

|  |
| --- |
| HTL St Pölten/Abteilung Informatik |
| NVS1 - Netzwerke |
| 4. Jahrgang |

|  |
| --- |
| DI Weixlbaum Martin  V0.3 |

Inhalt

[1 OSI-Modell 1](#_Toc532377309)

[2 Layer 1 (Physical Layer) 3](#_Toc532377310)

[2.1 Übertragung mittels Strom 3](#_Toc532377311)

[2.1.1 Koaxialkabel 3](#_Toc532377312)

[2.1.2 Twisted Pair 4](#_Toc532377313)

[2.1.3 Qualitätsmerkmale der Kabel 4](#_Toc532377314)

[2.1.4 Ethernet-Standards 6](#_Toc532377315)

[2.2 Übertragung mittels Licht 6](#_Toc532377316)

[2.2.1 Verbindungsarten von LWL 8](#_Toc532377317)

[2.2.2 Vor- und Nachteile von LWL 9](#_Toc532377318)

[2.3 Übertragung mittels Funks (WLAN) 9](#_Toc532377319)

[2.3.1 2.4 GHz 9](#_Toc532377320)

[2.3.2 5 GHz 11](#_Toc532377321)

[2.3.3 Übertragungtechniken 11](#_Toc532377322)

[2.3.4 WLAN Standards 12](#_Toc532377323)

[2.3.5 Verschlüsselung und Authentifizierung 12](#_Toc532377324)

[3 Layer 2 (Data Link layer) 13](#_Toc532377325)

[3.1 Zugriffsverfahren CSMA/CD 13](#_Toc532377326)

[3.2 Kollisionsdomänen 14](#_Toc532377327)

[3.3 Physische Adressen (MAC) 14](#_Toc532377328)

[3.4 Frameformate 15](#_Toc532377329)

[3.4.1 Ethernet II (DIX) Frame 15](#_Toc532377330)

[3.4.2 802.3 Frame 15](#_Toc532377331)

[3.4.3 802.3 Frame mit SNAP Header 15](#_Toc532377332)

[3.4.4 VLAN Tag 15](#_Toc532377333)

[3.5 Switching 16](#_Toc532377334)

[3.5.1 Funktionsweise 16](#_Toc532377335)

[3.6 Spanning Tree Protokoll 19](#_Toc532377336)

[3.7 Kanalbündelung 21](#_Toc532377337)

[3.8 802.1X 21](#_Toc532377338)

[3.9 VLAN 22](#_Toc532377339)

[3.9.1 InterVLAN Routing 23](#_Toc532377340)

[3.9.2 VTP 23](#_Toc532377341)

[4 Layer 3 (Network Layer) 24](#_Toc532377342)

[4.1 IPv4 Protokollfamilie 24](#_Toc532377343)

[4.1.1 IP Adressen 24](#_Toc532377344)

[4.1.2 Subnetting 25](#_Toc532377345)

[4.1.3 IPv4 Header 27](#_Toc532377346)

[4.1.4 ARP 28](#_Toc532377347)

[4.1.5 ICMP 29](#_Toc532377348)

[4.1.6 DHCP 30](#_Toc532377349)

[4.1.7 NAT 33](#_Toc532377350)

[4.2 IPv6 Protokollfamilie 34](#_Toc532377351)

[4.2.1 IPv6 Adressen 34](#_Toc532377352)

[4.2.2 IPv6 Header 36](#_Toc532377353)

[4.2.3 NDP 37](#_Toc532377354)

[5 Routing 38](#_Toc532377355)

[5.1 Statisches Routing 38](#_Toc532377356)

[5.2 Dynamische Routingprotokolle 38](#_Toc532377357)

[5.2.1 Einteilung 38](#_Toc532377358)

[5.2.2 Vergleich IGP und EGP 38](#_Toc532377359)

[5.2.3 Vergleich statisches und dynamisches Routing 39](#_Toc532377360)

[5.2.4 Begriffe 39](#_Toc532377361)

[5.2.5 Distance Vector Routing 40](#_Toc532377362)

[5.2.6 Link State Routing 41](#_Toc532377363)

[5.3 EIGRP (Distance Vector) 41](#_Toc532377364)

[5.3.1 Metrik 42](#_Toc532377365)

[5.3.2 DUAL 43](#_Toc532377366)

[5.4 OSPF 44](#_Toc532377367)

[5.4.1 Pakettypen 44](#_Toc532377368)

[5.4.2 Router Typen 45](#_Toc532377369)

[5.4.3 OSPF Algorithmus 45](#_Toc532377370)

[5.4.4 Areas 45](#_Toc532377371)

[5.4.5 OSPF verifizieren 46](#_Toc532377372)

[5.4.6 Metrik 47](#_Toc532377373)

[5.4.7 OSPF in Multiaccess-Netzwerken 48](#_Toc532377374)

[6 Layer 4 49](#_Toc532377375)

[6.1 Ports 49](#_Toc532377376)

[6.2 UDP 50](#_Toc532377377)

[6.3 TCP 51](#_Toc532377378)

[7 Monitoring und Troubleshooting 54](#_Toc532377379)

[8 WAN 54](#_Toc532377380)

[8.1 Punkt zu Punkt Verbindungen 54](#_Toc532377381)

[8.1.1 HDLC 54](#_Toc532377382)

[8.1.2 PPP 54](#_Toc532377383)

[8.2 Frame Relay 54](#_Toc532377384)

# OSI-Modell

OSI steht für *Open System Interconnection* und wurde von der ISO *(International Standards Organisation*) und der ITU (*International Telecommunication Union*) definiert. Es dient zur plattformunabhängigen Einteilung von Kommunikationsservices.

Im OSI-Modell werden die Aufgaben in 7 Schichten eingeteilt, die über definierte Schnittstellen miteinander kommunizieren. Einzelne Schichten können dabei ausgetauscht werden.

Es werden nicht immer alle 7 Schichten implementiert (z.B. TCP/IP-Modell).

|  |  |  |
| --- | --- | --- |
| **Schicht** | **Aufgabe** | **Beispiele** |
| 7 Application Layer | * Netzanwendungen | HTTP (Hyper Transfer Text Protokoll)  FTP (File Transport Protokoll)  DNS (Domain Name Service)  VOIP (Voice over IP  Protokolle: SIP, H323)  IMAP  TFTP (Trivial File Transport Protokoll   SNMP |
| 6 Präsentation Layer | * Zeichenorientiert: * Bit orientiert * Auszeichnungssprache | Zeichenorientiert:   * + ASCII (7 Bit immer gleich,  1 Bit Sonderzeichen für ü,ä,..)   + Unicode   + EBCDIC   Bit orientiert:   * + JPEG-Datei   + GIF-Datei   Auszeichnungsprache:  - HTML |
| 5 Session Layer | * Referenzpunkte an denen die Datenübertragung fortgesetzt werden kann. (Verbindung ist schon hergestellt)  z.B. Falls die Verbindung einmal kurz unterbrochen ist, dass man wieder bei diesem Punkt weiterarbeiten kann und nicht wieder von vorne anfangen muss. |  |
| 4 Transport Layer | * Segmentierung * Verbindungslos/verbindungsorientiert * Verbindungsmanagement (Aufbau, Übertragung, Abbau), * Fehlerkorrektur * Flusssteuerung * Multiplexing | Verbindungslos:  UDP  Verbindungsorientiert:  TCP, SPX |

|  |  |  |  |
| --- | --- | --- | --- |
| 3 Network Layer | | * Logische Adressierung (Gruppenbildung) * Wegewahl (Routing) | Logische Adressierung:  **IP** (Netz ID ist abhängig von der Klasse  32 Bit – Dezimal Darstellung z.B. 10.1.2.3 (4mal 8Bit Blöcke)), **IPX** (Internet Protokoll x – Change von Novell) 32 Bit Netz ID und 48 Bit Host ID, **IPv6** (128 Bit – Hexadezimale Darstellung z.B. abc1:0010:…), **ICMP**, **ARP** |
| 2 Data Link Layer | LLC  (Locical Link Control) | Peer to Peer (Punktverbindung)   * Framing: 0111 1110 (Startbit – 8 Bit) * Flusssteuerung: das nicht zu viele Daten auf einmal kommen (PC mit Router oder Switch) * Fehlererkennung: Erkennung durch Prüfsumme (nach Daten eine Prüfsumme) – schmeißt die fehlerhaften Pakete weg | Startbyte:  0111 1110  Flusssteuerung:  Stop and go Protokolle  Fehlererkennung:  Parity Bit, CRC (99,997% aller Fehler erkennbar) |
| MAC  (Media Access Control) | * Medienzugriffssteuerung (MAC) – Wer darf reden?   - Masterprinzip (einer bestimmt  wer reden darf)  - Nach Zufälligkeit  (CSMA/CD = Carrier Sense  Multiple Access/Collision Detection )   * Physikalische Adressierung (MAC-Adresse) | Medienzugriffssteuerung:  Master Slave  CSMA/CD  CSMA/CA  Token-Passing  L2-Addressierung  MAC-Adresse |
| 1 Physical Layer | | * Übertragungsmedien (Luft, Strom, Licht) * Steckverbindungen * Signalpegel * Übertragungsrate | Übertragungsmedien:  Fiberoptic (Glasfaserkabel)  Twistet Pair (TP)  WLAN, Bluetooth, Infrarot (IR)  Steckverbindungen:  RJ45, DB9, RJ11 (Telefon), RS232 (Serielle Schnittstelle)  Signalpegel:  Manchester-Codierung,  Übertragungsrate:  100 MB = 10 Millionen Bit pro Sekunde (LAN) |

# Layer 1 (Physical Layer)

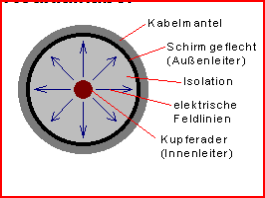
Beim Physical Layer werden **3 Übertragungsmedien** zur Verfügung gestellt:

1. Strom
2. Licht
3. Luft

## Übertragung mittels Strom

Damit die Datenübertragung mittels Strom möglich ist, ist ein elektrischer Leiter notwendig. Dabei kann zwischen **Hochfrequenzkabeln** (z.B.: Koaxialkabel) und **Niederfrequenzkabel** (Twisted Pair (TP)) unterschieden werden.

### Koaxialkabel

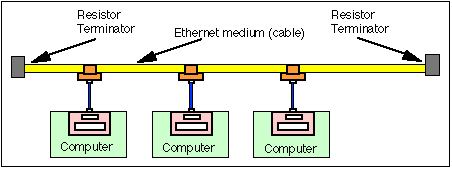
****

Besteht aus:

* **Schirmgeflecht**
* **Innenleiter**

Wurde am Beginn der Ethernet-Verkabelung verwendet, ist aber nicht mehr in Verwendung

Verwendete Topologie: **Bustopologie**



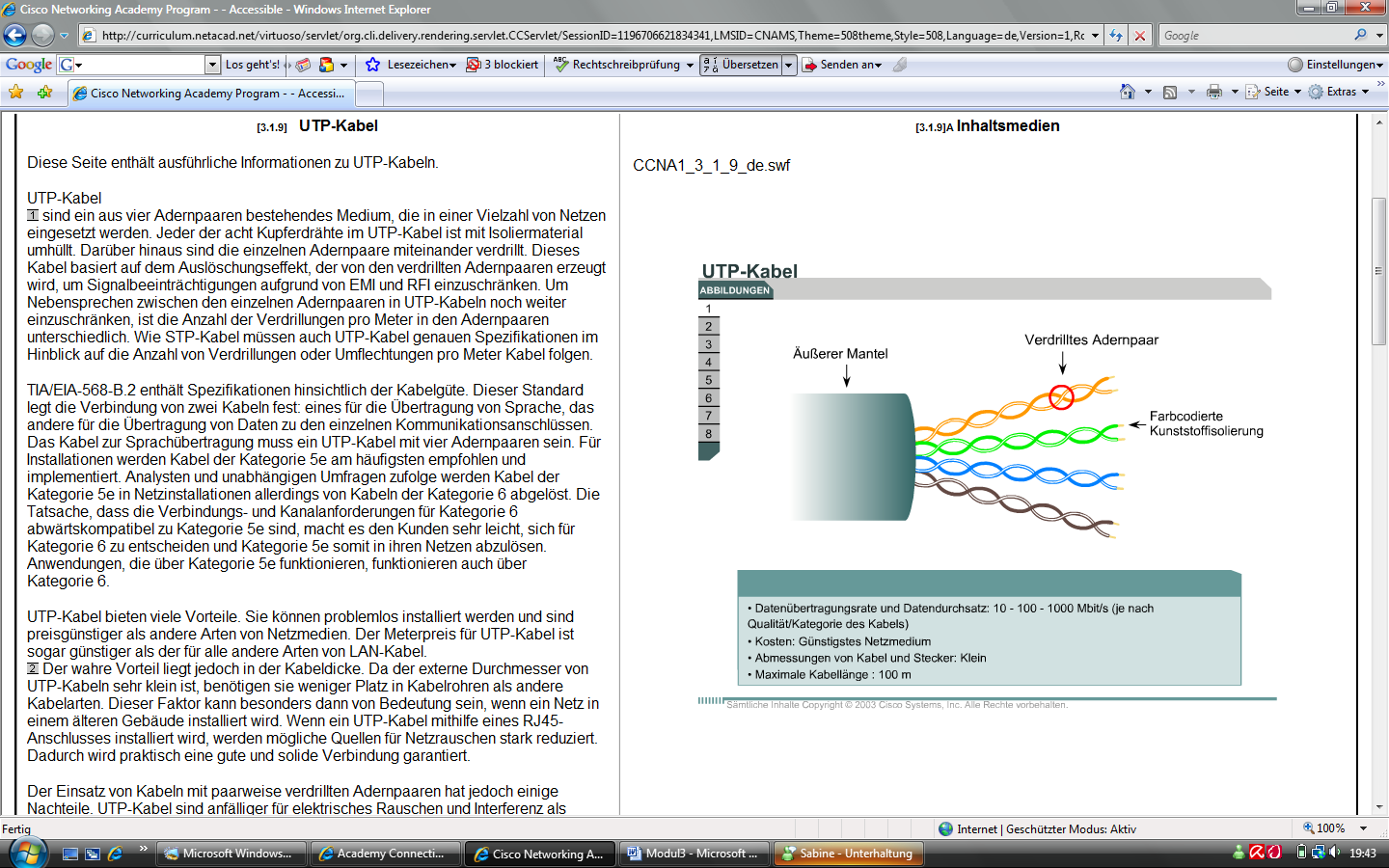
**VT:**

* einfach
* leicht erweiterbar

**NT:**

* sehr fehleranfällig
* wenn ein T-Stück unterbrochen ist, funktioniert das gesamte Netzwerk nicht mehr, da der Abschlusswiderstand fehlt.

### Twisted Pair



Damit das System elektromagnetisch unempfindlicher ist, sind die **Drähte verdrillt** (heben gegenseitig die Magnetfelder auf). **4 Paare (= 8 Adern)** sind verdrillt, die wiederum miteinander als Ganzes verdrillt sind.

**2 Realisierungsvorschläge:**

* **STP** (shilded twisted pair)   
  
* **UTP** (unshilded twisted pair)



Bei einem geschirmten Kabel muss auch der Stecker geschirmt sein! Geschirmt bedeutet, dass ein Schirmgeflecht (Metallfolie) über den Drähten vorhanden ist.

Verwendete Topologie: **Sterntopologie**

**VT:**

* Fehlersuche leichter
* billiges Kabel
* geringe Störempfindlichkeit

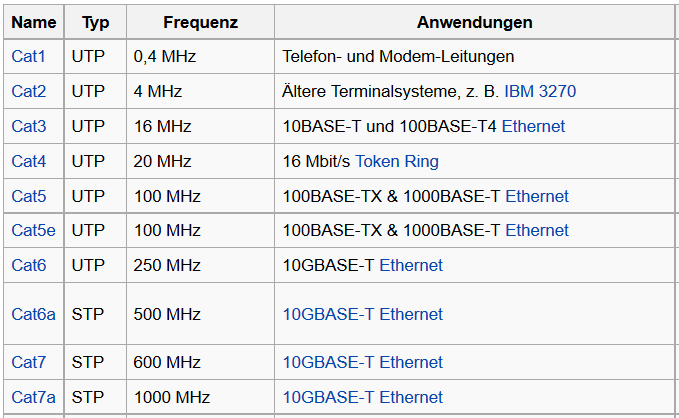
**NT:**

* große Kabellänge ( von jedem PC muss ein Kabel zum Hub, Switch gehen)

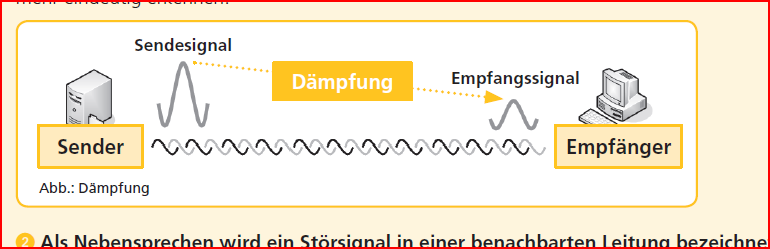
### Qualitätsmerkmale der Kabel

Die Kabel sind in **Kategorien (CAT)** eingeteilt. Die **höchste** **ist 7**. Das Kabel ist umso besser je höher die Kategorie ist.

Qualitätsmerkmale sind unter anderem die Dämpfung, Next, Fext und ACR. Wenn die Kennwerte bis zu einer vorgegebenen Grenzfrequenz unter einem definierten Wert liegen entsprechen sie den Qualitätsanforderungen.



#### Dämpfung

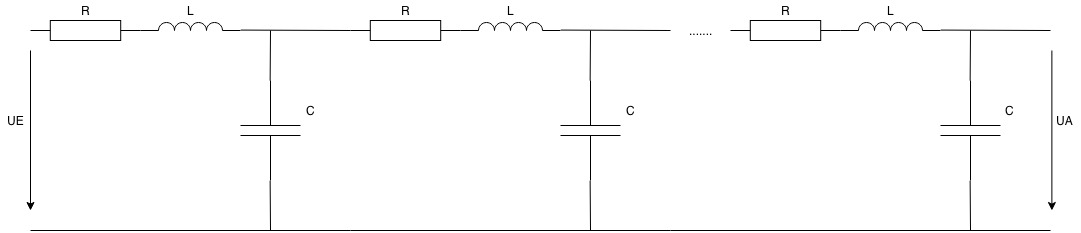
****

Das Signal, das bei der zweiten Netzwerkkarte ankommt (UA), ist schwächer, als das Signal das gesendet wurde (UE). Dies ist für die Übertragungslänge wichtig, dass das Signal stark genug ankommt.

Je länger das Kabel ist umso schwächer wird das Signal und umso flacher (verwaschener) werden die Flanken. Bei zu großer Dämpfung kann es sein, dass die Netzwerkkarte ein falsches Signal erkennt.

