ZUSAMMENFASSUNG KOMMUNIKATIONS-TECHNOLOGIEN

Version: 1.0.1

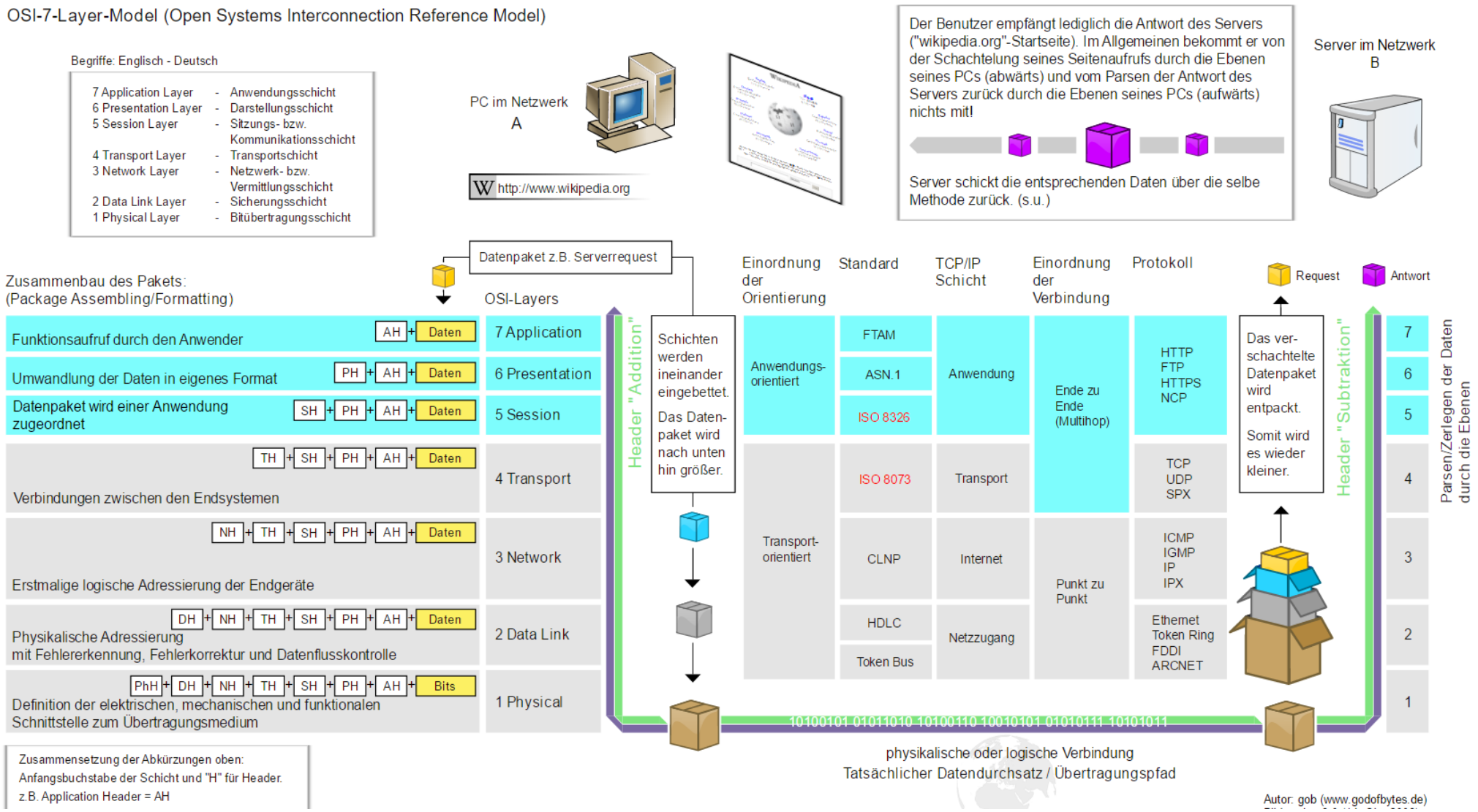
Study: 3. Semester, Bachelor in Business and Computer Science

School: Hochschule Luzern - Wirtschaft

Author: Kevin Stadelmann, Janik von Rotz (http://janikvonrotz.ch)

1 INHALTSVERZEICHNIS

2 EINSTIEG NETZWERKE

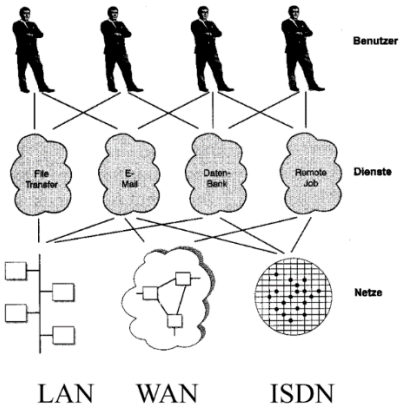


3 NETZWERKARCHITEKTUR

Bezieht sich auf die Unterlagen aus dem 1. Kursteil.

- „proprietäre" versus „offene" Architekturen
- Anwendungen tauschen Daten aus
- Verschiedene Anwendungen brauchen gemeinsame Vereinbarungen für die Kommunikation
- „Kompatibilität" erfordert Standards
- Abstraktionshilfe für technische Kommunikationsprozesse: Unterteilung in verschiedene **„Schichten"**
- Schnittstellen
  - Ebene der Interaktion zweier kommunizierender Systeme
- Protokolle
  - Vereinbarungen über die Rahmenbedingungen

3.1 3 Ebenen

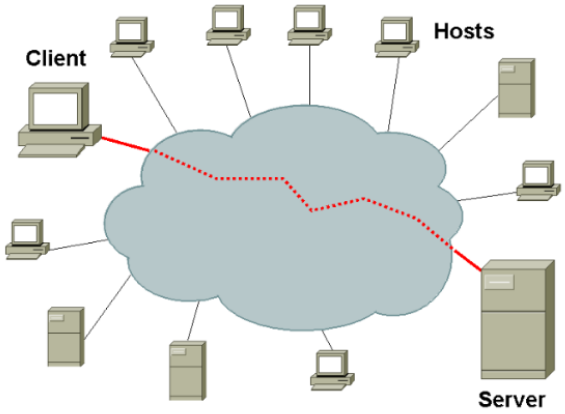


- Benutzer
  - P2P Sicht
  - C/S Sicht
- Dienste
  - Filetransfer
  - E-Mail
  - DB-Zugriff
  - Nutzung entfernter Systeme
- Netze
  - LAN
  - WAN
  - ISDN

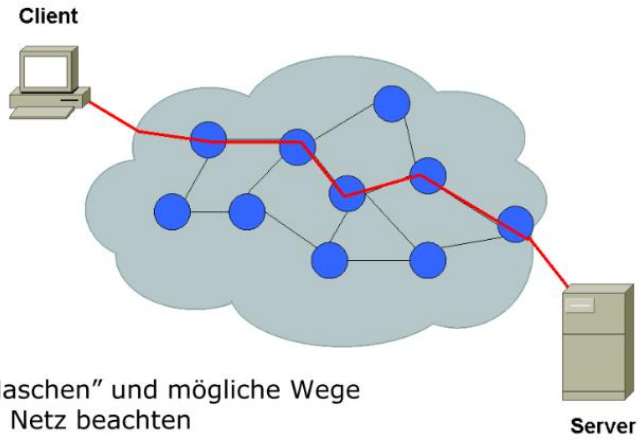
World Wide Web ist ein Dienst auf dem Internet

3.2 Sichten und Topologien

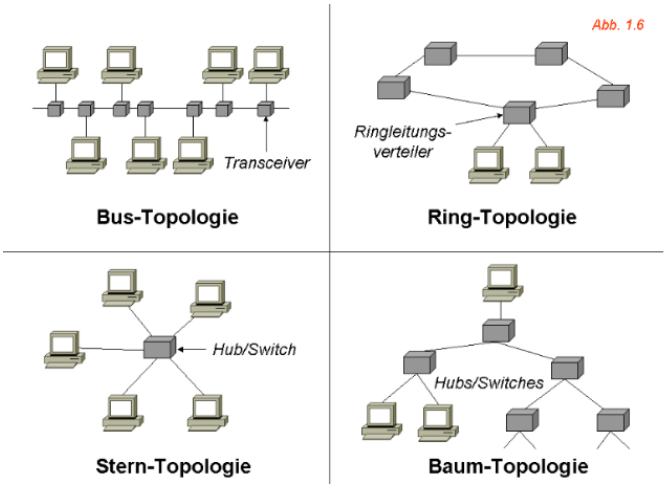
Benutzersicht



Betreibersicht



Weitere Topologien



Ring- und Bus-Topologien kommen heute selten oder gar nicht mehr zum Einsatz.

Mainframe mit Terminalnetz

„klassische" DV

- hoher Organisationsgrad
- schwerfällige Programmierung
- aufwändiger Betrieb
- i.d.R. sicher und zuverlässig
- „Legacy System"

Wichtig:
„Mainframe",
nicht „Host"

Dezentrale Datenverarbeitung

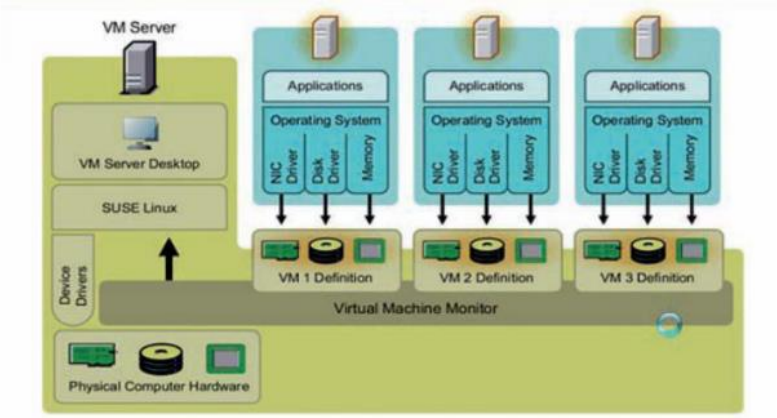
Nachteile:
- Neigung zur „chaotischen" Evolution
- Kompatibilität?
- Sicherheitsprobleme

Vorteile:
- preiswerte Software
- ergonomisch
- beliebig konfigurier- und erweiterbar mit Peripherie

Serverfarmen

- Verbunden durch leistungsfähige Netzwerke
- Vernetzte Areitssationen als intelligente Terminals
- "Farm" von (Terminal-) Servern

Virtuelle Systeme



Ein Wirt-System(grün) beherbergt drei Virtuelle Maschinen (türkis) als Gäste und stellt ihnen seine (reelle) Hardware zur Verfügung. In der Konfiguration werden Disk-Grösse, RAM, NIC, etc. für die Gastsysteme festgelegt. Diese „merken" nicht, dass ihre „Hardware "umgebung nicht real ist. Der sog. „Remote Desktop Zugriff" erlaubt die Benutzung der VM übers Netzwerk.

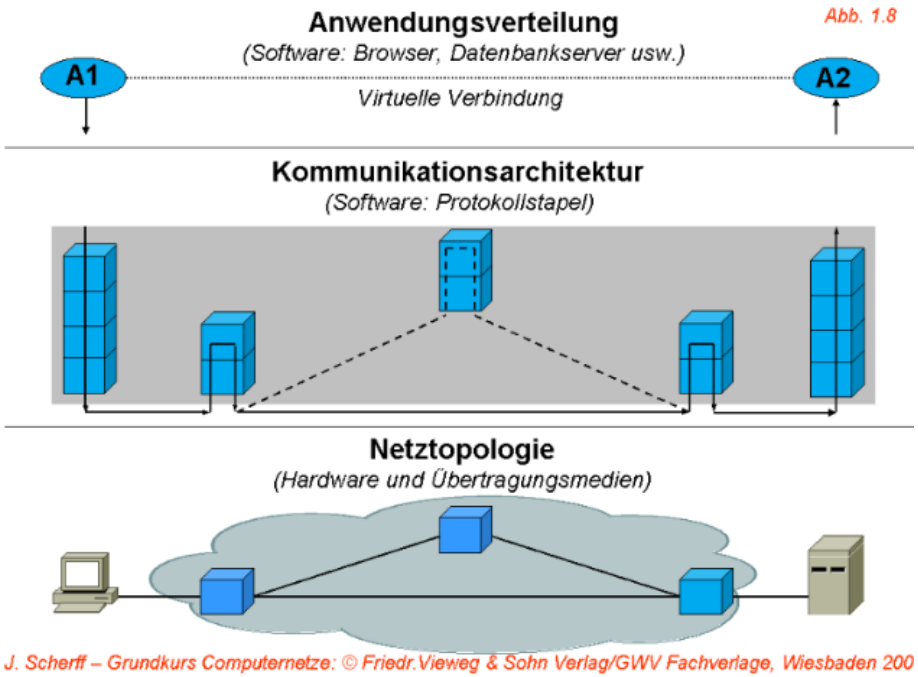
3.3 Aufgaben, Ziele und Funktionen

Warum Netzwerke überhaupt eingesetzt werden.

- Datenverbund
  - Gemeinsamer Zugriff auf (konsistente) Datenbestände
- Funktionsverbund
  - z.B. gemeinsame Nutzung aufwändiger Datensicherungsverfahren
- Verfügbarkeitsverbund
  - z.B. redundante Systeme zur Überbrückung von Ausfällen
- Leistungsverbund
  - verteilte, ggf. parallele Verarbeitung (nicht für vieles geeignet)
- Lastverbund
  - Dispatching von Aufträgen auf verschiedene Rechner
  - z.B. e-Shop-Lösungen grosser Anbieter

3.4 Netzwerkschicht

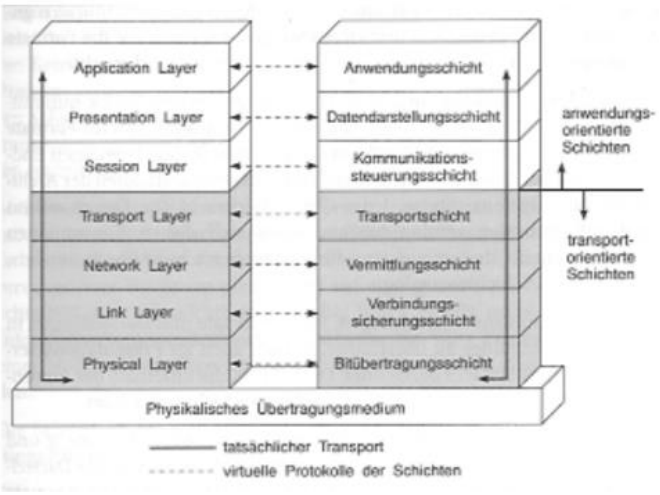
Kommunikation über das Netzwerk wird in verschiedenen Layern abstrahiert.



Jede Schicht übernimmt eine bestimmte Funktion und vereinfacht den überliegenden Protokollen die Kommunikation.

OSI Referenzmodell (Open Systems Interconnection)

- Anschauliche Beschreibung der Netzarchitektur
- Allgemein anerkannter Standard
- Zu komplex für reale Implementation!
- Dennoch sehr geeignet und häufig verwendet zur Illustration von Zusammenhängen



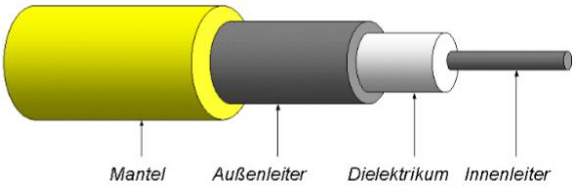
4 LAYER 1 – MEDIEN- UND ZUGRIFFVERFAHREN

Bezieht sich auf die Unterlagen aus dem 2. Kurs.

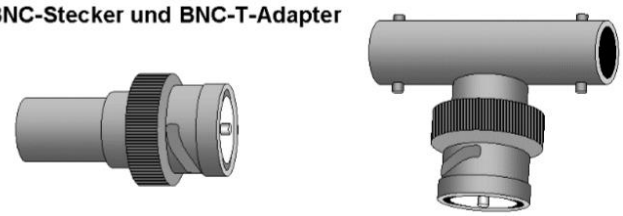
4.1 Übertragungskabel

Koaxialkabel

Koaxialkabel: Sobald der Innenleiter ein Unterbruch hat, ist das ganze Signal verloren. Das Koaxialkabel wird heute praktisch nicht mehr eingesetzt. (Militärantennen)



BNC-Stecker und BNC-T-Adapter



CU-Kabel (Kupfer)

TP = Twisted Pair

Sobald Strom durch die Kabel fliesst, entsteht ein elektromagnetisches Feld. Durch das Verdrillen will man die entstehenden Felder aufheben.

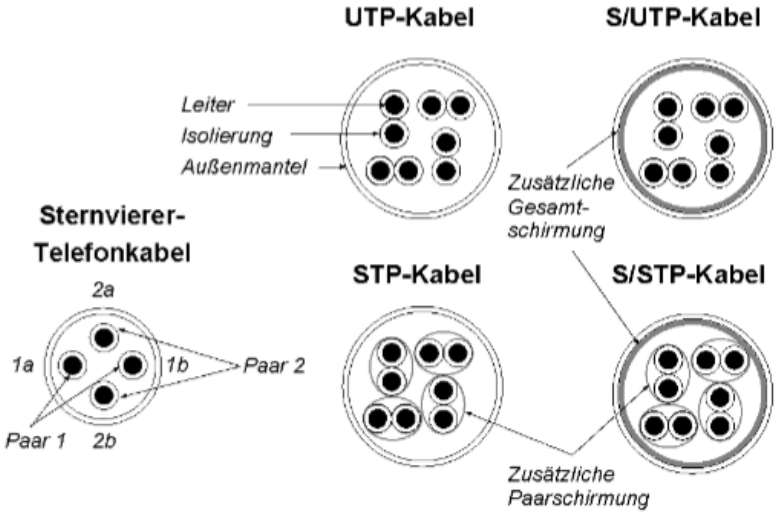
STP = Shielded Twisted Pair

Wiederstand: Stromstärke lässt sich regulieren.

