv6 in IPv4 Datgrams gekapselt. (20Byte IPv4 Header, MTU ⇒ Fragmentation)

GRE: Genereic Routing Encapsulation Hiermit lassen sich IP-Protokolle tunneln und somit IPv6 Verbindungen über ein IPv4 Netzwerk umsetzen.

6to4

Hierbei wird die IPv4 Adresse hexadezimal in eine IPv6 "codiert". 6to4 hat immer den IPv6 Prefix von 2002::/16. IPv4 a.b.c.d = IPv6 2002:0a0b:0c0d::

6RD: IPv6 Rapid Deployment

6RD verfolgt die gleiche Idee wie 6to4 mit dem Unterschied, dass sie keinen speziellen Adressbereich (2002::/16), sondern den IPv6 Adressbereich des Providers verwendet. Die 6RD Domain wird so berechnet, dass man den gegebenen ISP 6RD-Prefix verwendet und diesen mit der IPv4 des CE (umgerechnet in Hex) auf /64 erweitert. Ist der Provider Range nicht genau 32 Bits lang, werden die Bits der IPv4 Adresse von rechts nach links genommen.

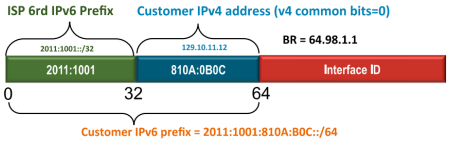


Abbildung 14: 6RD Prefix Calculation

11.2. IPv6 Header

Der IPv6 Header wurde vereinfacht.

- Header length wurde weggelassen, da diese neu fix 40Bytes gross ist
- Die Payload Length definiert die Länge des Payloads inklusive den Extension Headers. Der IPv6 Payload $2^{16} = 65536$Bytes gross sein
- Es wurden nur noch die essentiellen Headers eingefügt. Selten genutze Header können in speziell dafür vorgesehen Extension Headers vor den Payload gepackt werden. Mehrerere Extension Headers werden über das Next Header Feld verlinkt.

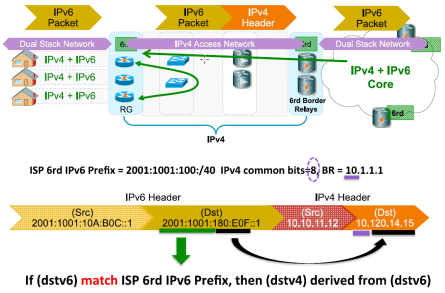


Abbildung 15: 6RD Prefix Calculation

- Fragment Offset wurde weggelassen, da es unter IPv6 keine Fragmentierung mehr gemacht wird. Falls dies trotzdem erwünscht ist, muss es über die Extensions Headers gelöst werden.
- Header Checksum wurde weggelassen, da Fehler auf L3 sehr unwahrscheinlich sind. Dies erlaubt schnellers Routing, da die Checksumme nicht für jedes Paket berechnet werden muss. Fehlerbehandlung wird unter IPv6 nur noch auf L2 und L4(UDP/TCP) gemacht.
- Type of Service (QoS) wurde durch das 8Bit grosse Traffic Class ersetzt. Zusätzlich kann über das 20Bit grosse Flow Label, QoS Parameter übergeben werden.
- IPv6 unterstützt Extensions Headers die dem Basis Header angehängt werden.
- Das Protokoll Feld wurde durch das Next Header Feld ersetzt. Es definiert welches Protokoll auf dem nächst höheren Layer verwendet wird (TCP/UDP). Falls Extension Headers verwendet werden, wird darüber der Verweis auf den nächsten erweiternden Header gemacht.
- Es gibt keine Fragmentierung mehr. Ist die MTU zu gross für einen Link, returniert dieser eine Fehlermeldung (Too Big) dass der Client Pakete mit kleinerer MTU sendet. (MTU Discovery)