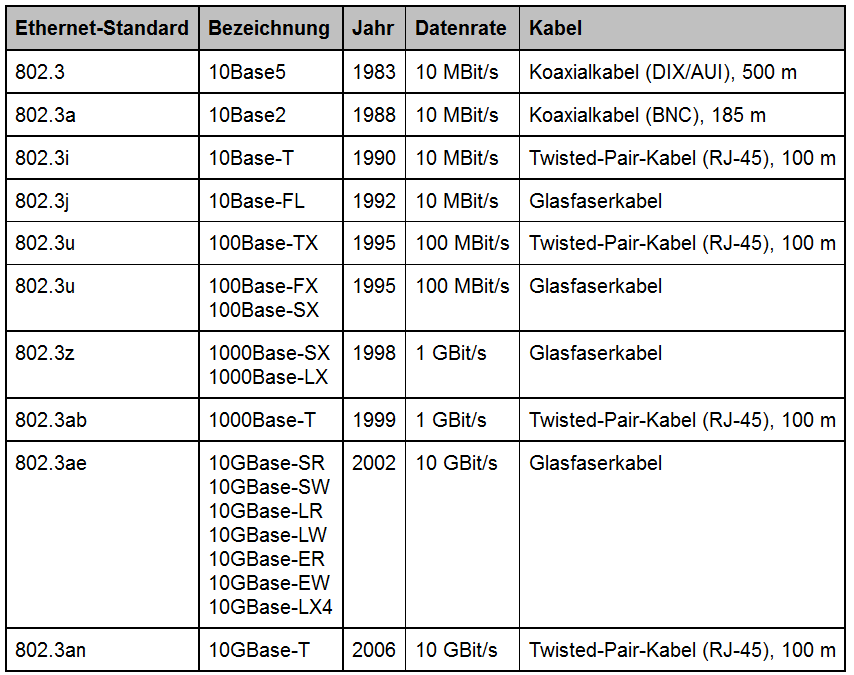
Die Dämpfung berechnet sich als:

Man kann sich ein Kabel als Aneinanderreihung von unendlich vielen RLC-Elementen vorstellen:



Der Widerstand (und somit die Dämpfung) ist daher neben der Länge des Kabels auch von der Frequenz des Signals abhängig.

### Ethernet-Standards

Die Art des Kabels und die jeweiligen Maximallängen ergeben sich aus dem verwendeten Standard. Die Ethernet-Standards werden unter dem Standard **IEEE 802.3** zusammengefasst.

## Übertragung mittels Licht

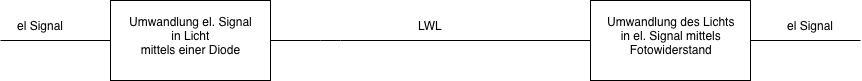
Das zu übertragene Signal wird zur Übertragung aufbereitet (kodiert) und im elektro/optischen

Wandler (LED) in Lichtimpulse umgewandelt. Diese Lichtimpulse werden über den

Lichtwellenleiter zum Empfänger transportiert. Dort werden die Lichtimpulse mittels einer

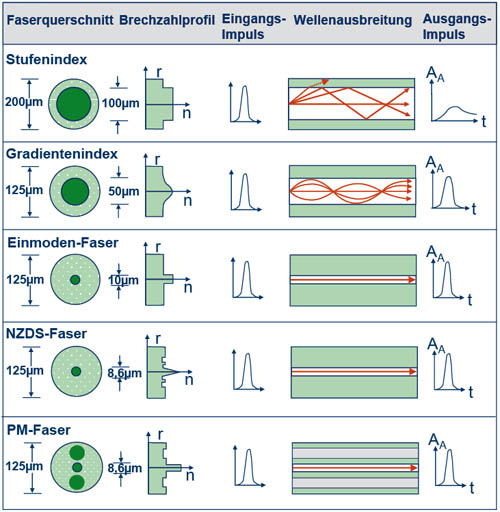
Fotodiode wieder in ein elektrisches Signal zurückgewandelt. Als Strahlungsquellen kommen dabei

Leuchtdioden bzw. Laserdioden zum Einsatz.



Je nach Anwendungsgebiet ergeben sich verschiedene Durchmesser und Verläufe der Brechungszahlen:

* Stufenindexprofil
* Gradientenindexprofil
* Stufenindexprofil (Monomodefaser)



#### Multimode-Faser (Stufenindex-Faser)

Multimode-Fasern haben einen relativ großen Durchmesser   
(> 100 µm). Dadurch können sich mehrere Moden durch die Faser ausbreiten. Solche Fasern weisen eine stärkere Dämpfung und kleinere Bandbreite (< 100 MHz·km) auf; wegen der unterschiedlichen Laufzeiten der verschiedenen Moden tritt eine erhebliche Impulsverbreiterung auf.

Typische Anwendung: Kurze Strecken (< 300 m), heute in der Datenkommunikation nicht mehr verbreitet.

#### Multimode-Faser (Gradientenindex-Faser)

Bei einer Gradientenindex-Faser ändert sich der Brechungsindex allmählich vom Kern zum Mantel hin. Solche Fasern zeichnen sich durch geringe Laufzeitdifferenzen, geringe Impulsverbreiterung und geringe Dämpfung aus; die Bandbreite beträgt < 1 GHz·km.

Typische Anwendung: 50/125-µm- oder 62,5/125-µm-Fasern für lokale Netzwerke (< 500 m).

#### Single-Mode-Faser

Bei einer Stufenindex-Faser haben Kern und Mantel unterschiedliche Brechungsindizes. Der Durchmesser von Single-Mode-Fasern ist sehr gering (< 9 µm). Dadurch kann sich nur eine einzige Mode (Welle) in der Faser ausbreiten. Solche Fasern zeichnen sich durch sehr geringe Dämpfung und große Bandbreite (> 10 GHz·km) aus; wegen der stets konstanten Signallaufzeit der einen Mode tritt außerdem keine Impulsverbreiterung auf.

Typische Anwendung: 9/125-µm-Fasern für Übertragung über große Entfernungen im 1310-nm oder 1550 nm-Fenster.

### Verbindungsarten von LWL

Um zwei Glasfasern miteinander zu verbinden gibt es mehrere Möglichkeiten. Jede davon hat ihre Vor- und Nachteile:

* Steckverbindung
  + große Dämpfung, aber vergleichsweise einfach anzuwenden
  + Eine Übersicht über verwendete Steckertypen finden Sie unter:

<http://www.opternus.de/wissen/kleine-lwl-stecker-lehre.html>

* mechanische Spleiße
  + die beiden gerade geschnittene Enden werden mit einer Hülse verbunden
  + geringere Dämpfung als die Steckverbindung
  + einfache Anwendung, allerdings muss sehr sauber gearbeitet werden
* thermische Spleiße
  + die Enden werden miteinander verschmolzen, dadurch bleibt fast keine Dämpfung
  + Spleißgerät ist sehr teuer

|  |  |  |
| --- | --- | --- |
| SC Stecker | ST Stecker | LC Stecker |
|  |  |  |

### Vor- und Nachteile von LWL

#### Vorteile:

* hohe verfügbare Bandbreiten
* geringe Dämpfung (dadurch hohe Reichweiten)
* störunempfindlich gegen elektromagnetische Strahlen
* Abhörsicher
* Isolation (keine Potentialunterschiede)

**Nachteile:**

* teurer (Werkzeug und Komponenten)

## Übertragung mittels Funks (WLAN)

Im Gegensatz zu einem verkabelten Netzwerk ist ein Funknetzwerk wesentlich flexibler, vor allem wenn es sich um mobile Geräte handelt. Oft ist aber auch eine nachträgliche Verkabelung zu aufwändig oder gar nicht möglich.

WLAN ist im Standard IEEE 802.11 standardisiert. Hier wird u.a. die Übertragungsart, die Übertragungsfrequenz und die max. Sendeleistung geregelt.

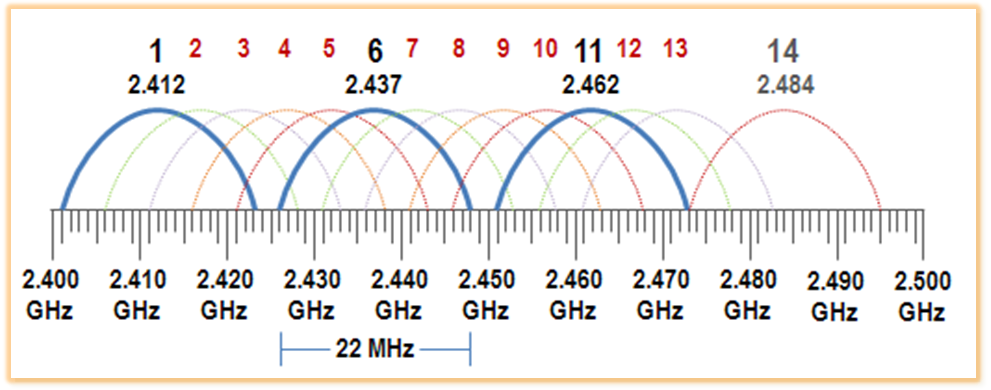
Bei den Frequenzen wird zwischen 2.4 GHz (b, g und n Standard) und 5GHz (a, n und ac Standard) unterschieden. Bei 802.11 kommen nur offene Frequenzbänder zum Einsatz. Diese unterscheiden sich von Land zu Land (auch innerhalb der EU). Für die Einteilung der Frequenzen in Österreich ist das Bundesministerium für Verkehr, Innovation und Technologie ([www.bmvit.gv.at](http://www.bmvit.gv.at/)) zuständig. Entsprechende Geräte müssen für das Land, in dem sie verwendet werden, genehmigt werden!

### 2.4 GHz

In Europa steht das Frequenzband von 2,400 – 2,4835 GHz zur Verfügung. Dieses Band wird in

13 Kanäle unterteilt (vergl. USA → 11 Kanäle).

Da jeder Kanal 22 MHz Bandbreite benötigt, ist eine Überschneidung der einzelnen Kanäle gegeben. Zur Verfügung hat man 83 MHz (2,4835 – 2,4 =0,0835 GHz = 83.5 MHz). Darum können nur 3 Kanäle überlappungsfrei betrieben werden. Bei Verwendung von 40MHz Kanälen sind überhaupt nur zwei Kanäle möglich!



#### Planung

Der Administrator hat dafür zu sorgen, dass sein gesamtes WLAN Netz überlappungsfrei

betrieben wird. Treten Störungen in einem Bereich auf so kann ein Nachbarkanal verwendet

werden.

Aufteilung der Kanäle in einem mehrstöckigen Gebäude:

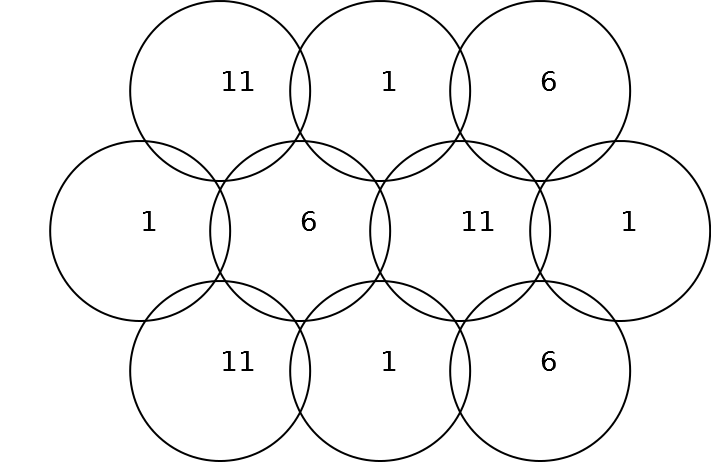
3.Stock 11 1 6

2.Stock 6 11 1

1.Stock 1 6 11

Erdgeschoss 11 1 6

In einer Ebene könnte die Aufteilung etwa so aussehen:



Bei der Plannung eines WLAN's muss mit Hilfe des Gebäudeplans eine Aufteilung der Access Points (AP) geplant werden, damit alle Bereiche möglichst gleichmäßig ausgeleuchtet werden. Danach werden die Kanäle überlappungsfrei aufgeteilt, wobei natürlich auch übereinander liegende Stockwerke beachtet werden müssen. Diese Planung kann mit entsprechender Software unterstützt werden.

Es wird in vielen Fällen nicht möglich sein, eine solche Aufteilung zu realisieren. In diesem Fall werden alle APs mit einer zentralen Steuereinheit verbunden. Diese misst die Belegung der Kanäle jedes einzelnen APs und wählt dann automatisch die passenden Kanäle und Sendeleistungen aus. Dadurch, dass die Sendeleistung der APs reduziert wird, kann die Störung auf die anderen reduziert werden.

Die Steuereinheit kann auch dynamisch auf neue Störungen reagieren (z.B. neues WLAN im Nachbargebäude) und die Kanäle entsprechend anpassen.

#### Sendeleistung

Um die Beeinträchtigung der Gesundheit von Arbeitnehmern (und natürlich Schülern) möglichst gering zu halten, wird die Sendeleistung in Österreich auf max. 100mW begrenzt. Dies ist wesentlich weniger als bei DECT (250mW) und GSM (1W).

### 5 GHz

Da das 2.4GHz Band extrem ausgelastet ist (WLAN, Bluetooth, ...) und es viele Störer (z.B. Mikrowellenherd) gibt, ist es sinnvoll auf das noch relativ freie 5GHz Band auszuweichen.

Im Gegensatz zum 2.4 GHz Band wird eine maximale Sendeleistung von 200mW (in Sonderfällen bis 1000mW!) erlaubt.

Die max. Reichweite ist meist geringer. Allerdings sind 19 überlappungsfreie Kanäle mit 20MHz Bandbreite (bzw. 9 Kanäle mit 40MHz) verfügbar. Damit ist die Planung wesentlich einfacher.

Die eingesetzten Kanäle sind folgendermaßen aufgeteilt (Quelle: http://www.tomsnetworking.de):

Das 5 GHz Band war zu Beginn in Europa noch nicht freigegeben. Dadurch sind hier 2.4GHz Geräte wesentlich häufiger im Einsatz. Bei 802.11n Geräten muss auf die Herstellerangabe geachtet werden.

Die Geräte von Apple (Macbook, iPad, iPhone, …) unterstützen meist 5GHz, allerdings nicht immer in jedem Standard. Beim iPhone 5 ist z.B. 802.11n nur mit 2.4GHz möglich.

### Übertragungtechniken

Um die hohen Bandbreiten kombiniert mit der hohen Störunanfälligkeit zu realisieren werden unterschiedliche Übertragungstechniken eingesetzt:

* **FHSS** (Frequency Hopping Spread Spectrum):  
  während der Übertragung wird ständig die Übertragungsfrequenz geändert.
* **DSSS** (Direct Sequence Spread Spectrum):  
  das Signal wird durch Frequenzspreizung „robuster“ gemacht
* **OFDM** (Orthogonal Frequency-Division Multiplexing):  
  Aufteilung der Information auf mehrere Trägerfrequenzen
* **MIMO** (Multiple Input Multiple Output):  
  gleichzeitige Verwendung mehrer Übertragungskanälen

### WLAN Standards

Die Eigenschaften der verschiedenen Standards werden in folgender Tabelle zusammengefasst. Die angegebenen Datenraten sind maximale Bruttodatenraten. Die tatsächlich erzielten sind teilweise wesentlich geringer.

|  |  |  |  |
| --- | --- | --- | --- |
| Standard |  | Frequenzband | Datenübertragungsraten |
| IEEE 802.11 | 1 | 2,4 GHz | 2 Mbit/s maximal |
| [IEEE 802.11a](http://de.wikipedia.org/wiki/IEEE_802.11a) |  | 5 GHz | 54 Mbit/s maximal |
| [IEEE 802.11b](http://de.wikipedia.org/wiki/IEEE_802.11#802.11b.2Fg) | 2 | 2,4 GHz | 11 Mbit/s maximal |
| [IEEE 802.11g](http://de.wikipedia.org/wiki/IEEE_802.11#802.11b.2Fg) | 3 | 2,4 GHz | 54 Mbit/s maximal |
| [IEEE 802.11n](http://de.wikipedia.org/wiki/IEEE_802.11n) | 4 | 2,4 GHz | 289 Mbit/s maximal (Verwendung von [4x4 MIMO](http://de.wikipedia.org/wiki/MIMO_%28Nachrichtentechnik%29)-Technik) |
| 4 | 5 GHz | 600 Mbit/s maximal (Verwendung von [4x4 MIMO](http://de.wikipedia.org/wiki/MIMO_%28Nachrichtentechnik%29)-Technik) |
| [IEEE 802.11ac](http://de.wikipedia.org/w/index.php?title=IEEE_802.11ac&action=edit&redlink=1) | 5 | 5 GHz | 6933 Mbit/s (Verwendung von [8x8 MIMO](http://de.wikipedia.org/wiki/MIMO_%28Nachrichtentechnik%29)-Technik) |
| IEEE 802,11ax | 6 | 2.4 und 5GHz | 600-9608Mbit/s |

### Verschlüsselung und Authentifizierung

802.11 muss als Funkstandard natürlich besonderes Augenmerk auf Sicherheit im Sinne von Datenverschlüsselung und Benutzerauthentifizierung legen. Die folgenden Sicherheitstechniken können grundsätzlich mit jedem WLAN-Standard verwendet werden.

#### WEP (Wired Equivalent Privacy)

Wurde mit 802.11b verwendet und der verwendete Algorithmus RC4 gilt inzwischen als veraltet. Durch Mitschneiden von wenigen Minuten der Daten kann der Schlüssel reproduziert werden. Es wird mit einem PSK (*pre shared key*) betrieben und beinhaltet keine Authentifizierung.

#### WPA/WPA2/WPA3 Personal

WPA (*Wifi Protected Access*) verwendet ebenfalls RC4. Allerdings werden die Schlüssel dynamisch gewechselt (→ *Temporal Key Integrity Protocol, TKIP*). Wurde als Zwischenschritt eingeführt, um alte (leistungsschwache) Hardware weiterverwenden zu können.

WPA2 (802.11i) verwendet zur Verschlüsselung den sicheren AES (*Advanced encryption standard*) Algorithmus. Das macht leistungsfähigere Hardware notwendig.

Mit WPA3 soll eine Designschwäche von WPA2 entfernt werden wobei die Sicherheit von der Passwortstärke abhängt.

Bei den Personal-Varianten wird ein PSK verwendet. Die Sicherheit hängt vom verwendeten Passwort ab welches auch regelmäßig gewechselt werden sollte. Diese Variante ist für kleinere Netzwerke geeignet.

Jeder der den PSK kennt, kann sich anmelden. Dadurch ist keine Authentifizierung möglich. Die Anmeldungen können eventuell durch MAC-Filter eingeschränkt werden.

#### WPA/WPA2/WPA3 Enterprise

Die Enterprise Varianten verwenden dieselben Verschlüsselungsalgorithmen. Zur Authentifizierung kommt allerdings zusätzlich 802.1x und EAP (*Extensible Authentication Protocol*) zum Einsatz.

Damit können sich Benutzer u.a mit Benutzernamen/Passwort an einem RADIUS-Server (*Remote Authentication Dial-In User Service*, z.B. Windows Server) anmelden. Jeder Benutzer bekommt einen eigenen Sitzungsschlüssel. Die Kommunikation kann damit von anderen nicht abgehört werden.

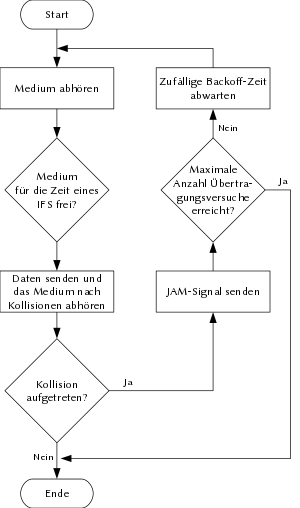
Die Enterprise-Variante ist sicherer, allerdings ist der Aufwand auch wesentlich größer.

# Layer 2 (Data Link layer)

In den 80er Jahren wurde Ethernet entwickelt.   
Ethernet beinhaltet ein Zugriffsverfahren in lokalen Netzen das andere Varianten wie z.B. *Token Ring* gänzlich abgelöst hat.

Entwickelt wurde das Verfahren aufgrund von Ideen von Robert Metcalfe ein Entwickler bei der Firma Xerox im Beginn der 80er Jahre. Unter den Firmen Intel, Xerox und Digital (DIX) wurde es dann zur Marktreife weiterentwickelt und schließlich mit dem Standard IEEE(Institut für Electrical and Electronic Engineers) 802.3 festgelegt.

