Prüfungsvorbereitung dnet1

Modul Datennetze 1 (dnet1)

Simon Wächter

2017

Inhalt

[1 Lernziele 2](#_Toc496475842)

[1.1 Kapitel 1: Übersicht Datennetze 2](#_Toc496475843)

[1.2 Kapitel 2: Konfiguration von Netzelementen 4](#_Toc496475844)

[1.3 Kapitel 3: Netzwerkprotokolle und Kommunikation 5](#_Toc496475845)

[1.4 Kapitel 4: Schichten 1 und 2 als «Network Access» 8](#_Toc496475846)

[1.5 Kapitel 5: Ethernet 13](#_Toc496475847)

[1.6 Kapitel 6: Die Netzwerkschicht 17](#_Toc496475848)

[1.7 Kapitel 7: IP Adressierung 23](#_Toc496475849)

# Lernziele

## Kapitel 1: Übersicht Datennetze

* Client-Server: Zentrale Serversysteme die stetig laufen, wohingegen Clientsysteme auf die Server zugreifen und regelmässig an- und wieder ausgeschaltet werden
  + Netztypen
    - Heimnetze
    - Small Office/Home Office Netze
    - Unternehmensnetze
    - Öffentliche Internet
* Peer-to-Peer: Rechner stellt gleichzeitig als Server Ressourcen zur Verfügung, konsumiert aber auch von anderen Systemen (Rechner mit Print Sharing und anderer Rechner mit File Sharing)
  + Vorteile
    - Einfach aufzusetzen
    - Geringe Komplexität
    - Geringere Kosten, da keine dedizierten Server benötigt werden
    - Anwendbar auf einfache Tätigkeiten wie Print/File Sharing
  + Nachteile
    - Keine zentralisierte Administration
    - Geringere Sicherheit
    - Keine Skalierbarkeit
    - Geringere Performance da Systeme als Server und Client agieren
* Komponenten eines Netzes
  + Devices: Rechner (End Devices), Netzwerkkomponenten (Intermediary Devices)
  + Medien: Kupferkabel, Glasfaser, Luft (Network Media)
  + Dienste: Anwendungsdienste
* Physikalische Darstellung von Netzen: Zeigt, wo sich Komponenten befinden und wie sie verkabelt sind
* Logische Darstellung von Netzen: Zeigt, wie die Komponenten zu Gruppen/IP-Netzen zusammengefasst sind
* Kriterien für die Klassifikation von Netzen
  + Punkt-zu Punkt Netze: Leitungen von A nach B
  + Multiaccess Netze: Netz mit vielen Clients und Servern
  + Geografische Ausdehnung
* LAN-Netz: Limited Area Network/Local Area Network mit einer typischen Distanz von weniger als 100 Metern
* WAN-Netz: Wide Network Area, verbindet verschiedene Orte/Netze über mehr oder weniger lange Strecken. Sowohl der Internetanschluss eines Haushaltes als auch eine Leitung Bern-Zürich zählen
* MAN: Metropolitan Area Network, kleiner als WAN aber grösser als LAN, umfasst mehr oder weniger einen Ort/Stadt
* SAN: Storage Area Network, Netzinfrastruktur zur Anbindung von Speicher für Server
* Internet, besteht aus vielen LANs
  + Leitungen (Anschlussstellen, Backbone Leitungen)
  + Paketvermittlungsstellen
  + Satz von Protokollen
* Intranet: Netzwerk, welches nur für die Endgeräte darin zugänglich sind
* Extranet: Wie ein Intranet, doch haben gewisse Zulieferer/Firmen auch Zugriff
* Dedizierte Netze: Für jeden Dienst (Telefonie, Verteildienste und Computer) gibt es ein eigenes, getrenntes Netz
* Konvergierende Netze: Netze, auf welchen verschiedene Dienste (Triple Play à la Daten, Sprachen und Video) angeboten werden
  + Streaming via SwisscomTV benötigen oft Multicast, welches in öffentlichen Netzwerken nicht verwendet werden kann. Da Swisscom aber ein ISP ist und ihr Netz beeinflussen kann, können sie Multicast verwenden
* Grundanforderungen an zuverlässige Netze
  + Fehlertoleranz (Leitungsunterbruch): Erfüllt
  + Skalierbarkeit: Erfüllt
  + Dienstgüte (Quality of Service): Nicht erfüllt
    - Priority Queuing kann in nichtöffentlichen Netzen verwendet werden, um die Priorität von Inhalten zu garantieren 🡪 Verletzt Netzneutralität
    - Jitter: Abweichung von einen zyklischen Paketversenden (20 ms Intervalle mit 0 ms Jitter für VoIP)
  + Sicherheit (Abhören, Manipulation): Nicht erfüllt
* Leitungsvermittlung
  + Vor dem Beginn einer Sprachkommunikation wird eine feste, nicht mehr ändernde, Leitung zwischen Telefon A und Telefon B gewählt. Bandbreite: 64 kbps
  + Das Sprachsignal wird mit 8 kHz abgetastet und jeder Abtastwert mit 8 bit codiert
  + Durch die zeitliche Verschiebung kann ein Zeitmultiplexing (Time Division Multiplex, TDM) verwendet werden, um mehrere Verbindungen gleichzeitig zu ermöglichen
  + Norm für Europa (E1): Signal mit 2048 kbps und 30 möglichen Sprachkanälen à 64 kbps, 1 Signalisierungskanal à 64 kbps und 1 Zeitschlitz à 64 kbps
  + In der USA wird die Norm T1 mit einer Bandbreite von 1.5 Mbps verwendet
  + Kleine und konstante Verzögerung, aber sehr hohe Verfügbarkeit
* Paketvermittlung
  + Es gibt keinen kontinuierlichen Strom von Daten mehr
  + Die Informationen werden stattdessen in Segmente und Pakete mit einer Zieladresse abgepackt
  + Diese Pakete werden an Netzwerkknoten gesendet, welche anhand ihrer Routingtabellen die Pakete weiterleiten
* Skalierbare Architektur des Internet
  + Tier 1: Grösse ISP, untereinander mit Direktleitungen verbunden, stellen das Backbone dar
  + Tier 2: ISP, welche sich an einem Tier 1 anbinden lassen und so schauen, dass ihr Verkehr in ihren Tier 2 Netzen gut funktioniert
  + Tier 3:ISPs, die Endanwender anbinden und Tier 2 Netze für den Zugang bezahlen
* Entwicklung in der Datenkommunikation
  + Trends im Networking
    - Bring your own Device: Sicherheitsrisiko, Datenverlust
    - Online Collaboration Tools: Dezentralisierung
    - Videokommunikation: Anforderung an Datenkommunikation, z.B. Jitter
    - Data Center: Umdenken bedingt durch Virtualisierung, weg von Spanning Tree Protocol
    - Cloud Computing: Auslagern einer Applikation auf einen gemeinsam verwendeten Server, spart Energie und Traffic
    - Software Defined Networks (SDN): Softwarebasierte, zentrale Konfiguration von mehreren Netzen
  + Trends zu Hause
    - Internet of Things: Steuerung von Apparaten übers Internet
    - Steigende Gebäudevernetzung
    - Neue Anschlüsse wie drahtloses Breitband oder Fiber
  + Trends in der Netzwerksicherheit
    - Äussere Gefahren
      * Viren und Würmer
      * Trojaner und Spyware
      * Hackerangriffe
      * (Distributed) Denial of Service Angriffe
      * Data Interception and Theft
      * Identity Theft
    - Innere Gefahren: Eigene Mitarbeiter
    - Massnahmen
      * Antivirus- und Antispywaresoftware
      * Firewallfilterung des Verkehrs
      * Access Control Listen
      * Intrusion Detection Systems (IDS) und Intrusion Prevention Systems (IPS)
      * Virtuelle Private Netze (VPN)