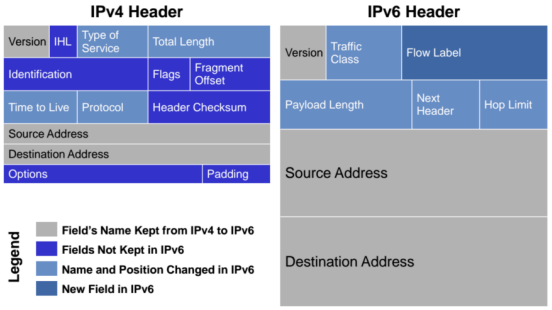


Abbildung 16: IP Header im Vergleich

11.3. Adressierung

- 128Bit lange hexadezimale Adresse (8x16Bit = 8xQuad Nibbles)

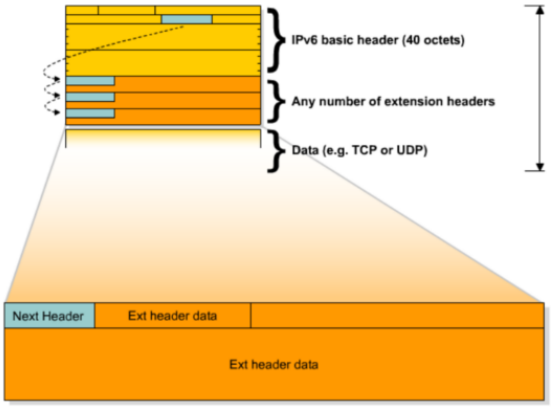


Abbildung 17: Extension Headers

- $3.4 \cdot 10^{38}$ mögliche Adressen
- Leading Zero können weggelassen werden
- Ganze 0-Blöcke können mit einem '::' ersetzt werden. Pro IPv6 Adresse ist nur ein '::' erlaubt, da ansonsten nicht mehr unterschieden werden kann, wo wievielte 0-Blöcke eingesetzt werden müssen.
- Die Loopback Adresse lautet ::1 (= 127.0.0.1)
- Die default Route lautet ::/0 und wird auch als platzhalter verwendet, wenn keine andere Adresse verfügbar ist.
- Normalerweise ist eine IPv6 Adresse wie folgt aufgebaut: Das pendant zur öffentlichen IPv4 Adresse wird Global Unicast Address genannt.
  - 48 Bit Provider
  - 16 Bit Site
  - 64 Bit Host
  - und startet mit 2001::/16 (IANA allocated space)
- Unterstützt auch Anycast Adressen. (one-to-one-of-many / one-to-nearest) Bei Anycast haben mehrere Clients die selbe IPv6 Adresse. Der Sender sendet die Pakete immer an den nächsten Knoten.

11.4. Adress Scopes

IPv6 Adressen werden in drei Scopes unterteilt:

Link Local
FE80::/10 sind Link Local Adressen und werden nicht geroutet. Eine Link Local Adresse ist das pendant für die MAC-Adresse, jedoch auf L3. Diese gilt nur für ein Interface.

Unique Local
FC00::/7 sind Unique Local Adressen, welche nur im lokalen Netz verwendet werden. Sie können nicht geroutet werden.

Global
Global Unicast Adresses sind das pendant zur öffentlichen IPv4 Adresse

11.5. SLAAC: Stateless Address Autoconfiguration

Dient der automatischen Konfiguration von IPv6 Adressen. Ein Host erzeugt sich unter Zuhilfenahme zusätzlicher Informationen sein IPv6 Konfiguration für sein Interface selbständig. Um SLAAC verwenden zu können ist eine Subnetzmaske von /64 nötig. Da SLAAC keine Möglichkeit vorsieht um den DNS Server zu konfigurieren ist diese Variante in der Praxis eher irrelevant.

1. Zuerst wird die Link Local Adresse berechnet (EUI-64):
   a) 7Bit im ersten MAC-Block (U Bit) auf 1 setzen (IEEE administrated).
   b) 8Bit im ersten MAC-Block (G Bit) auf 0 setzen (Unicast Adress)
   c) In der Mitte der MAC Adresse das FF:FE einschieben
   d) Den Link Local Prefix FE80::/10 voranstellen
2. Link Local Adresse wird mittels Neighbor Discovery auf seine Eindeutigkeit geprüft. Ist sie eindeutig wird sie dem Interface hinzugefügt
3. Der Client sendet eine Router Solicitation
4. Bekommt er vom Router eine Antwort (Router Advertisement) verwendet er den Netzteil der Router Source Adresse (/64) als seinen Prefix.
5. Zusätzlich wird die komplette Source Adresse des Router als default Gateway verwendet