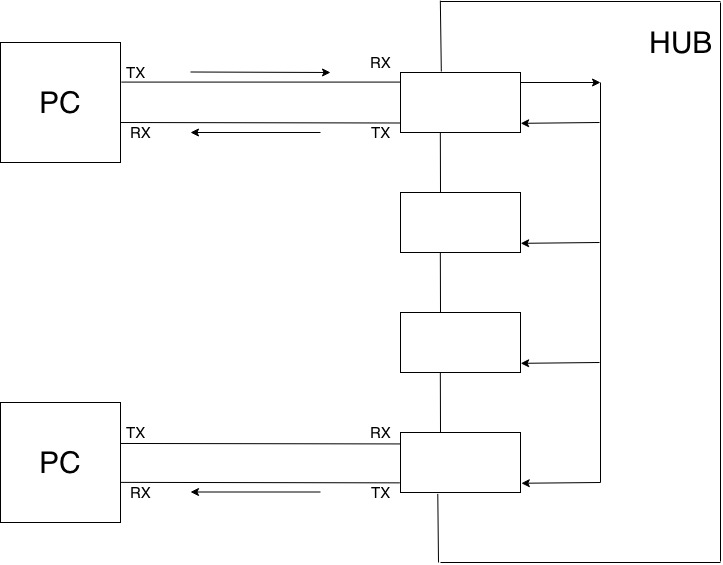
## Zugriffsverfahren CSMA/CD



Bei den Standards 10Base5 and 10Base2 waren nach einer Bustopologie aufgebaut. Das Koaxialkabel ist dabei ein *Shared Medium,* bei dem sich alle Teilnehmer das eine Kabel teilen. Daher muss der Zugriff geregelt werden.

Zu Beginn war das *CSMA/CD* (Carrier sense, multiple access, collision detect).

Der Vorteil ist der einfache Ablauf (kann leicht in Hardware umgesetzt werden) und das keine Steuerungseinheit vorhanden sein muss. Der Nachteil ist,   
dass es kein deterministisches Verhalten hat.

Bei 10BaseT/100BaseT und der Verwendung von *Hub* hatte das Netzwerk zwar physisch eine Sterntopologie, logisch ist es allerdings noch immer ein Bus.

Der Hub diente dabei nur als el. Verteiler. Damit war auch nur *half-duplex* Übertragung möglich. Hubs sind veraltet und nicht mehr erhältlich.

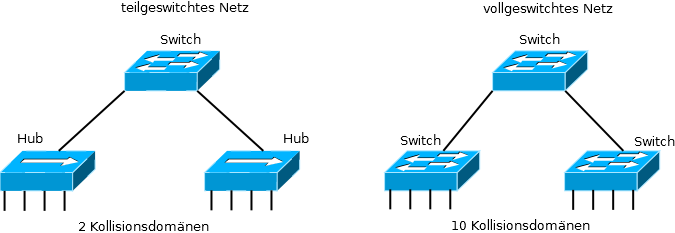
## Kollisionsdomänen

Unter *Kollisionsdomänen* versteht man jenen Bereich, in welchem bei gleichzeitigem Aussenden von zwei oder mehreren PCs, sich die Daten überlagern und dadurch eine Kollision entsteht.

Der erste Ethernet Standard schrieb eine maximale Ausdehnung von 2500m vor. Das ergibt eine Signallaufzeit von 51.2μs. Um eine Kollision garantiert zu erkennen war eine minimale Framelänge von 512Bit bzw. 64 Byte notwendig

Bei 100MBit wurde die maximale Ausdehnung auf 250m reduziert, da man sonst die minimale Framelänge auf 640Byte erweitern hätte müssen.

Die Kollisionsdomäne wird von Switches unterteilt. Bei einem voll geswitchten Netz treten keine Kollisionen mehr auf. Somit hat CSMA/CD keine Bedeutung mehr. Weiters ist damit *full-duplex* Kommunikation möglich!



## Physische Adressen (MAC)

Im Falle von Ethernet-Netzen besteht die MAC-Adresse aus 48 Bit (sechs Bytes). Die Adressen werden in der Regel hexadezimal geschrieben. Üblich ist dabei eine byteweise Schreibweise, wobei die einzelnen Bytes durch Bindestriche oder Doppelpunkte voneinander getrennt werden.

MAC Adressen sind meist weltweit eindeutig und werden durch die IEEE verwaltet bzw. können auch lokal gültig sein (meist Broadcast Adresse).

Typisches Beispiel einer lokal gültigen Broadcastadresse ist FF:FF:FF:FF:FF:FF

Aufbau:



* I/G = 0: Individual-Adresse (Unicast Address), Adresse für einen Netzwerkadapter
* I/G = 1: Gruppen-Adresse (Multicast Address), Ziel-Adresse für eine Gruppe von Stationen
* U/L = 0: universelle, weltweit eindeutige und unveränderbare Adresse
* U/L = 1: lokal veränderbare Adresse

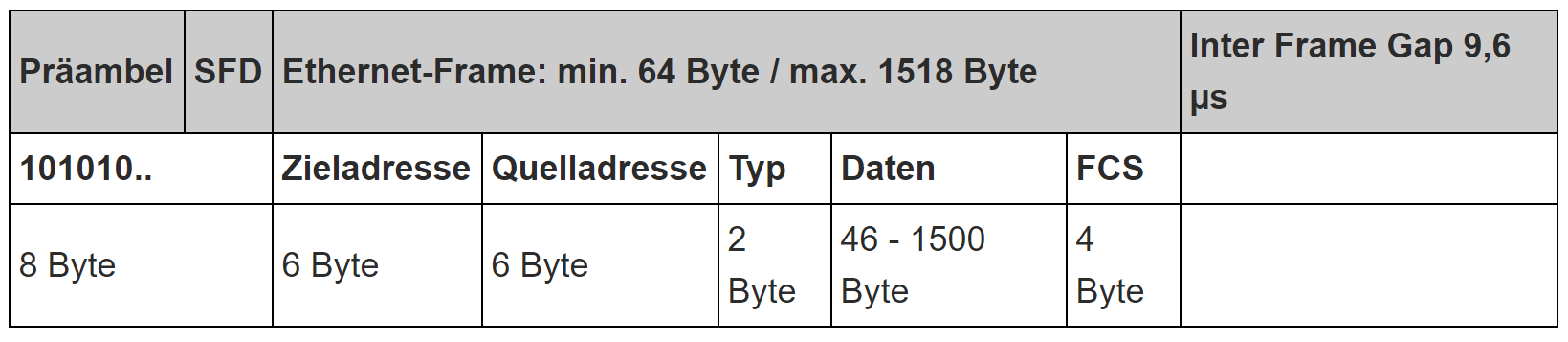
Vom 3. bis zum 24. Bit wird der Hersteller der Netzwerkkarte gekennzeichnet. Man bezeichnet diese Bitfolge als *Organizationally Unique Identifier* (OUI).

Die hinteren 24 Bit, also vom 25. bis zum 48. Bit, bezeichnet man als *Organizationally Unique Address* (OUA). Die darf der Hersteller an seine produzierten Geräten vergeben. Er muss nur dafür sorgen, dass er jede MAC-Adresse nur einmal vergibt.

## Frameformate

Im Rahmen der Entwicklung wurde der Aufbau eines Ethernetframes immer erweitert und angepasst. Im Einsatz sind alle der angeführten Typen.

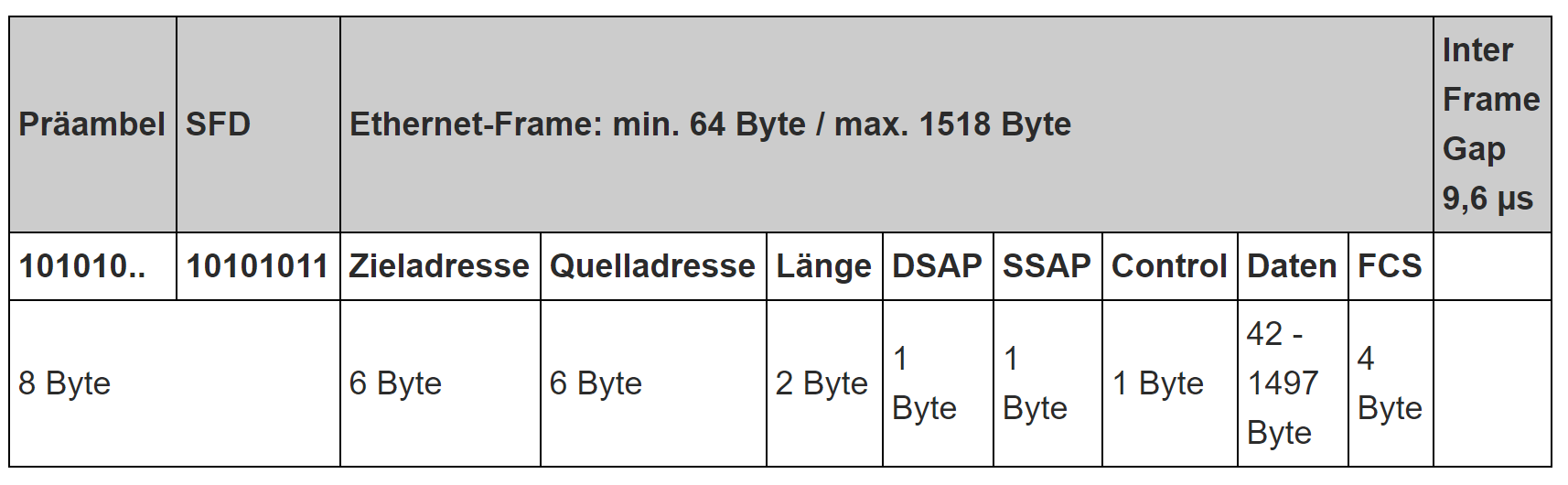
### Ethernet II (DIX) Frame



* Nicht standardisiert
* Kein Längenfeld

### 802.3 Frame

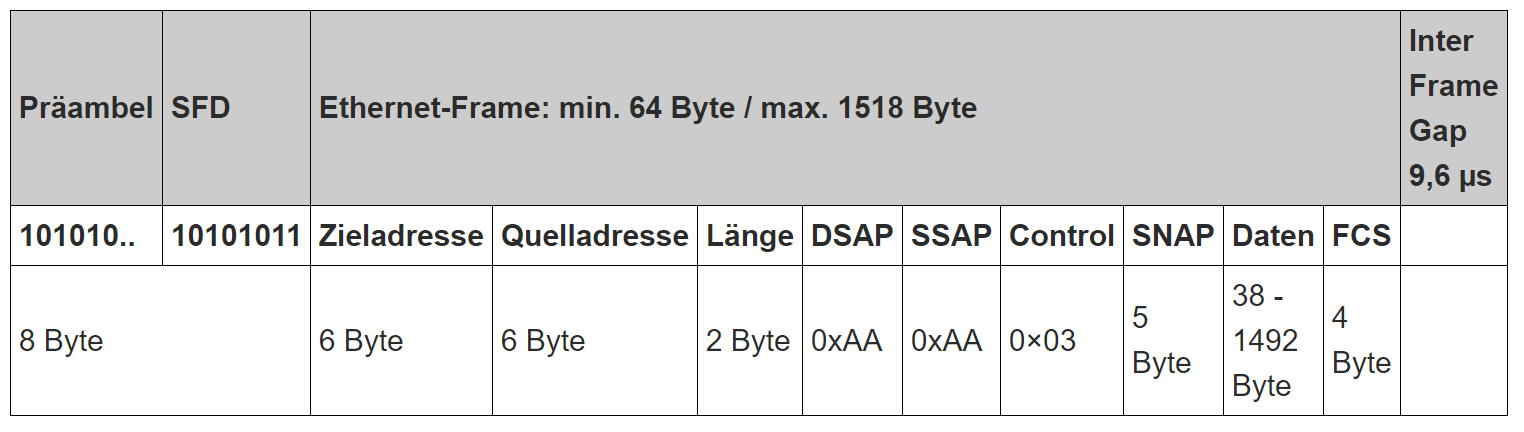
Der Ethernet II Frame bzw. der 802.3raw Frame wurden um einen 802.2 Header erweitert.



DSAP Destination Service Access Point (Sendeprotokoll)

SSAP Source Service Access Point (Empfangsprotokoll), beide müssen gleich sein

### 802.3 Frame mit SNAP Header



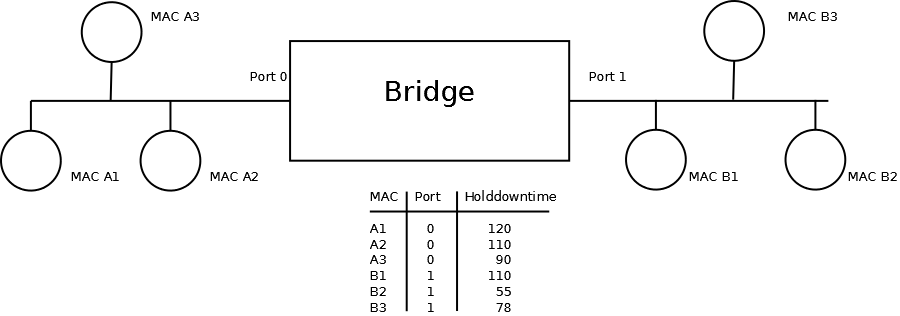
### VLAN Tag

SNAP steht für *Subnetwork Access Protocol* und wird verwendet um am Layer 2 herstellerspezifische Protokolle (z.B. CDP) zu übertragen. DASP und SSAP haben fix den Wert 0xAA.

## Switching

### Funktionsweise

Eine Bridge verbindet zwei Ethernet-Segmente. Dabei wird ein Frame aber nur dann in ein anderes Segment weitergeleitet, wenn der Empfänger dort ist. Dazu muss die Bridge eine Tabelle mit den MAC-Adressen der angeschlossenen Stationen führen.



Der Inhalt der Tabelle wird automatisch „gelernt“. Dazu werden die Source-Adressen der einzelnen Frames ausgewertet.

Die Größe der MAC-Tabelle ist beschränkt, da diese bei jedem Frame durchsucht werden muss. Typisch ist eine Größe von 8000 MAC-Adressen (vgl. Cisco 2950).

Damit keine alten/ungültigen Adressen in der Tabelle bleiben, wird für jeden Eintrag ein Holddown-Timer geführt. Wenn dieser abgelaufen ist, wird der Eintrag gelöscht.

Bei der Verarbeitung der Frames werden verschiedene Betriebsarten unterschieden:

* **Store and Forward**

Bei dieser Betriebsart wird das Paket empfangen, zwischengespeichert und danach

weitergeleitet.

VT: Fehlerhafte Pakete werden erkannt

NT: hohe Verzögerungszeit (Latenz)

* **Cut Through**

Bei dieser Betriebsart wird das Paket nach Empfang des Headers sofort weitergeleitet. (im Header steht, wohin das Paket gehen soll)

VT: schnell, geringe Verzögerung

NT: Fehlerhafte Pakete werden in andere Segmente weitergeleitet, auch kollidierte Pakete

werden weitergeleitet

* **Fragment Free**

Nach Empfang der ersten 64 Byte wird das Paket weitergeleitet. Diese Betriebsart ist nur beim teilgeswitchten Netz notwendig

VT: kollidierte Pakete werden erkannt und nicht an die restlichen Segmente weitergeleitet

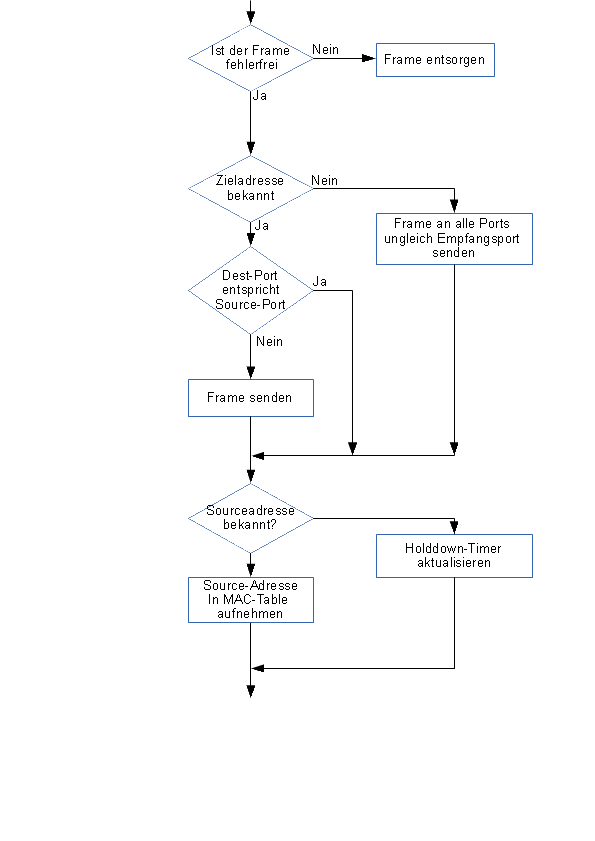
NT: Fehlerhafte Pakete werden in andere Segmente weitergeleitet

* **Adaptiver Mode**

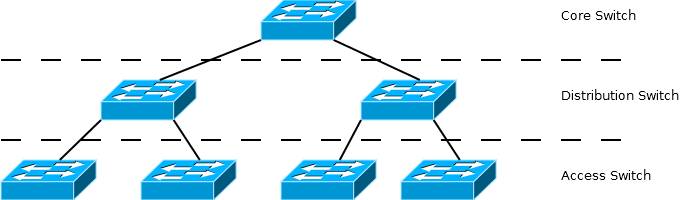
Switch beginnt mit dem *Store and Forward* Mode und überprüft die Fehlerrate. Wir ein

bestimmter Prozentsatz unterschritten, wechselt er in den *Cut Through* Mode.

Ein Switch verhält sich wie eine Bridge, allerdings mit mehr als zwei Ports.

Die Bearbeitung eines Frames läuft folgendermaßen ab:

Bei einer strukturierten Verkabelung können verschiedene Ebenen identifiziert werden:



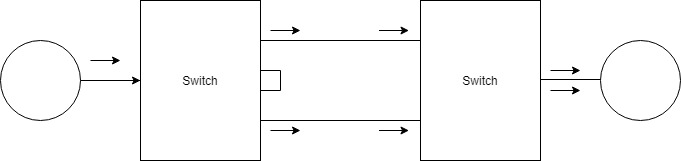
Je nach Eben werden sehr unterschiedliche Anforderungen an die Leisungsfähigkeit eines Switches gestellt.

Wenn ein Access-Switch 16x1 Gigabit Ports hat, ist ein Uplink mit 32 Gigabit/s erforderlich   
(Full Duplex). Bei obigen Bild müsste der Core-Switch 128 Gigabit/s verarbeiten können!

Diese Übertragungsleistungen können durch entsprechende Übertragungstechnologien   
(Ethernet max. 40 Gbit/s, teuer) bzw. durch Bündelung mehrerer paralleler Ports/Kabel erreicht werden. Dazu ist eine Technologie wie Etherchannel notwendig.

In vielen Fällen macht es Sinn Verbindungen redundant auszuführen. Damit sollte einerseits die Fehleranfälligkeit gesenkt, andererseits aber auch die Übertragungsgeschwindigkeit erhöht werden.

Dabei treten allerdings Probleme auf:



Effekte:

* Pakete werden mehrfach zugestellt
* Broadcaststorms (ein Broadcast wird vervielfältigt und im Kreis geschickt).

Abhilfe:

* redundanter Switch wird erst im Fehlerfall in Betrieb genommen
* automatische Erkennung und Beseitigung von Schleifen

## Spanning Tree Protokoll

Das Spanning Tree Protokoll ist eine Möglichkeit, eine schleifenfreie Netzwerkstruktur zu garantieren. Dazu wird das Netzwerk als Baum strukturiert.