## Kapitel 2: Konfiguration von Netzelementen

* Ablauf IOS Start
  + IOS Image wird vom Loader aus dem Flashspeicher geladen und gelesen
  + Konfiguration wird die Datei «startup-config» aus dem NVRAM gelesen und als «running-config» ins RAM kopiert
* Zugriff auf ein IOS System
  + Console via blauen Management Port
  + Auxiliary Port via schwarzen Management Port
  + Telnet respektive SSH via gelben Data Port
* Unterschiedliche Konfiguration
  + Lokale Konfiguration via Console und COM Schnittstelle oder neuerdings auch USB
  + Remote Konfiguration
    - Früher wurde an den Auxiliary Ausgang des Gerätes ein Modem angehängt, über welches via Telefonleitung auf das Gerät zugegriffen werden konnte
    - Heute wird ein Daten-Interface mit einer IP versehen und via SSH (früher Telnet) kommuniziert. Dabei muss auf dem Server ein Dienst bereitgestellt werden
* Navigation in IOS
  + User Exec Mode (Standart) 🡪 Router>
  + Priviledged Mode (Via enable erreichbar) 🡪 Router#
  + Global Config Mode (Via configure erreichbar) 🡪 Router(config)#
  + Interface/Routing/Line Config Mode (Via interface/router/line erreichbar) 🡪 Router(config-if)#
* Hilfreiche Befehle
  + cl? 🡪 Zeigt alle möglichen Befehle an (Hier clear und clock)
  + clock set ? 🡪 Zeigt die nachfolgenden möglichen Argumente mit einer Erklärung
  + no COMMAND 🡪 Löscht den Befehl
* Drei Fehlertypen
  + Ambiguous command
  + Incomplete command
  + Invalid input

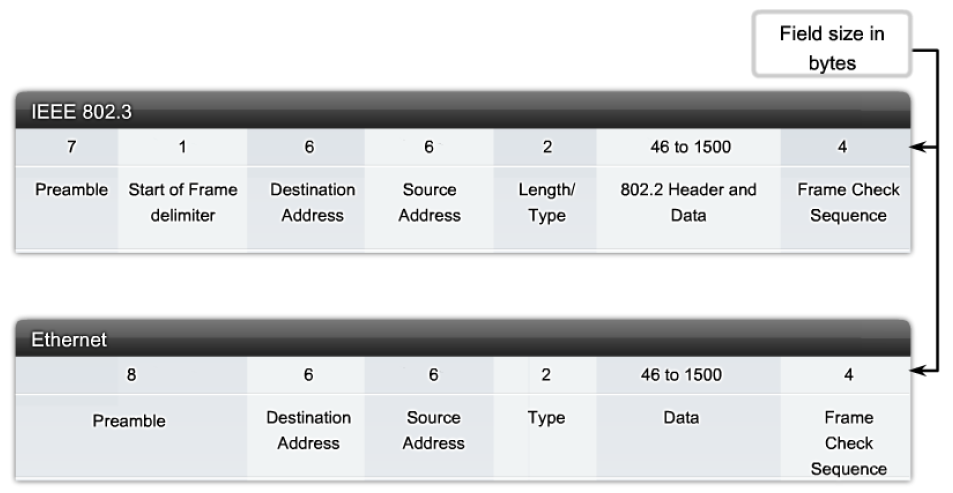
## Kapitel 3: Netzwerkprotokolle und Kommunikation