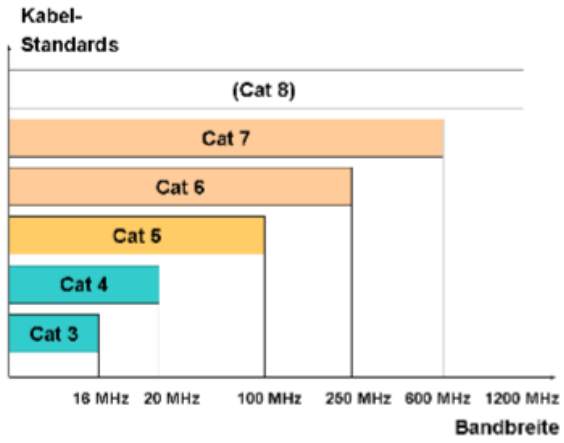
12 Volt und 1 Ohm-Widerstand = 12Amper

12Volt und 10 Ohm-Widerstand = 1.2Amper

Dämpfung: Amplitude von Schwingungen nimmt mit der Zeit ab



Kategorien von Twisted Pair Kabeln



Kat.	Beschreibung
3	Wird nicht mehr Verkauft, früher Standardkabel für Telefonanschluss in den USA Basis für 4-Mbit Tokenring
4	Häufig in der USA verlegt, jedoch zugunsten der Kategorie 5 ignoriert Basis für 16-Mbit Tokenring
5	Überwiegender Standard, RJ45-Kabel basieren auf dieser Kategorie Basis für Verkabelungen von Fast- oder Gigabit-Ethernet Netzwerken
6	Anwendungsfeld: Sprach- und Datenübertragung Basis für 10-Gigabit-Ethernet Netzwerk

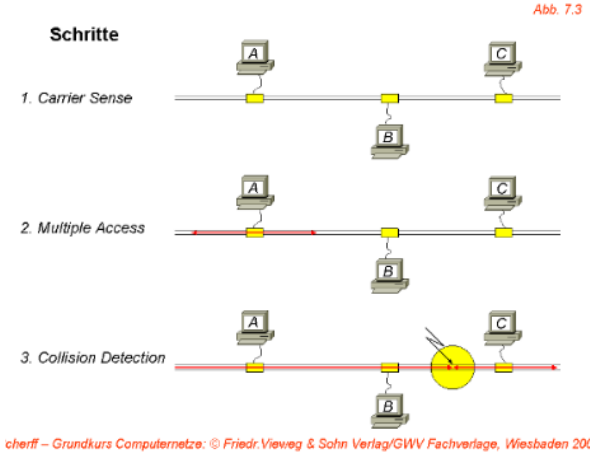
Glasfaser

#ergänzen

4.2 Zugriffsverfahren

Verfahren wie

CSMA/CD



- Zuhören, ob Leitung frei
- Mit Senden beginnen
- Mithören, ob Kollision stattfindet
- Im Falle einer Kollision abbrechen, Jam-Signal senden
- nach zufällig gewählter Wartezeit wieder von vorne beginnen

(stochastisch)

Token Ring und Token-Passing

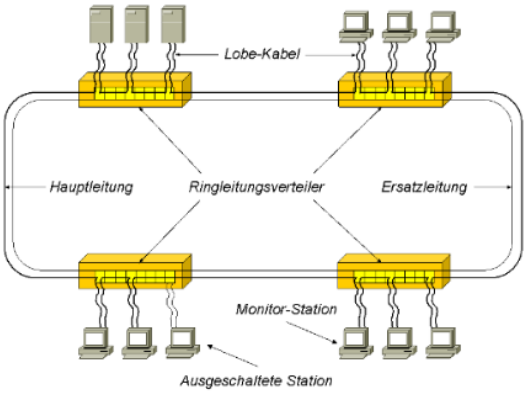


Abb. 7.4

cherff – Grundkurs Computernetze: © Friedr.Vieweg & Sohn Verlag/GWV Fachverlage, Wiesbaden 2006

- Ring-Struktur geeignet
- Sendeberechtigung (Recht auf Kabelbenützung) wandert wie eine Spielmarke (Token) im Kreis
- Kann für eine Zeiteinheit benutzt oder weitergegeben werden
- Auslastung und Kapazität einfach berechenbar, da jede Station Token erhält (deterministisch)

5 LAYER 2 – SICHERUNGSSCHICHT

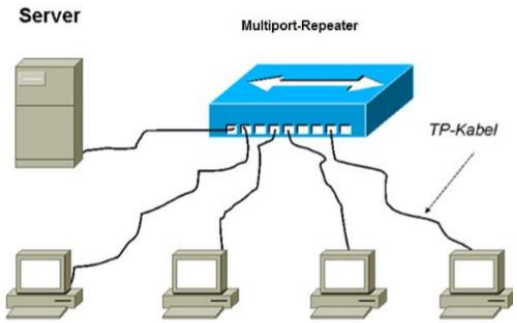
Bezieht sich auf den 3. Kursteil.

Aufgabe der Sicherungsschicht ist es, eine zuverlässige, das heißt weitgehend fehlerfreie Übertragung zu gewährleisten und den Zugriff auf das Übertragungsmedium zu regeln.

5.1 Netzwerkgeräte

Repeater

Ein Repeater ist in der Kommunikationstechnik ein elektrischer oder auch optischer Signalverstärker/aufbereiter zur Vergrösserung der Reichweite eines Signals.



Hub

Ein Hub verbindet mehrere Stationen in einem Netzwerk miteinander. Somit verbinden Hubs Netzsegmente auf der physikalischen Schicht (Schicht 1), wodurch eine gemeinsame Kollisionsdomäne entsteht. Der Hub hat also nur eine Verteilerfunktion, indem er Datenpakete entgegen nimmt und an alle anderen Ports weiterleitet. Das heißt insbesondere auch, dass ein Hub Datenpakete auch an Stationen weiterschickt, die eigentlich nicht Empfänger der Daten sind.

Bridges

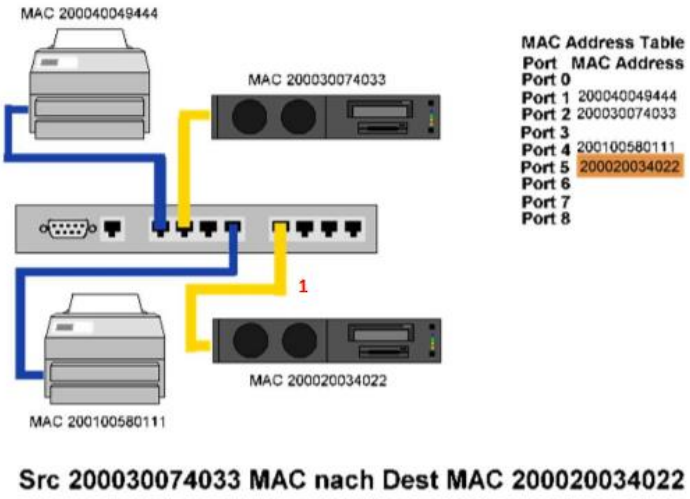
Brücken oder Bridges sind dazu da, 2 Computersegmente im Netzwerk zu verbinden. Brücken unterbrechen hierbei Kollisionsdomänen, indem Datenpakete nur dann in das jeweils andere Segment weitergeleitet werden, wenn sich der jeweilige Empfänger in diesem Segment befindet. Im Gegensatz zu Hubs, werden also Datenpakete nicht einfach an alle Ports weitergeleitet, sondern die Weiterleitungsentscheidungen werden auf Basis der der Ziel-Mac-Adresse getroffen. Im Schichtenmodell, arbeiten Brücken im Gegensatz zu Hubs auf Schicht 2 (Sicherungsschicht).

Switch

Switches sind, ähnlich wie Brücken, Kopplungselemente die auf der Sicherungsschicht arbeiten und die Kollisionsdomäne unterbrechen. Im Gegensatz zu Brücken haben Switches aber mehr als zwei Ports. Switches und Hubs werden häufig miteinander verwechselt, nicht zuletzt weil die Geräte fast identisch aussehen (können), während ein Hub aber nur ein stupider Sternverteiler ist, kann ein Switch auch eine Direktverbindung zwischen angeschlossenen Computern schalten.

Braucht ein Switch eine IP-Adresse? „JEin“: Nur wenn man den Switch über eine Management-Oberfläche konfigurieren möchte.

Switches „lernen“ während der Benutzung Ihr Netzwerk:



Src 200030074033 MAC nach Dest MAC 200020034022

5.1.1 ARTEN VON SWITCHING

Cut Trough

Beim Cut-Trough Verfahren wird nicht gewartet, bis das eintreffende Paket vollständig geladen ist, sondern nur bis die ersten Bytes, die die Zieladresse beinhalten, geladen sind. Nach dem auswerten der Zieladresse (interne Adresstabelle) wird der Datenstrom bereits auf den entsprechenden Ausgangsport geleitet. Das Datenpaket wird ohne Fehlerkorrektur weitergeitet. Auf diese Art ist die Latenzzeit extrem gering.

Store and forward

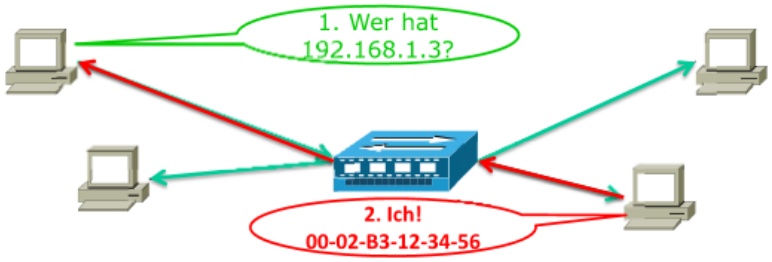
Wie der Name dieses Verfahrens bereits sagt, wird das ganze Datenpaket (bzw. „Frame“) als erstes gespeichert. Danach wird die Prüfsumme berechnet und mit dem CRC-Wert des Pakets überprüft. Besteht keine Differenz, wird das Paket der entsprechenden Zieladresse weitergeleitet. Falls eine Differenz und somit ein Fehler aufgetreten ist, wird das Paket verworfen. Store and forward ist somit die sicherste Methode im Switching, um die Datenströme fehlerfrei zu behalten, jedoch auch mit Abstand das langsamste. (Nicht für Streaming möglich, aber dafür für Short Message Services wie Whatsapp etc.)

5.2 Protokolle

Address Resolution Protocol (ARP)

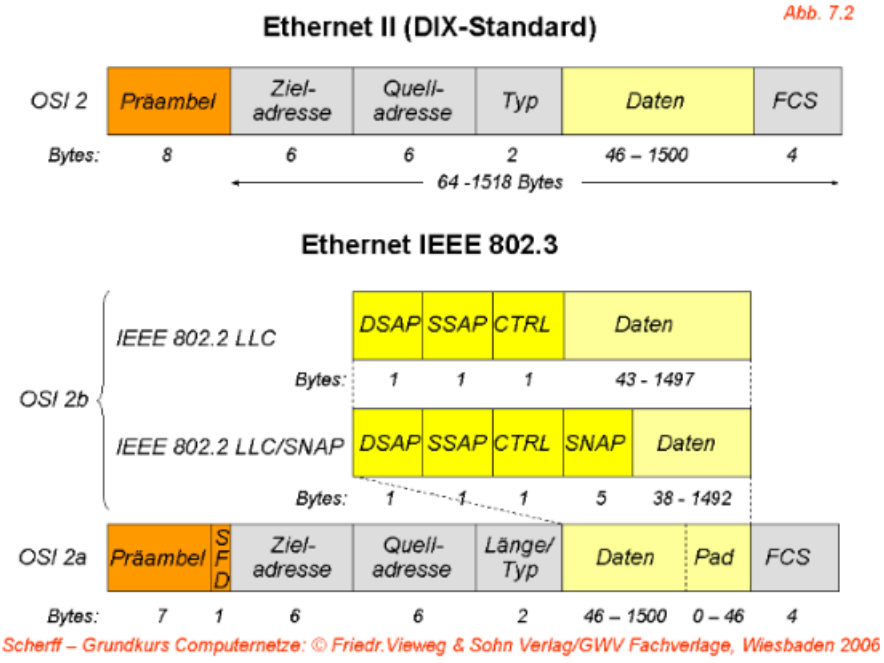
Das Address Resolution Protocol (ARP) ist ein Netzwerkprotokoll, das zu einer Netzwerkadresse der Internetschicht die physikalische Adresse (Hardwareadresse) der Netzzugangsschicht ermittelt und diese Zuordnung gegebenenfalls in den so genannten ARP-Tabellen der beteiligten Rechner hinterlegt.

Es wird fast ausschließlich im Zusammenhang mit IPv4-Adressierung auf Ethernet-Netzen, also zur Ermittlung von MAC-Adressen zu gegebenen IP-Adressen verwendet, obwohl es nicht darauf beschränkt ist. Für IPv6 wird diese Funktionalität nicht von ARP, sondern durch das **Neighbor Discovery Protocol (NDP)** bereitgestellt.



Ein Rechner A will einem Rechner B Daten versenden. Für das braucht er die physikalische Adresse (MAC) des Empfängers. Bekannt ist nur die logische Adresse (IP) des Empfängers. Rechner A prüft als erstes ob die Empfänger IP im gleichen Netz ist. Wenn ja, versendet Rechner A ein Paket mit seiner IP- und MAC-Adresse als Broadcast und fragt wer die IP-Adresse 192.168.1.3 hat. Der Rechner mit der angefragten IP-Adresse speichert die Daten des Anfragenden Rechners in seiner ARP-Tabelle und füllt seine MAC-Adresse ins Paket und schickt sie zurück. Nun ist beiden, Sender und Empfänger, alles bekannt, sie können Daten austauschen.

Ethernet



Das „einfache" Original von **D**igital, **I**ntel und **X**erox

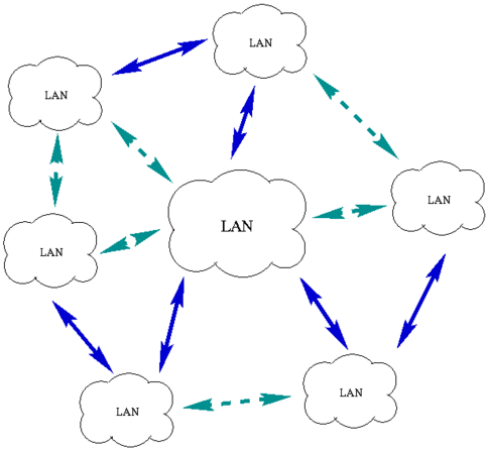
Der komplexe Aufbau des inneren LLC-Frames im Standard IEEE 802.3 ermöglicht den Simultanbetrieb verschiedener Service Access Points (SAP)

Wir gehen hier nicht auf Details ein und unterscheiden erst auf höheren Layern

Spanning Tree Protocol (STP)

Der Spanning Tree Algorithmus wird eingesetzt, um bei Verknüpfungen von Netzwerken redundante Pfade (sog. Loops) durch einen deterministischen logischen Pfad im Netz zu ersetzen.

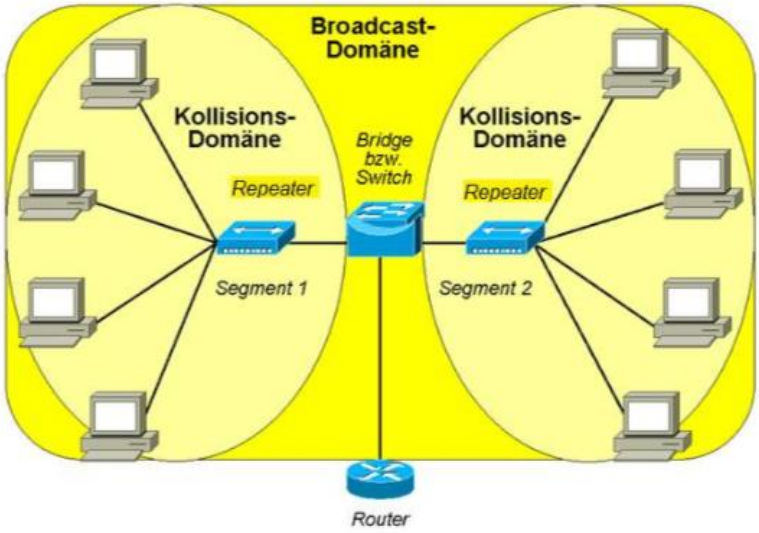
Im Beispiel rechts sind verschiedene LANs durch Bridges (Pfeile) miteinander verknüpft. Wie leicht zu sehen ist, würden alle Bridge-Links zusammen redundante Pfade im Netz ermöglichen. Dieses hätte sog. endlos kreisende Pakete zur Folge. Mit dem Spanning Tree Algorithmus wird einer der möglichen logischen Pfade im Netz ausgewählt, der dann keine Loops mehr enthält. Das Ergebnis sind hier die blauen (ungebrochenen) Pfeile. Im Extremfall kann hierdurch auch eine Bridge total aus dem Netzverkehr herausfallen



5.3 Kollisions- und Broadcast-Domänen

Eine Broadcast-Domäne ist ein logischer Verbund von Netzwerkgeräten in einem lokalen Netzwerk, der sich dadurch auszeichnet, dass ein Broadcast alle Domänenteilnehmer erreicht.

Die Kollisionsdomäne ist ein Teilbereich bestehend aus Teilnehmerstationen auf Layer 1 des OSI-Schichten Modells. Sie umfasst alle Netzwerkgeräte, die gemeinsam um den Zugriff auf ein Übertragungsmedium (geteilte Ressource) konkurrieren (Kabel oder Funknetz). Beginnen zwei Teilnehmerstationen gleichzeitig zu senden, kommt es zu Kollisionen. Die Signale (Spannungsimpulse) werden im Übertragungsmedium vermischt/überlagert und die Informationen dadurch zerstört.

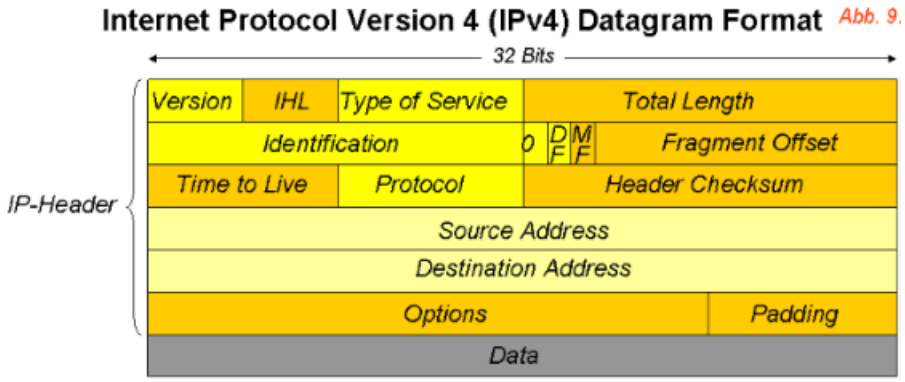


6 LAYER 3 – VERMITTLUNGSSCHICHT

Bezieht sich auf den 4. Kursteil.