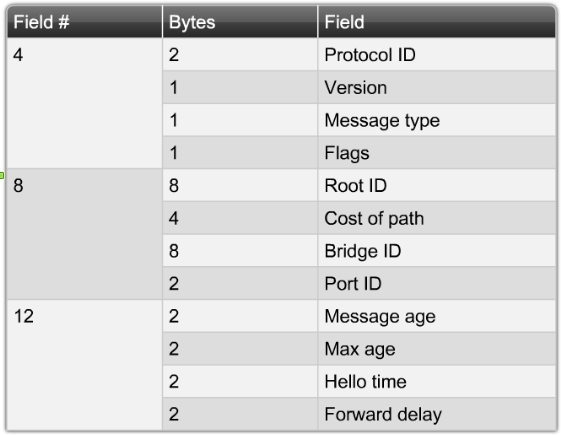
Jeder Switch bekommt eine Bridge-ID. Diese setzt sich aus einer eindeutigen MAC-Adresse und einer wählbaren Priorität (16Bit) zusammen.

Priorität

MAC-Adresse

Der Ablauf des Spanning Tree Algorithmus teilt sich in mehrere Schritte:

#### Wahl der Root-Bridge

Der Switch mit der niedrigsten Bridge-ID wird die Root Bridge. Dazu senden alle Switches auf allen Ports BPDU[[1]](#footnote-1) Pakete aus. Diese Pakete enthalten unter anderem die eigene Bridge-ID und die Root-Bridge-ID.

Jeder Switch setzt als Root-ID seine eigene BridgeID ein. Wenn er auf einem Port ein BPDU Paket mit einer niedrigeren (=höher Prioren) Bridge-ID empfängt, sendet er ab diesem Zeitpunkt diese Bridge-ID als Root-ID aus. Nach kurzer Zeit senden jetzt alle Switches BPDU-Pakete mit der gleichen Root-ID aus. Wenn das erreicht ist, sendet **nur noch die Root-Bridge BPDU-Pakete aus**.

#### Wahl des Root-Ports

Die Switches, die mit der Root-Bridge verbunden sind, empfangen die BPDU-Pakete von der Root-Bridge. Je nach Empfangsport tragen sie die Pfadkosten in das BPDU Paket ein und senden es an alle anderen Ports weiter. Der nächste Switch empfängt das BPDU-Paket und addiert (je nach Empfangsport) wieder seine Pfadkosten.

Der Port mit den niedrigsten Kosten zur Root-Bridge wird der Root-Port.

|  |  |
| --- | --- |
| **Übertragungs-**  **Geschwindigkeit** | **Pfadkosten**  **short, (802.1d)** |
| 10 MBit/s | 100 |
| 100 MBit/s | 19 |
| 1 GBit/s | 4 |
| 10 GBit/s | 2 |

Es werden nur noch BPDU Pakete vom Root-Port weitergesendet.

#### Wahl des Designated/Non-Designated Ports

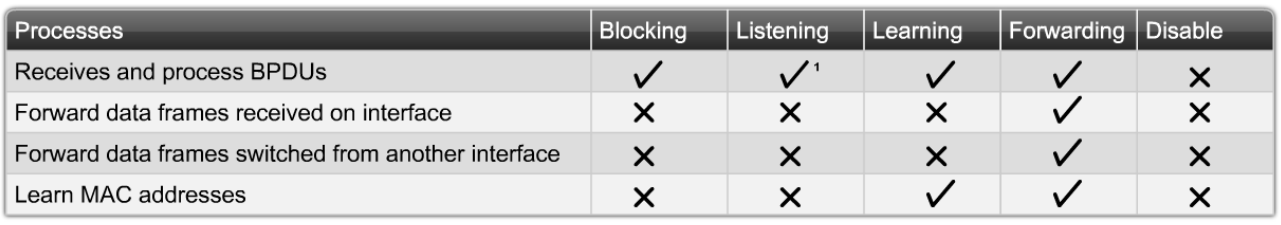
Wenn jetzt noch BPDU-Pakete an einem Port ankommen, der nicht der Root-Port ist, dann existiert eine Schleife.

Der Port, der geringere Kosten zur Root-Bridge hat, ist der Designated Port. Falls die Kosten gleich sind entscheidet die niedrigere Bridge-ID. (Wenn auch die gleich ist (gleicher Switch) dann entscheidet noch die PortID).

Der andere Port ist der Non-Designated-Port. Dieser Port wird in den Blocking-Mode versetzt. In diesem Mode leitet er nur noch BPDU-Pakete weiter (keine Datenpakete!).

Dadurch, dass die Root-Bridge periodisch BPDU-Pakete aussendet, werden Topologie Änderungen (z.B. durch Drahtbruch) erkannt und der Blocking-Port kann wieder in der Forward-Mode geschalten werden.

Folgende Tabelle zeigt die möglichen Port-Zustände und ihre Eigenschaften



Beim Einschalten eines Switches durchläuft ein Port die Zustände:



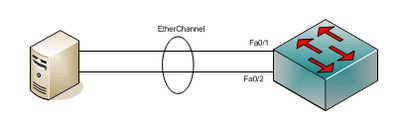
Im Listening-State werden BPDU Pakete ausgewertet. Im Learning-State werden MAC-Adressen gelernt, aber noch keine Datenpakete weitergeleitet. Frühestens nach 30s werden Datenpakete gesendet. Das ist in vielen Fällen (z.B. DHCP) zu langsam. In diesem Fall kann der Port in den *Portfast*-Mode geschalten werden (nur Access Ports!!!!).

Wenn es eine Topologie Änderung gibt, werden alle Ports 20s(!) in den *Blocking* Zustand versetzt. Dafür gibt es weiterentwickelte Protokolle wie RSTP (Rapid Spanning Tree)

Es ist darauf zu achten, dass die Rootbridge im Zentrum des Netzwerks (Coreswitch) ist!

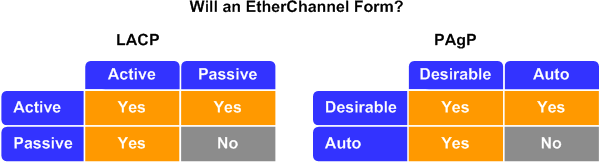
## Kanalbündelung

Um die Bandbreite oder die Ausfallssicherheit zu erhöhen können mehrere Ethernet Verbindungen gebündelt werden. Dazu kann LACP[[2]](#footnote-2) (802.3ad) bzw. PAgP[[3]](#footnote-3) (ein CISCO proprietäres Protokoll) verwendet werden. Diese Protokolle dienen zur Erkennung von defekten Verbindungen, d.h. ein logischer Link kann auch ohne diese Protokolle aufgebaut werden.



Die Bezeichnung dieser Technologie ist je nach Hersteller unterschiedlich, bei CISCO Ether-channel, bei HP Port Trunking usw.

Alle Ports müssen am selben Switch sein und müssen dieselbe Geschwindigkeit aufweisen. Weiters gibt es einen aktiven und einen passive Mode. Diese müssen passend kombiniert werden:



Es können max. 8 Verbindungen zu einem Link gebündelt werden.

## 802.1X

Bei der Standard Port Security wird das Endgerät anhand seiner MAC-Adresse authentifiziert. Das ist unsicher, da diese leicht gefälscht werden kann. Weiters ist es nicht möglich ein Gerät einem User zuzuordnen.

Bei 802.1X handelt es sich um eine Methode um Geräte bzw. User am Layer 2 zu authentifizieren. Dazu werden 3 Bereiche unterschieden:

* Supplicant
* Authenticator
* Authentication Server

Beim Verbindungsaufbau kann der Supplicant nur EAP[[4]](#footnote-4) Pakete an den Authenticator senden.

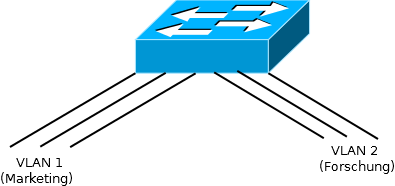
EAP ist dabei ein Framework, um verschieden Authentifizierungsmethoden anzubieten (z.B. EAP-TLS, EAP-PSK, EAP-MD5…). Beim Authenticator handelt es sich um einen 802.1x fähigen Switch oder Access Point.

Der Authenticator nimmt über das RADIUS-Protokoll[[5]](#footnote-5) Kontakt mit dem Authentication Server auf und überprüft die Credentials des Benutzers bzw. des Geräts. Die Credentials können als Username/Passwort oder auch als Zertifikat angegeben werden.  
Für den Authentication Server gibt es verschiedene Implementierungen wie z.B. Windows Server bzw. FreeRadius unter Linux.

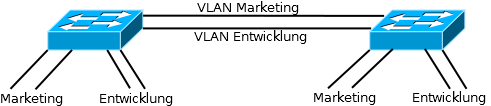
Bei erfolgreicher Authentifizierung wird der Port für alle Pakete freigeschalten.

## VLAN

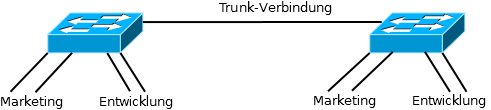
Da die physische LAN-Verkabelung (horizontal und vertikal) oft nicht mit der tatsächlichen Unternehmens-Struktur übereinstimmt, kann das LAN in virtuelle LAN’s (VLAN’s) unterteilt werden. Weiters können Änderungen wesentlich schneller durchgeführt werden.



Dabei wird jedem Port am Switch einem VLAN zugeteilt. Jedes VLAN hat eineindeutige VLAN-ID (1..4095) und einen (frei wählbaren) Namen. Zwischen den einzelnen VLAN’s können keine Pakete ausgetaucht werden. Das erhöht die **Sicherheit** (absolute Trennung von Marketing und Forschung) und verkleinert die **Broadcastdomäne** (höhere Geschwindigkeit).



Um mehrere Switches zu verbinden braucht es daher eine Verbindung pro VLAN. Das ist aber nicht flexibel. Damit die Pakete mehrerer VLAN’s über eine Verbindung übertragen werden, muss eine Trunk-Verbindung eingerichtet werden.



Über die Trunk-Verbindung werden Pakete von verschiedenen VLAN’s übertragen. Damit diese unterschieden werden können, müssen die Pakete markiert (getagged) werden.

Dazu wird *IEEE 802.1Q* verwendet. Dabei wird der Ethernet Frame erweitert (siehe VLAN-Tag). Ein anderes (veraltetes) Protokoll ist *ISL* (Inter Switch Link). Dieses CISCO-proprietäre Protokoll erzeugt einen eigenen Frame und verändert den Ethernet Frame daher nicht.

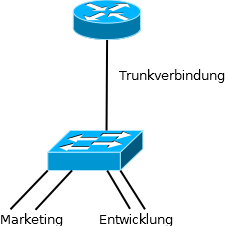
Diese VLAN-Tags werden nur auf Trunk-Ports verwendet und von normalen Endgeräten nicht verstanden. Auf einer Trunk-Verbindung kann meist auch **ein** *Default-VLAN* definiert werden. Dieses wird nicht getaggt und die Frames können auch von Endgeräten verarbeitet werden.

Ein VLAN (normalerweise VLAN 1) wird als *Management VLAN* verwendet. Diese VLAN kann eine IP-Adresse gegeben werden. Der Switch kann dann über Ports in diesem VLAN konfiguriert werden (Telnet, SSH oder Web). Dadurch können Access-Ports (Endbenutzer) und Management-Ports getrennt werden.

### InterVLAN Routing

Da über den Layer 2 keine Pakete zwischen den VLAN’s ausgetauscht werden, muss dazu Routing (Layer 3) eingesetzt werden. Die Pakete können hier wesentlich besser gefiltert und kontrolliert werden.

Damit der Router nicht ein Verbindungskabel pro VLAN benötigt, kann auch hier eine Trunkverbindung verwendet werden:



Dazu wird am Router für jedes VLAN ein virtuelles Interface eingerichtet. Zwischen diesen Interfaces kann dann geroutet werden. Diesen Aufbau bezeichnet man als *Router on a Stick*.

### VTP

VTP (*Virtual trunking protocol*) ermöglicht es, die VLAN-Konfiguration auf ihre gesamte Switch Infrastruktur zu verteilen (damit man nicht an jedem Switch diese Konfiguration eingeben muss). Dabei werden periodisch über Multicast die Informationen ausgesandt.

Für den Betrieb gibt es 3 Betriebsarten:

**VTP – Server**

Beim VTP – Server werden die VLANs erstellt, verändert und gelöscht.

**VTP – Client**

Lernt die VLANs vom Server. Es können keine VLANs erstellt werden.

**Transparent**

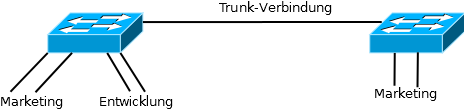
Bei dieser Betriebsart nimmt der Switch nicht am VTP - Prozess teil. Es werden die

VTP – Pakete weitergeleitet. Am Switch selber können VLANs erstellt werden.

Diese haben jedoch nur lokale Bedeutung

Alle VTP Geräte müssen sich in der gleichen VTP-Domäne befinden. Dieser kann ein beliebiger Name zugewiesen werden. Weiters muss darauf geachtet werden, dass zumindest die Version 2 (aktuell 3) verwendet wird.

Mit VTP kann auch *Pruning* eingesetzt werden. Damit kann sichergestellt werden, dass über eine Trunk-Verbindung nur solche Pakete übertragen werden, für die es auch zugeteilte Ports gibt.



# Layer 3 (Network Layer)

Der Layer 3 wird dominiert vom IP(v4) Protokoll. Inzwischen ist allerdings absehbar, dass IPv6 diese Aufgaben übernehmen wird. Behandelt werden hier beide Versionen.

## IPv4 Protokollfamilie

IPv4 wurde 1981 in der RFC791 definiert.

Beim IP Protokoll handelt es sich um ein **verbindungsloses** (unzuverlässiges) Protokoll.

Es abstrahiert die darunter liegende physikalische Übertragung, d.h. für die darüber liegenden Schichten ist es egal ob die Daten per Modem, Ethernet/Token Ring/… übertragen werden.

Dazu muss es z.B. die Paketgröße an die Übertragung (z.B. MTU Ethernet 1500Byte) angepasst werden.

### IP Adressen

Die Adressen sind 32Bit breit und werden üblicherweise dezimal angeschrieben.

Die Adresse teilt sich in einen Netzwerkbereich (NetID) und einen Hostbereich (HostID).   
Bei der Anzahl der Hosts muss die erste (Netzadresse, HostID=0) und die letzte Adresse (Broadcast adresse, HostID=lauter Einser) abgezogen werden

.

Die Aufteilung erfolgte ursprünglich nach den Netzwerkklassen:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Klasse |  |  |  |  |  | |  |  |  | | Netze | | Hosts |
| A | 0NNN NNNN |  | H |  | H | |  | H |  | | 0-127(27) | | 224-2 |
|  |  |  |  |  |  | |  |  |  | |  | |  |
| B | 10NN NNNN |  | N |  | H | |  | H |  | | 128-191(214) | | 216-2 |
|  |  |  |  |  |  | |  |  |  | |  | |  |
| C | 110N NNNN |  | N |  | N | |  | H |  | | 192-223(221) | | 28-2 |
|  |  |  |  |  |  | |  |  |  | |  | |  |
| D | 1110 xxxx |  |  | | | Multicast | | | | 224-239 | |
|  |  |  |  |  |  | |  |  |  | |  | |  |
| E | 1111 xxxx |  |  | | | Reserviert | | | | 240-255 | |

Da diese Aufteilungen zu starr waren, wurde die Subnetzmaske (Netzmaske) eingeführt. Die Netzmaske markiert den Netzanteil mit 1, den Hostanteil mit 0. Um aus einer IP-Adresse die NetID zu ermitteln, muss diese Adresse mit der Netzmaske verundet werden.

Für die private (interne) Nutzung sind folgende Bereiche reserviert:

|  |  |
| --- | --- |
| A | 10.0.0.0 – 10.255.255.255 |
| B | 172.16.0.0 – 172.31.255.255 |
| C | 192.168.0.0 – 192.168.255.255 |

Weiters ist noch das Netzwerk 127.0.0.0/8 (Loopback) und 169.254.0.0/16 (Link-local) reserviert.

### Subnetting

Die IP-Adressen sind logische Adressen. Damit kann die Struktur eines Unternehmens nachgebildet werden. Dazu ist es notwendig, bestehende Netzwerke in kleinere zu unterteilen.

Weiters reduziert sich dadurch die Broadcastdomäne, wodurch die Performance erhöht wird.

Die Unterteilung erfolgte in mehreren Schritten. Die zugehörigen Beispiele befinden sich in der Mitschrift.

#### Classful Subnetting

Beim Classful-Subnetting bleiben nach wie vor die Netzwerkklassen erhalten. Daher kann nur von einem Klasse A Netz auf Klasse B Netzwerke bzw. von Klasse B auf Klasse C Netzwerke.

Um Verwechslungen vorzubeugen, darf das erste Netzwerk (nulltes Netz) und das letzte Netzwerk nicht verwendet werden.

**Bsp.:** Klasse B – Netz (170.1.0.0)

Teilen Sie dieses Netzwerk in Klasse C Netzwerke auf

#### Classless Subnetting (CIDR)

Beim Classless Subnetting werden einzelne Bits von der HostID in die NetID übernommen. Durch die Einführung von CIDR (Classless Inter Domain Routing, 1993) wurde auch die Verwendung des ersten und letzten Netzwerks erlaubt.

Durch CIDR wurde auch die Notation der Netzmaske in Suffixform (z.B. /25) eingeführt.

**Bsp.:** 193.4.2.0/24

Subnetting für 5 logische Netze

Geben Sie jeweils die Netzadresse (+Netzmaske), Hostadresse und die Broadcastadresse an.

**Bsp:** Host: 177.17.17.32

Subnetzmaske: 255.255.248.0

Wie lautet die:

* Netz ID (verundet die Host- Adresse mit der Subnetzmask)
* Hosts
* Broadcast

**Bsp:** Klasse B 133.25.0.0/16

1000 log. Netze

Geben Sie für die ersten (z.B. 5) Netze die Netzadresse (+Netzmaske), Hostadresse und die Broadcastadresse an.

#### VLSM

Beim *Classless Routing* sind alle Netzwerke gleich groß. Das entspricht oft nicht den realen Anforderungen. Abhilfe schafft *Variable Length Subnet Mask* (VLSM). Dadurch können Netzwerke unterschiedlicher Größe kombiniert werden. Dadurch wird die Verschwendung von Adressen minimiert.

**Bsp: Klasse C 199.1.1.0**

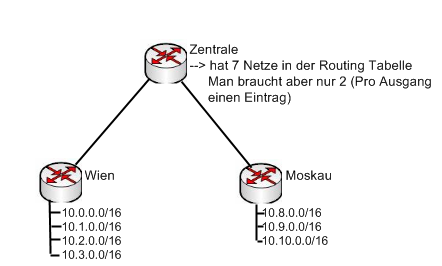
* 1 Netz a‘ 100 Hosts
* 2 Netze a‘ 30 Hosts
* 3 Netze a‘ 2 Hosts

#### Supernetting

Durch die Aufteilung der Netzwerke werden die Routingtabellen immer länger. Daher ist es sinnvoll diese in den Routern wieder zu größeren Blöcken zusammen zu fassen.

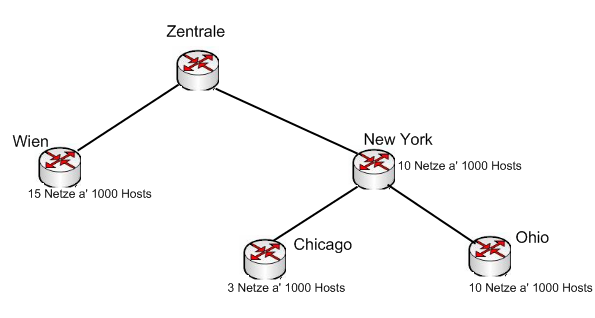
Es muss bereits bei der Planung der Adressbereiche bedacht werden, dass etwaige Blöcke zusammengefasst werden können.