* In der Kommunikation zwischen Menschen werden Regeln eingehalten
  + Identifizierung von Sender und Empfänger mit Namen
  + Gemeinsame Sprache und Grammatik
  + Geschwindigkeit der Sprache
  + Bestätigung des Empfängers, dass es verstanden hat und noch zuhört
* Für Rechner gibt es auch Regeln
  + Kodierung der Daten (7 Bit, 1 Byte, 2 Byte)
  + Format und Kapselung der Nachricht (Welche Informationen müssen ausgetauscht werden? Wie?)
  + Erlaubte Grösse der Nachricht
  + Zeitliche Abfolge
  + Optionen, auf die sich beide Seiten einigen können
* Diese Regeln werden Protokolle genannt, sprich ein Protokoll ist ein Satz von Regeln
* Es gibt diverse Protokollsuiten wie TCP/IP, ISO, AppleTalk und Novell Netware, wobei heute nur noch das erste vorzufinden ist
* TCP/IP Layer
  + Application Layer (DNS, DHCP, SMTP, FTP, http)
  + Transport Layer (UDP, TCP)
  + Internet Layer (IP, NAT, ICMP)
  + Network Access Layer (ARP, Ethernet)
* Standardisierungsbehörden
  + Internet Society (ISOC)
    - Internet Architecture Board (IAB)
      * Internet Engineering Taskforce (IETF)
      * Internet Research Taskforce (IRTF)
  + Institute of Electrical and Electronics Engineers (IEEE)
  + International Standardization Organization (ISO)
  + Internet Assigned Numbers Authority (IANA)
* Verwaltung
  + ISOC: Verwalten Protokolle der Schichten Netzwerk, Transport und Anwendung
  + IEEE: Verantwortlich für die Schicht Network Access mit allen LAN und WAN Technologien
  + IETF: Stellt Requests for Comments auf, z.B. das Internet Protocol
  + ISO: Referenzmodell mit sieben Schichten
  + IANA: Vergibt IP-Adressen und AS-Nummern
* OSI Referenzmodell (In Klammern TCP/IP Layer)
  + Schicht 7: Application
    - TCP/IP Schicht: Application
    - Protokolle: HTTP, DNS, DHCP, FTP
    - Aufgabenbereich: Stellt die Dienste und Funktionalität für den Anwender bereit. Anwendungsentwickler arbeiten auf der Schicht 7
  + Schicht 6: Presentation
    - TCP/IP Schicht: Application
    - Protokolle: HTTP, DNS, DHCP, FTP
    - Aufgabenbereich: Verwaltet die Darstellungsinformation des Dateninhaltes, beispielsweise ob die Daten verschlüsselt oder komprimiert sind
  + Schicht 5: Session
    - TCP/IP: Application
    - Protokolle: HTTP, DNS, DHCP, FTP
    - Aufgabenbereich: Verwaltet die verschiedenen Sitzungen (Sessions) zwischen Endpunkten, beispielsweise Synchronisation von Bildern und Sprache bei einer Videokonferenz. Anderes Beispiel: Der Kontroll- und der Übertragungskanal bei Dateiübertragungen (FTP)
  + Schicht 4: Transport
    - TCP/IP: Transport
    - Protokolle: TCP, UDP
    - Aufgabenbereich: Bildung von Segmenten und Nummerierung dieser Segmente. Am Ziel Zusammenfügen der Segmente zur ursprünglichen Dateneinheit (Ende-zu-Ende). Optional: Flusssteuerung und Fehlerkorrektur
  + Schicht 3: Network
    - TCP/IP: Internet
    - Protokolle: IPv4, IPv6, ICMPv4, ICMPv6
    - Aufgabenbereich: Wegleitung der Pakete durch die verschiedenen Netze. Bildung und Adressierung von Paketen für Ende-zu-Ende Übertragung
  + Schicht 2: Data Link
    - TCP/IP: Network Access
    - Protokolle: PPP, Frame Relay, Ethernet
    - Aufgabenbereich: Weiterleitung der Pakete innerhalb eines Netzes. Bildung von Rahmen für die Übertragung innerhalb eines LANs oder über eine Punkt-zu-Punkt Leitung («Link»). Detektion von Übertragungsfehlern. Optional: Fehlerkorrektur auf einem Link
  + Schicht 1: Physical
    - TCP/IP: Network Access
    - Protokolle: PPP, Frame Relay, Ethernet
    - Aufgabenbereich: Bitübertragung von A nach B
* Das OSI Model arbeitet «top-down» und ordnet die Komplexität der Kommunikationssysteme in sieben Aufgabenebereiche/Schichten
* Die ISO hat die Entwicklung eines Protokollstacks streng nach dem Schichtenmodell veranlasst, jedoch mit recht wenig Erfolg
* Das TCP/IP Model arbeitet «buttom up», da die Protokolle schon da waren und man deshalb die Schichten nachdefiniert hat
  + Application: Represents data to the user plus encoding and dialog control
  + Transport: Supports communication between diverse devices across diverse networks
  + Internet: Determines the best path through the network
  + Network Access: Controls the hardware devices and media that make up the network
* Gesichtspunkte des TCP/IP Stack
  + Der Ansatz mit den Schichten 3 und 4 (Sowohl im OSI als auch im TCP/IP Model) hat den Vorteil, dass existierende LAN Protokolle weiterexistieren konnten
  + Durch die Schichten Transport und Internet konnten Anwendungen über Netzwerkgrenzen hinaus miteinander kommunizieren. Der Preis dafür ist, dass ein Rechner zwei Adressen (Schicht 2 und 3 besitzt)
* Verteilung
  + Schicht Anwendung: Software, die auf dem Rechner installiert werden muss
  + Schicht Transport und Internet ist im Betriebssystem des Rechners/Netzelementes
  + Schicht Network Access: Im Netzwerk Interface
* Datenkapselung
  + Viele Teilnehmer benützen gleichzeitig eine Datenleitung 🡪 Datenblöcke müssen durch den Absender in kleinere Einheiten segmentiert werden
  + Damit die Segmente zum richtigen Empfänger gelangen und dort richtig zusammengebaut werden können,
  + Damit der Empfänger die Segmente wieder zusammenbauen kann,
  + Um die Segmente wieder zusammensetzen zu können, müssen sie über eine Nummer und eine Adresse verfügen
  + Es bleibt die Frage, wie der Empfänger mit numerisch ausbleibenden Elementen umgeht
* Verpackung von Dateneinheiten («Encapsulation») und «Protocol Data Units»
  + Jedes Protokoll unterscheidet zwischen Daten (Payload) und einem Protokollheader
  + Die Anwendung Mail übergibt der Transportschicht eine Email mit der Grösse von 2 MB
  + Die Transportschicht spaltet die zu versendende Datei in Segmente mit einer maximalen Grösse von 1500 Bytes auf. In diesem Fall würde dies etwas mehr als 1330 Segmente ergeben
  + Ein Segment bildet die Payload für das Transportprotokoll
  + Das Protokoll TCP fügt einen Header vor die Payload und die Einheit Protokollheader + Daten werden zusammen Protocol Data Unit (PDU) des Protokolles TCP genannt.
  + Die PDU der Transportschicht bildet die Daten/Payload für die darunterliegende Internetschicht und so weiter – die PDU der Schicht N wird als zu den Daten der Schicht – 1 (Jedes Protokoll fügt einen Header hinzu)
* Zugang zu lokalen Daten
  + Jedes Protokoll des TCP/IP Stacks fügt einer Dateneinheit eine Adresse/Metainformationen hinzu
    - Upper Layers: Encoded Application Data
    - Transport: Destination and Source Process Number (Ports)
    - Network: Destination and Source Logical Network Addresses (IP)
    - Data Link: Destination and Source Physical Addresses (MAC)
    - Physical: Timing and Synchronization Bits
  + System PC1 (192.168.1.110 mit AA als MAC) möchte mit dem FTP Server (192.168.1.9 mit CC als MAC) kommunizieren
    - Zuerst prüft der Absender PC1, ob sich der Empfänger Server im gleichen Netz befindet 🡪 Ja
    - Der Absender PC1 tätigt mit der IP Adresse einen ARP (Address Resolution Protocol) Request, um an die MAC Adresse des Empfängers zu gelangen. Die Destination MAC Adresse ist dabei genullt
      * Data Link
        + Destination: FF:FF:FF:FF:FF:FF (Broadcast)
        + Source: AA
      * Network Layer
        + Source: 192.168.1 (Network), 110 (Host)
        + Destination: 192.168.1 (Network), 9 (Host)
    - Der Empfänger Server antwortet auf den ARP und schickt PC1 seine MAC Adresse zurück
    - PC1 kann nun ein reguläres Frame mit IP/MAC des Absenders und Empfängers bauen und FTP Anfragen stellen
      * Data Link
        + Destination: CC
        + Source: AA
      * Network Layer
        + Source: 192.168.1 (Network), 110 (Host)
        + Destination: 192.168.1 (Network), 9 (Host)
  + Hinweis: In der lokalen Kommunikation kann man die MAC Adressen seiner Nachbarn in Erfahrung bringen. Bei einer internen Kommunikation verwendet er gleich den Empfänger als MAC Destination
* Zugang zu entfernten Daten
  + System PC1 (192.168.1.110 mit AA als MAC) möchte mit dem FTP Server (172.16.1.99 mit AB12 als MAC) kommunizieren
    - Zuerst prüft der Absender PC1, ob sich der Empfänger Server im gleichen Netz befindet 🡪 Nein
    - Der Absender PC1 tätigt mit der IP Adresse einen ARP (Address Resolution Protocol) Request, um an die MAC Adresse des Default Gateways zu gelangen. Die Destination MAC Adresse ist dabei genullt
      * Data Link
        + Destination: FF:FF:FF:FF:FF:FF (Broadcast)
        + Source: AA
      * Network Layer
        + Source: 192.168.1 (Network), 110 (Host)
        + Destination: 192.168.1 (Network), 1 (Host)
    - Das Default Gateway antwortet auf den ARP und schickt PC1 seine MAC Adresse zurück
    - PC1 kann nun ein reguläres Frame mit IP/MAC des Absenders, der IP des Empfängers und MAC des Default Gateways bauen und FTP Anfragen stellen
      * Data Link
        + Destination: 11 (Default Gateway)
        + Source: AA
      * Network Layer
        + Source: 192.168.1 (Network), 110 (Host)
        + Destination: 172.16.1 (Network), 99 (Host)
  + Hinweis: In der entfernten Kommunikation kann man die MAC Adressen der entfernten Systeme nie in Erfahrung bringen. Bei der entfernten Kommunikation verwendet er gleich das Default Gateway als MAC Destination