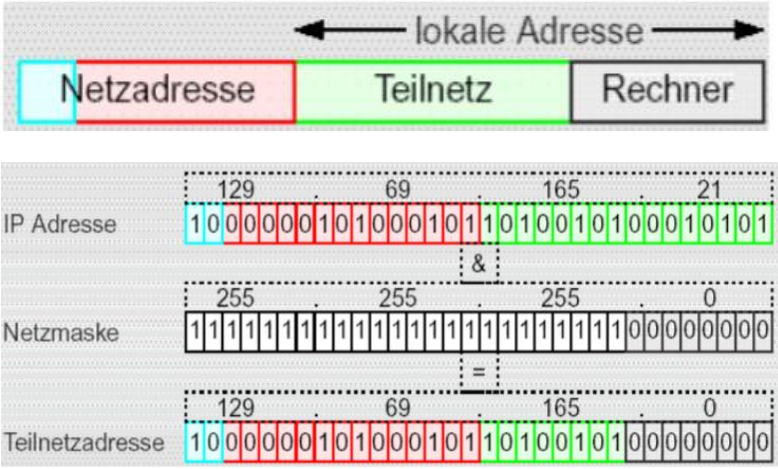
6.1 Internet Protocol (IP)

In Layer 3 gelten andere Adressen als in Layer 2 (physische Adressen, MAC-Adressen). Durchgesetzt hat sich das IP-Adressierungssystem. IP-Adressen sind weltweit gültig, eindeutig, einheitlich und werden deshalb zentral verwaltet. Die Koordination dabei übernimmt die Organisation IANA – Internet Assigned Numbers Authority.



- Traffic Class: Was gebe ich durch
- Payload Length: Länge der Daten
- Time To Live: wie viele "hops" das IP-Paket macht

Eine IPv4 Adresse ist 32 Bit breit (IPv6 128 Bit).



Netzmaske zeigt an, wie viele Bits die Netzwerkkennung definieren. Im obigen Netz werden 24 Bits für die Netzwerkkennung benutzt („24-Bit-Netz“), 8 Bits sind frei verfügbar für Geräteteile. Die Teilnetzadresse ist die Netzerkennung für diese eine Teilnetz (immer am Schluss eine „0“).

6.2 Spezielle IP-Adressen und Klassen

In Subnetzen gibt es auf Layer 3 (IP) fest reservierte Adressen, die keinem Host zugewiesen werden dürfen. Das sind:

Subnetzadresse	Die kleinste Verfügbare Adresse ist die Bezeichnung des Subnetzes.
Broadcast-Adresse	Die grösste Verfügbare Adresse ist für die Rundspruchsendung. Datenpakte für diese Adresse müssen von jedem Netzwerkgerät entgegen genommen werden.
Auto Private IP Adress (APIPA)	169.254.0.1 – 169.254.255.255, kommen dann zum Einsatz wenn kein „DHCP“ Dienst vorhanden ist.
Superprivate Adressen	127.x.x.x

Wichtig: Durch die Segmentierung von Netzen gehen immer Minimum zwei Adressen für Endgeräte verloren. Beachtet man noch den benötigten Router für Netzwerk-Netzwerk Kommunikation, sind es sogar drei Adressen die „verloren“ gehen.

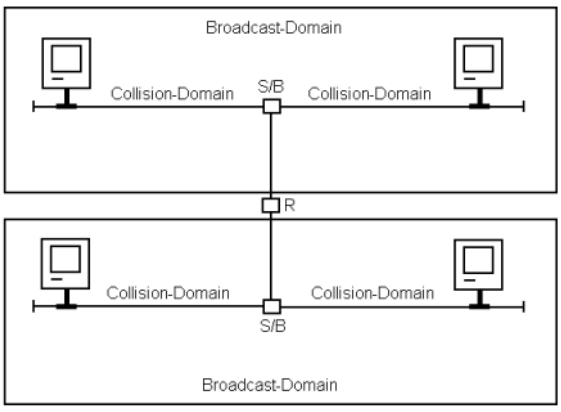
Adressklassen

Man unterscheidet zwischen fünf Klassen von Adressen. Grosser Unterschied zwischen ihnen ist die Anzahl Hosts, welche adressiert werden können -> Grösse der möglichen Netze.

Klasse	Start-Adr	End-Adresse	Binär 1. Byte	Netzwerkteil	Hostteil	Private Adressen
A	0.0.0.0	127.255.255.255	0000 0000	1. Byte fix	3 Bytes frei	10.x.x.x (1 Netz)
B	128.0.0.0	191.255.255.255	1000 0000	1.+2. Byte fix	2 Bytes frei	172.(16-31).x.x (16 Netze)
C	192.0.0.0	223.255.255.255	1100 0000	1.,2.+3. Byte fix	1 Byte frei	192.168.x.x (256 Netze)
D	224.0.0.0	239.255.255.255	1110 0000		Multicast	
E	240.0.0.0	255.255.255.255	1111 0000	Test/Entwicklung		

6.3 Broadcast

Alle 65536 Hosts einer B-Klasse Adresse auf Layer 1 oder 2 zu kommunizieren zu lassen, macht keinen Sinn. Alleine die Rundsendungen (Broadcasts) würden das Netzwerk zum Erliegen bringen. Deshalb unterteilt man die Netze in so genannte Subnetze.

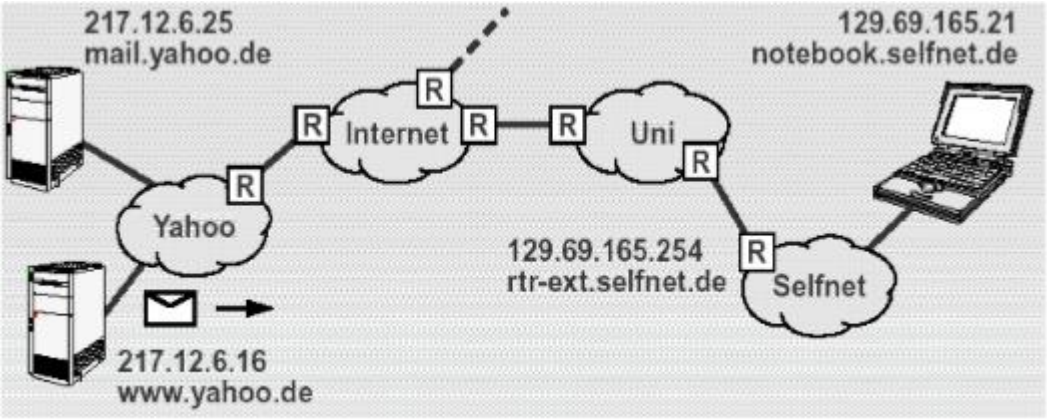


1.Layer	Hubs und Medium Konverter
2.Layer	Switches und Bridges -> trennen Kollisionsdomänen
3.Layer	Router -> trennen Broadcast-Domänen

Die Kommunikation erfolgt innerhalb von Broadcastdomänen auf Layer 2 mithilfe von **ARP** (Address Resolution Protocol) und zwischen ihnen über Router auf Layer 3.

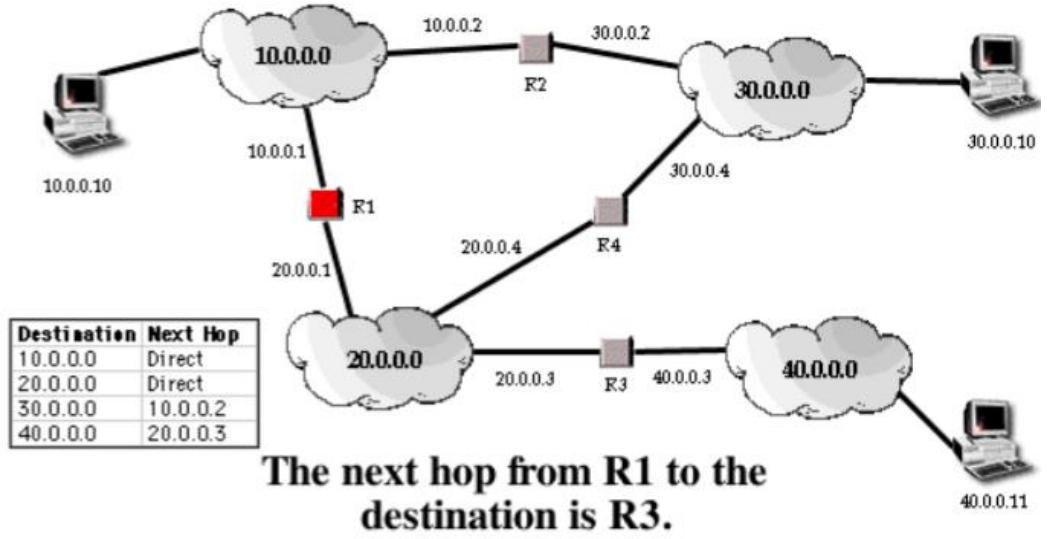
6.4 Routing

Jedes IP-Paket enthält eine Ziel- und Herkunftsadresse. Falls ein Rechner sich nicht im gleichen Netz befindet, wird das Paket in Richtung des Zielnetzes weitergeschickt. Für das Weiterschicken sind die Geräte an den Netzübergängen zuständig – die Router.



Statisches Routing

Dieses Verfahren ist *nicht adaptiv*, sehr einfach und kommt daher eher in sehr kleinen Netzen zum Einsatz. Jeder Router („Knoten“) unterhält eine Tabelle mit einer Zeile für jeden möglichen Zielrouter („Zielknoten). Grösster Nachteil ist, dass sich die Routing-Tabellen nicht verändern. Um eine fehlerfreie Datenkommunikation zu ermöglichen, darf sich das Netzwerk nicht verändern.



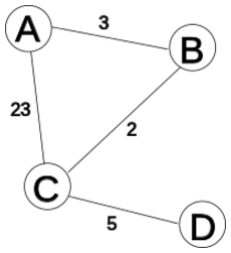
Dynamisches Routing

Der grosse Vorteil beim dynamischen Routing ist, das die Routing-Tabellen automatisch aktualisiert werden. Nachfolgend werden zwei bekannte Methoden auf möglichst einfache Art und Weise erklärt.

6.5 Ermittlung von Routen

Distance Vetor Verfahren

Situation: Ein Netz mit vier Routern ist geben. Die Zahlen zwischen den Routern beschreiben die „Zeitkosten“ für Datenpakete.



1. Erzeuge eine Kostenmatrix, welche Router über welche Nachbarn und zu welchen Kosten erreichbar sind und anfangs nur die (bekannten) Kosten zu direkten Nachbarn enthält.

T=0

von A	via A	via B	via C	via D
zu A				
zu B		3		
zu C			23	
zu D				

von B	via A	via B	via C	via D
zu A	3			
zu B				
zu C			2	
zu D				

von C	via A	via B	via C	via D
zu A	23			
zu B		2		
zu C				
zu D				5

von D	via A	via B	via C	via D
zu A				
zu B				
zu C			5	
zu D				

2. Erzeuge eine Aufstellung mit Informationen, welche Router wir zu welchen Kosten am besten erreichen können und schicke sie an alle Nachbarn.
3. Warte auf Aufstellungen dieser Art von anderen Routern, rechne diese dann in die eigene Kostenmatrix ein.
4. Ändern sich dadurch die minimalen Kosten, zu denen wir einen Router erreichen können: fahre mit Schritt 2 fort, sonst mit Schritt 3.

Tiefe Konvergenz: Veränderungen werden nur von den erhaltenen Datenpakte übermittelt und jeweils nur für die eine Strecke die sie durchlaufen haben. Beispiel Protokoll ist das RIP

Link State Routing

Beim Link-State-Routing werden nur die Informationen über die direkten Nachbarn verschickt, dafür aber gleich an alle Router des Netzwerks. Mit diesen Informationen kann dann jeder Router seine Routing-Tabelle berechnen. Da die Änderungen verbindungsorientiert an die benachbarten Router propagiert werden, besitzen Routing-Protokolle mit dem LSA eine gute Konvergenz.

Wenn es viele Veränderungen in der Routingtabelle gibt und die Routingtabelle oft oder regelmäßig aktualisiert werden muss, empfiehlt es sich, ein Link-State-Routingprotokoll zu verwenden. Dabei werden nur die jeweiligen Änderungen unter den Routern ausgetauscht.

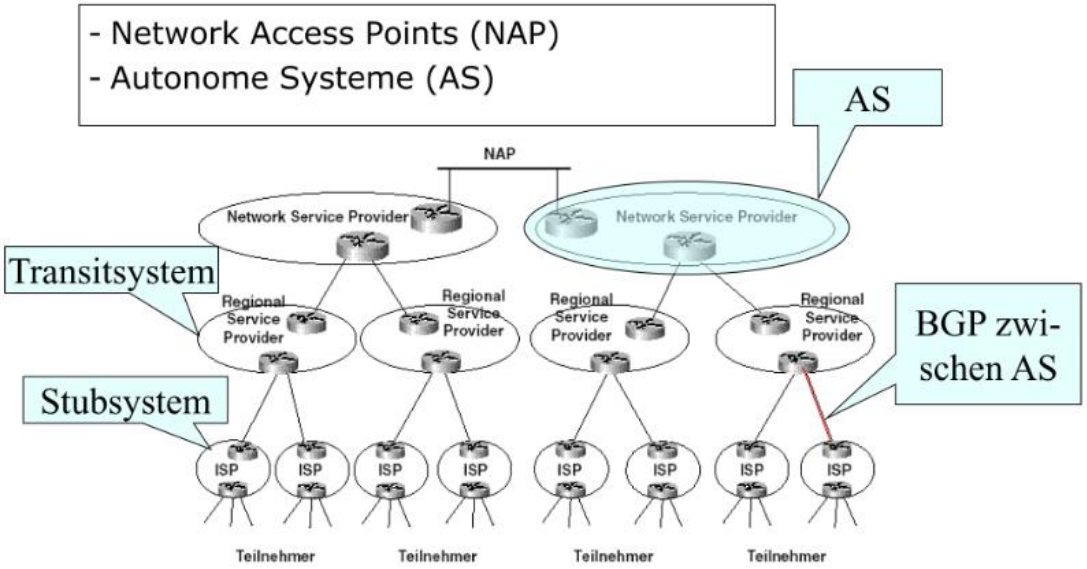
6.6 Routing Protokolle

Das Routing muss Koordiniert werde, da nicht alle Router alle Netze kennen können.

Netze werden zu Autonomen System (AS) gruppiert. Innerhalb des AS erfolgt das Routing mit dem Interior Gateway Protocol (IGP). Dieses wiederum nutzt RIP und OSPF.

Innerhalb der AS erfolgt die Kommunikation mit dem Exterior Gateway Protocol (EGP). Dieses nutzt das BGP (Border Gateway Protocol).

Dazu die hierarchische Routingstruktur des Internet



Routing Information Protocol (RIP)

- RIP ist ein IGP (Interior Gateway Protocol)
- Hop-Metrik mit Ursprung plus 1
- Unzuverlässiger Informationstransport via UDP
- Broadcast (Version 1) und Multicast (Version 2)
- Default Routen können definiert werden
- Distance Vector Algorithmus implementiert
- Es gibt eine passive Version für Hosts, die Informationen von benachbarten Routern einholen wollen
- Aufbau des Distance-Vectors
  - Service-Advertisment
  - [Zielnetz, Distanz] (maximale Distanz: 16 hops)

Open Shortest Path First (OSPF)

- Skaliert besser als RIP
- Typische Implementation innerhalb eines AS
- Austausch von Informationen über Link-State Broadcast
- Subnetting und CIDR (Classless Inter Domain Routing)
- Authentifizierter Nachrichtenaustausch
- Import von Routing-Informationen, z.B. von BGP
- Hierarchisches Routing möglich
  - durch Einteilung in „Bereiche"
  - Broadcast auf Bereiche beschränkt

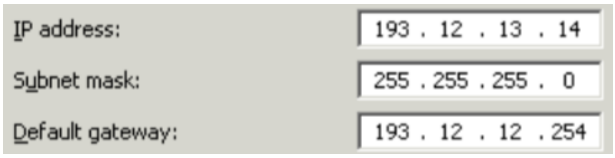
Border Gateway Protocol (BGP)

- NAPs bilden zusammen Core (Kern, höchste Hierarchie)
- Routen als Pfad von Autonomen Systemen (nummeriert von 1 bis 65535, ab 64512 privat deklariert)
- Keine Metrik, da AS unterschiedliche Metriken verwenden
- Policies: Konfigurierbar, welche Angaben nach aussen
- Transit-Systeme und Stub-Systeme konfigurierbar
- Zuverlässiger Informationsaustausch
  - via TCP/IP, well known Port 179
  - Authentisierung der „Nachbarn", mit denen Infos ausgetauscht werden
- Derzeit aktuell: Version 4 (BGP-4)

7 DNS UND IP KONFIGURATION

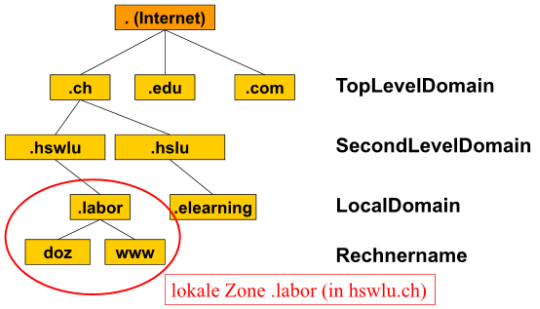
Bezieht sich auf den 5. Kursteil.

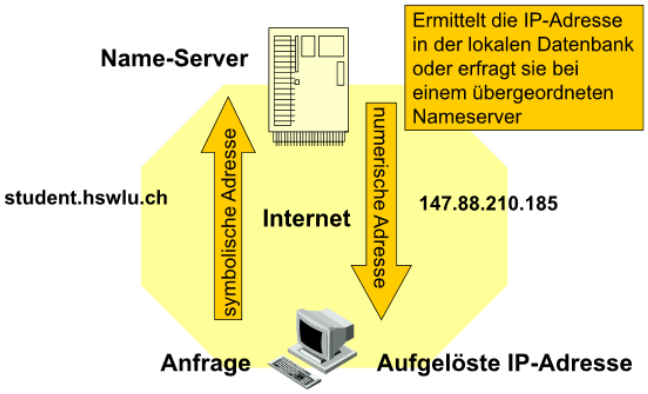
Subnetzmaske gibt vor das die ersten drei Bytes gleich sein müssen. Entweder ist die IP-Adresse oder der Default Gateway falsch.



7.1 Domain Name System (DNS)

Das Domain Name System (DNS) ist einer der wichtigsten Dienste in vielen IP-basierten Netzwerken. Seine Hauptaufgabe ist die Beantwortung von Anfragen zur Namensauflösung.





www.labor.hswlu.ch. -> Von links nach rechts, von unten nach oben. Ein bekanntes Programm für die Namensauflösung ist **nslookup** („name server look up“).