11.5.1. EUI-64: Extended Unique Identifier

Hierbei wird die 48Bit lange MAC Adresse genommen und auf 64Bits erweitert, damit sie als eindeutige IPv6 Adresse verwendet werden kann. Dazu wird in der Mitte der MAC Adresse ein "FF:FEëingeschoben. (falls keine Privacy Extension) Zusätzlich wird das 2Bit von rechts im ersten Block (Individual/Group Bit der MAC Adresse) geflipt. Dies erlaubt einer Station sich eine eindeutige IPv6 Adresse zuzuweisen.

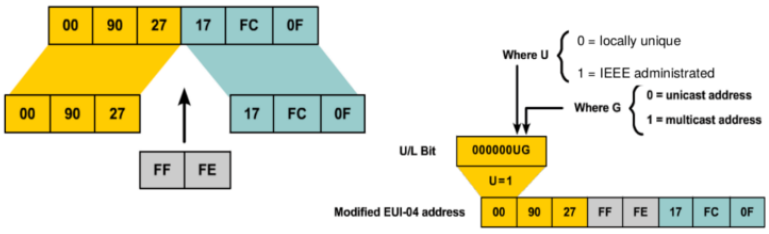


Abbildung 18: EUI-64 Adresse

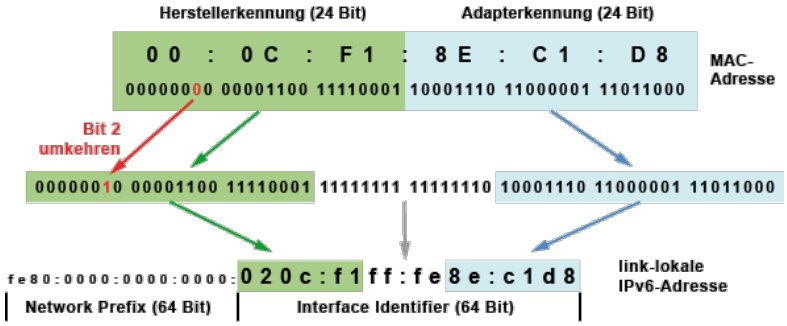


Abbildung 19: Adressumsetzung von EUI-64 in IPv6 Adresse

Privacy Extension Privacy Extensions ist eine Erweiterung SLAAC von IPv6, um IPv6-Adressen zu bilden, die keinen Rückschluss auf die Client MAC Adresse zulassen. Inzwischen gehört die Privacy Extension zum Default in fast allen Betriebssystemen. Die nötigen 64 Bit werden bei der Privacy Extension zufällig generiert. (kein FF:FE) Zum aktuellen NTP-Zeitstempel mit 64 Bit kommt die MAC-Adresse hinzu und dann macht man daraus einen SHA1-Hash mit einer Länge von 64 Bit. Fertig ist der ßufälligeİnterface Identifier.

11.6. DHCPv6

Der Client sendet ein DHCP Request an die Multicast Adresse FF05::1:3

11.6.1. Stateless

Der Client konfiguriert sich eine IPv6 Adresse selbständig und bezieht nur Zusatzoptionen wie z.B der DNS Server vom DHCP.

11.6.2. Stateful

DHCPv6 im stateful Mode ist weitgehend vergleichbar mit der IPv4 Variante, mit dem Unterschied, dass keine Broadcast Adressen existieren, sondern die Multicastadresse FF02::1:2 dafür verwendet wird.