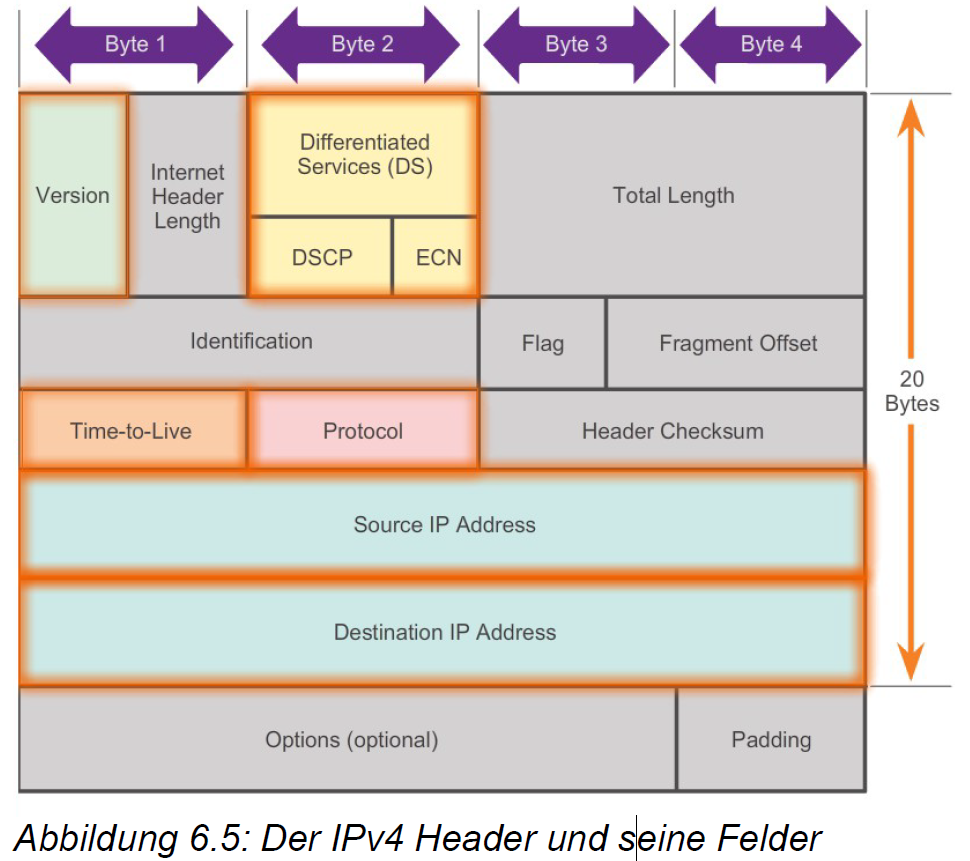
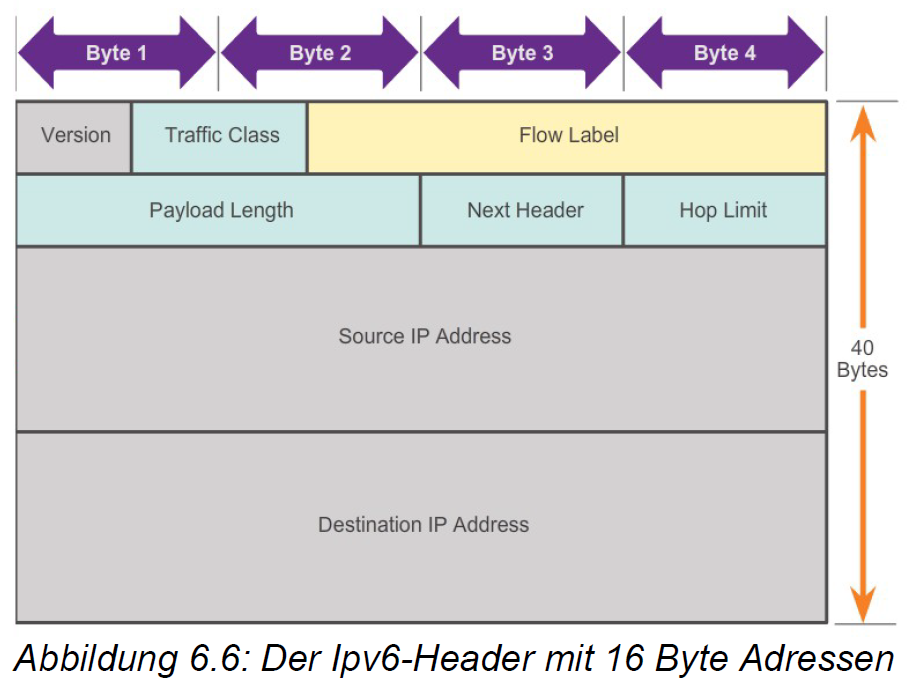
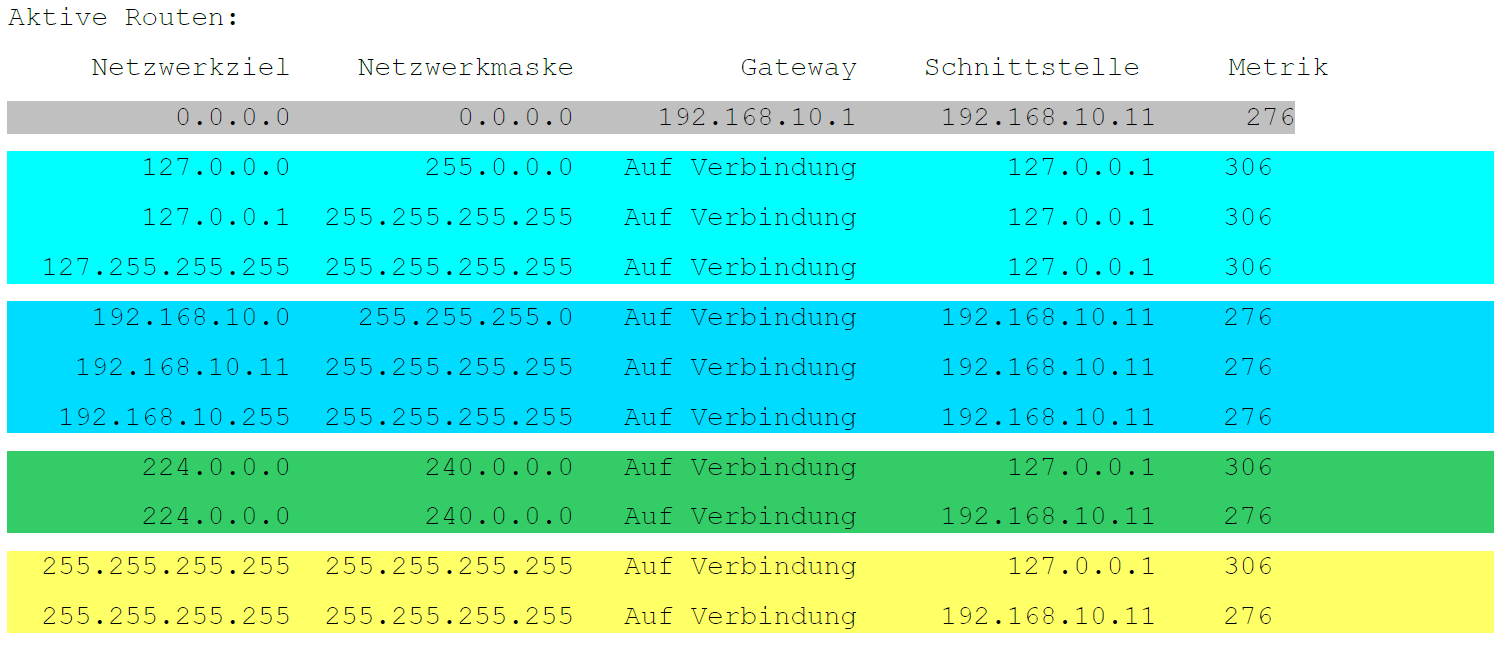