Es gibt folgende zwei Namens-Server

TLD Server (Top-level domain)	Sind zuständig für com, edu, org, uk, ch und alle anderen Top Level Domains.
Authoritative DNS	Ist der Namensserver einer Organisation, welche eine Domäne betreibt. Dieser liefert Namensauflösungen zu allen Hosts innerhalb dieser Organisation. (Wird entweder von der Organisation selber betrieben oder vom Internet Service Provider)

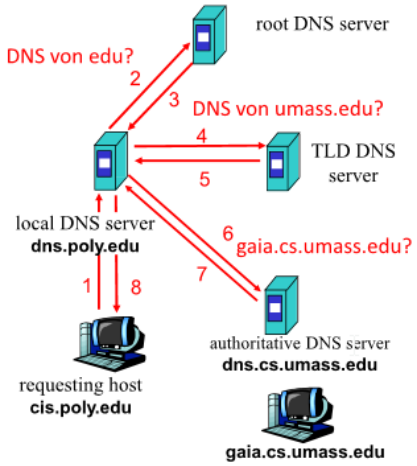
Es werden zwei Auflösungsarten unterschieden:

Iterative Auflösung

Iterative Query: Server antwortet mit zuständigem Server. „Ich kenne diesen Namen selber nicht, aber frag doch den da!“

Bspl. www.gaia.cs.usmass.edu

1. Zum eigenen DNS
2. Dieser kennt den Zuständen TLD-Server für „edu“
3. „Edu“ TLD kennt „usmass“
4. „Usmass“ kennt alle Hosts innerhalb von seinem Netz, also auch „gaia.cs“

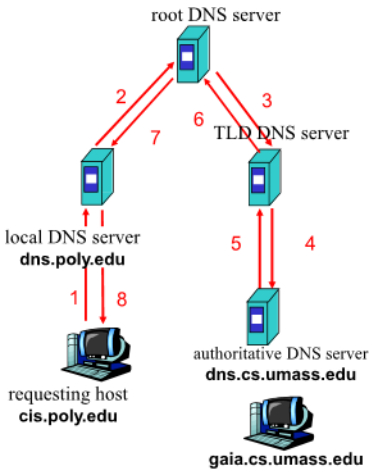


Rekursive Auflösung

Rekursive Query:

Der angefragte Server trägt die Last, deshalb nur noch intern bei Autoritativen DNS Server verwendet.

Funktioniert „fast“ wie iterative, grosser Unterschied ist das die „Anfragelast“ beim angefragten Server hängen bleibt. Dieser darf nicht nur einfach eine Antwort geben und weiterleiten, sondern muss auf eine Antwort warten und darf sie erst dann weiterleiten.



DNS Caching

Jeder Namensserver speichert („caching“) seine gelernten Namensauflösungen aus Performance Gründen. So ein Eintrag kann folgendermassen aussehen:

RR format: **(name, value, type, ttl)**

Im Type-Feld wird unterschieden, was für ein Namensauflösung gemacht wird (Host, Domäne, Mailserver, etc.)

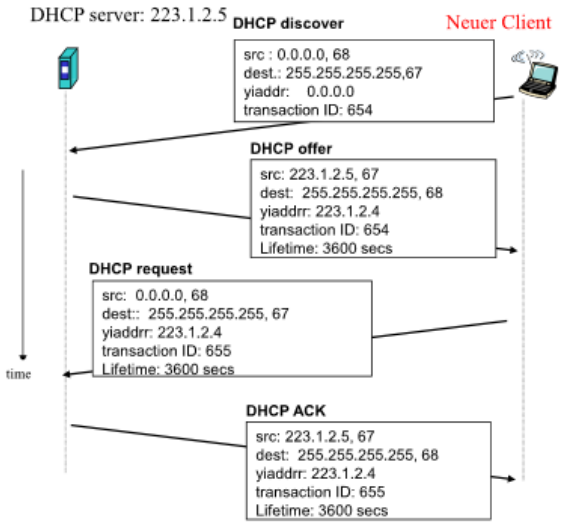
- Type=A
  - **name** ist der Hostname
  - **value** ist die IP Addresse
- Type=NS
  name ist die domain (foo.com)
  value ist der Hostname des zuständigen DNS-Servers für die Domain
- Type=CNAME
  - **name** ist alias Name für den “canonical” (wirklichen) Namen
    `www.ibm.com` ist eigentlich `servereast.backup2.ibm.com`
  - **value** ist der wirkliche Name
- Type=MX
  - **value** ist der Name eines Mailservers für die betreffende Domäne

7.2 Dynamic Host Configuration Protocol (DHCP)

Es ermöglicht die Zuweisung der Netzwerkkonfiguration an Clients durch einen Server. Ziel vom DHCP ist eine dynamische Vergabe der IP-Konfiguration.

Ablauf einer DHCP Konfiguration:

1. Neuer Client schickt eine **DHCPDISCOVER** Nachricht (mit seiner MAC-Adresse) als Broadcast (255.255.255.255, UDP Port 67) und weil er noch keine IP hat, ist die Absender IP 0.0.0.0 mit UDP Port 68.
2. Nun schicken alle DHCP’s im Netz eine **DHCPOFFER** (entweder als Broadcast oder als Unicast an 0.0.0.0+Mac-Adresse.
3. Client entscheidet nun anhand von selbstdefinierten Regeln welcher DHCPOFFER er annimmt und schickt eine **DHCPREQUEST**.
4. Der DHCP-Server bestätigt in einer **DHCPACK**-Nachricht (DHCP-Acknowledged) die IP-Adresse mit den weiteren relevanten Daten.



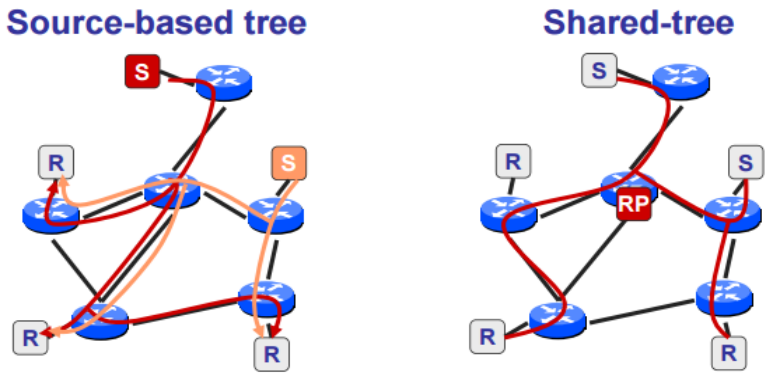
Der Client kann am Schluss mit einer ARP-Request im Netz nachfragen, ob er wirklich der einzige ist mit dieser IP. Falls ein anderes Gerät antwortet, kann die vorgeschlagene Adresse mit einer DHCPDECLINE-Nachricht zurückgewiesen werden.

7.3 Multicast Routing

Das Ziel von Multicast-Routing ist, einen Baum von Verbindungen zu ermitteln, der alle Router mit angeschlossenen Hosts enthält, die Mitglieder der Multicast-Gruppe sind. „Baum“, weil nicht alle Verbindungen zwischen den Routern geflutete werden sollen. Zwei Varianten werden unterschieden:

Source-based: jeder Sender baut seinen eigenen Baum. Merkmale sind: effiziente Bäume, kleine Verzögerungen und gleichmässige Last Verteilung

Shared-tree: gleicher Baum für alle Gruppenmitgleder. Merkmale sind: grössere Verzögerungen, schlechtere Lastverteilung (RP-Router trägt hohe Last)



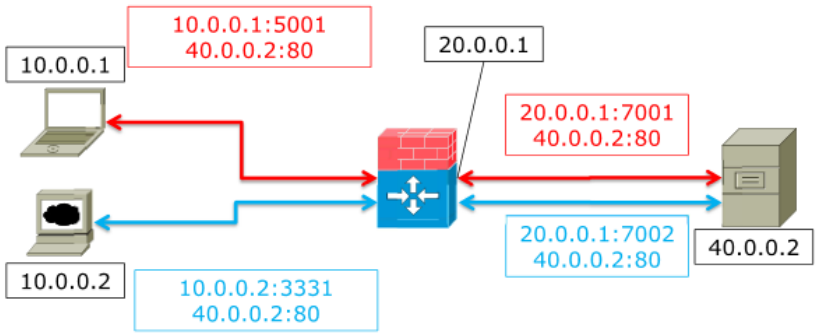
RP: „Rendevouz Point“; Router am RP verteilt die Datenpakete weiter.

7.4 Network Address Translation (NAT)

Port and Address Translation (PAT) oder **Network Address Translation** (NAPT) ist eine Technik, die in Computernetzwerken verwendet wird. Sie ist eine spezielle Form von NAT (1 zu n NAT).

Dabei werden im Gegensatz zu NAT nicht nur die IP-Adressen, sondern auch Port-Nummern umgeschrieben. **PAT** wird eingesetzt, wenn mehrere private IP-Adressen aus einem LAN zu einer öffentlichen IP-Adresse übersetzt werden sollen.

Gegeben sei folgendes Netzwerk: die beiden Clients (linke Seite vom Router) haben die gleiche IP-Adresse, sobald sie nach aussen (rechts vom Router) kommunizieren



Der „Firewall-Router“ muss nun eine Tabelle pflegen, um die Verbindungen zu den Clients unterscheiden zu können. Zur Unterscheidung werden zu den IP-Nummern noch Portnummern hinzugefügt (Portnummern bis 1024 sind „Well-Known ports“ und sollten nicht genutzt werden).

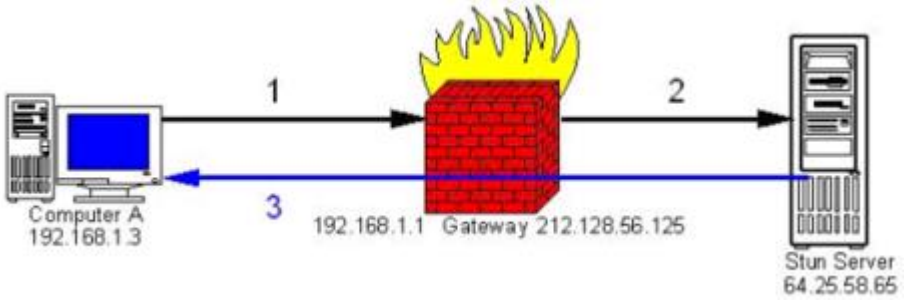
10.0.0.1:5001 | 20.0.0.1:7001 10.0.0.2:3331 | 20.0.0.1:7002

Wieso „Firewall-Router“? Firewalls leiten nur Antworten auf eine Anfrage wieder ins eigene Netz hinein, somit ist eine höhere Sicherheit gewährleistet.

Session Traversal Utitilites for NAT (STUN)

Ermöglicht es NAT-Clients (Computer hinter einer Router-Firewall wie im NAT-Beispiel) die mit UDP kommunizieren, z.B. Kommunikation mit einem VoIP-Provider ausserhalb des lokalen Netzwerks, aufzubauen.

Mit Hilfe des STUN-Servers können Clients ihre öffentliche IP-Adresse, das NAT-Gerät, hinter dem sie sich befinden, und den nach außen veröffentlichten, Internet-seitigen Port ermitteln, dem per NAT ein bestimmter lokaler Port zugewiesen wurde. Diese Informationen werden zur UDP-basierten Kommunikation zwischen dem Client und dem VoIP-Provider verwendet, um einen Anruf aufzubauen.



UDP: User Datagram Protocol. „Verbindungslose Übertragung von Daten über das Internet“ -> Stun macht eine virtuelle Verbindung für UDP (siehe blauer Pfeil).

8 LAYER 4 – TRANSPORTSCHICHT

Bezieht sich auf den 6 Kursteil.

Die Transportschicht ist die erste Schicht, die direkt mit bestimmten Services kommuniziert. Das IP-Protokoll bietet einen verbindungslosen Transport der Daten an, das heißt ohne jegliche Sicherung.

8.1 Ports und Sockets

Port

Wollen zwei Prozesse miteinander kommunizieren, dann identifizieren sich die Prozesse gegenüber TCP/IP mit einer *Port-Nummer*. Das ist eine 16-Bit Zahl, somit gibt 65535 Ports für jedes Transport-Protokoll (UDP und TCP). Die Port-Nummer sagt also aus, an welchen Prozess ein bestimmtes Paket weitergereicht werden möchte.

Socket

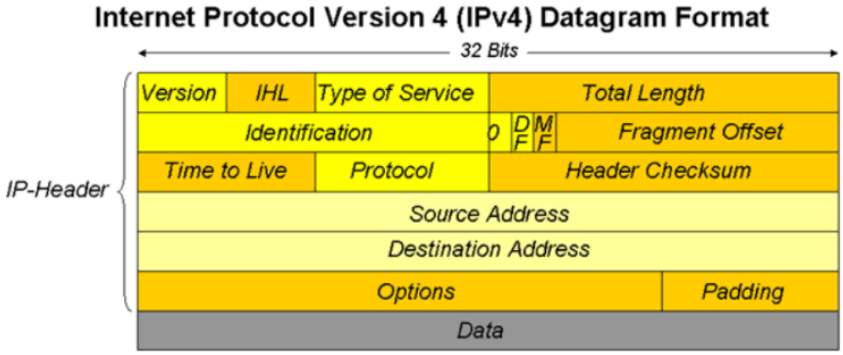
IP-Adresse + Port Nummer = Socket

Ein Socket ist ein Kommunikationsendpunkt (ein Objekt), durch das Datenpakete sowohl gesendet als auch empfangen werden (bidirektionaler Datenfluss). Man unterscheidet dabei zwei verschiedene Typen von Sockets:

- **Streamsockets** (TCP Sockets = Transmission Control Portocol)
- **Datagrammsockets** (UDP Sockest = User Datagramm Protocol)

8.2 Transmission Control Protocol (TCP)

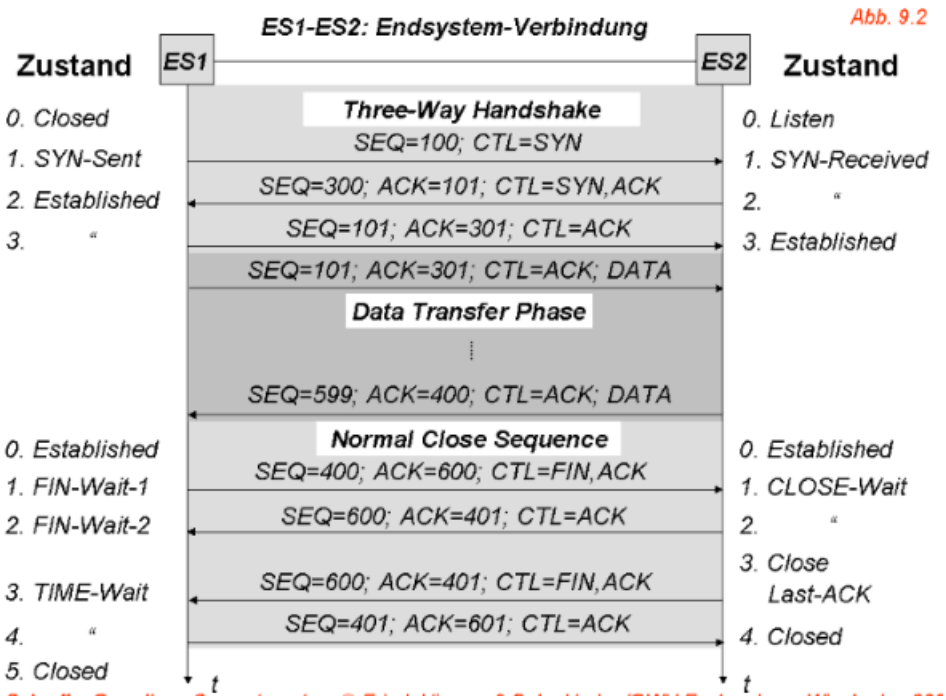
Das Transmission Control Protocol („Übertragungssteuerungsprotokoll“) ist ein Netzwerkprotokoll, das definiert, auf welche Art und Weise Daten zwischen Computern ausgetauscht werden sollen. Die zentrale Aufgabe von TCP/IP ist dafür Sorgen zu tragen, dass Datenpakete innerhalb eines dezentralen Netzwerks beim Empfänger ankommen. Dafür stellt TCP/IP die folgenden zentralen Funktionen bereit.



- Logische Adressierung / Logical Addressing (IP)
- Wegfindung / Routing (IP)
- Fehlerbehandlung und Flussteuerung / Error Control and Flow Control (TCP)
- Anwendungsunterstützung / Application Support (TCP)
- Namensauflösung / Name Resolution (DNS)

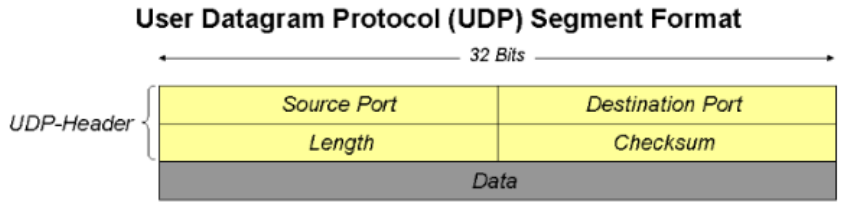
3-Way-Handshake

Bei jedem Verbinungsaufbau erfolgt ein 3-Weg-Austausch unter den Kommunikationspartner.



8.3 User Datagram Protocol (UDP)

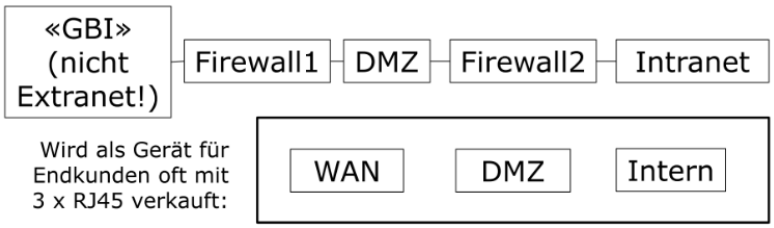
Ist ein verbindungsloses Transport-Protokoll. Es hat damit eine vergleichbare Aufgabe, wie das verbindungsorientierte TCP. Allerdings arbeitet es verbindungslos und damit unsicher. Das bedeutet, der Absender weiss nicht, ob seine verschickten Datenpakete angekommen sind. Während TCP Bestätigungen beim Datenempfang sendet, verzichtet UDP darauf. Das hat den Vorteil, dass der Paket-Header viel kleiner ist und die Übertragungsstrecke keine Bestätigungen übertragen muss. Einfacher Aufbau eines UDP-Headers:



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.

8.4 Firewall

Ein Konzept (nicht ein Gerät) zur Verbindung von Netzwerken unterschiedlicher Sicherheitsstufen.



Die Firewall ist eine Art Filter, zwischen dem Computer und dem Internet oder jeder anderen Form von Netzwerk. Sie prüft unter anderem, ob Programme auf das Internet oder aus dem Internet auf den Computer zugreifen wollen und dürfen. Die Firewall schützt vor unberechtigten Zugriffen von innen und von außen.