11.7. IPv6 Multicast

- FF00::/8 sind Multicast Adressen (1111 1111)
- Die L2 (MAC) Multicast Adresse wird wie folgt gebildet: 33:33:<letzte 32 Bit der IPv6 Multicast Adresse>

Adress	Scope	Meaning
FF01::1	Node Local	All Nodes
FF02::1	Link Local	All Nodes
FF01::2	Node Local	All Routers
FF02::2	Link Local	All Routers
FF05::2	Site Local	All Routers
FF02::1:FFXX:XXXX	Link Local	Solicited Node

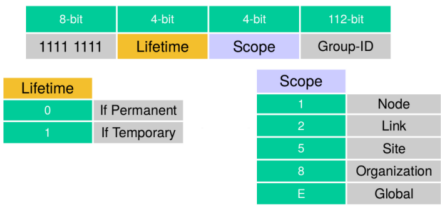


Abbildung 20: Adressumsetzung von EUI-64 in IPv6 Adresse

11.7.1. Solicited Node Multicast Address berechnen

Jede IPv6 Unicast und Anycast Adresse besitzt eine Solicited Node Multicast Adresse. (Diese sind unter "Joined group addressesßu finden)

1. In der Mitte der MAC-Adresse FF:FE einschieben. Die 48Bit lange MAC Adresse wird somit in zwei 24Bit lange Teile unterteilt und um 16Bit erweitert. Das Resultat ist der EUI64
2. Der Adresse ff02:0000:0000:0000:0000:0001:ffxx:xxxx die letzten 24Bit rsp. 6 Hex Zeichen des EUI64 ersetzen.

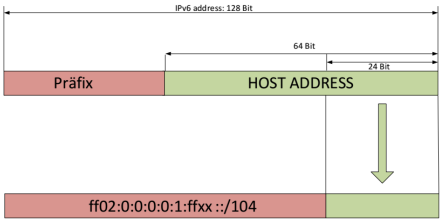


Abbildung 21: Solicited Node Multicast Adress

11.8. Netzwerk Adress Schemas

ULA: Unique Link Local only (nicht empfohlen)
Dieses Schema ist kann man mit dem IPv4 Ansatz vergleichen. Die Adressen sind nur lokal signifikant und werden ins Internet ge-NAT-ed. Dieser Ansatz hat ebenfalls den Nachteil, dass es aktuell keine guten IPv6 NAT Lösungen gibt.

ULA & Global (nicht empfohlen)
Jeder Client hat eine ULA und globale Adresse. Mittels SAS (Source Address Selection) wird bestimmt, welche Adresse für die Kommunikation verwendet wird.

Global (empfohlen)
Alle Clients haben nur eine global ansprechbare Adresse. Einziger Nachteil ist, dass man somit die Netzwerk Topologie nach aussen nicht versteckt.

11.9. Adresszuordnung

Stateless Autoconfiguration Adresszuordnung via SLAAC.

Stateless Autoconfiguration + stateless DHCP DHCP wird verwendet um DNS Informationen zu verteilen

Stateful Autoconfiguration Ähnlich wie DHCP bei IPv4 (Client sendet DHCP Solicit Message an die All-DHCP-Agents Multicast Adresse)

Statische Adresszuordnung Alles manuell

11.10. ICMPv6: Internet Controll Message Protocol V6

ICMPv6 wird verwendet, um folgende Nachrichten zu versenden.

NDP: Neighbor Discovery Protocol Ersatz für ARP (Address Resolution Protocol) unter IPv4 und wird dazu benutzt um IPv6 Adressen in Hardwareadressen (L2) aufzulösen.

RARP: Reverse Address Resolution Protocol Ermöglicht die Zuordnung von Hardwareadressen zu Internetadressen

IGMP: Internet Group Management Protocol Dient der Organisation von Multicast Gruppen. IGMP existiert nur unter IPv4.

MLD: Multicast Listener Discovery Ist das IPv6 Pendant zu IGMP. Es wird also genutzt um Multicast Abonnements zu verwalten.

11.11. Neighbor Discovery / Router Discovery

Mit Neighbor Discovery wird herausgefunden, ob eine IPv6 Adresse unique ist. Mit Router Discovery wird das Default Gateway für eine eine Station evaluiert.