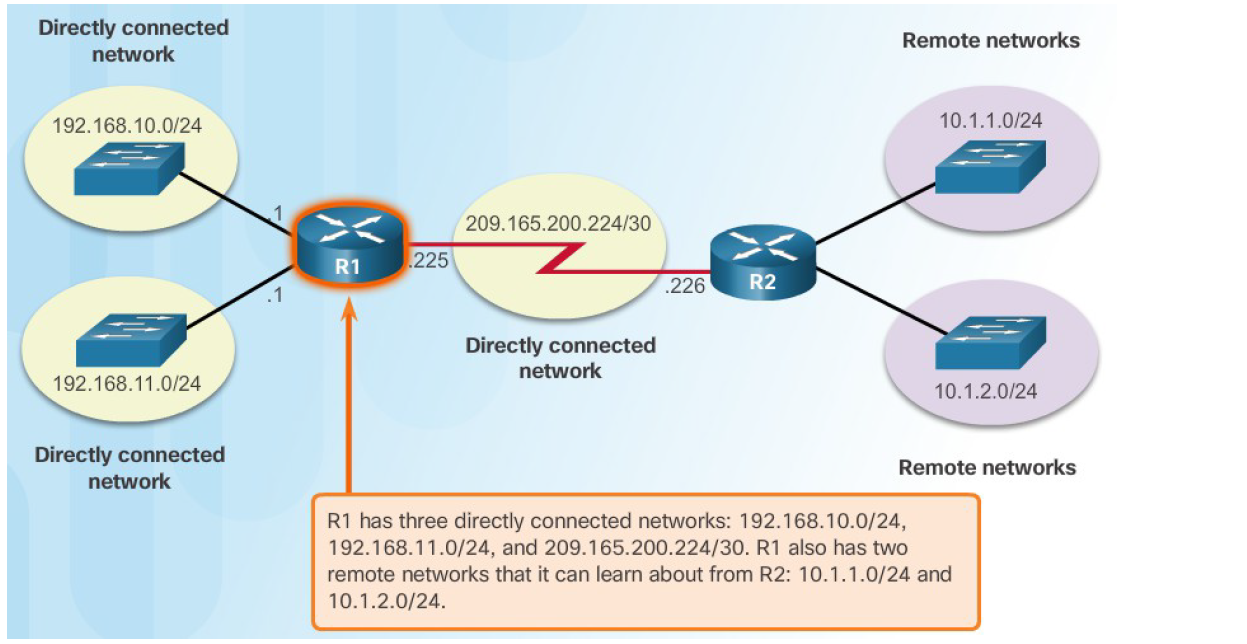
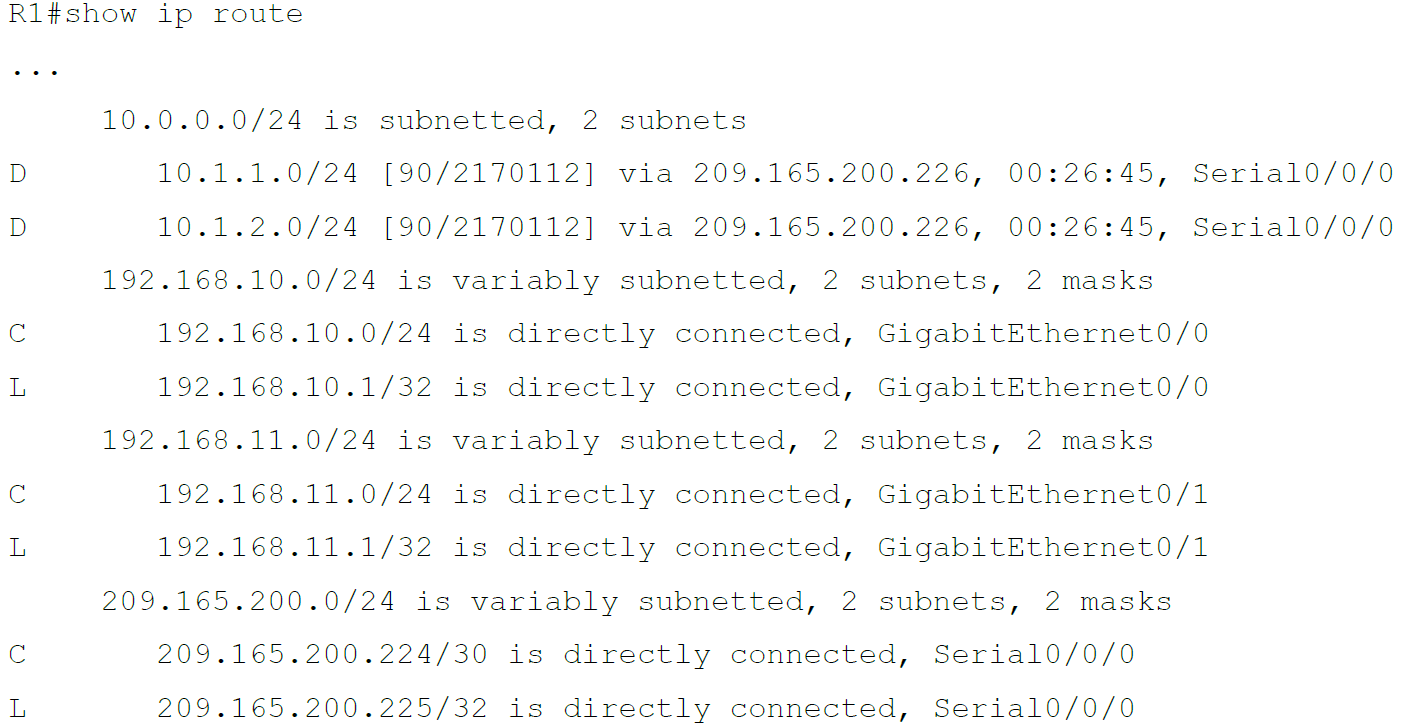
## Kapitel 4: Schichten 1 und 2 als «Network Access»