Unterschied zwischen Router und Firewall

Eine Firewall ist im Prinzip nichts anderes als ein Router, jedoch mit einer invertierten Weiterleitungsphilosophie. Ein Router ist maximal offen, bestrebt, hat also das Ziel, so viel als möglich Daten weiter zu transportieren. Hier müssen gewünschte Beschränkungen bewusst konfiguriert werden (sogenannte Access-Control-Lists, ACL). Unerwünschter Verkehr muss also bewusst durch Konfiguration verboten werden. Eine Firewall verhält sich genau andersherum. Hier ist jeglicher Verkehr von vornherein verboten. Will man bestimmte Daten weiterleiten, muss dies explizit durch Konfiguration erlaubt werden.

9 VIRTUAL LAN (VLAN)

Bezieht sich auf den 7. Kursteil.

Ist eine isolierte und partionierte Broadcast Domäne innerhalb eines OSI Layer 2 Netwerks.

Broadcast-Domain

Innerhalb dieser Domäne, also eine Anzahl von Peers, die durch ihre Netzwerkkonfiguration zusammengeschlossen sind, werden Broadcasts zugestellt. Ab einer bestimmten Peer-Anzahl führt das zu einer Überlastung der Netzwerkkapazitäten. Mit VLANs möchte man den Netzwerkverkehr eindämmen.

MAC-basierte VLAN

Dynamische VLAN. Die Zuteilung eines VLAN Tag erfolgt automatisch durch eine Software.

- Die Zuordnung zu den VLAN Domänen erfolgt durch die MAC-Adresse.
- Anfällig auf Spoofing-Angriffe.

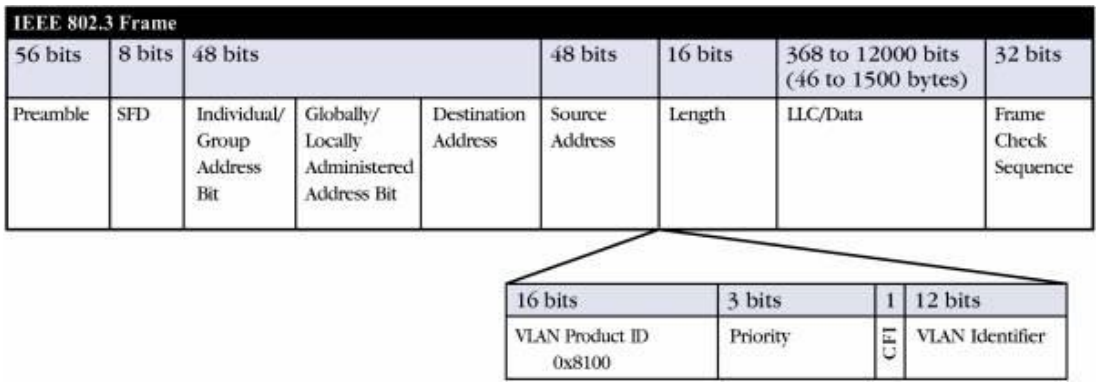
Port-basierte VLAN

Auch statische VLANs genannt.

- Jeder Port erhält eine ID
- Unflexible zuordnung -> muss neu gepatcht werden.
- Einfach zu realisieren

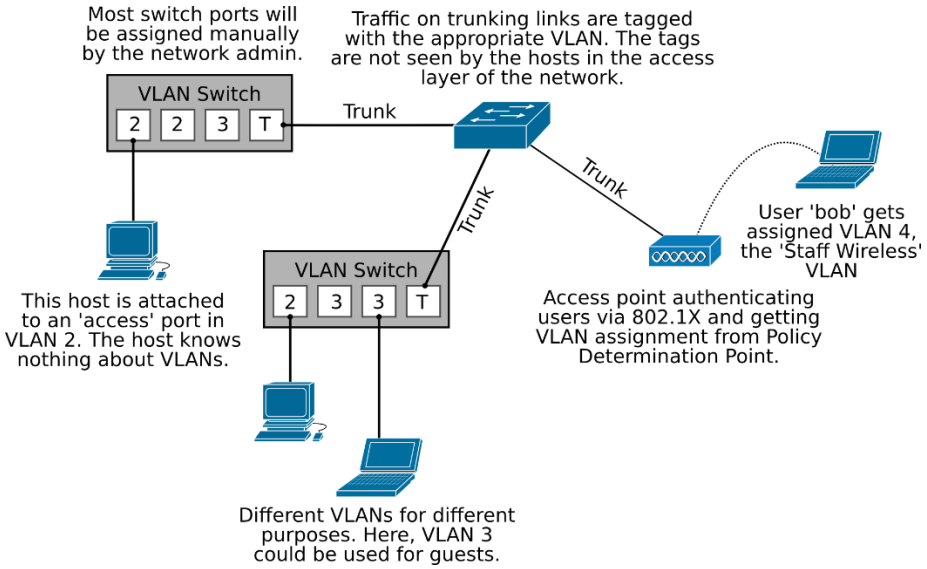
VLAN-Tags

Jedes Ethernet Frame erhält einen VLAN Tag auf dem Switch Port. Mit dem Tag werden die VLANs unterschieden.



Trunk

Verbindet mehrere VLANs.



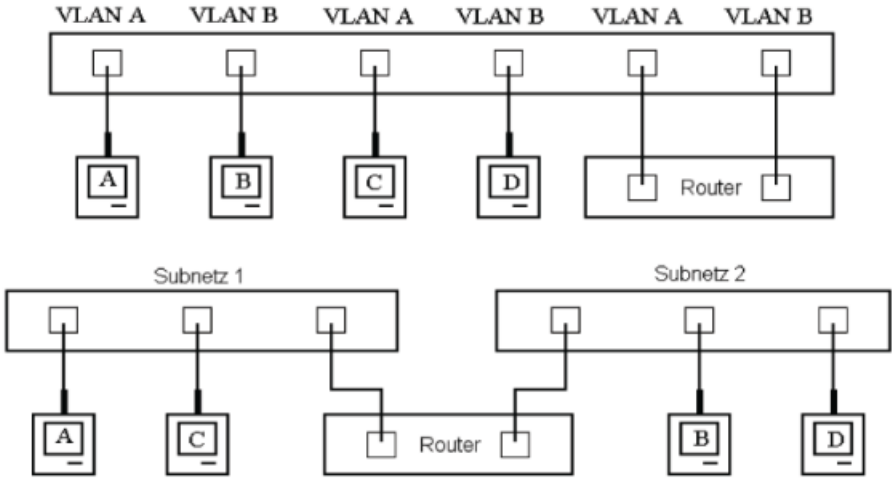
Standards

Jeder Hersteller hat eigene Standards definiert.

- 802.1q (u.a. ZyXEL) -> bekannteste
- Cisco ISL (“Inter Switch Link”)
- 3Com VLT (“Virtual LAN Trunk”)

Verbindung zwischen VLANs

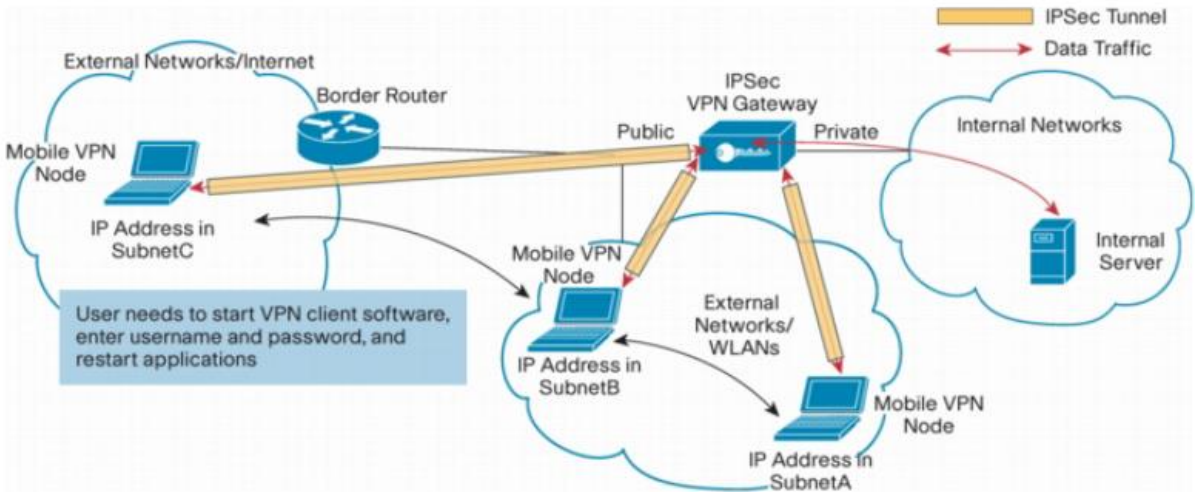
Ein Router (Layer 3) merkt nichts vom Tagging, ein Switch (Layer 2) nichts vom Routing. Ungetaggte VLANs müssen als zwei Subnetze über einen Router verbunden werden.



10 VIRTUAL PRIVATE NETWORK (VPN)

Bezieht sich auf den 8. Kursteil.

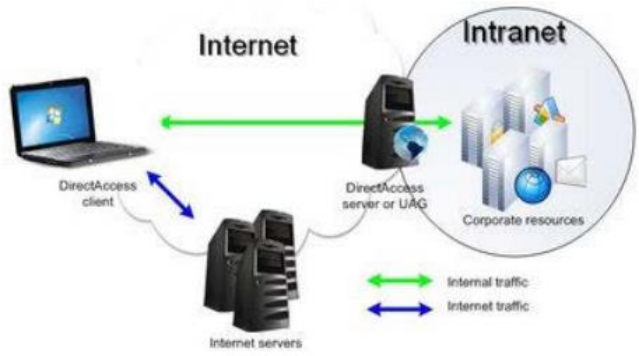
Kommunikation für einem Netzwerk oder einem Partner wird getunnelt.



VPN Gatewy (nicht Server) routet Subnetze A, B, C der Client.

Bei IP-Änderung bricht VPN-Verbindung zusammen.

Split Tunnels



- Diese geschossenen Tunnel verursachen viel Traffic.
- Die Split Tunnels bieten Angriffspunkte für Angreifer aus dem Internet.
- Der Client dient dabei als Hop-Node.
- Als Gegenmassnahme ist nur eine Verbindung auf dem Client erlaubt.

10.1 Verschlüsselung

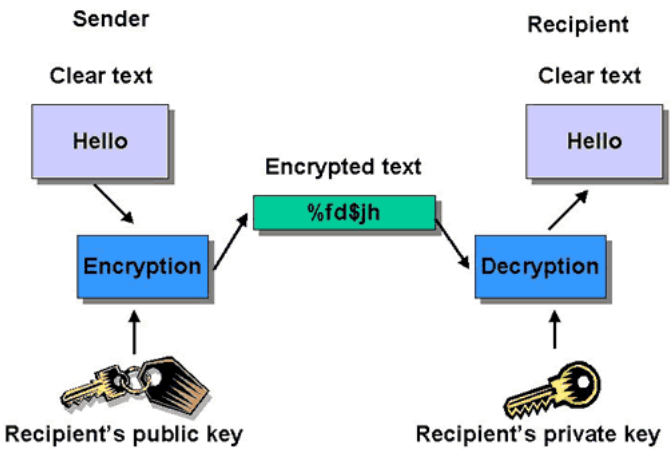
Verschüsselungsverfahren:

- DES
- 3DES
- IDEA
- AES -> aktueller Standard.

Symmetrisch

Gleiche Schlüssel werden zum Verschlüsseln und Entschlüsseln verwendet. Problem dabei ist die Schlüsselverteilung, aso wir erhält mein Gegenüber den Schlüssel zur Entschlüsselung einer Nachricht auf sichere Art und Weise.

Asymmetrisch



Mathematisch „verwandtes" Schlüsselpaar (siehe Diffie-Helmann). Prinzip ist einfach, Nachrichten die mit dem öffentlichen Schlüssel verschlüsselt werden können nur mit dem Private-Key entschlüsselt werden. Verteilung des public Key ist daher unproblematisch, er kann veröffentlicht werden. Einzige Problematik ist die Frage der Authentizität (wirklich Bob's Schlüssel?). Aus diesem Grund gibt es im Internet Certificate Authorities (CA).

Hybrid

Mit asymmetrischem Verfahren einen symmetrischen Schlüssel für die gemeinsame Benutzung übertragen

Authentizität

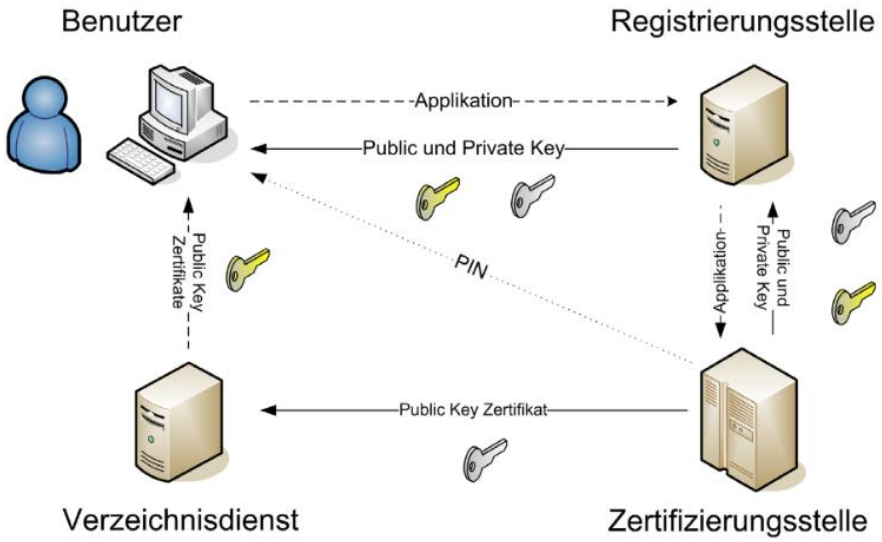
Sicherstellen, dass Gegenstelle authentisch ist, z.B. durch Prüfen der Kenntnis eines gemeinsamen Geheimnisses (PSK = Pre Shared Key)

Datenintegrität

Den einzelnen Datenpaketen wird ein MAC (Message Authentication Code) angehängt, eine komplizierte Prüfzahl, die am Ziel erneut berechnet wird und den Originalwert ergeben muss. Ein HMAC kombiniert das Verfahren mit dem Hashwert eines gemeinsamen Geheimnisses (Authentizität)

Public Key Infrastructure (PKI)

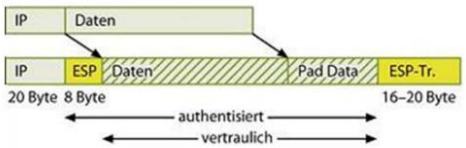
Die Schlüssel- und Zertifikatsverteilung muss geregelt ablaufen.



10.2 IPSec

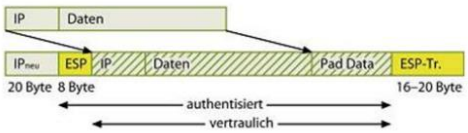
Dient dazu eine verschlüsstelte Verbindung aufzubauen.

IPSec kann in zwei verschienden Modis betrieben werden.



Transportmode

- Nur Payload vertraulich, IP-Header nicht
- Braucht „echte" IP
- „Sparvariante"



Tunnelmode

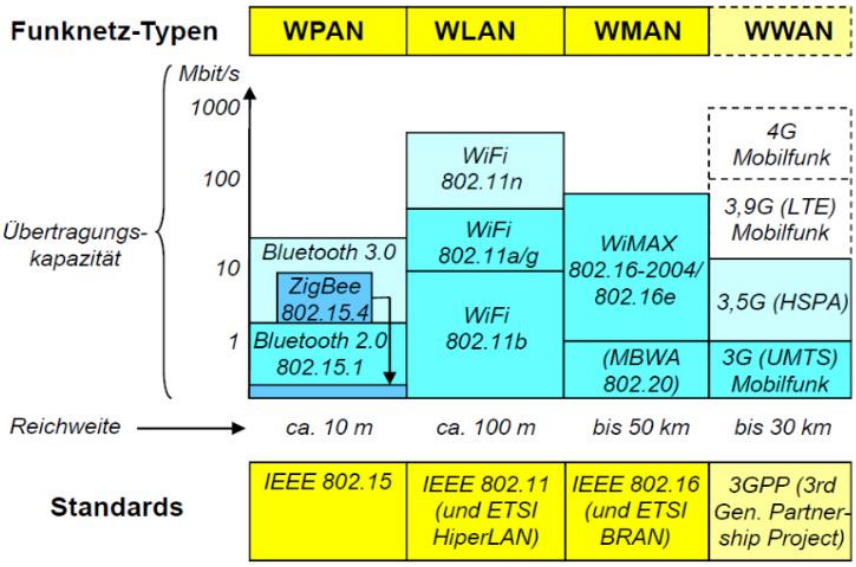
- Normalfall für site-to-site VPNs
- Ganzes IP-Datagramm wird eingepackt
- Braucht nur für Gateways „echte" IP (IP_{neu})

11 WLAN, FUNKNETZE, VOIP

Bezieht sich auf den 9. Kursteil.

11.1 Funknetze

Eine Übersicht der verschiedenen Funknetzstandards.



MBWA

Mobile Broadband Wireless Access IEEE 802.20

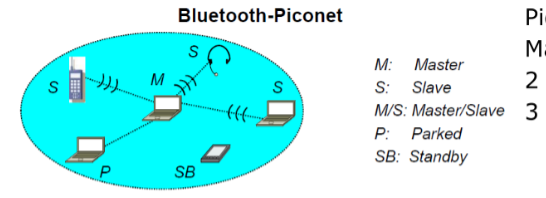
ZigBee

Ist ein Funknetz-Standard. PHY- und MAC-Layer basieren auf IEEE 802.15.4, der es ermöglicht, Haushaltsgeräte, Sensoren, uvm. auf Kurzstrecken (10 bis 100 Meter) zu verbinden.