**Bsp:**

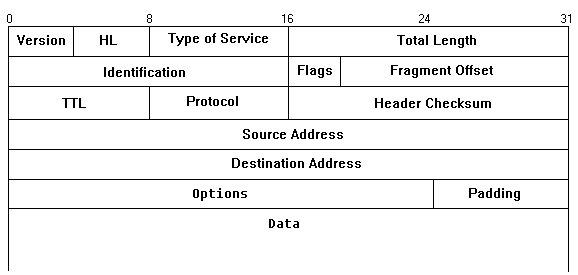


**Bsp:** Gegeben ist das Netzwerk 177.10.0.0/16.

Teile Netzwerk entsprechend auf, damit es sich möglichst gut zusammenfassen lässt.



### IPv4 Header

Version

Kennzeichnet die IP-Protokollversion

HL (Header Length)

Die Angabe der Länge des IP-Headers erfolgt in 32-Bit-Worten (normalerweise 5). Da die Optionen nicht unbedingt auf Wortlänge enden, wird der Header gegebenenfalls aufgefüllt.

Type of Service

Alle Bits haben nur "empfehlenden" Charakter. 'Precedence' bietet die Möglichkeit, Steuerinformationen vorrangig zu befördern.

Total Length

Gesamtlänge des Datagramms in Bytes (max. 64 KByte).

Identification

Dieses und die beiden folgenden Felder steuern die Reassembly. Eindeutige Kennung eines Datagramms. Anhand dieses Feldes und der 'Source Address' ist die Zusammengehörigkeit von Fragmenten zu detektieren.

Flags

Die beiden niederwertigen Bits haben folgende Bedeutung:

* Don't fragment: Für Hosts, die keine Fragmentierung unterstützen
* More fragments: Zum Erkennen, ob alle Fragmente eines Datagramms empfangen wurden

Fragment Offset

Die Daten-Bytes eines Datagramms werden numeriert und auf die Fragmente verteilt. Das erst Fragment hat Offset 0, für alle weiteren erhöht sich der Wert um die Länge des Datenfeldes eines Fragments. Anhand dieses Wertes kann der Empfänger feststellen, ob Fragmente fehlen. Beispiel siehe unten.

Time-to-live (TTL)

Jedes Datagramm hat eine vorgegebene maximale Lebensdauer, die hier angegeben wird. Auch bei Routing-Fehlern (z. B. Schleifen) wird das Datagramm irgendwann aus dem Netz entfernt. Da Zeitmessung im Netz problematisch ist, und keine Startzeit im Header vermerkt ist, decrementiert jeder Gateway dieses Feld --> de-facto ein 'Hop Count'.

Protocol

Da sich unterschiedliche Protokolle auf IP stützen, muß das übergeordnete Protokoll (ULP, Upper Layer Protocol) angegeben werden. Wichtige ULPs sind

* 1: ICMP Internet Control Message P.
* 3: GGP Gateway-to-Gateway P.
* 6: TCP Transmission Control P.
* 8: EGP Exterior Gateway P.
* 17: UDP User Datagram P.

Header Checksum

16-Bit-Längsparität über den IP-Header (nicht die Daten)

Source Address

Internet-Adresse der Quellstation

Destinantion Address

Internet-Adresse der Zielstation

Options

Optionales Feld für weitere Informationen (deshalb gibt es auch die Header-Länge). Viele Codes sind für zukünftige Erweiterungen vorgesehen. Die Optionen dienen vor allem der Netzsteuerung, der Fehlersuche und für Messungen. Die wichtigsten sind:

* Record Route: Weg des Datagramms mitprotokollieren
* Loose Source Routing: Die sendende Station schreibt einige Zwischenstationen vor (aber nicht alle)
* Strict Source Routing: Die sendende Station schreibt alle Zwischenstationen vor.
* Timestamp Option: Statt seiner IP-Adresse (wie bei Record Route) trägt jeder Gateway den Bearbeitungszeitpunkt ein (Universal Time).

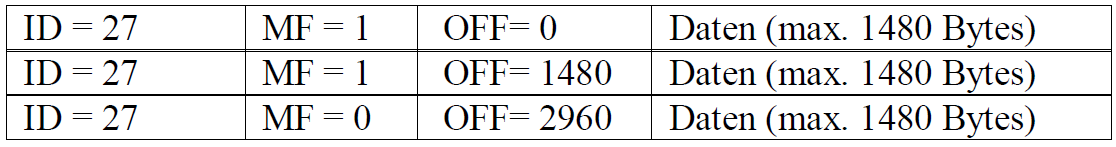
Padding

Füllbits

#### Fragmentierung

Wenn ein IP Paket größer ist als die Maximum Transfer Unit (MTU), muss es aufgeteilt werden. Dies erfolgt mit den Feldern Identification, Flags und Fragment Offset.

Wenn z.B. ein Paket mit 4000Byte über Ethernet (MTU=1500Byte) übertragen werden soll, wird es folgendermaßen aufgeteilt:



Die 1480 Byte ergeben sich daraus, dass der IP-Header 20 Byte beansprucht und daher von den 1500 abgezogen werden muss.

### ARP

Mit dem Address Resolution Protocol (ARP) ermitteln Sie in IPv4-Netzen die MAC Adresse zu einer IP-Adresse. Sie können damit auch einer MAC-Adresse eine IP-Adresse manuell zuweisen.

Normalerweise arbeitet das ARP-Protokoll ohne direkten Benutzereingriff unauffällig im Hintergrund. Daten sollen von A nach B geschickt werden, Sie geben jeweils die IP Adresse auf dem OSI-Layer 3 an. Das ARP-Protokoll fragt alle erreichbaren Netzwerkteilnehmer, ob sie über die gesuchte IP-Adresse verfügen. Der Zielrechner antwortet entsprechend und gibt seine MAC-Adresse dem Fragesteller bekannt. Die Kommunikation zwischen den beiden wird nunmehr aufgebaut.



Das Beispiel in Abbildung zeigt Ihnen den Ablauf detailliert. Der linke Rechner sendet die ARP-Anfrage mit der eigenen IP und MAC-Adresse (IP(S), MAC(S)), die IP-Adresse des Empfängers (IP(E)) und die Broadcast- Adresse ff:ff:ff:ff:ff:ff. Die erreichbaren Rechner prüfen, ob ihnen die angegebene Adresse gehört. Der angesprochene Zielrechner sendet daraufhin ein Paket mit seiner MAC-Adressangabe zurück (MAC(E)). Die anderen Rechner verwerfen das Paket.

Beide Rechner speichern normalerweise die erfolgreiche ARP-Anfrage im ARP-Cache. Wie lange die Informationen dort verbleiben, ist unterschiedlich. Gebräuchlich sind Zeiten zwischen 5 und 10 Minuten. Ist die IP-Adresse unbekannt, können Sie mittels des Reverse Address Resolution Protocol (RARP) einen zentralen Rechner kontaktieren und nach dieser abfragen. Dieses Netzwerkprotokoll ist aber kaum mehr von Bedeutung.

**Proxy-ARP und Sicherheit:** Im seltenen Fall, dass ein Router zwei Netze mit gleichem IP Adressbereich verbindet, antwortet dieser anstelle des Zielrechners. Listet man den ARP-Cache auf, so taucht die IP-Adresse des Routers anstelle der des Zielrechners auf.

**Proxy-ARP oder ARP-Spoofing:** Wenn Sie den ARP-Cache des abfragenden Rechners auflisten und finden zu ein und derselben MAC-Adresse verschiedene IP-Adressen, so befindet sich entweder ein Proxy-ARP-Server im Netz, oder es liegt ARP-Spoofing vor. In diesem Fall hat ein Angreifer vor, den Netzwerkverkehr zu belauschen oder zu manipulieren! Rechner versenden einen ARP-Broadcast mit der eigenen IP-Adresse als Absender und Ziel mit dem Zweck, die neue, eigene MAC-Adresse allen erreichbaren Rechnern des eigenen Netzwerksegmentes bekannt zu geben (*Gratuitous ARP*). Das ist beim Laden oder Netzwerkstart eines Rechners ganz normal. Die benachrichtigten Rechner ergänzen oder ändern daraufhin die entsprechenden Einträge des ARP-Caches. Wenn Sie zwei oder mehrere Rechner redundant betreiben, so wird damit allen anderen Teilnehmergeräten der Umstieg auf die Reserve, was das Netzwerk angeht, bekannt gemacht.

### ICMP

ICMP (*Internet Control Message Protocol*) ist ein Protokoll, das IP als Transportprotokoll verwendet und zum Fehler und Informationsaustausch zwischen den Rechnern verwendet wird.

|  |  |  |
| --- | --- | --- |
| IP Header  (Prot. Nr. 1) | ICMP Header | Payload Data |

Die ICMP Nachrichten unterteilen sich in verschiedene Typen:

* Echo Antwort
* Fehler
* Zielentlastung (Flusskontrolle)
* Echo Anfrage
* Zeitlimits
* ….

Diese können noch weiter unterteilt werden

Codes für Fehlermeldungen (beispielsweise):

* Destination unreachable
* Network unreachable (Router findet das Zielnetz nicht)
* Protocol unreachable (Zielrechner schickt es zurück – Layer 4 P. nicht erkannt)
* Port unreachable (Layer 7 – ein Port wird nicht erkannt)
* Host unreachable (falsche IP-Adresse)
* Can’t fragment (wenn das Flag gesetzt ist)

Die Payload-Data (Nutzlast) hat keine Bedeutung im Sinne der Datenübertragung, kann aber für die Fehlersuche eingesetzt werden.

### DHCP

(Quelle: Techchannel)

Netzwerke unterliegen einem ständigen Wandel: Ältere Geräte werden aussortiert, neue Rechner

kommen hinzu, mobile Anwender klinken sich ein und aus. Bei manueller Konfguration bedeutet

dies einen erheblichem Aufwand. Dynamic Host Confguration Protocol (DHCP) löst dieses Problem durch die dynamische Vergabe von IP-Adressen.

In einem TCP/IP-basierten Netzwerk besitzt jeder Rechner zumindest eine IP-Adresse und eine

Subnetzmaske, um mit anderen Geräten im Netzwerk zu kommunizieren.

Schon in einem kleinen Netzwerk lohnt es sich, die Adressenvergabe durch einen zentralen Rechner

zu steuern. Für den Administrator hat das Verfahren gleich mehrere Vorteile: Die Pflege ist

weniger zeitaufwendig, da keine Arbeiten an den einzelnen Clients erforderlich sind.

Adresskonfikte gehören der Vergangenheit an, da der DHCP-Server die Vergabe der IP-Adressen zentral steuert.

DHCP basiert auf BOOTP4, bietet aber gegenüber seinem Vorgänger verschiedene Vorteile. Der

wohl interessanteste: die dynamische Vergabe von IP-Adressen. Dabei schöpft der DHCP-Server

aus einem vorgegebenen Adressenbereich (Range, wird manchmal auch als Scope bezeichnet) und

weist den anfragenden Clients eine Adresse für einen bestimmten Zeitraum (Lease) zu. Innerhalb

der Lease-Zeit fordert ein DHCP-Client beim Systemstart vom Server keine neue Adresse, sondern

lediglich eine Bestätigung über die bestehende Lease an.

Auch mögliche Fehlerquellen minimiert DHCP: So überträgt das Protokoll neben den IP-Adressen

auf Wunsch auch weitere Parameter wie zum Beispiel:

* Standard-Gateway
* Netzmaske
* Rechnername und Domänenname
* Standardgateway
* Adressen der Nameserver

...

Die technischen Spezikationen des DHCP-Protokolls sind in RFC 2131 definiert.

#### Interaktion zwischen Client und Server

Schon eine vereinfachte Beschreibung der Adressenvergabe macht den zyklischen Verlauf der Interaktion zwischen Client und Server deutlich. Der gesamte Verteilungs- und Abstimmungsprozess

lässt sich durch vier Schritte beschreiben:



* Der Client verschickt eine DHCPDISCOVER-Nachricht an die im Netzwerk befindlichen DHCP-Server. Sie entspricht im Wesentlichen der einfachen Auforderung: An alle DHCP Server im Netz, ich benötige eine IP-Adresse. Da der Client bislang noch keine IP-Adresse besitzt, kann er auch nicht TCP/IP für die Kommunikation mit anderen Netzwerksystemen verwenden. Daher greift derClient zur Kommunikation auf UDP zurück.
* Als Anwort auf die Anfrage des Clients übermittelt der DHCP-Server dem Client einen Vorschlag, indem er mit DHCPOFFER eine IP-Adresse übermittelt.
* Nun ist der Client wieder an der Reihe. Er muss sich für eine der ihm angebotenen Adressen entscheiden. Hier ist die Art der DHCP-Implementierung wichtig: Die Kriterien dieser Auswahl sind nicht im RFC festgelegt, sondern unterscheiden sich von Plattform zu Plattform. Sobald die Entscheidung für eine Adresse gefallen ist, sendet der Client eine DHCPREQUEST-Meldung an den entsprechenden Server aus. Auch dabei wird wieder UDP als Transportprotokoll verwendet.
* Beim vorläufig letzten Schritt liegt der Ball wieder in den Händen des Servers. Auf den Request übermittelt der Server eine temporäre IP-Adresse mittels DHCPPACK an den Client. Nachdem der Client diese Nachricht entgegengenommen hat, führt er in der Regel einen Check durch, um sicherzustellen, dass die Adresse nicht bereits ein anderer Rechner verwendet (ping). Schließlich übernimmt der Client die übermittelten Netzwerkparameter in seine Systemkonfiguration.

#### DHCP-Refresh

Nachdem ein DHCP-Server einen Client mit einer IP-Adresse ausgestattet hat, weist er ihm zusätzlich die so genannte Lease-Zeit zu. Diese legt die Gültigkeitsdauer der Einstellungen fest. Im Hintergrund laufen dabei zwei Uhren:

* T1 entspricht der halben Lease-Zeitspanne,
* T2 ist auf 87,5 Prozent

der maximalen Lease-Zeit gesetzt. Beide Werte lassen sich über die DHCP-Optionen des Servers bearbeiten, sofern diese Funktionen implementiert sind.

Nachdem T1 abgelaufen ist, sendet der Client eine DHCPREQUEST-Nachricht an den Server und fragt nach, ob dieser die Lease-Zeit verlängern kann. Man bezeichnet diesen Zustand auch als Renewing Status. In der Regel antwortet der Server mit einer DHCPACK-Nachricht samt einer neuen Lease-Zeit. Die Werte T1 und T2 setzt der Server dabei zurück. Erhält der Client bis zum Ablauf von T2 keine DHCPACK-Nachricht, beginnt der Rebinding Status. Der Client muss nun eine DHCPREQUEST-Nachricht verschicken, damit die Lease-Zeit verlängert wird. Diese Anforderung kann der Server durch DHCPACK bestätigen. Bleibt auch dieser Request unbeantwortet, muss der Client eine komplett neue IP-Adresse anfordern. Hierbei kommt der ursprüngliche Mechanismus zum Einsatz, der alle DHCP-Server im Netz anspricht.

Manuell kan die Erneuerung der IP-Adresse durch

C:\ipconfig/renew

angeworfen werden.

#### Range und Lease

Bevor ein DHCP-Server die angeschlossenen Netzwerk-Clients überhaupt mit IP-Adressen versorgen kann, muss man ihn mit Informationen füttern, welche Ranges er verwenden darf. Eine Range stellt einen IP-Adressbereich dar, der durch eine Start- und End-Adresse definiert ist. Je nach Implementierung sind auch Ausschlussbereiche vorgesehen, also Adressen, die nicht für die Vergabe herangezogen werden können. Auf diese Weise ist sichergestellt, dass feste und dynamische IP-Adressen in einem Netzwerk problemlos nebeneinander existieren können. Grundsätzlich wird auch zwischen statischen und dynamischen DHCP unterschieden. Beim statischen DHCP bekommen die Clients immer die gleiche IP-Adresse zugewiesen, beim dynamischen wird eine beliebige (freie) Adresse aus dem Range gewählt.

Die Lease-Dauer wird in der Regel durch die Angabe von Tagen, Stunden und Minuten definiert. Eine allgemeine Regel für die optimalen Parameter gibt es nicht. Diese Einstellungen, sofern sie denn überhaupt in den einzelnen Produkten implementiert sind, müssen auf Beanspruchung des Servers, Client-Verhalten und Netzwerkstabilität abgestimmt sein. Entscheidend ist zum einen die Anzahl der möglichen Clients. Als Richtwert gilt: Die Lease-Zeit ist doppelt so lange wie die Zeitspanne, die beim Serverausfall für die Wiederinbetriebnahme benötigt wird.

Wichtig: Bei längeren Lease-Zeiten dauert es entsprechend länger, bis Änderungen der DHCP Optionen auf der Client-Seite greifen.

#### Alternative Konfiguration und APIPA

Wenn ein Windowssystem auf DHCP eingestellt ist und keine Adresse zugewiesen bekommt, gibt

es zwei Möglichkeiten:

Wenn eine alternative Konfiguration eingetragen ist werden diese Einstellungen verwendet

Wenn keine alternative Konfiguration vorhanden ist, so wird über APIPA (Automatic Private IP Adressing) eine Adresse aus dem Bereich 169.254.0.0 bis 169.254.255.255 zufällig ermittelt. Auf diese Weise können auch unkonfigurierte Windows-PC's miteinander kommunizieren.

### NAT

Die drohende Adressknappheit bei IPv4 in den 90iger Jahren führte zu einigen Workarounds, wobei NAT sicher der effektivste war.

Die Idee dahinter ist, dass im internen Netz keine weltweit eindeutigen Adressen verwendet werden. Dafür wurden interne (private) Adressbereiche definiert (siehe oben). Diese internen Adressen werden im Internet nicht geroutet und müssen daher übersetzt werden. Dazu gibt es mehrere Möglichkeiten:

#### NAT (Network address translation)

Es gibt einen Pool von öffentlichen Adressen. Wenn ein Paket vom internen Netz in der in das externe gesendet wird, wird die interne Adresse durch eine öffentliche ersetzt. Das NAT-Gateway muss daher eine Tabelle führen, die eine Beziehung zwischen den Adressen herstellt. Nach dem das Antwortpaket zurückgekommen ist, kann die öffentliche Adresse wieder in den Pool zurückwandern. Wenn der Pool ausgeschöpft ist können keine Pakete mehr gesendet werden, bis wieder Adressen frei geworden sind.

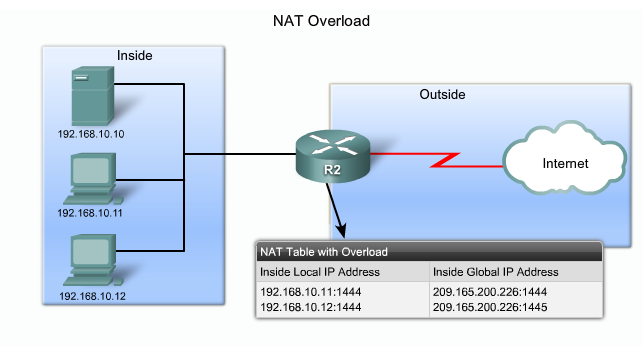
#### Static NAT

Funktioniert wie NAT, nur ist eine fixe Beziehung zwischen den internen und externen Adressen.

Dadurch können interne System auch Dienste nach außen anbieten.

#### PAT (Port address translation, NAT overload)

Es wird meist von NAT gesprochen, aber PAT gemeint. Der Nachteil von NAT ist, das mehrere öffentliche Adresse vorhanden sein müssen. Das ist oft nicht der Fall bzw. mit Kosten verbunden.