* Physical Layer bekommt vom Data Link Layer eine Bitfolge und muss diese übertragen. Sie weiss nicht wo die Rahmen anfangen und aufhören
* Vor dem Senden der Bits wandelt das Physical Layer diese in einen an den Kanal angepassten Leitungscode um
  + Glasfaser kann -3, -1, +1 und +3 übermitteln, also nicht nur ein Bit sondern gleich zwei
* Wichtige Medien und Leitungscode
  + Copper Cable
    - Physical Components: UTP, Coaxial, Connectors/NICs/Ports/Interfaces
    - Frame Encoding Technique: Manchester Encoding, No-Return to Zero (NRZ)
    - Signalling Method: Changes in the electromagnetic field, intensity of the electromagnetic field, phase of electromagnetic wave
  + Fiber Optic Cable
    - Physical Components: Singlemode Fiber, Multimode Fiber, Connectors/NICs/Ports/Interfaces
    - Frame Encoding Technique: Pulses of Light, Wavelength Multiplexing using different colours
    - Signalling Method: A pulse equals 1, no pulse equals 0
  + Wireless Media
    - Physical Components: Access Points, NICs, Radio, Antennae
    - Frame Encoding Technique: DSSS (Direct-sequence spread-spectrum), OFDM (Orthogonal frequency division multiplexing)
    - Signalling Method: Radio waves
* Medium Glasfaser
  + Die Intensität des Lichtes wird binär moduliert, sprich es können verschiedene Signal mit unterschiedlicher Wellenlänge gleichzeitig multiplexiert werden
* Frame Encoding Technique
  + Non return to zero: Der Wert wird durch einen [positiven] festen Spannungs- oder Leistungspegel codiert (Wie bei digital)
  + Manchester Encoding: Der Wert wird durch eine Flanke codiert. Tief nach hoch kodiert eine 1, hoch nach tief eine 0
  + Syhcorne und Asynchrone Übertragung: Bei der synchronen Übertragung wird das Taktsignal über die Leitung mitübertragen. Bei asynchroner Übertragung wird nur das Signal übertragen und beim Empfänger muss das Taktsignal zurückgewonnen werden (Meist mit Phase Locked Loop, kurz LPLL, realisiert)
* Auf Leitungen erfährt das elektrische Signal Dämpfungen und Dispersion
  + Dämpfung: Je höher die Frequenz, desto höher die Dämpfung
  + Dispersion: Ein kurzes Eingangssignal wird auf der Leitung zeitlich verbreitert. Dies kann nachfolgende Pulse beeinflussen, aber deterministisch mit einem Entzerrer herausgerechnet werden. Mit elektrischen Störströmen liegt die Fehlerwahrscheinlichkeit bei 10^-9
* Zuständige Behörden für die Standardisierung im Network Access
  + Layer 7 -3: IETF
  + Layer 2 – 1: ISO, EIA/TIA, ITU-T, ANSI, IEEE
* Grundbegriffe der physikalischen Schicht
  + Bandbreite (Bandwidth): Wie viele Informationen über diesen Kanal pro Zeiteinheit übertragen werden können (Brutto)
  + Durchsatz (Throughput): Wie viele Datenbytes pro Zeiteinheit tatsächlich übertragen werden können (Netto)
  + Verzögerung (Latency): Die Zeit die vergeht, vom Moment wo die Übertragung beginnt bis der Empfänger das Paket vollständig erhalten hat
* Übertragungsmedien
  + Kupfer
  + Glas
  + Luft
* Kupferverkabelung
  + Drei Typen
    - Nicht abgeschirmte, verdrillte Kupferadern (Unshielded twisted pair, UTP). Am Empfänger wird die Spannungsdifferenz gemessen. Vier verdrillte Paare
    - Abgeschirmte, verdrillte Kupferadern (Shielded twisted pair, STP). Wie UTP, aber mit Leiter abgeschirmt
    - Koaxialkabel (Einzelnes Kabel). Schneller als UTP/STP
  + Kabelbelegung bei UTP
    - Pin 1: TD+
    - Pin 2: TD-
    - Pin 3: RD+
    - Pin 4: Unbelegt
    - Pin 5: Unbelegt
    - Pin 6: RD-
    - Pin 7: Unbelegt
    - Pin 8: Unbelegt
  + Der Sender auf einem Rechner/Router verwendet die Adern 1 und 2. Der Empfänger benützt die Adern 3 und 6. Ein Switch hat die Eingänge 1 und 2 sowie 3 und 6 vertauscht Er empfängt auf 1 und 2 und sendet auf 3 und 6
  + Will man einen Rechner direkt an den Routereingang anschliessen, muss ein gekreuztes Kabel (1 und 2 auf 3 und 6) verwendet werden. Moderne NIC erkennen diesen Miss Match aber und kreuzen automatisch
* Faseroptische Leitungen
  + Zwei Typen
    - Single Mode Fasern
      * Sehr schmaler Kern welcher in wenig Dispersion resultiert 🡪 Direkter Pfad für das Licht
      * Geeignet für sehr lange Distanzen
      * Verwendet einen Laser als Lichtquelle
      * Verwendung in WAN/Backbones über mehrere Kilometer
      * Teuer in der Anschaffung
    - Multi Mode Fasern
      * Grösserer Kern welcher in grösserer Dispersion resultiert 🡪Licht wird an den Wänden durch Totalreflexion hin und hergeworfen
      * Geeignet für lange Distanzen
      * Verwendet ein LED als Lichtquelle
      * Verwendung in LAN über mehrere hundert Meter
      * Teuer, aber billiger als eine Single Mode Faser
  + Fasern sind gegen elektromagnetische Störungen immun und so für den Industriebetrieb interessant
  + Auf langen Leitungen lohnt es sich teilweise, ein Fasern Multiplex einzusetzen, da so mehrere Signale gleichzeitig übertragen werden können, ohne sich gegenseitig zu beeinflussen. Für einen solchen Fall muss das Licht aber aus mehreren verschiedenen und teuren Halbleiterlasern eingespeist werden
* Vergleich Kupfer gegen Glas
  + Bandbreite: 10 Mb/s – 10 Gb/s (UTP), 10 Mb/s – 100 Gb/s (Fiber)
  + Distanz: 1 – 100m (UTP), 1 – 100’000m (Fiber)
  + Resistenz gegen EMI/RFI: Gering (UTP), immun (Fiber)
  + Resistenz gegen Elektro Hazards: Gering (UTP), immun (Fiber)
  + Kosten für Medium und Connectors: Gering (UTP), hoch (Fiber)
  + Komplexität Einbau: Gering (UTP), hoch (Fiber)
  + Vorsichtsmassnahmen: Gering (UTP), hoch (Fiber)
* Drahtlos
  + Drei Technologien
    - WiFi: LAN Technologie um Rechner anzuschliessen
    - Bluetooth: Die Personal Area Technologie
    - WiMAX: [Toter] drahtloser breitbandiger Internetanschluss
  + Vorteile von drahtloser Übertragung
    - Keine Verkabelung
    - Teilnehmer kann sich bewegen
  + Nachteile von drahtloser Übertragung