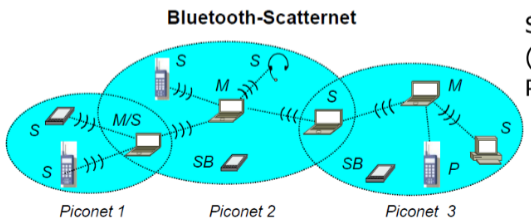
HSPA

High Speed Packet Access ist eine Weiterentwicklung des UMTS, die höhere Datenübertragungsraten ermöglicht

Bluetooth



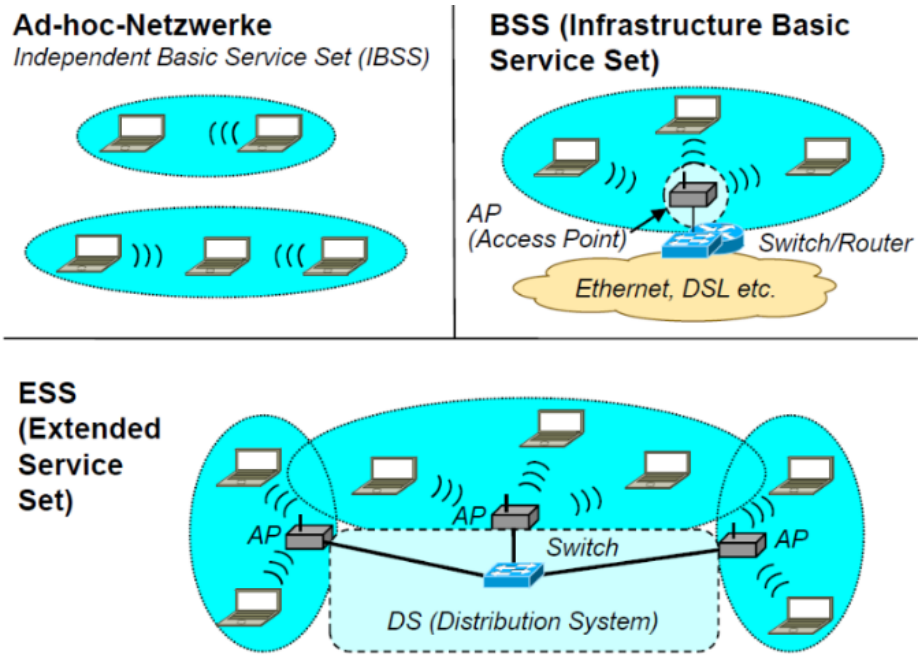
Piconet
Master/Slave(s)
2 Mbps netto
3 Leistungsstufen



Scatternet
(Verbund von
Piconets) möglich

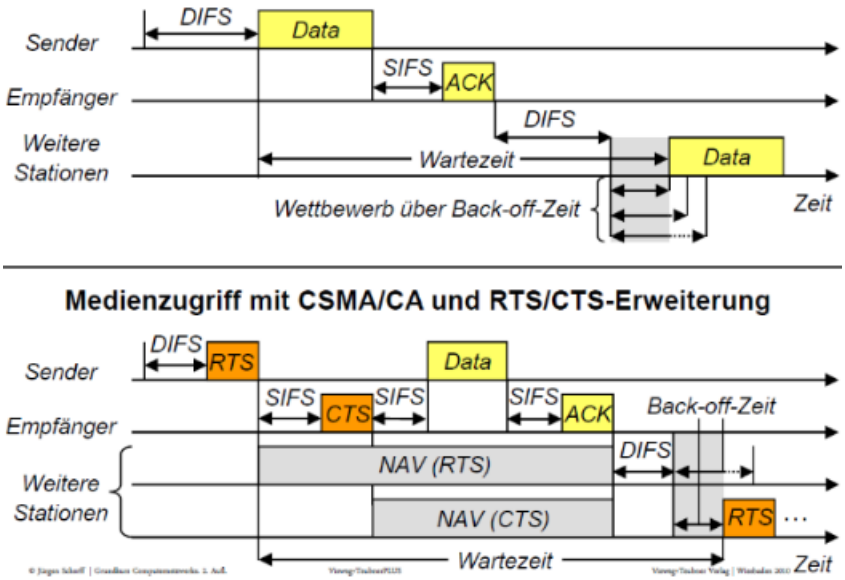
WLAN

Kann in verschiedenen Modis betrieben werden.



CSMA/CA und RTS/ CTS

Kollisionserkennung gibt es auch in WLANs.



IEEE 802.11 definiert eine DCF (Distributed Coordination Function) um den Zugriff auf das gemeinsame Medium fair zu koordinieren, da gleichzeitiges Senden und Abhören des Kanals nicht funktioniert.

DCF Inter Frame Space (DIFS) heisst die minimale Wartezeit während der der Kanal frei sein muss, bevor man senden darf. Nach DIFS wird noch eine zufällige Zeit gewartet, bis mit der Sendung begonnen wird.

Für Acknowledgment (ACK) Pakete wird nur Short Inter Frame Space (SIFS) gewartet, damit sie Priorität haben.

RTS und CTS enthalten Angaben über die Menge der zu übertragenden Daten, woraus alle anderen Stationen im Netz berechnen können, wie lange das Netz für sie unbenutzbar bleibt: NAV(RTS) bzw. NAV(CTS) (Network Allocation Vector)

11.2 WLAN Sicherheit

Wired Equivalent Privacy (WEP)

- Standard-Verschlüsselungsalgorithmus für WLAN
- Nutzt RC4-Algorithmus (Stromchiffre)
- Regelt Zugang zum Netz (Authentifzierung)
- Sollte Vertraulichkeit und Integrität der übetragenen Daten sicherstellen

Jedoch

- WEP-Schlüssel ist für alle der Gleiche
- WEP wurde fehlerhaft implementiert
- Es existieren verschiedene Angriffe

Wireless Protected Access (WPA)

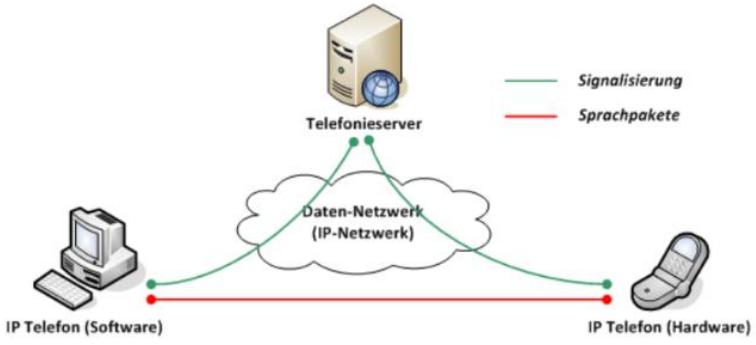
- Antwort auf WEP
- Nutzt TKIP zur besseren Authentisierung
- Angriffe auf Preshared Key bleibt möglich

Wireless Protected Access 2 (WPA2)

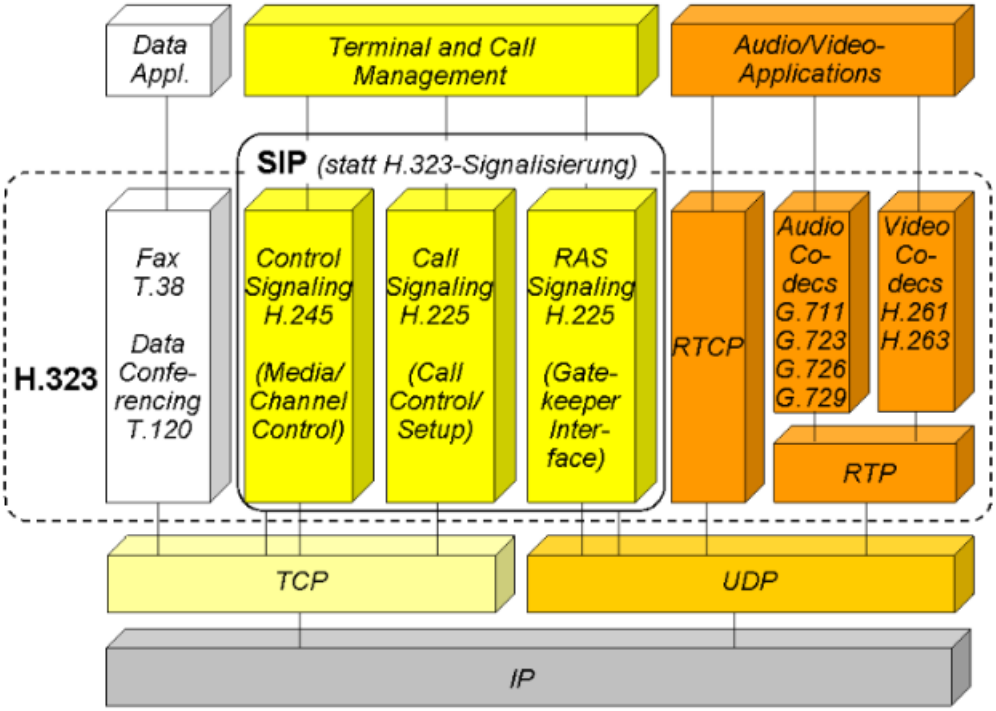
- Standard IEEE 802.11i
- Verschlüsselung basiert auf AES (Advanced Encryption Standard)
- Braucht mehr Rechenleistung
- Gilt derzeit als sicher
- Schlüsselmanagement wurde verbessert
    - Mehrere Preshard Key mögich
    - Benutzer Credentials bei Verbindungsaufbau (WPA2 Enterprise)

11.3 Voice over IP (VoIP)

Ermöglich das Telefonieren über das IP-Netzwerk. Sprachpakete werden i.d.R. über das verbindungslose UDP übertragen. Ist der Client hinter einer Firewall kommt STUN zum Einsatz.

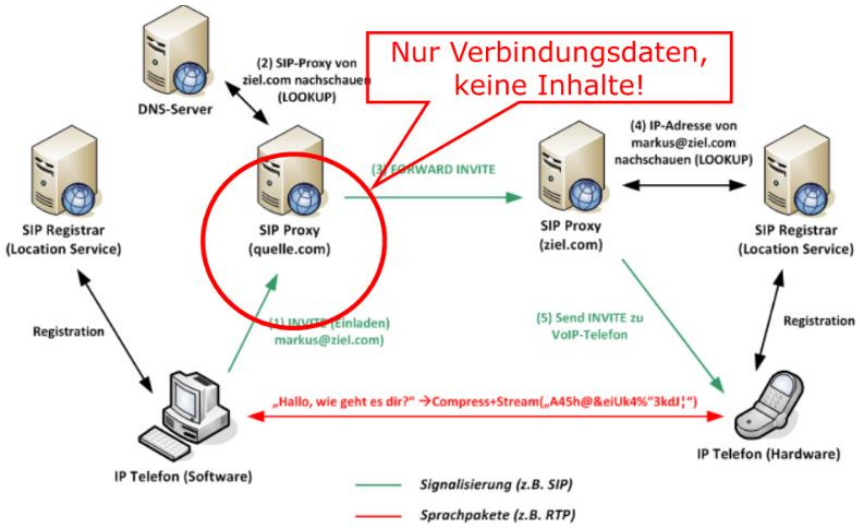


Dazu eine Übersicht der Standards und VoIP Prtokolle.



Session Initiation Protocol (SIP)

Ist ein VoIP Protokoll.

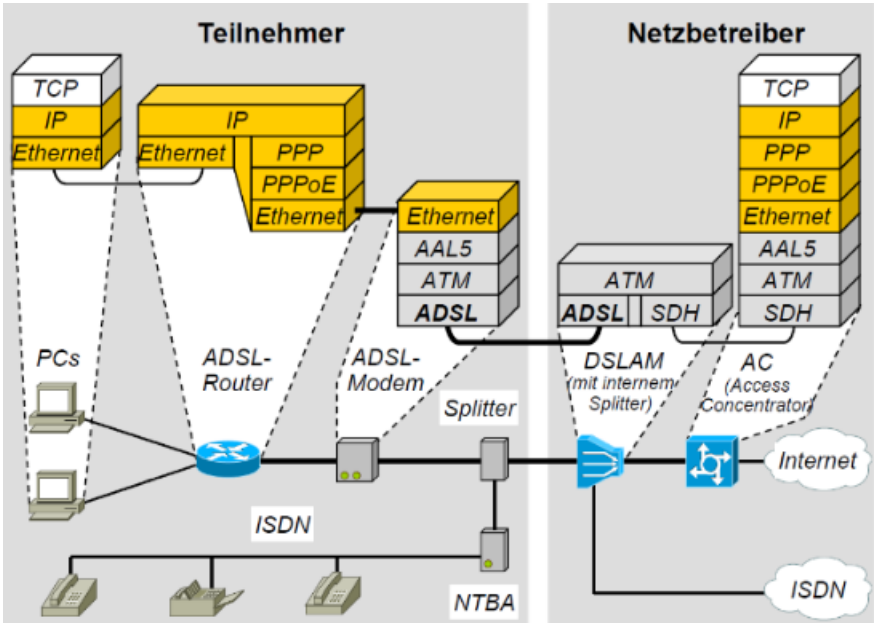


12 NETZZUGÄNGE – SZENARIEN

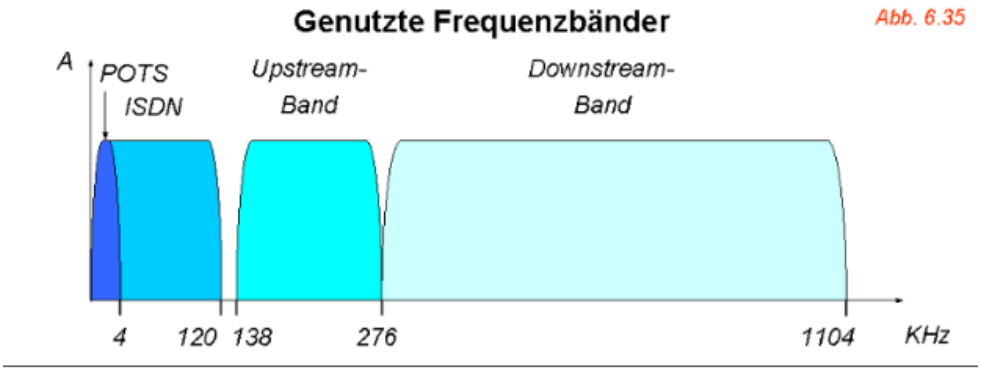
Der Zugang zum Internet für den Privatanwender wird über verschiedene Technologien und Protokolle ermöglicht.

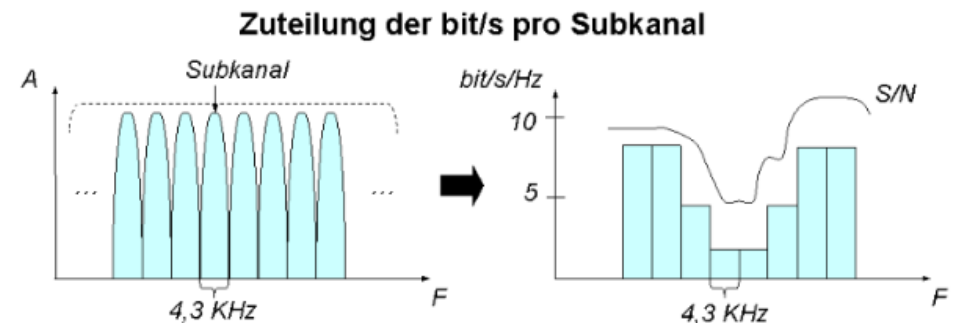
Asymmetric digital subscriber line (ADSL)

Ist der bekannteste Standard für die Datenkommunikation über eine Telefonleitung. Mit der asynchronen Kommunikation kann die Bandbreite erhöht werden.



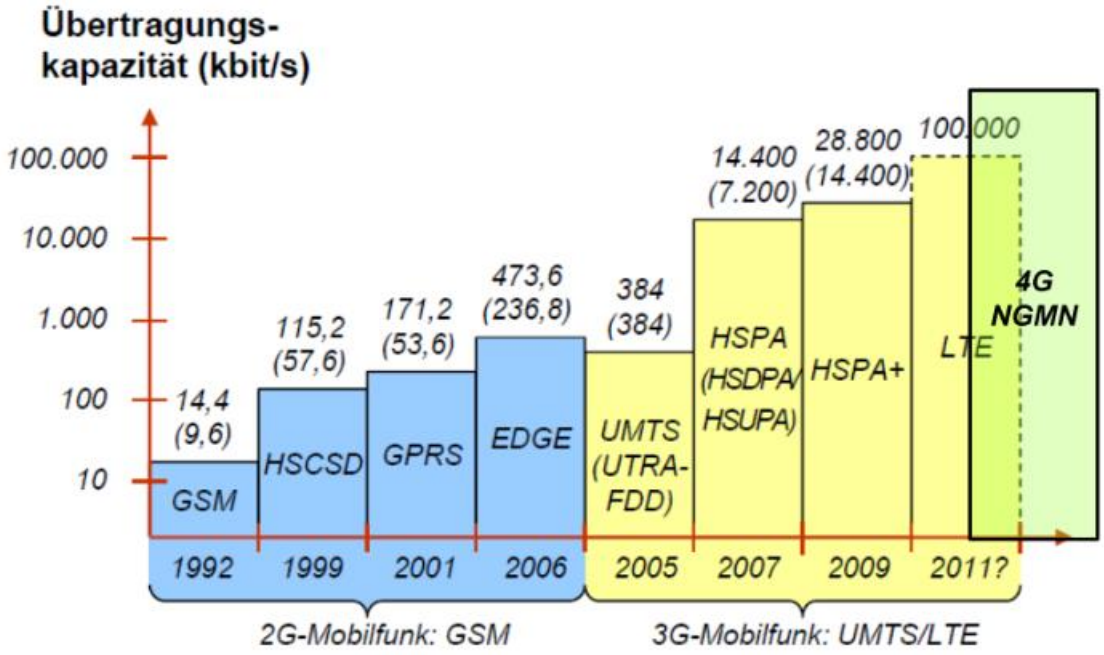
Auf unterschiedlichen Frequenzen werden die Daten übertragen.





Mobilfunk

Eine Übersicht der Mobilfunktechnologien.