Bei PAT wird nur eine externe Adresse verwendet. Die Beziehung wird über die Portnummern hergestellt (siehe unten).Schwierig ist es jedoch, externe Dienste anzubieten. Jeder Port kann nur einmal nach außen verbunden werden. Dabei spricht man von *Port forwarding*.

Ein Vorteil von NAT ist, dass das interne Netzwerk nach außen nicht sichtbar ist. Manchmal wird daher auch von einer NAT-Firewall gesprochen. NAT ist allerdings **keine** Sicherheitsmaßnahme!

Ein Nachteil ist, dass keine End-to-End Verbindung möglich ist. Das behindert z.B. die Verschlüsselung.

## IPv6 Protokollfamilie

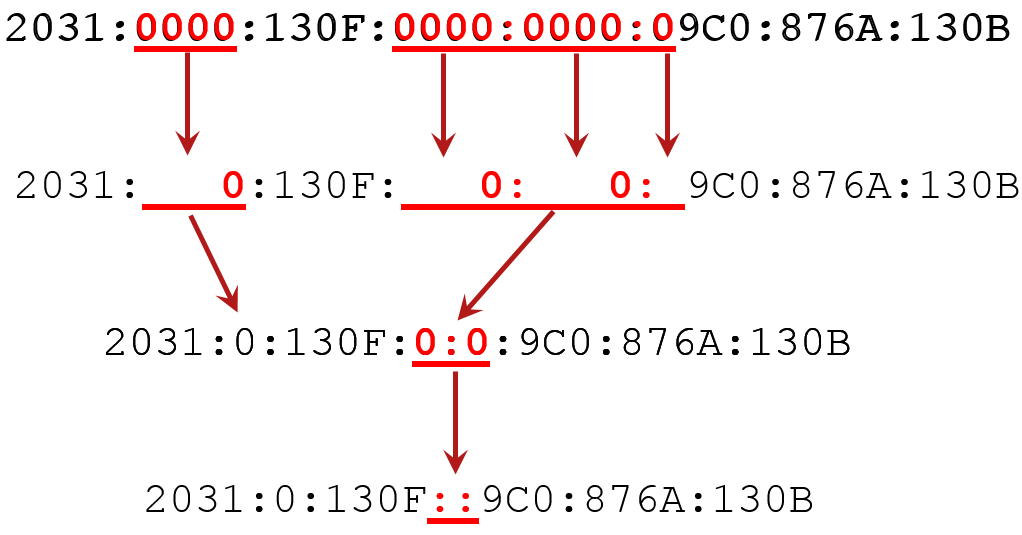
Neben der Adressknappheit wurden mit IPv6 einige Unzulänglichkeiten von IPv4 ausgemerzt. So bringt es mit IPSec die Möglichkeit der Verschlüsselung mit und der Header wurde vereinfacht und kann erweitert werden. Durch den großen Adressraum sind Provisorien wie NAT nicht mehr notwendig und auch nicht mehr vorgesehen.

### IPv6 Adressen

Im Gegensatz zu IPv4 ist eine IPv6 Adresse 128Bit lang. Um diese Adressen handhaben zu können gelten bestimmte Regeln:

* Die Adresse wird in 8 hexadezimalen Blöcken a‘ 4 Ziffern, die durch einen Doppelpunkt getrennt sind, notiert
* Führende Nullen können weggelassen werden
* Mehrere Blöcke von Nullen können durch :: zusammengefasst werden (nur einmal!)

Beispiel:

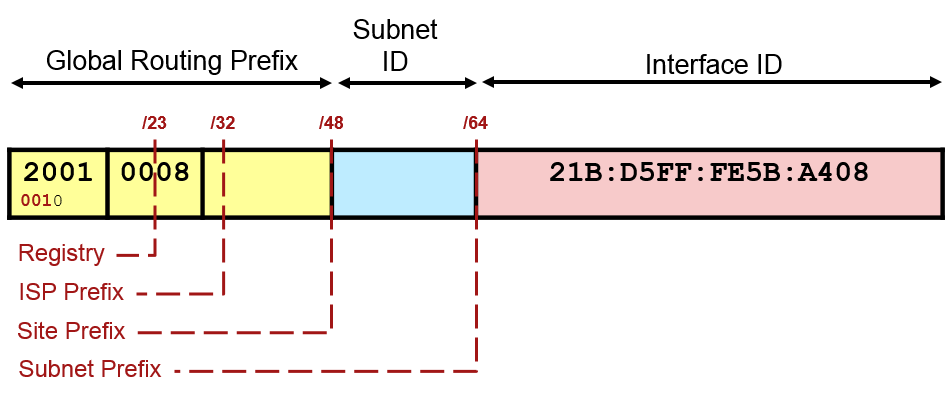


IPv6 Adressen verwenden ausschließlich die CIDR Notation. Es werden verschieden Arten von Adressen unterschieden:

* **Multicastadressen**, gehen an eine Gruppe von Empfängern (aus dem Bereich FF00::1/8)

Unter IPv6 sind keine Broadcasts mehr vorgesehen!

* **Link local Adresse** (FE80::/10). Gelten nur lokal. Wird auf jeder Schnittstelle generiert, gilt nur lokal (wird nicht geroutet)
* **Loopbackadresse**, identifiziert den eigenen Computer 0000:0000:0000:0000:0000:0000:0000:0001  
  wird vereinfacht zu ::1/128
* keine Adresse ::/128
* **Unicastadressen** adressieren genau ein Gerät. Zurzeit sind nur Adressen aus dem Bereich 2001 von der IANA freigegeben. Die Adressen teilen sich in fest definierte Bereiche auf (siehe Abbildung)

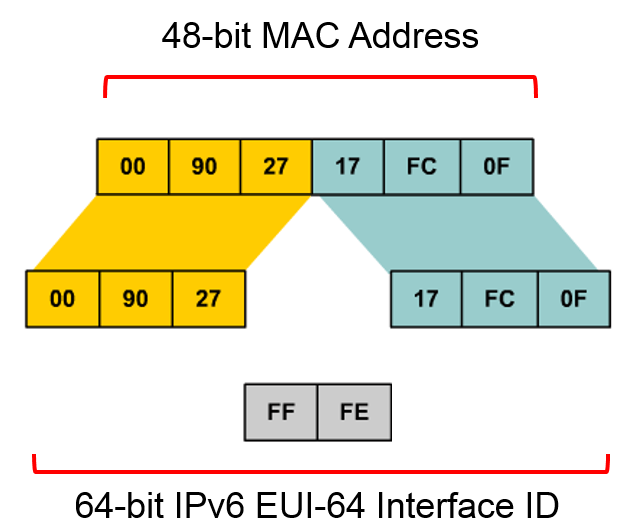


Die ersten 64Bit sind die NetID. Die zweiten 64Bit entsprechen der HostID.

Zur Aufteilung von Subnetzen (VLSM) sollte die Subnet-ID verwendet werden. Die Interface-ID sollte dafür nicht mehr verwendet werden.

Die Interface-ID kann auf mehrere Arten zugewiesen werden:

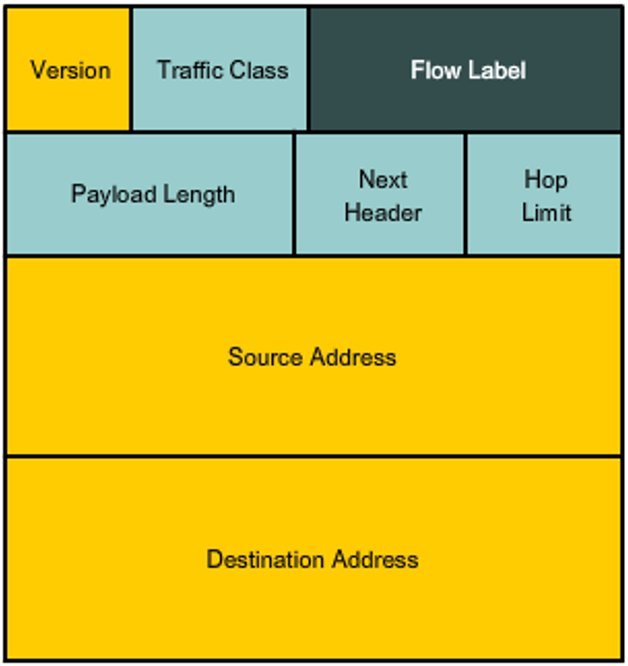
* DHCP
* Manuell
* EUI-64: Die Adresse wird aus der MAC-Adresse generiert:



Mit EUI-64 kann eine „Stateless Autoconfiguration“ realisiert werden.

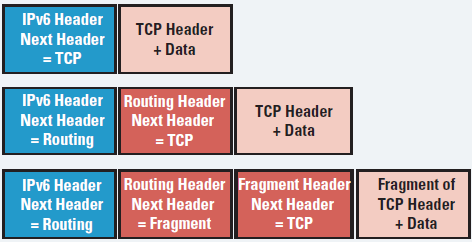
### IPv6 Header

Der IPv6 Header wurde auf das Wesentliche reduziert. Alle Felder die nicht immer benötigt werden, werden in Erweiterungsheader ausgelagert.

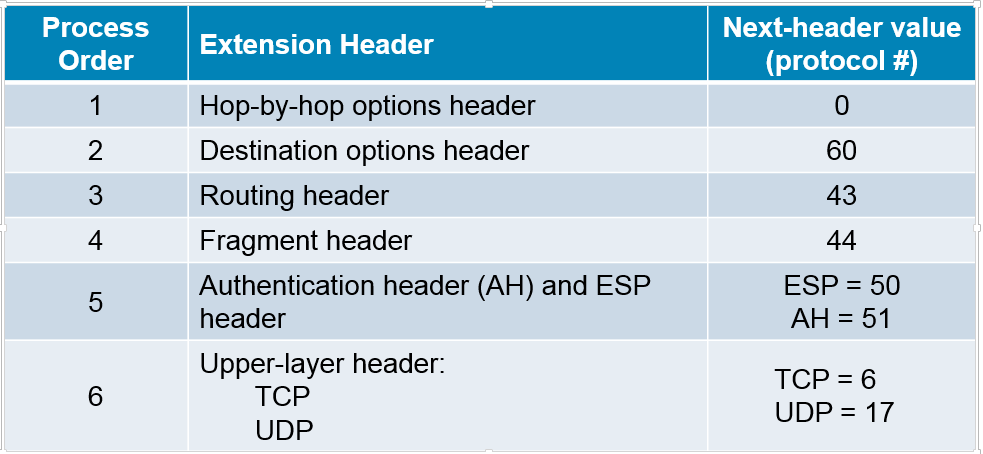


Der IPv6 Header ist immer gleich lang. Dadurch ist auch die Header-Length nicht mehr notwendig. Das TTL-Feld wurde auf Hop-Limit umbenannt. Die Traffic-Class entspricht der Priorität. Die Checksum wurde komplett gestrichen.

Der Header enthält ein Feld Next Header, das entweder auf einen Erweiterungsheader bzw. auf die beinhalteten Daten zeigt.

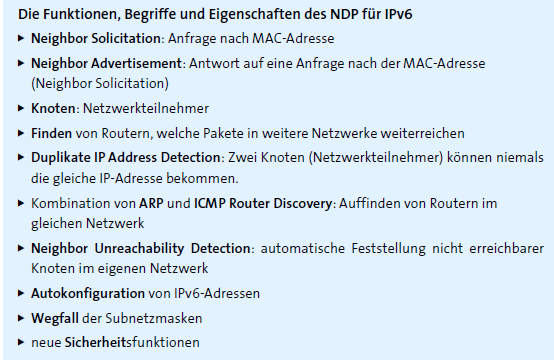


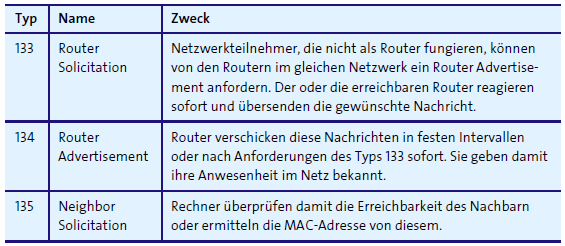
Die Erweiterungsheader sollten in der folgenden Reihenfolge vorhanden sein:

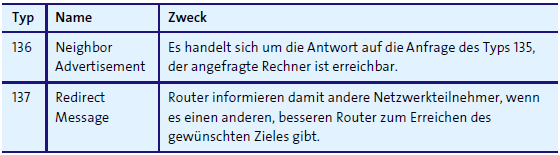


### NDP

Die Aufgaben des ARP-Protokolls beim IPv4-Protokoll werden bei IPv6 vom *Neighbor Discovery Protocol* übernommen. NDP bietet aber auch noch andere Funktionen:







# Layer 4

Ein großer Teil dieses Kapitels ist dem Buch *Computer-Netzwerke* von Harald Zisler entnommen.

Der weltweite Datentransport geschieht überwiegend innerhalb von IP-Netzen. Ihre Daten werden hier in Pakete zerlegt und am Zielort wieder zusammengesetzt. Den dabei entstehenden Datenstrom können Sie kontrolliert per TCP übertragen. Damit entlasten Sie die Anwendung, welche die Korrektheit und Vollständigkeit überprüfen müsste. Natürlich erkaufen Sie sich diese Sicherheit mit erhöhter Netzlast. Diese senken Sie dadurch, dass Sie UDP zur Datenübertragung einsetzen. In diesem Fall sendet Ihr Rechner auf gut Glück die Datenpakete ins Netz. Die jeweils kommunizierenden Anwendungen kontrollieren den Fluss, die Korrektheit und Vollständigkeit der Daten selbst – und verursachen sowohl bei Sender als auch Empfänger eine höhere Rechnerauslastung.

## Ports

Mittels der IP-Adresse allein können die Anwendungen Ihrer Rechner nicht miteinander kommunizieren. Die IP-Adressen sind nur für die Adressierung zwischen den Rechnern zuständig. Eine Netzwerkanwendung selbst kann nicht mit einer IP-Adresse versehen werden. Die sendenden und empfangenden Anwendungen benötigen für ihre Kommunikation im Netzwerkverkehr aber eine Art Kanal, was mit den Ports umgesetzt wird.

Die von Ihnen bemühten Netzwerkdienste benötigen ebenfalls einen Antwort-Port, einen Rückkanal. Ihre Client-Anwendungen benutzen dafür nicht die Standard-Port- Nummern, sondern verwenden welche aus dem dynamischen Bereich (49152–65535). Diese Port-Nummer übergibt Ihre Client-Anwendung schon beim Verbindungsaufbau dem betreffenden Netzwerk-Service.

Bei verbindungsorientierten Verbindungen mittels TCP bildet die IP-Adresse zusammen mit einem Port einen *Socket*. Ipv6-Sockets können Sie mit unterschiedlichen Schreibweisen darstellen.

IPv4, Telnet: **192.168.1.125:23**

IPv6, Telnet: **[fd91:e4a5:5e03::dd05]:23**

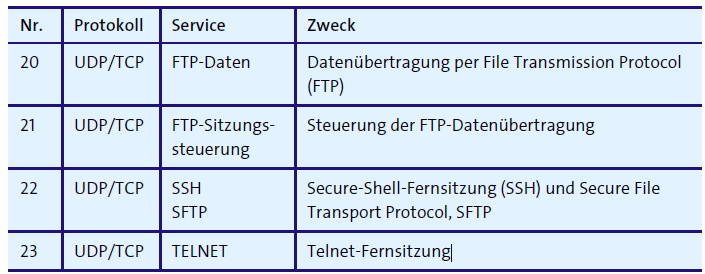
Die Ports finden Sie in drei Gruppen unterteilt:

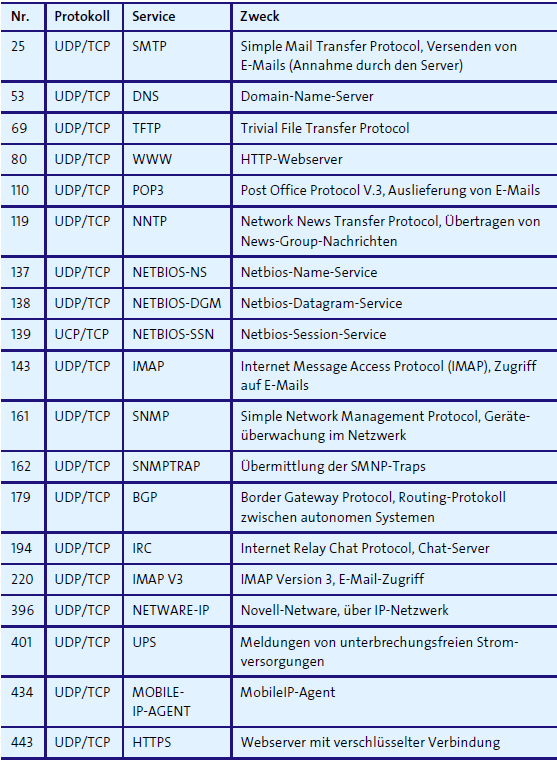
0–1023: *Well-known-Ports*, diese sind weltweit eindeutig durch die IANA festgelegt.

1024–49151: *Registered Ports*, teilweise für Anwendungen bei der IANA registriert

49152–65535: frei für dynamische Nutzung

Die komplette Liste finden Sie unter [*http://www.iana.org/assignments/port-numbers*](http://www.iana.org/assignments/port-numbers)*.*



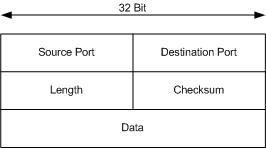


## UDP

UDP hat dieselbe Aufgabe wie TCP, nur das nahezu alle Kontrollfunktionen fehlen, dadurch schlanker und einfacher zu verarbeiten ist.

So besitzt UDP keinerlei Methoden die sicherstellen, dass ein Datenpaket beim Empfänger ankommt. Ebenso entfällt die Nummerierung der Datenpakete. UDP ist nicht in der Lage den Datenstrom in der richtigen Reihenfolge zusammenzusetzen. Stattdessen werden die UDP-Pakete direkt an die Anwendung weitergeleitet. Für eine sichere Datenübertragung ist deshalb die Anwendung zuständig.

In der Regel wird UDP für Anwendungen und Dienste verwendet, die mit Paketverlusten umgehen können oder sich selber um das Verbindungsmanagement kümmern. Typisch sind DNS-Anfragen, VPN-Verbindungen, Audio- und Video-Streaming.



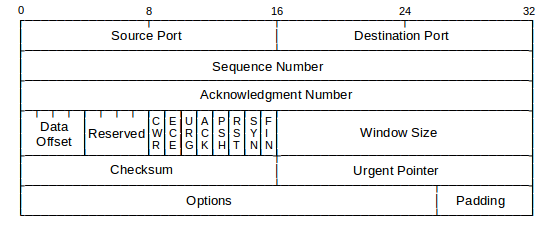
## TCP

TCP liegt in den Schichten oberhalb von IP, der Transportschicht. TCP setzt ausschließlich auf IP auf. Das TCP arbeitet im Gegensatz zum IP verbindungsorientiert, was heißt, dass vor dem Übertragen von Datenpaketen eine bidirektionale virtuelle Verbindung auf und später wieder abgebaut wird. Während in den Schichten unterhalb vom TCP kaum Überlegungen hinsichtlich möglicher Verluste ganzer Datenpakete angestellt werden, wird dies hier berücksichtigt. Das TCP überträgt aus Sicht des Dienstnutzers einen kontinuierlichen, aus Bytes bestehenden Datenstrom in beliebige Richtungen. Dabei legt es die Blockgrößen und das Weiterleiten von Daten selbst fest.