    - Beschränkte Bandbreite, geteilt unter allen Teilnehmern
    - Sicherheit, da jeder das Signal empfangen und mithören kann
    - Interferenzen, da die Übertragung in freien Frequenzbändern (IMS-Band) erfolgt und jeder dort senden darf
  + Komponenten
    - WLAN Access Point: Drahtloser Switch und Router in einem
    - NIC für die drahtlose Kommunikation
  + Standards
    - Standard in 802.11a, b, g, n, ac und ad
    - Geschwindigkeit von 54 Mb/s bis zu 7 Gb/s
    - Frequenz von 5 GHz zu 2.4 GHz/5GHz und 60 GHz
    - Ab 802.11g rückwärtskompatibel
* Zweck der Sicherungsschicht Data Link
  + Die eigentliche Aufgabe der Schicht 2 besteht darin, sicherzustellen, die Pakete, die sie von der Schicht 3 erhält, innerhalb eines Netzes an das richtige Ziel zu transportieren
  + Teilaufgaben
    - Rahmenbildung um das Paket der Schicht 3
    - Regelung des Zugriffs auf den Übertragungskanal
    - Optional: Aufbau, Halten und Auflösen einer Verbindung
    - Fehlererkennung
    - Optional: Fehlerkorrektur durch Übertragungswiederholung
    - Optional: Flusssteuerung
* IEEE Normierung: Die IEEE wollte eine einheitliche Schnittstelle zur Netzwerkschicht, die unabhängig von der darunterliegenden Technologie (Ethernet, WLAN etc.) ist. Deshalb wurde das OSI Layer 2 in zwei Teilschichten unterteilt
  + Obere Teilschicht LLC (Link Layer Control): Enthält Informationen, welches Schicht 3 Protokoll transportiert wird (Leider halten sich bei Ethernet die meisten Applikationen nicht an den IEEE Standard und lassen das LLC weg)
  + Untere Teilschicht MAC (Medium Access Control): Ist für die Rahmenbildung, Kanalzugang und Adressierung zuständig
* Rahmen der Schicht 2
  + Aufbau
    - Header
      * Frame Start (Flag und Endflag)
      * Addressing (Ziel- und Quelladresse)
      * Priorit/QoS Feld (Optional)
      * Type: Zeigt auf das transportierte Protokoll, z.B. IP
      * Control (Optional): Art des Rahmen, logische Verbindung (bei Multicast Netzen), Sequenznummern, Flusskontrolle
    - Packet (Data)
      * Data
    - Trailer
      * Error Detection (Prüfsumme)
      * Frame Stop (Flag)
  + Erklärung: Da die Daten umrahmt werden, redet man von einem Sicht 2 Rahmen
  + Beim Weiterleiten eines Rahmens durch einen Router terminiert dieser das Schicht 2 Protokoll, das heisst, er berechnet die Prüfsumme aus dem erhaltenen Inhalt und vergleicht diese mit der Prüfsumme im Trailer. Falls nicht, wird der Rahmen weggeworfen, ansonsten entfernt er den Schicht 2 Rahmen und übergibt das darin enthaltene Paket der Schicht 3. Diese ist für die Weiterleitung zuständig und entscheidet auf welches Interface das Paket hinausgegeben wird. Das Ausgangsinterface wird dann das Schicht 3 Paket der Schicht 2 übergeben, wo es in einen neuen Schicht 2 Rahmen abgepackt und versendet wird
  + Beim Weiterleiten via Switch wird hingegen der Schicht 2 Rahmen nicht verändert
* Protokolle der Schicht 2
  + LAN
    - Ethernet 2 (DIX Digital Intel Xerox)
    - Ethernet 802.3 (IEEE)
    - WLAN 802.11 (IEEE)
    - Token Bus 802.4 (IEEE)
    - Token Ring 802.5 (IEEE)
  + WAN
    - HDLC (High-Level Data Link Control) (ISO)
    - PPP (IETF)
    - FrameRelay (ITU-T)
* Kanalzugriffsverfahren
  + WAN Topologien
    - Point-to-Point: Verbindung zwischen zwei Routern, können aneinandergereiht werden
    - Hub and spoke: Sternförmige Struktur mit zentralem Router
    - Full mesh: Vermaschte Struktur mit diversen Routern
  + LAN Topologien
    - Multi-Access mit zentralem Bus und angehängten Clients
    - Ring
  + Verwendung der Topologien
    - Point-to-Point, Hub and spoke und full mesh sind Fullduplex (MAC) und geeignet für HDLC, PPP und FrameRelay (Schicht 2 Protokoll)
    - Multi-Access sind geeignet für reguläre Netze mit Carrier Sense Multiple Access Collsion Detection/Avoidance (CSMA-CD/CA) (MAC) und Ethernet und WLAN (Schicht 2 Protokoll)
    - Ring ist geeignet zum Herumreichen eines Tokens (MAC) mit TokenRing oder FDDI (Schicht 2 Protokoll)
  + Regelung des Kanalzugriffs
    - Shared Medium (Viele Stationen benützen denselben Kommunikationskanal/Bus) versus Point-to-Point (An beiden Enden der Leitung hängt eine Station)
    - Half Duplex (Ein Endgerät kann gleichzeitig nur senden oder aber empfangen) versus Full Duplex (Ein Endgerät kann gleichzeitig senden und empfangen)
    - Auf Multiaccess Netzwerken (Shared Medium, meistens LAN) gibt es zudem zwei Arten des Kanalzugangs
      * Controlled Access (TokenRing, FDDI): Jede Station hat eine für ihn reservierte Zeit, in welcher er senden darf (Lesen geht immer)
      * Contention-based Access (Wettbewerb) (Ethernet mit Hubs, Wireless LAN): Wettbewerb – der schnellere darf senden. Es ist ein Verfahren definiert, wie vorzugehen ist, wenn zwei Stationen gleichzeitig senden
  + Rahmen der Sicherungsschicht
    - Wird ein Schicht 2 Rahmen durch ein Netzwerk befördert und es tritt ein Fehler bei der Übertragung auf, so stimmen die Prüfsummen nicht mehr überein und der Rahmen wird weggeworfen
    - Es gibt aber auch Schicht 2 Protokolle, die ein fehlerhaftes Rahmen nochmals anfordern
    - Der Protokoll Header sieht für verschiedene Schicht 2 Protokolle unterschiedlich aus und wird entsprechend dem Kommunikationskanal gewählt
      * Satellitenverbindung: Relativ hohe Fehlerwahrscheinlichkeit, niedrige Datenrate und hohe Verzögerung. Man wählt also ein verbindungsorientiertes Protokoll (Header mit Sequenznummern und Acknowledge Nummern) aus und baut viele [rasche] Fehlerkorrekturmechanismen gleich auf Schicht 2 ein, wodurch das Frame komplexer wird
      * LAN Umgebung: Relativ geringe Fehlerwahrscheinlichkeit. Man wählt also ein verbindungsloses Protokoll aus und baut wenige bis gar keine Fehlerkorrekturen ein. Fehler werden erst auf Layer 3 oder sogar erst 4 gehandhabt, was in einem schlanken Frame resultiert