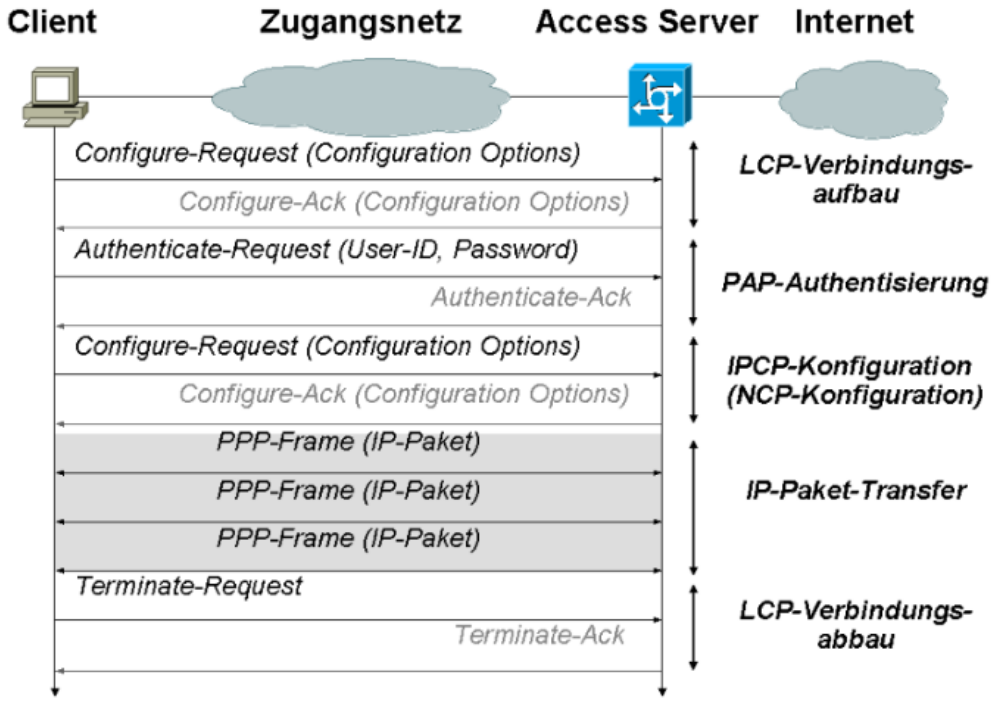
Nochmals die Reihenfolge:

- Groupe Systèmes Mobiles später Global System for Mobile Communication
- High Speed Circuit Switched Data
- General Packet Radio Service
- Enhanced Data Rates for GSM Evolution
- Universal Mobile Telecommunications System
- High Speed Downlink/Uplink Packet Access (auch 3.5G)
- Long Term Evolution (Oberbegriff für UMTS-Nachfolgeentwicklungen, 3.9G usw…)
- 4G Next Generation Mobile Networks (überlappt mit LTE / Terminologie nicht immer sehr genau)

12.1 Point to Point Protocol (PPP)

Wird von ISPs für den Verbindungsaufbau der Kunden verwendet. Es unterstützt:

- Authentifizierung
- Übertragungsverschlüsselung
- Datenkompression



Password Authentication Protocol (PAP)

Ein einfaches Authentifizierungsprotokoll, das sein Passwort benutzt. Es übertrag Passwörter in Klartext und ist daher die letzt Wahl der für PPP verfügbaren Verschlüsselungsprotokolle.

Challenge Handshake Authentication Protocol (CHAP)

- Verhindert Replay-Attacke im Vergleich zu PAP.
- Arbeitet mit einem Client- und Serverschlüssel.

NCP (Network Control Protocol)

- zum Aushandeln der Konfigurationsparameter bei PPP.
- Ist ein Bestandteil von PPP.
- Ein Beispiel ist das IPCP: IP Control Protocol

13 IPV6

Bezieht sich auf den 11. Kursteil.

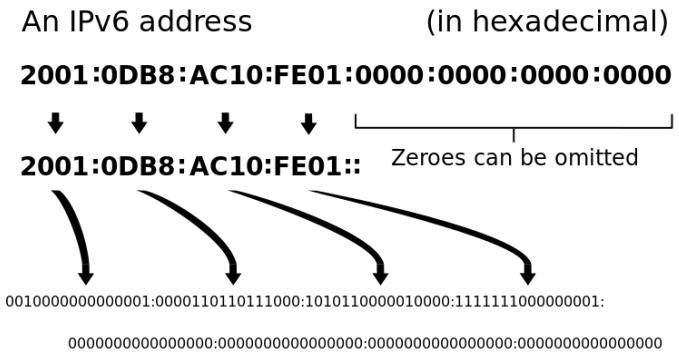
Allgemein

- Grösserer Adressraum: 2^128
- Variable und minimaler Header

- Provider-Hierarchie in der Adresse ist Konzeptionellunverändert
- Routing Präfix und Host Suffix

Adresse

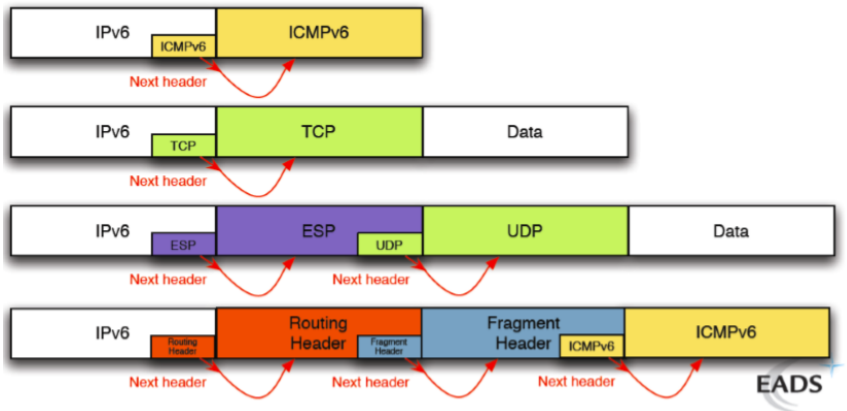
IPv6 Adressen sind weitaus komplizierter als IPv4 Addressen.



Extension Header

Der Header von Ipv6 hat im Vergleich zu Ipv4 viel weniger Felder.

Der Extension-Header gibt an welchers Protokoll folgt.

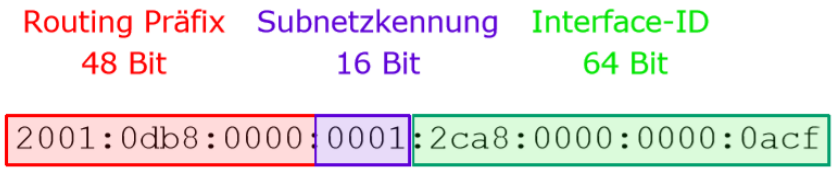


Netzklassen

Es gibt keine Netzklassen mehr bei IPv6. Auch bei IPv4 haben sie nur noch historische Bedeutung, da praktisch alle Router mit CIDR (Classless Inter Domain Routing) arbeiten.

Adressfelder

Bestimmte Felder in der Adresse haben unterschiedliche Funktionen.



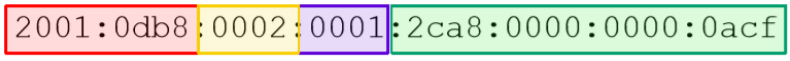
Service Provider erhalten 32 Bit Präfixe. Diese geben 48 Bit Netze weiter an die Kunden.

Das innere Format des Routing Präfix:

Format, Top Level Aggregation, reserved, Next Level Aggregation

Beispiel 1

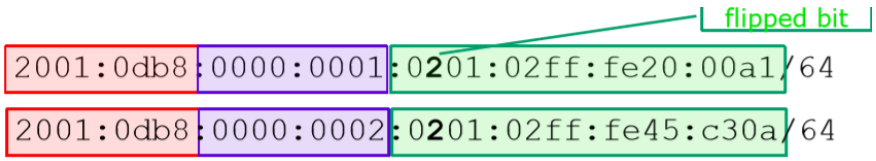
Kunde erhält das Netz 2001:0db8:0002/48 und definiert einen Host im subnetz 0001



Das Minimum für eine Kunde-IP sind 64 Bit. 64 Bit weil der Kunde kein Subnetting machen darf.

Beispiel 2

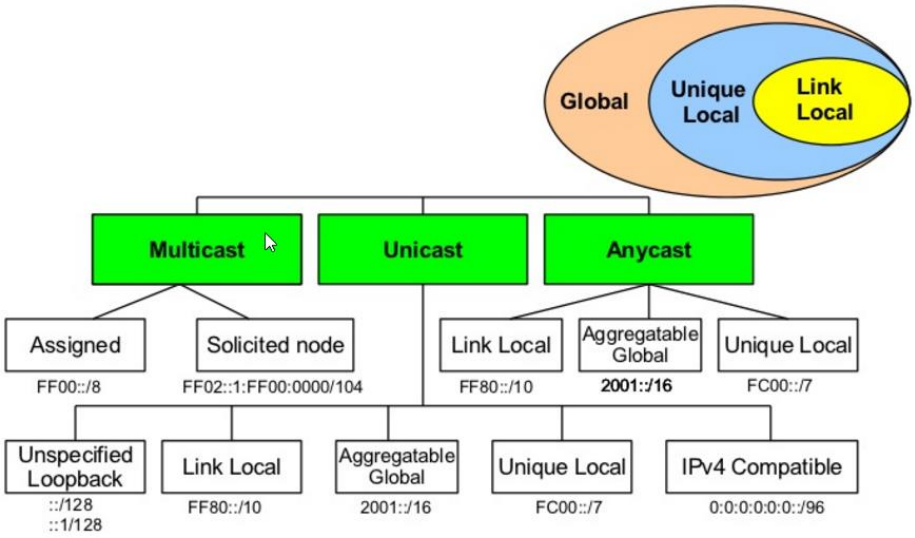
benachbarte /64er Kunden mit NICs von 3Com mit Herstellercode 00:01:02



Unicast Adressen

Global Unicast	`wie oben`	«normale» weltweit geroutete IP mit Routing-Präfix, Subnet-ID, Interface-ID
Link Local	`FE80::/10`	not routed! Pro Interface 1 Adresse (sinngemäss analog APIPA)
Unique Local	`FC00::/7`	nicht geroutete «private» Adresse eines Netzes (sinngemäss 192.168.0.0)
Unspecified	`::/128`	«keine» Adresse, z.B. Source-Adresse in einem DHCP-Request
Loopback	`::1/128`	analog 127.0.0.1 in IPv4
IPv4-mapped	`::FFFF:0:0/96`	Für Hosts mit Dual-Stack und IPv4 Adresse

Reservierte Adressen



Die Solicited Node Multicast

Ist eine Adresse innerhalb des local-link. Jeder Ipv6 host hat eine solche Adresse. Diese Adresse wird vom Neigbhor Discovery Protocol (NDP) benutzt.

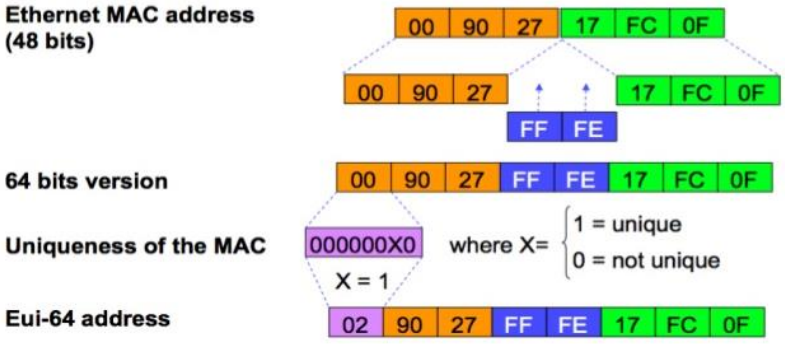
Beispiel – Wie man die Adresse erstellt:

```
fe80::2aa:ff:fe28:9c5a                          Target address (compressed notation)

fe80:0000:0000:0000:02aa:00ff:fe28:9c5a         Target address (uncompressed notation)

                                   -- ----      the last 24-bits

ff02::1:ff00:0/104                              Solicited-node Multicast Address prefix

ff02:0000:0000:0000:0000:0001:ff00:0000/104     (uncompressed)

---- ---- ---- ---- ---- ---- --               The first 104 bits

ff02:0000:0000:0000:0000:0001:ff28:9c5a         Result

ff02::1:ff28:9c5a                               Result (compressed notation)
```

Link Local Address

- Extended Unique Identifier oder Link-Local Address.
- Jedes Interface hat eine solche Adresse.
- Wird entweder weltweit eindeutig vergeben oder aus der MAC gebildet.

Beispiel – Wie die Adresse erstellt wird.



Beispiel Adressbildung

Ausgangslage:

- Routing Präfix 2001:620:110::/48
- Subnetz C101
- MAC-Adresse 00-50-56-c0-00-08

Lösung für MAC generierte Adresse:

Für den Client generierte Adresse:

- Loopback: ::1
- Link-Local: fe80::250:56ff:fec0:8
- Global Unicast: 2001:620:110:c101:250:56ff:fec0:8

Adressen auf die gehört werden muss:

- All nodes Multicast: ff02::1 (link local wegen «im LAN»)
- Solicited Node Multicast: ff02::1:ffc0:8
- Weitere Multicast: ff00::/8 (diese Antwort könnte auch für die oberen 2 gegeben werden!)

Lösung für von Hand zugewiesene fixe IP: 2001:638:d:c101**:acdc:1979:3:1008**

- Loopback: ::1
- Link-Local: fe80::**acdc:1979:3:1008**
- Global Unicast: 2001:638:d:c101**:acdc:1979:3:1008**
- All nodes Multicast: ff02::1 (link local wegen «im LAN»)
  Solicited Node Multicast: ff02::1:ff03:1008
  Weitere Multicast: ff00::/8 (diese Antwort könnte auch für die oberen 2 gegeben werden!)weitere Ipv6 Protokolle

Stateless Address Autoconfiguration – SAA

Netzwerkkonfiguration von Hand.

1. Link-Local mit EUI-64 Formation erzeugen
2. Die zugehörige Solicited-Node Multicast auf Einmaligkeit prüfen
3. Router Solicitation an FF02::2
4. Router Advertiment mit Netzparametern empfangen
5. Neighbor-Advertisment an FF02:1

Stateful Autoconfiguration mit DHCPv6

1. Nach SAA DHCPv6 Request via UDP an Port 546; Identifiziert durch DUID und IAIDs (eindeutige IDs, die bei Neustart nicht ändern = Rolle der MAC-Adresse in IPv4)
2. Antwort enthält DNS, NTP, SIP, NIS, … mit Ablaufdatum

Neighbor Detection Protocol (NDP)

IPv4 equivalent ist ARP

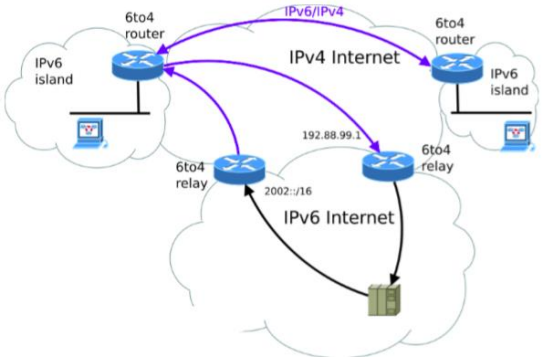
1. Neighbor Solicitation Message an Solicited Multicast Adresse des Partners z.B. FF02::1:ff12:3456 senden
2. Diese Solicitation enthält die Layer-2 Adresse des Absenders
3. Partner antwortet mit Neighbor Advertisment, das seine Layer-2 Adresse enthält
4. Beide können im lokalen Netz via MAC auf Layer 2 kommunizieren

Wenn ein Host seine IP ändert, teilt er das allen Hosts über die All-Nodes Multicast Adresse (FF02::1) mit. Alle aktiven Hosts im Netz übernehmen diese Änderung und können die neue IP der MAC Adresse richtig zuordnen

Benutzt die IPv6 mulicast Adressen -> Kein ARP mehr nötig.

6to4 (STF)

Verbindung von Ipv6 Netzen über ein Ipv4 Netz.




```
FE80::/64:<ipv4-Adresse>

2002::/16 ist der Präfix für 6to4 Adressen, bei 6in4 globale Präfixe.
```

```
IPv4:       192.0.2.4
                ↓  ↓  ↓  ↓
IPv6: 2002:c000:0204::/48
```

6over4

Verbindung von IPv4 und IPv6 Netzwerken.

Aus der IPv4-Adresse: 91.198.174.225 leitet sich folgende link-local-Adresse ab:

```
fe80:0000:0000:0000:0000:0000:91.198.174.225
```

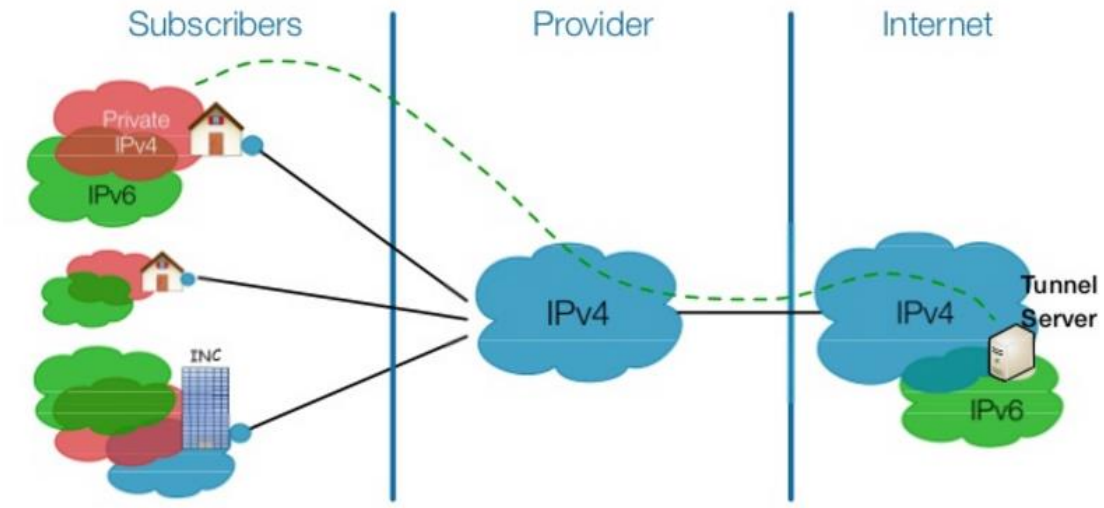
bzw.

```
fe80:0000:0000:0000:0000:0000:5BC6:AEE1
```

oder kurz:

```
fe80::5BC6:AEE1
```

6in4



Bei 6in4 wird der Datenverkehr in IPv4-Datenpakete verpakt, deren Protkollnummer im IP-Header 41 ist. Direkt auf den IPv4-Header folgt das transportierte IPv6-Datenpaket.