1. ICMP Type Feld 135 = Neighbor Solicitation
   - Ein Neighbor Solicitation Nachricht wird gesendet, um die Hardwareadresse (Link Local Address) eines Nachbars ausfindig zu machen. Die Zieladresse ist dabei die IPv6 Multicast Adresse. (nicht wie bei ARP an die Broadcast Adresse)
2. ICMP Type Feld 136 = Neighbor Solicitation Advertisement. Ist die Antwort auf auf die Neighbor Solicitation und beinhaltet die Link Local Addresse (MAC Pendant) der Station.
   - Die Meldungen werden auch verwendet um herauszufinden ob eine IPv6 Adress unique ist.
3. ICMP Type Feld 133 = Router Solicitation
   - Hiermit bittet eine Station um ein Router Advertisement
   - Ein Client sendet eine RS an die All-Routers Multicast Adresse
   - Werden von einer Station beim Aufstarten versendet, damit nicht auf das nächste Update Intervall gewartet werden muss
4. ICMP Type Feld 134 = Router Advertisement
   - Hiermit machen sich Router im Netz bekannt und verbreiten Informationen für die IP-Autokonfiguration (SLAAC).

- Werden periodisch oder auf Anfrage (Router Advertisement) von einem IPv6 konfigurierten Router Interface an eine Multicast Adresse versendet. (All Node Multicast der Clients)
- Beinhaltet Hop Limit, Router Lifetime (Default Router für max $2^{16}s \approx 18h$), Erreichbarkeits Timeout Preferierter, Auflösuns-Timeout Router (pref), Proxy (ja, nein)
- Auf diese Weise erfahren alle Hosts die Adresse des Default-Routers und die linklokalen und globalen Präfixe.

5. Neighbor Cache: Der Neighbor-Cache entspricht dem ARP-Cache unter IPv4.

11.12. Ablauf

1. Router 1 (2001:db8::1/64) will Router 2(2001:db8::2/64) eine Meldung senden
2. Router 1 berechet die Solicited Node Multicast Adresse von Router 2 (ff02::1:FF00:0002)
3. Router 1 sendet eine Neighbor Solicitation (135) an die berechnete Solicited Node Multicast. Er bittet damit Router 2 um dessen Link Layer Adresse
4. Der Router 2 antwortet mit seiner Link Layer Adresse mit einem Neighbor Advertisement (136)

11.13. DAD: Optimistic Duplicate Address Detection

DAD ist eine Erweiterung von Neighbor Discovery und SLAAC mit dem Ziel dass eine IPv6 Adresse unique ist. Ein Client mit der Source Adresse ::/0 (noch nicht konfiguriert) sendet an **seine** Solicited Node Multicast Adresse eine Neighbor Solicitation und fragt ob die Adresse, die er sich zuweisen möchte, schon besetzt ist.

12. Optische Netzwerke / Fiber

Es gibt 6 verschiedene Bänder (Kabelstandards) mit unterschiedlichen Wellenlängen die sich in der Dämpfung und somit in der Reichweite unterscheiden. Je höher die Dämpfung, desto kleiner ist folglich die Reichweite. Ein optisches Kabel darf nicht zu viel gebogen werden, da ansonsten der Winkel der Lichtwelle so spitz wird, dass das Signal in den Mantel durchgeht. Der Winkel, wie eine Lichtwelle auf den Mantel aufprallt, muss so gewählt sein, dass die Welle vom Mantel reflektiert wird. In ein optisches Kabel darf niemals hinein geschaut werden.

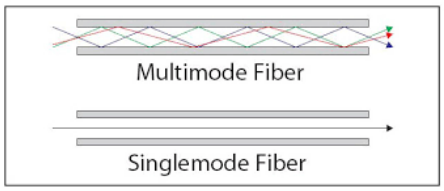


Abbildung 22: Singlemode und Multimode Fasern

Brechungsindex
Der Unterschied zwischen dem Brechungsindex vom Glas und dem Mantel sollte möglichst gross sein. Dies unterstützt eine Totalreflexion welche für die verlustfreie Übertragung der Daten nötig ist.

Multimode Fiber
Multimode Fiber erlauben mehr als 500MHz/km und setzen auf mehrere Lichtwellen. In der Schweiz sind zwei Multimode Typen im Umlauf. Der erste Wert ist dabei der Kerndurchmesser und der zweite der Manteldurchmesser.

- $50/125\mu m$ (grössere Distanz aber teurer)
- $62.5/125\mu m$ (wegen grösserer Kernbreite legen die Lichtstrahlen einen grösseren Weg zurück und sind somit grösserer Dispersion ausgesetzt.)