Die Daten werden gesichert durch:

* Sequenznummern
* Prüfsummenbildung mit Empfangsquittungen
* Quittung mit Zeitüberwachung
* Segmentwiederholung nach Quittungszeitablauf

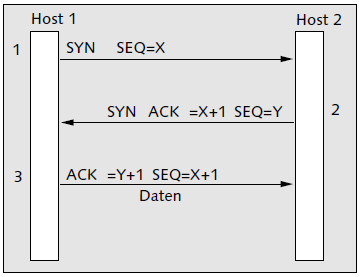
Der TCP Header hat eine Länge von mindestens 20 Byte und gliedert sich wie folgt auf:



|  |  |
| --- | --- |
| Source Port | Beschreibt den Quellport des Paketes |
| Destination Port | Beschreibt den Zielport des Paketes |
| Sequenz Number | Bei jeder TCP-Verbindung werden Nummern zwischen den Kommunikationspartner ausgehandelt. Während der Verbindung werden diese Nummern verwendet um die TCP-Pakete eindeutig zu identifizieren |
| Acknowledgement Number | Alle Datenpakete werden bestätigt. Dazu dienen das ACK-Flag und die Acknowledgement-Nummer, die sich aus der Sequenz-Nummer und der Anzahl von empfangenen Bytes errechnet. Damit kann der Sender feststellen, ob die Daten beim Empfänger vollständig angekommen sind |
| Data Offset (HL) | Hier steht die Anzahl der 32-Bit-Blöcke des TCP-Headers. Die Mindestmenge beträgt 5 |
| Window Size | Der Empfänger sendet dem Sender in diesem Feld die Anzahl an Daten, die der Sender senden darf. Dadurch wird das Überlaufen des Empfangspuffers beim Empfänger verhindert. Den Vorgang nennt man Windowing und dient der Datenflusssteuerung |
| Checksum | Dieses Feld dient der Kontrolle von Header- und Datenbereich. |
| Urgent Pointer | Zusammen mit der Sequenz-Nummer gibt dieser Wert die genaue Position der Daten im Datenstrom an. Der Wert ist nur gültig, wenn das URG-Flag gesetzt ist. |
| Options | Dieses Feld beinhaltet optionale Informationen. Um die 32-Bit-Grenze einzuhalten wird das Options-Feld mit Nullen aufgefüllt |
| Flags | Kennzeichnung bestimmter für die Kommunikation und Weiterverarbeitung der Daten wichtiger Zustände (URG, ACK, PSH, RST, SYN, FIN). |

#### Verbindungsaufbau

Zunächst sendet Host 1 ein Anfragepaket an Host 2 (SYN). Im Beispiel nimmt er die Anfrage an und sendet seine Zustimmung als SYN ACK-Paket zurück. Host 1bestätigt wiederum mit einem ACK den Erhalt und beginnt mit der Übermittlung der Datenpakete. Schon beim Verbindungsaufbau kommen beidseitig Sequenznummern zum Einsatz.



Diese Sequenznummern bildet jeder Host für sich (SEQ = X, SEQ = Y). Bei der ersten Antwort sendet Host 2 die um den Wert 1 erhöhte als Bestätigungsnummer (ACK, ACKNummer) zusammen mit seiner eigenen Sequenznummer zurück. Host 1 bestätigt den Erhalt, indem er mit ACK und der um 1 erhöhten Sequenznummer des Hosts 2 als Bestätigungsnummer antwortet. Gleichzeitig erhöht er den Wert seiner eigenen Sequenznummer und übermittelt diese ebenfalls. Die Verbindung ist aufgebaut.

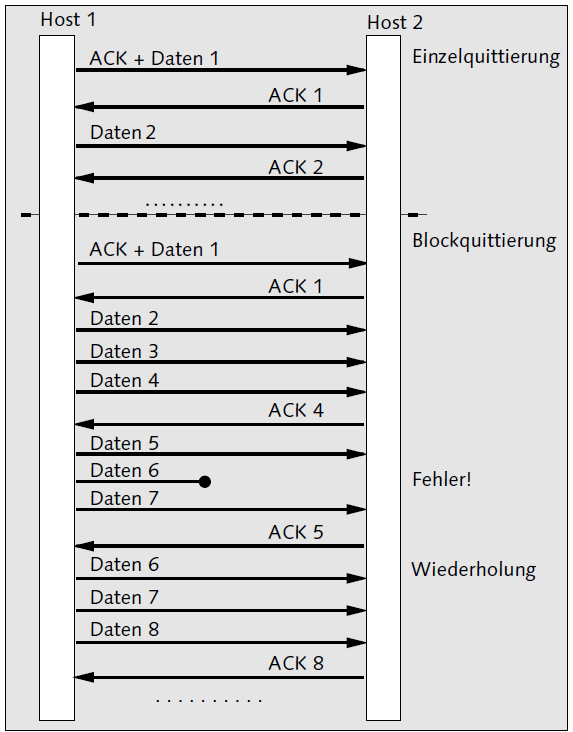
Einen Verbindungswunsch kann ein Host durch Senden eines Paketes mit dem RST-Flag ablehnen.

#### Datenübertragung

Nach dem erfolgreichen Verbindungsaufbau sendet Host 1 an Host 2 seine Daten. Für jedes erfolgreich übermittelte Paket antwortet Host 2 mit einem ACK Paket, welches auch die Bestätigungsnummer (= Sequenznummer des erhaltenen Paketes) beinhaltet. Im folgenden Beispiel sieht man zunächst den Ablauf der Einzelquittierung. Bei der reinen Datenübermittlung kommt diese kaum zum Einsatz, da diese das Netz zusätzlich belastet. Die gebräuchliche Blockquittierung erlaubt es dem Sender, mehrere Pakete zu übermitteln, wenn diese miteinander zusammenhängen. Der Empfänger gibt in seinem ACK-Paket als Bestätigungsnummer die letzte empfangene Sequenz zurück. Die Anzahl der maximal unbestätigten Bytes wird in der *Windowsize* angegeben. Die *Windowsize* wird während der Übertragung dynamisch angepasst.

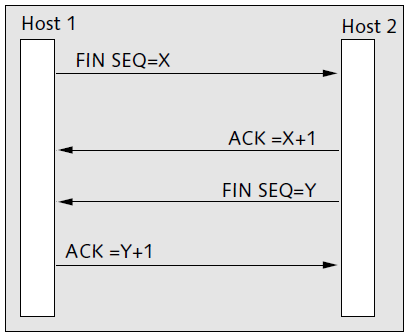
Tritt bei der Übermittlung ein Fehler auf, erkennt der Sender nach Ablauf eines Timers das Fehlen von unbestätigten Sequenzen (*Retransmission Timer*). Er sendet diese Pakete nochmals ab.

Wenn die Windowsize groß ist, müssen eventuell viele Daten neu übertragen werden.



#### Verbindungsabbau

Liegen keine zu übermittelnden Daten mehr vor, baut der Sender die TCP-Verbindung wieder ab. Auch dies unterliegt einem eigenen Formalismus. Der sendende Host 1 sendet ein Paket mit dem FIN-Flag, welches der Empfänger-Host 2 bestätigt. Dieser (Host 2) erklärt daraufhin seinerseits mittels eines FIN-Paketes die Verbindung für beendet. Host 1 bestätigt den Erhalt mittels ACK. Die TCP-Verbindung zwischen den beiden Rechnern ist damit aufgehoben.



Es ist notwendig, dass sich beide Hosts das Verbindungsende gegenseitig erklären. TCP Verbindungen sind bidirektional.

# Routing

Routen werden verwendet, um Pakete von einem Netzwerk in ein anderes Netzwerk senden zu können. Routing ist erst am Layer 3 (IP) möglich, da dazu die logischen IP Adressen (Aufteilung in NetID und HostID) notwendig sind.

## Statisches Routing

Statische Routen sind sehr einfach zu erstellen. Man kann sie am Router mit dem Befehl ip route setzen. Dazu muss man die Zielnetzadresse die dazugehörige Subnetzmaske und eine Schnittstelle auf der das Paket gesendet werden soll angeben.

Wien(config)#ip route 172.16.0.0 255.255.128.0 serial 0/0

S 172.16.0.0/17 is directly connected, Serial0/0

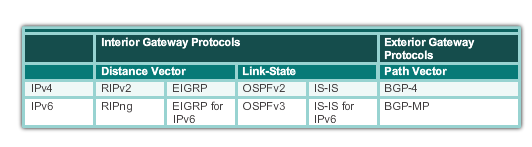
Dieses Verfahren ist sehr einfach und kommt daher häufig zum Einsatz.

Jeder Eintrag muss manuell vorgenommen werden, daher ist dieses Verfahren bei großen Netzwerken (mit häufigen Änderungen) sehr mühsam und kaum umsetzbar.

Jeder Router unterhält eine Tabelle mit einer Zeile für jeden möglichen Zielknoten. Vor der Weiterleitung eines Paketes wird der entsprechende Eintrag aus der Tabelle gewählt und auf eine der möglichen Leitungen gegeben.

## Dynamische Routingprotokolle

### Einteilung

Routingprotokolle sind nach verschiedenen Kriterien eingeteilt

* Interior vs. Exterior Gateway Protocol
* IPv4 vs. IPv6
* Distance Vector vs. Link State Protokoll
* Classless vs. Classful (heute bedeutungslos, z.B. RipV1, IGRP)

### Vergleich IGP und EGP

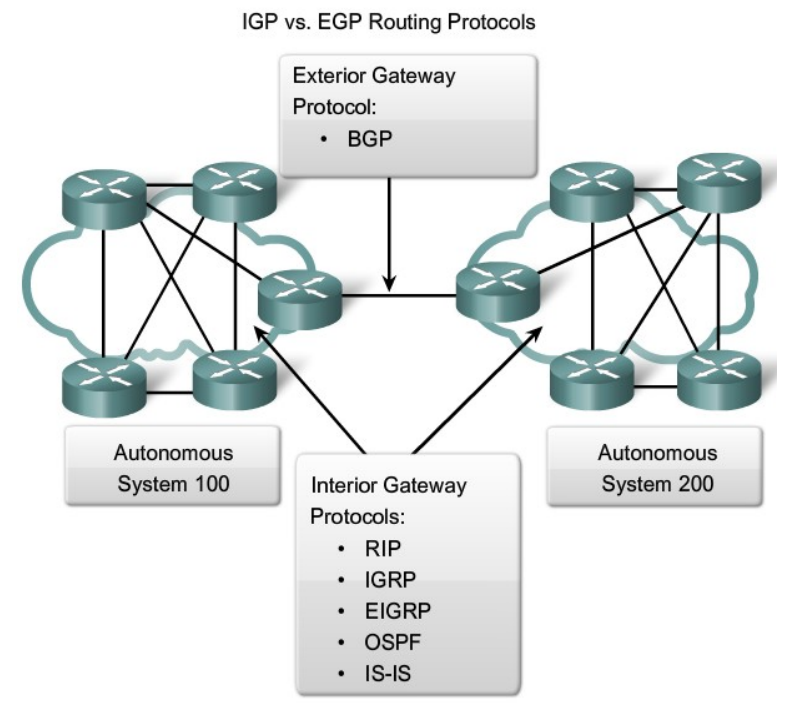
#### IGP (Interior Gateway Protocol):

Als IGP werden Routingprotokolle bezeichnet, die innerhalb von Systemen eingesetzt werden.

Im Gegensatz zu Exterior Gateway Protokollen (EGP) zeichnen sie sich durch besondere Fähigkeiten im Umgang mit komplizierten Netzwerktopologien aus.

#### EGP (Exterior Gateway Protocol):

Ein Exterior-Gateway-Protokoll (EGP) dient dazu, Erreichbarkeitsinformationen zwischen autonomen Systemen (AS) auszutauschen, d. h. Informationen darüber, welche Netze erreichbar sind. Diese Daten setzen dann die Router der Systeme in interne Routing-Informationen für IGP Routing-protokolle wie z. B. OSPF oder Routing Information Protocol (RIP) um.



### Vergleich statisches und dynamisches Routing

|  |  |  |
| --- | --- | --- |
|  | *Dynamic versus Static Routing* |  |
|  | **Dynamic Routing** | **Static Routing** |
| Komplexität | Unabhängig von der Netzwerkgröße | Abhängig von der Netzwerkgröße |
| Topologieänderungen | Werden automatisch übernommen | Müssen vom Administrator behandelt werden |
| Skalierbarkeit | Für große und kleine Netzwerke geeignet | Für kleine und einfache Netzwerke geeignet |
| Sicherheit | Weniger sicher als Statische Routen | Sicherer als Dynamisches Routing |
| Ressourcenbelegung | Verbraucht Ressourcen wie z.B.: CPU-Zeit, Speicher | Verbraucht keine Ressourcen |

### Begriffe

#### Konvergenzzeit

Unter Konvergenz versteht man die Fähigkeit eines Routing-Verfahrens, nach einer Netzänderung möglichst schnell in den stabilen Betriebszustand zurückzukehren.

Da das Netzwerk bei Änderungen in der Regel nicht vollständig funktionsfähig ist, ist eine schnelle Konvergenzzeit von großer Bedeutung.

Langsame Konvergenzzeit: RIP

Schnelle Konvergenzzeit: EIGRP und OSPF

#### Metrik

Die Metrik wird vom Routingprotokoll berechnet und wird zum Bewerten einer Route verwendet. Zur Berechnung der Metrik einer Route können die Bandbreite, der Delay, die Zuverlässigkeit der Hop-Count und die MTU verwendet werden.

Je nach Routingprotokoll wird die Metrik anders bestimmt. Diese unterschiedlichen Metriken können nicht miteinander verglichen werden!

#### Administrative Distanz

Jedem Routing-Protokoll ist eine Administrative Distanz zugeordnet. Diese ist eine Maß für die Seriosität eines Protokolls. Falls nun in einem Netzwerk verschiedene Routingprotokolle eingesetzt werden und diese für ein bestimmtes Paket verschiedene Routen vorsehen so wird das Protokoll mit der niedrigeren Administrativen Distanz ausgewählt.

|  |  |
| --- | --- |
| Protokoll | Wert der administrativen Distanz |
| Statisches Routing | 1 |
| Internal EIGRP | 90 |
| OSPF | 110 |
| IS-IS | 115 |
| RIP | 120 |

### Distance Vector Routing

Distance-Vector-Protokolle bestimmen die Erreichbarkeit durch einen Vektor aus Entfernung und Richtung. Sobald Änderungen der Netzwerktopologie bekannt werden, spiegeln sich diese in Update-Nachrichten wider. Entdeckt ein Router eine unterbrochene Verbindung oder den Ausfall seines Nachbarn, berechnet er die betroffenen Wege neu und verschickt Änderungsmeldungen an alle erreichbaren Knoten. Jeder Router, der eine derartige Meldung erhält, passt seine Routingtabelle an und propagiert diese Änderung.

#### Ablauf:

Das Austauschen der Routing-Tabellen erfolgt folgendermaßen: Router A gibt seine Informationen zu Router B weiter. Dieser Router B gleicht die neuen Informationen von Router A mit seinen vorhandenen Informationen ab und aktualisiert die Metrik (z.B. Anzahl der Hops). Nun gibt Router B die aktualisierte Routing-Tabelle an Router C weiter. Dieser Vorgang wiederholt sich bei jedem benachbarten Router. Zu beachten ist dabei, dass den Routern nicht die gesamte bzw. genaue Topologie des Netzwerks bekannt ist.

In der Praxis hat dieses Verfahren eine **langsame Konvergenz** und sind daher nur für kleine Netzwerke geeignet.

Ein Problem das auftreten kann sind Routingschleifen. Dazu gibt es verschieden Gegenmaßnahmen:

* **Split horizon**  
  Es werden keine Informationen zurückgeschickt woher sie gekommen sind
* **Triggerd Updates**  
  Änderungen werden sofort weitergeschickt (und nicht erst nach Ablauf des Timers)
* **Count to infinity**  
  Der maximale Hopcount wird auf 16 festgelegt. Eine Route gilt dann als nicht erreichbar
* **Route poisoning**  
  Eine unerreichbare Route wird mit der Metrik 16 eingetragen und wird dadurch nicht mehr verwendet

Beispiele für Distance Vector Protokolle:

* RIP
* IGRP

### Link State Routing

Link-State-Protokolle gelten als Alternative zu Distance-Vector-Ansätzen und versuchen demzufolge einige ihrer Schwächen auszugleichen. Im Gegensatz zu Distance-Vector-Protokollen, die nur eine eingeschränkte Sicht auf die Netztopologie haben, haben die Router bei Link-State-Protokollen einen vollständigen Überblick über den Aufbau des Netzes.

* Netze werden dazu in Bereiche (so genannte Areas) aufgeteilt.
* Alle Router innerhalb einer Area verfügen über die gleiche Datenbasis. Diese Datenbasis beschreibt die vollständige Topologie der Area.
* Jeder Router benutzt diese Datenbasis, um den optimalen Pfad abzuleiten und diesen in seine Routingtabelle zu stellen.
* Hello-Pakete stellen den Kontakt zu den Nachbarroutern her. Unter Ausnutzung des Multicast-Mechanismus werden alle Nachbarrouter angesprochen.

Zur Aktualisierung der Datenbasis verwendet das Link-State-Protokoll **keine periodischen Updates**, sondern sendet nur **bei Bedarf** ein Link-State-Update.

Dieser Bedarf entsteht, wenn:

* ein neuer Router entdeckt wird
* ein Router seinen Dienst einstellt
* die Kosten einer Verbindung sich ändern
* periodisch alle 30 Minuten.

Beispiele für Link-State Protokolle:

* OSPF
* IS-IS

## EIGRP (Distance Vector)

EIGRP (Enhanced Interior Gateway Protocol) ist ein erweitertes Distance-Vector-Routingprotokoll, welches sich beim Austausch mit benachbarten Geräten sowie bei der Speicherung von Routing-Informationen **wie ein Link-State-Routingprotokoll** verhält. Aufgrund der umfangreichen Merkmale, welche eher bei Link-State-Protokollen anzutreffen sind wird EIGRP daher oft auch als **Balanced-Hybrid-Routingprotokoll** klassifiziert. Mit Hilfe jener Link-State-Eigenschaften erreicht EIGRP im Verhältnis zu konventionellen Distance-Vector-Routingprotokollen eine sehr schnelle Konvergenz und ist immun gegenüber Routing-Schleifen.

Im Gegensatz zu RIP verwaltet EIGRP drei Tabellen (pro Protokoll, also IPv4, IPv6):

* **Neighbor Table**  
  Alle direkt benachbarten Router
* **Topology Table**  
  Alle verfügbaren Routen
* **Routing Table**  
  Die Routen, die zum Routing verwendet werden

Verwendet werden folgende 5 Pakettypen:

* **Hello**

Wird verwendet um Nachbarrouter zu erkennen

* **Ack**

Wird verwendet um Pakete zu bestätigen

* **Update**

Wird verwendet um neue Routen an die Nachbarrouter zu übertragen

* **Query**

Wird verwendet um Routinginformationen von den Nachbarroutern abzufragen

* **Reply**

Wird verwendet um auf ein Query zu antworten

Hello Pakete werden alle 5 Sekunden (bzw. alle 60 Sekunden auf langsamen Verbindung) auf allen Interfaces ausgesendet. Dazu wird die Multicastadresse 224.0.0.10 (bzw. FF02::A) verwendet. Auf den Interfaces wo Hello Pakete empfangen werden, werden Nachbarschaftsbeziehungen (*Neighbor Adjacency*) aufgebaut.

Der Default *Holddowntimer* beträgt 3 Mal die *Hellotime*. Wenn solange kein Hellopaket empfangen wird, wird die Neighbor Adjacency gelöscht.

Jeder EIGRP Prozess hat einen eigene *Autonomous System Number* die beim Konfigurieren angegeben werden muss. Damit können in einem Netzwerk mehrere EIGRP Prozesse nebeneinander ablaufen. Diese Nummer kann frei vergeben werden und muss nicht wie bei einem BGP bei der IANA registriert werden.