Intra-Site Automatic Tunnel Addressing Protocol (ISATAP)

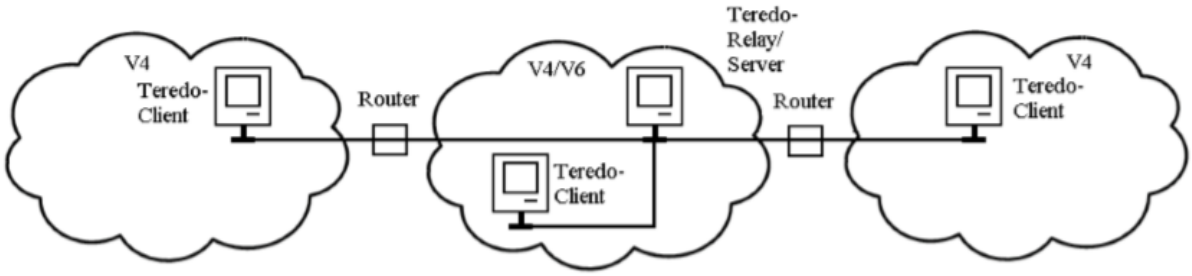
- In erster Linie für die Kommunikation reiner IPv6 Hosts in einem IPv4 Subnetz gedacht
- Die IPv4 Adresse wird direkt in die Interface-ID eingebaut: Interface ID = 0000:5EFE:<IPv4-Adresse>
- Sie ist automatisch Unique, wenn echte (ebenfalls eindeutige) IPv4 Adressen benutzt werden
- Das Präfix der IPv6 Adresse des Hosts kann global oder linklocal sein
- Bei globalen Präfixen ist Routing (oder relaying) ins IPv6 Internet möglich

Beispiel:

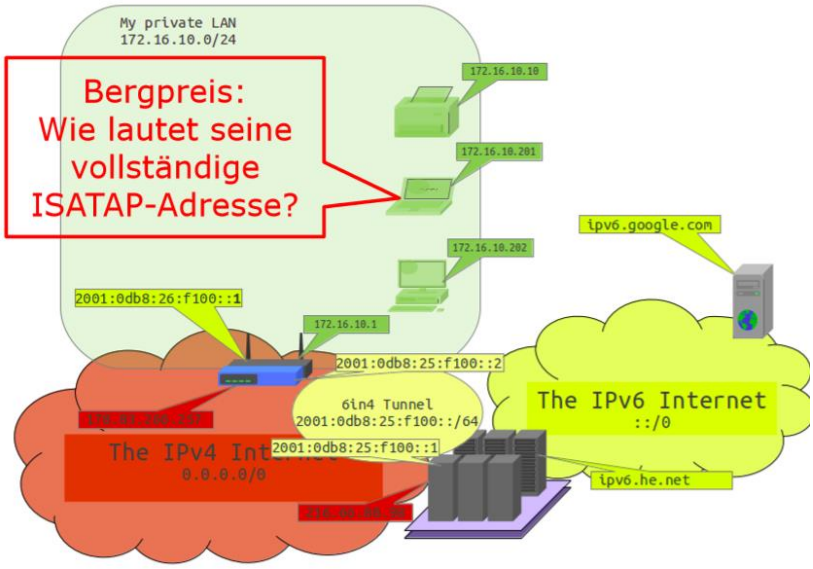
```
HSLU Adresse: 147.88.210.185

Interface-ID: 0000:5EFE: 9358D2B9
```

Teredo

- Workaround bei «dual-stack» Konfiguration, wenn z.B. 6to4 wegen NAT nicht möglich ist
- Der Protokolltyp 41 (IPv6 in IPv4 getunnelt) wird von den meisten NAT-Routern nicht geroutet (in der Payload befindet sich nämlich kein eigentliches IPv4)
- Der Transport durchs IPv4 Internet geschieht bei Teredo über UDP, wobei alle NAT-Infos mitgegeben werden. Es braucht allerdings einen Teredo Relay Server (3544/udp)!



13.1 IPv6 Fragen und Antworten



2001:db8::/32 wird global geroutet.

Antwort Bergpreis:

- 2001:db8:26:f100:0000:5efe:172.16.10.201 (erlaubte Notation)
- 2001:db8:26:f100:0000:5efe:ac10:0ac9 (erwünschte Notation)
- Nicht didaktische Notation: 2001:db8:26:f100::5efe:ac10:ac9 (erlaubte Nullenunterdrückung)
- Merke dazu: Wenn das Routing Präfix global unique ist, kann eine private IPv4 für ISATAP verwendet werden!

Weitere Fragen:

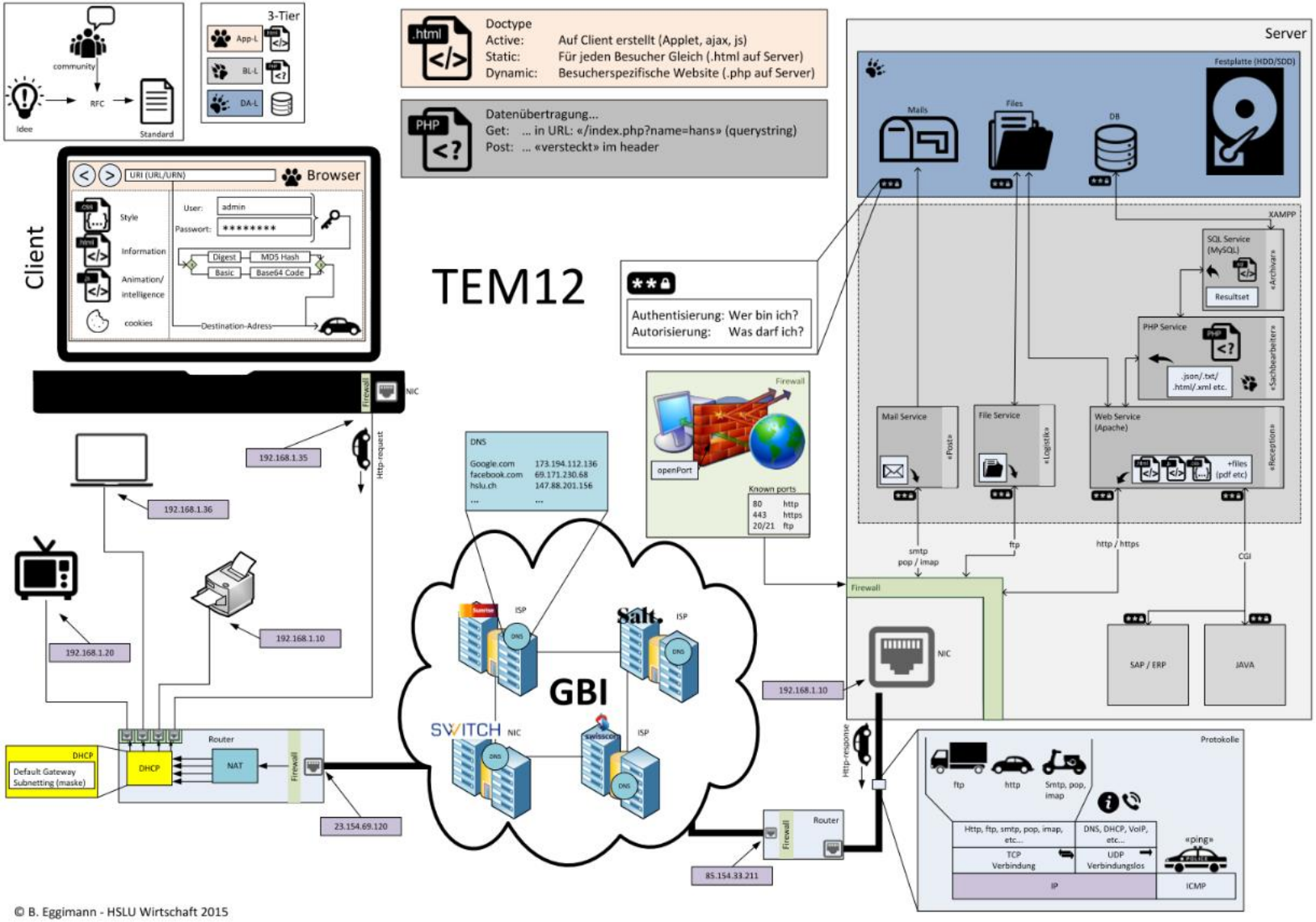
1. Der Drucker habe die MAC 00-01-02-10-20-30. Wie laute seine vollständige IPv6 Adresse
2. Kann ich obigen Drucker von der Adresse 147.88.210.185 aus pingen? Begründung zählt!
3. Unter welcher Adresse «sieht» mich der Server stud.hswlu.ch (der nur IPv4 versteht), wenn ich auf dem unteren PC surfe?
4. Unter welcher Adresse «sieht» mich ipv6.google.com?
5. Unter welchen Bedingungen kann ich aus dem privaten Netz auf stud.hswlu.ch zugreifen, wenn ich im privaten Netz nur noch IPv6 verwende?

Antworten:

1. Drucker hat 2001:db8:26:f100:0201:02ff:fe10:2030. Achtung: etwas böser wäre die Frage mit der MAC 11-12-13-10-20-30!!
2. Nein! Er hat eine private IP
3. Unter der IPv4 Adresse des NAT-Routers 178.83.266.257
4. Unter meiner IPv6 Adresse 2001:db8:26:<je nach MAC>
5. Wenn mein NAT Router meine IPv6 Adresse ins IPv4 Internet NATtet. Das geht, wenn ich ihm das Ziel als IPv4 mapped Adresse angebe.

14 CHEAT SHEETS

14.1 Big Picture



14.2 Common Ports

7	Echo	554	RTSP	2745	Bagle.H	6891-6901	Windows Live
19	Chargen	546-547	DHCPv6	2967	Symantec AV	6970	Quicktime
20-21	FTP	560	rmonitor	3050	Interbase DB	7212	GhostSurf
22	SSH/SCP	563	NNTP over SSL	3074	XBOX Live	7648-7649	CU-SeeMe
23	Telnet	587	SMTP	3124	HTTP Proxy	8000	Internet Radio
25	SMTP	591	FileMaker	3127	MyDoom	8080	HTTP Proxy
42	WINS Replication	593	Microsoft DCOM	3128	HTTP Proxy	8086-8087	Kaspersky AV
43	WHOIS	631	Internet Printing	3222	GLBP	8118	Privoxy
49	TACACS	636	LDAP over SSL	3260	iSCSI Target	8200	VMware Server
53	DNS	639	MSDP (PIM)	3306	MySQL	8500	Adobe ColdFusion
67-68	DHCP/BOOTP	646	LDP (MPLS)	3389	Terminal Server	8767	TeamSpeak
69	TFTP	691	MS Exchange	3689	iTunes	8866	Bagle.B
70	Gopher	860	iSCSI	3690	Subversion	9100	HP JetDirect
79	Finger	873	rsync	3724	World of Warcraft	9101-9103	Bacula
80	HTTP	902	VMware Server	3784-3785	Ventrilo	9119	MXit
88	Kerberos	989-990	FTP over SSL	4333	mSQL	9800	WebDAV
102	MS Exchange	993	IMAP4 over SSL	4444	Blaster	9898	Dabber
110	POP3	995	POP3 over SSL	4664	Google Desktop	9988	Rbot/Spybot
113	Ident	1025	Microsoft RPC	4672	eMule	9999	Urchin
119	NNTP (Usenet)	1026-1029	Windows Messenger	4899	Radmin	10000	Webmin
123	NTP	1080	SOCKS Proxy	5000	UPnP	10000	BackupExec
135	Microsoft RPC	1080	MyDoom	5001	Slingbox	10113-10116	NetIQ
137-139	NetBIOS	1194	OpenVPN	5001	iperf	11371	OpenPGP
143	IMAP4	1214	Kazaa	5004-5005	RTP	12035-12036	Second Life
161-162	SNMP	1241	Nessus	5050	Yahoo! Messenger	12345	NetBus
177	XDMCP	1311	Dell OpenManage	5060	SIP	13720-13721	NetBackup
179	BGP	1337	WASTE	5190	AIM/ICQ	14567	Battlefield
201	AppleTalk	1433-1434	Microsoft SQL	5222-5223	XMPP/Jabber	15118	Dipnet/Oddbob
264	BGMP	1512	WINS	5432	PostgreSQL	19226	AdminSecure
318	TSP	1589	Cisco VQP	5500	VNC Server	19638	Ensim
381-383	HP Openview	1701	L2TP	5554	Sasser	20000	Usermin
389	LDAP	1723	MS PPTP	5631-5632	pcAnywhere	24800	Synergy
411-412	Direct Connect	1725	Steam	5800	VNC over HTTP	25999	Xfire
443	HTTP over SSL	1741	CiscoWorks 2000	5900+	VNC Server	27015	Half-Life
445	Microsoft DS	1755	MS Media Server	6000-6001	X11	27374	Sub7
464	Kerberos	1812-1813	RADIUS	6112	Battle.net	28960	Call of Duty
465	SMTP over SSL	1863	MSN	6129	DameWare	31337	Back Orifice
497	Retrospect	1985	Cisco HSRP	6257	WinMX	33434+	traceroute
500	ISAKMP	2000	Cisco SCCP	6346-6347	Gnutella		
512	rexec	2002	Cisco ACS	6500	GameSpy Arcade		
513	rlogin	2049	NFS	6566	SANE		
514	syslog	2082-2083	cPanel	6588	AnalogX		
515	LPD/LPR	2100	Oracle XDB	6665-6669	IRC		
520	RIP	2222	DirectAdmin	6679/6697	IRC over SSL		
521	RIPng (IPv6)	2302	Halo	6699	Napster		
540	UUCP	2483-2484	Oracle DB	6881-6999	BitTorrent		

Legend

- Chat
- Encrypted
- Gaming
- Malicious
- Peer to Peer
- Streaming

14.3 IPv4 Subnetting

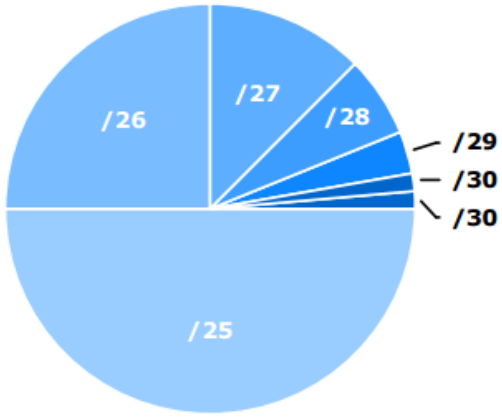
Subnets

CIDR	Subnet Mask	Addresses	Wildcard
/32	255.255.255.255	1	0.0.0.0
/31	255.255.255.254	2	0.0.0.1
/30	255.255.255.252	4	0.0.0.3
/29	255.255.255.248	8	0.0.0.7
/28	255.255.255.240	16	0.0.0.15
/27	255.255.255.224	32	0.0.0.31
/26	255.255.255.192	64	0.0.0.63
/25	255.255.255.128	128	0.0.0.127
/24	255.255.255.0	256	0.0.0.255
/23	255.255.254.0	512	0.0.1.255
/22	255.255.252.0	1,024	0.0.3.255
/21	255.255.248.0	2,048	0.0.7.255
/20	255.255.240.0	4,096	0.0.15.255
/19	255.255.224.0	8,192	0.0.31.255
/18	255.255.192.0	16,384	0.0.63.255
/17	255.255.128.0	32,768	0.0.127.255
/16	255.255.0.0	65,536	0.0.255.255
/15	255.254.0.0	131,072	0.1.255.255
/14	255.252.0.0	262,144	0.3.255.255
/13	255.248.0.0	524,288	0.7.255.255
/12	255.240.0.0	1,048,576	0.15.255.255
/11	255.224.0.0	2,097,152	0.31.255.255
/10	255.192.0.0	4,194,304	0.63.255.255
/9	255.128.0.0	8,388,608	0.127.255.255
/8	255.0.0.0	16,777,216	0.255.255.255
/7	254.0.0.0	33,554,432	1.255.255.255
/6	252.0.0.0	67,108,864	3.255.255.255
/5	248.0.0.0	134,217,728	7.255.255.255
/4	240.0.0.0	268,435,456	15.255.255.255
/3	224.0.0.0	536,870,912	31.255.255.255
/2	192.0.0.0	1,073,741,824	63.255.255.255
/1	128.0.0.0	2,147,483,648	127.255.255.255
/0	0.0.0.0	4,294,967,296	255.255.255.255

Decimal to Binary

Subnet Mask		Wildcard	
255	1111 1111	0	0000 0000
254	1111 1110	1	0000 0001
252	1111 1100	3	0000 0011
248	1111 1000	7	0000 0111
240	1111 0000	15	0000 1111
224	1110 0000	31	0001 1111
192	1100 0000	63	0011 1111
128	1000 0000	127	0111 1111
0	0000 0000	255	1111 1111

Subnet Proportion



Classful Ranges

A	0.0.0.0 – 127.255.255.255
B	128.0.0.0 - 191.255.255.255
C	192.0.0.0 - 223.255.255.255
D	224.0.0.0 - 239.255.255.255
E	240.0.0.0 - 255.255.255.255

Reserved Ranges

RFC 1918	10.0.0.0 - 10.255.255.255
Localhost	127.0.0.0 - 127.255.255.255
RFC 1918	172.16.0.0 - 172.31.255.255
RFC 1918	192.168.0.0 - 192.168.255.255

Terminology

CIDR
Classless interdomain routing was developed to provide more granularity than legacy classful addressing; CIDR notation is expressed as /XX

VLSM
Variable-length subnet masks are an arbitrary length between 0 and 32 bits; CIDR relies on VLSMs to define routes

14.4 IPv6

Protocol Header

Version (4 bits) · Always set to 6

Traffic Class (8 bits) · A DSCP value for QoS

Flow Label (20 bits) · Identifies unique flows (optional)

Payload Length (16 bits) · Length of the payload in bytes

Next Header (8 bits) · Header or protocol which follows

Hop Limit (8 bits) · Similar to IPv4's time to live field

Source Address (128 bits) · Source IP address

Destination Address (128 bits) · Destination IP address

Address Types

Unicast · One-to-one communication

Multicast · One-to-many communication

Anycast · An address configured in multiple locations

Address Notation

· Eliminate leading zeros from all two-byte sets

· Replace up to one string of consecutive zeros with a double-colon (::)

Address Formats

Global unicast

Link-local unicast

Multicast

EUI-64 Formation

· Insert 0xfffe between the two halves of the MAC

· Flip the seventh bit (universal/local flag) to 1

Multicast Scopes

1	Interface-local	**5**	Site-local
2	Link-local	**8**	Org-local
4	Admin-local	**E**	Global

Special-Use Ranges

::/0	Default route
::/128	Unspecified
::1/128	Loopback
::/96	IPv4-compatible*
::FFFF:0:0/96	IPv4-mapped
2001::/32	Teredo
2001:DB8::/32	Documentation
2002::/16	6to4
FC00::/7	Unique local
FE80::/10	Link-local unicast
FEC0::/10	Site-local unicast*
FF00::/8	Multicast

* Deprecated

Extension Headers

Hop-by-hop Options (0)
Carries additional information which must be examined by every router in the path

Routing (43)
Provides source routing functionality

Fragment (44)
Included when a packet has been fragmented by its source

Encapsulating Security Payload (50)
Provides payload encryption (IPsec)

Authentication Header (51)
Provides packet authentication (IPsec)

Destination Options (60)
Carries additional information which pertains only to the recipient

Transition Mechanisms

Dual Stack
Transporting IPv4 and IPv6 across an infrastructure simultaneously

Tunneling
IPv6 traffic is encapsulated into IPv4 using IPv6-in-IP, UDP (Teredo), or Intra-Site Automatic Tunnel Addressing Protocol (ISATAP)

Translation
Stateless IP/ICMP Translation (SIIT) translates IP header fields, NAT Protocol Translation (NAT-PT) maps between IPv6 and IPv4 addresses

15 PROTOKOLLE UND STANDARDS