Singlemode Fiber
Singlemode Fiber erlauben mehr als 100THz-km und haben nur eine einzige Lichtwelle die durch einen $9\mu m$ dicken Kern geschickt wird.

Augendiagramm
Je grösser der Abstand in der Vertikalen, desto einfacher kann man zwischen 0 und 1 unterscheiden. Je grösser der Abstand in der Horizontalen, desto mehr Zeit hat man das Signal zu samplen. Die horizontale Verschiebung wird Jitter genannt.

Spleissen Der Prozess des Zusammenführens zweier Glasfasern wird Spleissen genannt.

Dispersion
Dispersion hat zur Folge, dass ein Signal unscharf wird. (Verbreiterung des Pulses) Je grössere die gewünschte Bandbreite, desto schneller setzt die Dispersion ein. Bei kleineren Bandbreiten können daher grössere Distanzen überwunden werden.

- 2.5Gb/s = 980km
- 10Gb/s = 60km
- 40Gb/s = 4km

Reshaping Unter Reshaping versteht man das verkleinern der Dispersion. Ein verschmiertes Signal wird somit wieder kleiner.

Re-Timing Beim Re-Timing wird die Phasenverschiebung beim Samplen optimiert. Das Sampling ist im besten Fall genau in der Mitte des Signals

PON: Passive Optical Network Architektur
Es gibt eine Faser für mehrere Endkunden, welche dann bei einem Verteiler pro Endkunde aufgeteilt wird. Dabei kann man Fasern sparen, alle Endkunden sind aber von der Verfügbarkeit des Verteilers abhängig.

Point to Point Architektur
Hierbei gibt es eine direkte Verbindung zwischen Provider und Endkunde.

WDM: Wave Division Multiplexing
Mehrere Farben auf eine einzige Glasfaser.

DWDM: Dense Wave Division Multiplex
Dense Wave Division Multiplexing Systeme legen sehr viel mehr Wellenlängen auf ein kleineres Spektrum, was die Gesamtkapazität stark erhöht. Die Kosten von DWDM Systemen sind denn auch deutlich höher.

CWDM: Coarse Wave Division Multiplex
Coarse Wave Division Multiplexing Systeme haben einen grösseren Kanalabstand und können deshalb mit günstigerer Elektronik hergestellt werden. CWDM Systeme überbrücken deutlich kleinere Distanzen als DWDM und werden deshalb von allem im Städte (Metro) Bereich eingesetzt. Ebenso sind die Geschwindigkeiten auf 2.5 Gbps beschränkt.

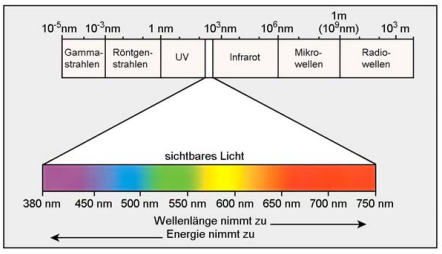


Abbildung 23: Singlemode und Multimode Fasern

$C = \lambda \cdot v$

C = Lichtgeschwindigkeit

λ = Wellenlänge (nm)

v = Frequenz

12.1. Power Budget

Das optische Budget wird in dB gemessen und kann wie folgt berechnet werden. Aus dem optischen Budget kann anschliessend die maximale Kabellänge berechnet werden, indem man das optische Budget durch die Dämpfung (db/km) teilt.

Optical Power Budget (dB) = Power of Sender(dB) − $Sensitivity of Receiver(dB)$

SR: Short Reach = 6dB

IR: Intermediate Reach = 13dB

LR: Long Reach = 26dB

13. Storage Network

DAS: Direct Attached Storage Direkt angehängtes Storage an einem Server. Kann nur von diesem einen Server angesprochen werden.

NAS: Network Attached Storage Ist ein konfigurierbarer Datenspeicher um in einem Netzwerk Speicherplatz zur Verfügung zu stellen. Dabei ist an NAS an keinen Server gebunden, sondern als eigenständige Einheit zu sehen.

SAN: Storage Area Network
Ist ein Datenspeicher Netzwerk in dem grosse Datenmengen gespeichert werden. Das Storage wird vom Server getrennt. Server übertragen die Daten via iSCSI auf Block Level in das SAN.