### Metrik

Die Metrik wird bei EIGRP beinhaltet folgende Komponenten:

* Bandbreite (Bandwidth, BW)
* Auslastung (load)
* Verzögerungszeit (delay)
* Zuverlässigkeit (reliability)

Die Metrik berechnet sich folgendermaßen:



Mit den Konstanten K können die einzelnen Faktoren gewichtet werden. Default mäßig sind alle 0 bis auf K1=1 und K3=1.

Damit reduziert sich die Berechnung auf:



Es macht allerdings keinen Sinn, da eine hohe Bandbreite eine niedrige Metrik bewirken sollte. Weiters setzt sich eine zusammengesetzte Bandbreite aus mehreren Teilstücken mit unterschiedlichen Bandbreiten und Delays zusammen. Die tatsächliche Formel für die Berechnung der Metrik lautet:



BW in Kilobit/s, Delay in Mikrosekunden.

Die Werte können dabei direkt aus der Interfaceinformation ausgelesen werden. Diese Werte können auch verändert werden ohne die Eigenschaften des Interfaces zu verändern.



### DUAL

EIGRP nutzt den sogenannten Diffusing Update Algorithm (DUAL). Dieser Algorithmus verhindert Schleifen und synchronisiert alle betroffenen Router zur selben Zeit. Router die von keinen Änderungen betroffen sind werden nicht miteinbezogen.

Eigenschaften:

* **Schnelle Konvergenzzeit**DUAL erlaubt es zusätzlich alternative Routen zu berechnen die bei einem Ausfall der besten Route verwendet werden können.
* **Teilweise Updates**EIGRP sendet bei Änderungen nicht die komplette Routing-Tabelle neu sondern nur die jeweiligen Änderungen, dies reduziert die Netzwerkbelastung.
* **Schleifenfreiheit**

Der Nachbarrouter der die beste Verbindung zu einem bestimmten Netzwerk hat ist der *Successor* für dieses Netzwerk. Die Metrik dieser Route nennt man die *Feasible Distance* (FD).



Ein Nachbarrouter der ebenso eine schleifenfreie Route in das Zielnetzwerk hat wird als Feasible Successor (FS) bezeichnet. Dazu muss er die *Feasibility Condition* erfüllen.

Die Metrik die vom Nachbarrouter gemeldet wird bezeichnet man als die *Reported Distance* (RD).

Die *Feasibility Condition* ist erfüllt, wenn die RD einer Route kleiner ist als die FD. Damit wird die Schleifenfreiheit gewährleistet.

Die FS werden in der Topologietable gespeichert und können beim Ausfall eines Successors schnell eingesetzt werden. Der Ablauf schaut dabei folgendermaßen aus:



## *OSPF*

Open Shortest Path First (OSPF) ist eines der Link State Routing Protokolle. Die erste Version war experimentell und wurde nie offiziell released. Definiert wurde sie in der RFC 2328. Die aktuelle Version ist OSPFv3. Version 3 unterstützt nur IPv6-Adressen. Bei Netzwerken mit IPv4 Adressen wird OSPFv2 verwenden. OSPF dient zur Routenberechnung und zum schleifenfreien Routing in großen und skalierbaren Netzwerken. Es gibt sowohl VLSM, als auch CIDR Unterstützung.

Allgemeine Merkmale von OSPF:

* Garantiert schleifenfreies Routing, durch Aufbau eines SPF-Trees
* Nutzt das Hello-Protokoll für die Überwachung des Nachbarn
* Unterstützt VLSM (Variable Length of Subnet Mask) sowie CIDR (Classless Inter-Domain Routing), indem Subnet-Informationen über die Updates propagiert werden.
* OSPF ist gut für große skalierbare Netze
* Das Area-Konzept vereinfacht Kommunikation und Wartung

### Pakettypen

Es gibt fünf verschiedene Arten von Pakete:

1. **Hello** Entdeckt Nachbarn, baut Verbindungen zwischen ihnen auf und gibt die Richtlinien vor, welche die Router akzeptieren müssen um Nachbarn zu werden. Es enthält die Router ID des sendenden Routers und wird normalerweise als Multicast (224.0.0.5) gesendet. Diese Hello-Nachrichten müssen in einem definierten Intervall gesendet werden. Dieses Intervall muss auf allen Routern gleich sein, sonst kann keine Verbindung aufgebaut werden. OSPF Dead Intervals werden verwendet um festzustellen, ob ein Router down ist. Die Standard-Zeit ist vier Mal das Hello-Intervall.
2. **Database Description (DBD)**: Ist für die Datenbank Synchronisation zwischen den Routern verantwortlich.
3. **Link-State Request (LSR)** Fragt spezifische Link-State Einträge von einem Router an.
4. **Link-State Update (LSU)** Sendet spezifische Link-State-Advertisments (LSA). LSAs enthalten Information über die Nachbarn und die Path costs.
5. **Link-State Acknowledgement (LSAck)** Bestätigt die anderen Pakettypen

#### LSA Typen

**Router LSA (Typ 1)**: Ein [Router](https://de.wikipedia.org/wiki/Router) sendet für jede [OSPF](https://de.wikipedia.org/wiki/OSPF)-Area, der er zugeordnet ist, eine LSA. Sie beschreibt die gesammelten Zustände der Schnittstellen des Routers. Sie wird nur in die Area geflooded, in der die jeweilige Schnittstelle sich befindet.

**Network LSA (Typ 2)**: Eine Network-LSA wird in Broadcast-Netzen gesendet und beschreibt die Router, die an das Netz angeschlossen sind. Sind mehrere Router in einem Broadcast-Netz (z.B. [Ethernet](https://de.wikipedia.org/wiki/Ethernet)) zusammengeschaltet, so werden zur Vermeidung überflüssigen [Traffics](https://de.wikipedia.org/wiki/Datenverkehr) Network-LSAs nur von einem einzelnen sog. Designated Router gesendet.

**Summary LSA (Typ 3 oder 4)**: Eine Summary-LSA wird von Area Border Routern (ABR) gesendet, diese sitzen an den Grenzen zwischen zwei OSPF-Areas. Ein ABR ist also an mindestens 2 Areas angeschlossen und kann Informationen, die er aus einer Area gelernt hat in einer anderen Area verbreiten. Dies ist zweckmäßig, damit eine Area Routen in Netze anderer Areas kennt, die Metriken für diese Routen werden aggregiert, d.h. der Aufbau anderer Areas muss nicht bekannt sein, sondern nur die Kosten für das Routing in ein Netz in einer anderen Area. Summary LSAs vom Typ 3 werden zwischen OSPF-Areas ausgetauscht, Summary LSAs vom Typ 4 beschreiben Routen zu AS Boundary Routern, also Routern, die an der Grenze zu Areas sitzen, in denen andere Routing-Protokolle zum Einsatz kommen. Somit wird der ASBR als nächster Hop für die Route in OSPF-externe Areas bekannt gegeben.

**Autonomous-System external LSA (Typ 5)**: AS-external LSAs werden von ASBR in alle Areas geflooded (außer in Stub-Netze) und enthalten Informationen über Ziele außerhalb des Autonomous Systems. Die Metriken in den externen Netzen werden entweder zu den OSPF-Metriken addiert oder es werden nur die externen Metriken ab dem ASBR propagiert.

### Router Typen

Über die Hello- Pakete werden der Designated Router (DR) und der Backup Designated Router (BDR) bestimmt.

* **DR** Dieser ist verantwortlich für das Updaten aller anderen OSPF Router. Dieser ist außerdem der einzige Router, welcher LSAs verschicken darf. So wird Flooding verhindert. Ohne ihn würde jeder Router bei jeder Netzwerkänderung LSAs an seine Nachbarn schicken.
* **BDR** Übernimmt die Aufgaben des DRs sollte dieser ausfallen.
* **Area Border Router (ABR)** Router zwischen einer regulären und einer Backbone Area. Bei einer Area mit mehr als einem Router gibt es auch einen Backup-ABR. Ein ABR kann LSA-Nachrichten filtern und über Route Summarization mehrere Router zusammenfassen.
* **Autonomous System Border Router (ASBR)** Ein Router der ein internes Netzwerk mit einem Externen verbindet.

### OSPF Algorithmus

Jeder OSPF Router baut eine **Link-State-Database** auf, welche die LSAs, die von den anderen Routern empfangen wurden, enthält. Aus dieser wird dann unter Verwendung des Dijkstra (Shortest Path First) **Algorithmus** ein SPF-Baum erstellt. Mithilfe dieser wird dann die Routing Tabelle erstellt.

Durch den SPF-Baum wird das Netzwerk schleifenfrei gehalten.

Je größer das Netzwerk wird desto größer wird die Link-State-Database, desto mehr Änderungen treten auf, desto langsamer wird alles. Areas lösen dieses Problem.

### Areas

Area dienen dazu die Flut von Informationen, die die Router bei Änderungen aussenden zu kontrollieren. Da bei jeder Änderung der Routing-Informationen alle Router in dieser Area benachrichtigt werden müssen, sollte man die Areas klug definieren um unnötige Netzwerkauslastung zu vermeiden.

#### Backbone Area

Dies ist die Verbindungsbrücke zwischen den Areas und hat die Nummer 0.

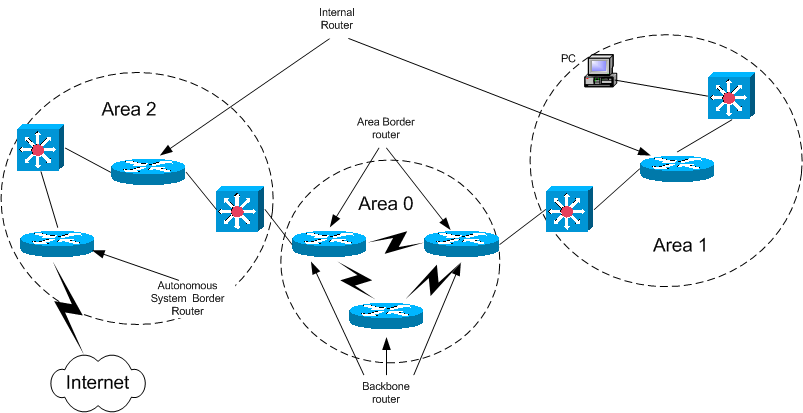
#### Reguläre Area

Alle anderen Areas sind reguläre Areas. Die Area-Nummer dieser liegt zwischen 1 und 232-1, kann aber auch eine äquivalente Netz-ID sein.

#### Transit Area

Reguläre Areas müssen direkt mit der Backbone Area verbunden sein. Sollte dies nicht der Fall sein müssen Virtual Links zur Überbrückung der im Weg liegenden Area definiert werden. Diese wird dann zur Transit Area.

Ein OSPF-Netzwerk könnte so aussehen:



#### Sonstiges

Der Standardwert der Administrativen Distanz von OSPF ist 110.

OSPF bietet die Möglichkeit für Authentifizierung. Damit kann man die gesendeten Informationen verschlüsseln und authentifizieren. Dies muss auf dem Interface spezifiziert werden. Router werden dann nur noch Pakete akzeptieren, welche mit den „richtigen“ Informationen authentifiziert wurden.

#### Router ID

Dies ist die Adresse welche zur Identifikation der Router verwendet wird. Für das generieren der Router ID werden folgende Informationen verwendet:

* Die Adresse welche mit dem router-id Befehl erstellt wurde.
* Sollte dies nicht geschehen sein, wird die höchste IP-Adresse eines loopback Interfaces verwendet. Loopback Interfaces werden bevorzugt, da diese nicht ausfallen können, im Gegensatz zu anderen Interfaces.
* Sollte es keines geben wird die höchste IP-Adresse eines aktiven Interfaces verwendet.

### OSPF verifizieren

Beispiel einer OSPF-Nachbar-Tabelle:

Wien#sh ip ospf neighbor

Neighbor ID Pri State Dead Time Address Interface

192.168.1.254 1 FULL/DR 00:00:39 10.0.0.2 FastEthernet0/0

192.168.3.254 1 FULL/BDR 00:00:32 10.0.0.1 FastEthernet0/0

**Neighbor ID** Hier handelt es sich um die Router ID des Nachbar-Routers.

**Priority** Der Router mit der höchsten Priority wird zum DR. Standart-Wert der Priority ist 1, ist der Wert auf 0 kann der Router nie DR oder BDR werden.

**State** Hier sieht man ob der Router DR oder BDR ist. Es gibt auch den Status DROTHER der angibt, dass der Router weder DR noch BDR ist.

**Dead Time** Gibt an wie lange der Router noch auf ein Hello-Packet vom Nachbar-Router wartet bis er ihn für down erklärt.

**Address** Die IP-Adresse des Interfaces das mit dem Nachbarn verbunden ist.

### Metrik

OSPF verwendet Kosten als Wert um die beste Route zu berechnen. Logischerweise ist die Route mit den geringsten Kosten die beste. Die Cost basiert auf der Bandbreite eines Interfaces und kann über folgende Formel berechnet werden:

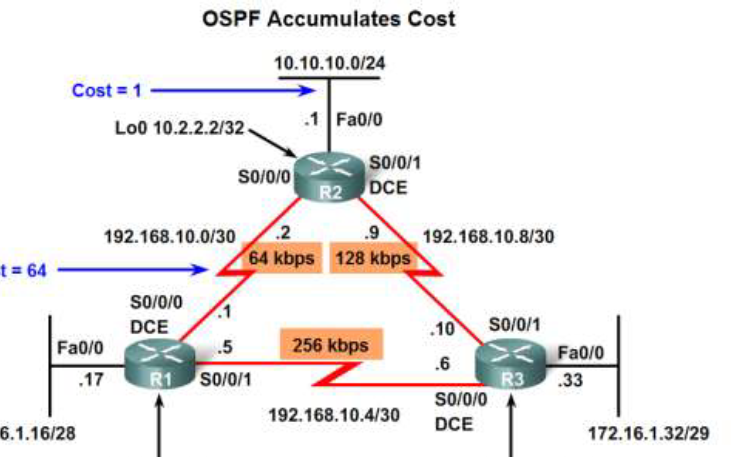
Referenzbandbreite in bps/Bandbreite in bps

Der Default-Wert dieser Referenzbandbreite ist 100 Mbps und kann über per Befehl verändert werden. Die Bandbreiten können aus der folgender Tabelle entnommen werden:

|  |  |
| --- | --- |
| Interface Typ | 108/bps = Kosten |
| Fast Ethernet und schneller | 108/100 000 000 bps = 1 |
| Ethernet | 108/10 000 000 bps = 10 |
| E1 | 108/2 048 000 bps = 48 |
| T1 | 108/1 544 000 bps = 64 |
| 128 kbps | 108/128 000 bps = 781 |
| 64 kbps | 108/64 000 bps = 1562 |
| 56 kbps | 108/56 000 bps = 1785 |

Ein Problem, welches sich aus der Referenzbandbreite von 108 ergibt ist, dass es keinen Unterschied zwischen einer Fast Ethernet Verbindung und einer schnelleren Route gibt. Alles ab 100 Mbit ist gleichwertig, für OSPF. Wenn man diese Referenzbandbreite verändern will, muss man dies auf allen Routern tun.

Die Kosten einer OSPF Route sind die Gesamtkosten aller Verbindungen, welche auf dem Weg liegen.



In diesem Fall wären somit die Kosten um von 10.10.10.0 zu Router R1 zu kommen 1 (aufgrund des Fa0/0 Interfaces) und 64 (Aufgrund der 64 kbps Schnittstelle). Dies bedeutet, dass die Gesamtkosten 65 betragen.

Beide Seiten einer Verbindung sollten die selbe Bandbreite haben. Man kann die Kosten auch direkt setzen. Wenn man das tut werden sie logischerweise nicht berechnet.

### OSPF in Multiaccess-Netzwerken

OSPF definiert fünf verschiedene Arten von Netzwerken:

1. Point-To-Point
2. Broadcast Multiaccess
3. Nonbroadcast Multiaccess (NBMA)
4. Point-to-multipoint
5. Virtual Links

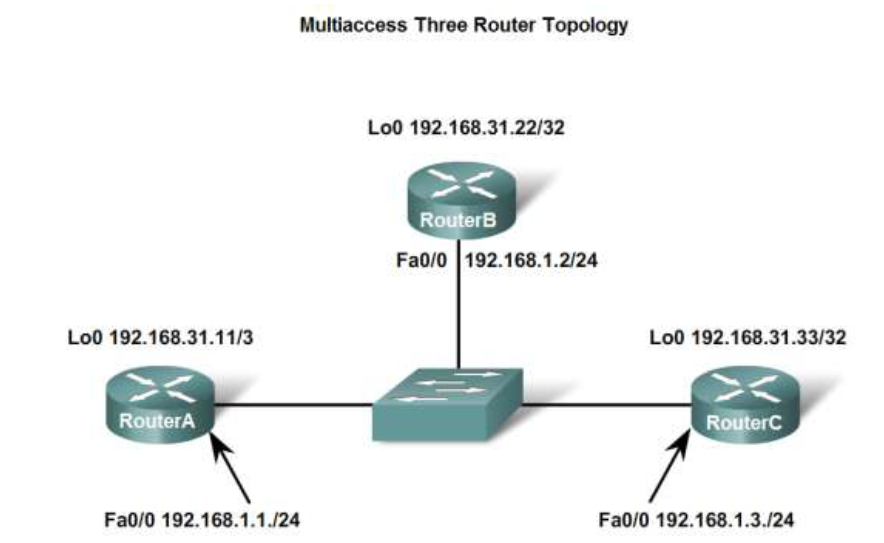
#### Herausforderungen in Multiaccess-Netzwerken

In Multiaccess-Netzwerken gibt es zwei Probleme:

* Mehrfache Adjacencies
* Umfangreiches LSA Flooding

Für jedes LSA muss ein Acknowledgement zurück zum Sender des LSAs geschickt werden. Dies führt dazu, dass viel Bandbreite für solche Nachrichten verwendet wird und der Netzwerktraffic zunehmend chaotisch wird (LSA - Flooding).   
Gelöst wird dies durch die Verwendung von DR und BDR. Nur der DR darf LSAs schicken, der BDR nur dann, wenn der DR ausgefallen ist. Sobald also ein DR von einem anderen DR die Benachrichtigung bekommt, dass das Netzwerk verändert wurde schickt er diese in seinem Bereich weiter. Somit ist das Problem des LSa-Flooding gelöst.

Dafür muss aber zunächst ein DR bzw. ein BDR bestimmt werden. (Dies geschieht nicht in Point-to-point Netzwerken)



#### Bestimmung des DRs

Der DR/BDR wird anhand dreier Kriterien ausgewählt:

1. DR: Hier wird der Router mit der höchsten OSPF Interface Priorität ausgewählt.
2. BDR: Der Router mit der zweithöchsten OSPF Interface Priorität.
3. Sollten die Prioritäten gleich sein entscheidet die höchste Router ID.

Dieser Wahl-Prozess beginnt sofort nachdem der erste Router sein Interface für multiaccess-Netzwerke aktiviert hat. Der DR bleibt der DR bis er, der OSPF Prozess oder das multiaccess-Interface ausfällt. Wenn man einen bestimmten Router als DR haben will kann man den Wahl-Prozess manipulieren, indem man diesen Router zuerst hochfährt, anschließend den gewünschten BDR und dann den Rest. Alternativ kann man auch das Interface auf allen Routern herunterfahren bis auf den gewünschten DR und BDR.   
Man kann die Priorität per Befehl verändern, der Standardwert ist 1.

# Monitoring und Troubleshooting

# WAN

## Punkt zu Punkt Verbindungen

### HDLC

### PPP

## Frame Relay

1. Bridge packet data unit [↑](#footnote-ref-1)
2. Link Aggregation Control Protocol [↑](#footnote-ref-2)
3. Port Aggregation Protocol [↑](#footnote-ref-3)
4. Extensible Authentication Protocol [↑](#footnote-ref-4)
5. Remote Authentication Dial-In User Service [↑](#footnote-ref-5)