SCSI: Small Computer System Interface SCSI ist ein Protokoll zur Steuerung der Kommunikation zwischen Massenspeicher und Controller.

iSCSI: Internet SCSI iSCSI ist ein L5 Protokoll, das die Übertragung von SCSI-Befehlen über ein TCP/IP-Netzwerk regelt

LUN: Logical Unit Number Für die eindeutige Identifizierung eines einzelnen SCSI-Gerätes wird die LUN verwendet, welche 64 Bit lang ist

RAID: Reduntant Array of Idependent Disks

- RAID 0: Keine ausfallsicherheit, dafür schnelle Lese und Schreibgeschwindigkeit
- RAID 1: Ausfallsicher, aber teuer, da immer nur die hälfte der verfügbaren Kapazität verwendet werden kann
- RAID 5: Ausfallsicher, je nach Controller aber langsame Schreibgeschwindigkeit. RAID 5 ist eine gute Kombination aus Datensicherheit und Speicherausnutzung (min 3 Platten nötig, wobei nur eine Platte ausfallen darf)
- RAID 6: Sehr ausfallsicher (mindestens 4 Platten nötig, wobei 2 davon ausfallen dürfen)
- RAID 0+1: RAID 0 wird mit RAID 1 gespiegelt
- RAID 1+0: RAID 1 wird mit zweitem RAID 1 via RAID 0 verbunden

13.1. FC: Fibre Channel

FC überträgt SCSI Befehle und Daten in serieller Form in ein SAN. Bei Fibre Channel wird davon ausgegangen, dass es kein Paketverlust gibt

13.1.1. Ports

- N Port (Node): Gerät ist direkt an eine Switched Fabric angeschlossen oder P2P mit einem anderen Gerät
- F Ports (Fabric): F Ports sind immer auf einer Switched Fabric. Ist mit einem N Port verbunden
- E Ports (Expansion): Verbindung zu einem anderen SAN Switch
- L Ports (Loop)

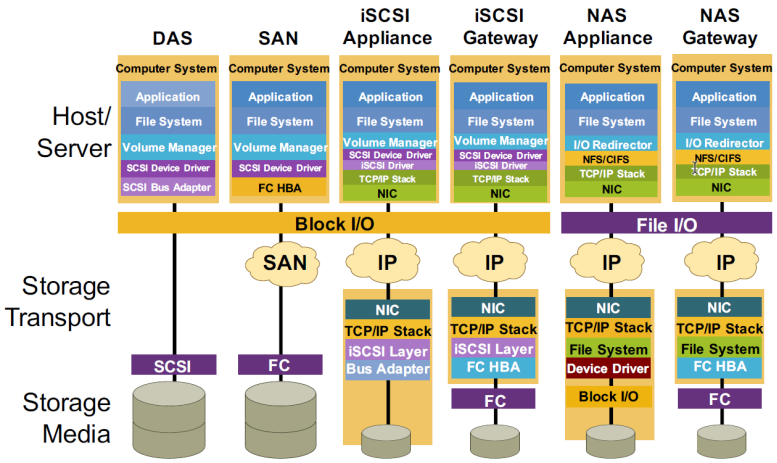


Abbildung 24: Fibre Channel Port Übersicht

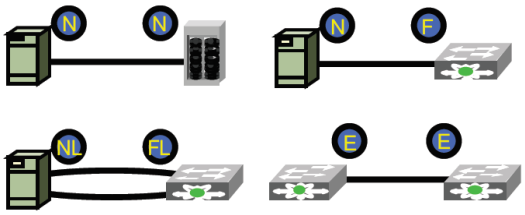


Abbildung 25: Fibre Channel Port Übersicht

13.1.2. Komponenten

- Fabric: Objekt, welches N Port verbindet. Kann entweder Point-to-Point, Arbitrated Loop (bis zu 127 Ports in einem Ring verbunden) oder Switches (bis zu 2^{24} Switches miteinander verbunden) sein
- Fabric Controller (Adresse FF FF FD): Jeder Switch hat einen Fabric Controller. Verantwortlich fü das Verhalten des Fabrics, das Routing und das Setup von Class 1 Verbindungen
- Directory Server / Name Server (Adresse FF FF FC) Ist eine zentrale Registrierungsstelle für alle Fibre-Channel Komponenten innerhalb eines Netzwerks. Ein N-Port hat die Möglichkeit die Informationen aus einem Directory abzufragen.

FLOGI: Fabric Login
Durch das FLOGI meldet sich ein N-Port bei der zuständigen Fabric an. (auf dem F-Port). Der Initiator oder das Target macht sich im FC Netzwerk bekannt und meldet sich beim Nameserver an, damit er für andere sichtbar und erreichbar wird.

PLOGI: Port Login
Das PLOGI ist bevor jeder Kommunikation zwischen zwei N-Ports notwendig. Wird für die Anmeldung eines Initiator beim Target und für die Registrierung am Name Server verwendet. Geht einer Datenübertragung voraus und ist mit einem TCP 3-way Handshake vergleichbar.

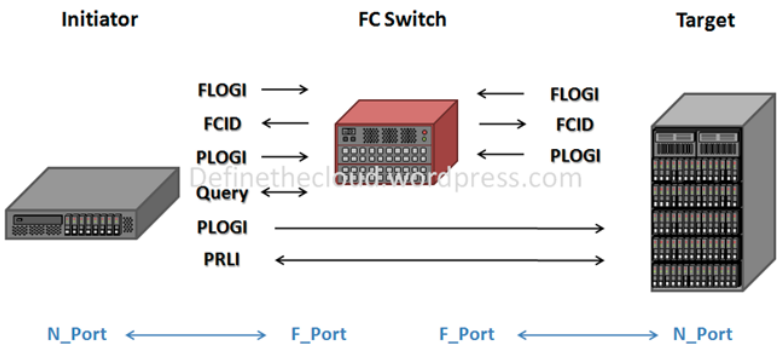


Abbildung 26: Fibre Channel Übersicht

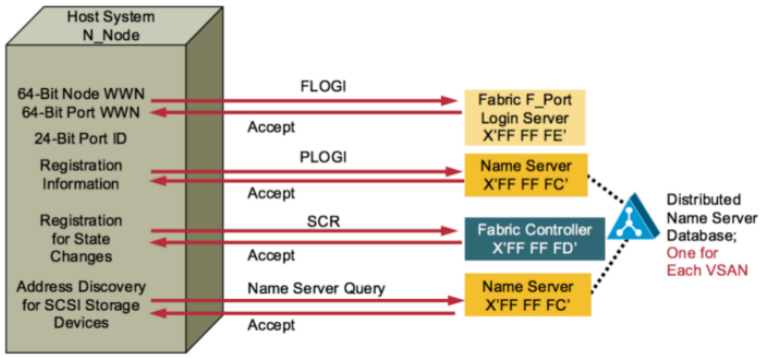


Abbildung 27: Fibre Channel Übersicht

13.1.3. Layers

L0: Physical Interface Definiert die physischen Interfaces Eigenschaften (Kabel, Stecker, Signal Rate)

L1: Transmission Code Definiert wie Eigenschaften Encoded/Decoded übertragen werden

L2: Signaling Protocol Definiert wie Informationen übertragen werden (Frames, Sequenzen, Login Sessions)

L3: Common Services Platzhalter für zukünftige Funktionen

L4: ULP Definiert wie die verschiedenen Protokolle in Fibre Channel gebraucht werden (SCI; IP FICON)

13.1.4. WWN: World Wide Name

Der WWN (World Wide Name) ist eine 64 oder 128Bit lange Kennung zum Identifizieren eines einzelnen Ports.

13.2. Buffer Credits

Pro Netzabschnitt sind eine bestimmte Anzahl Buffer Credits verfügbar. Diese werden beim herausgehen aus dem Interface heruntergezählt und erst beim Ankommen des Tokens zurück zum Ursprungsinterface wieder inkrementiert.

13.3. FSPF: Fabric Shortest Path First

FSPF routet den Traffic gemäss der Ziel Domain Id aus der FCID.

A. Listings

B. Abbildungsverzeichnis

C. Tabellenverzeichnis