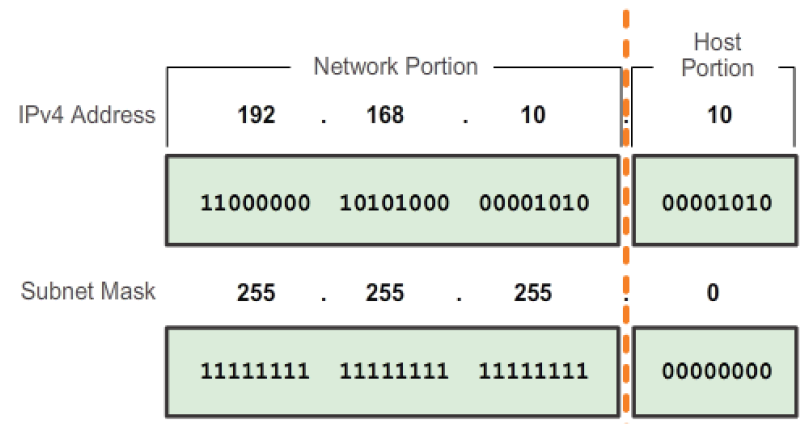
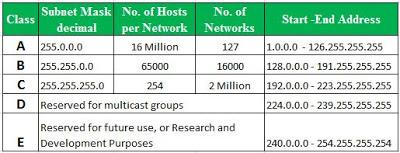
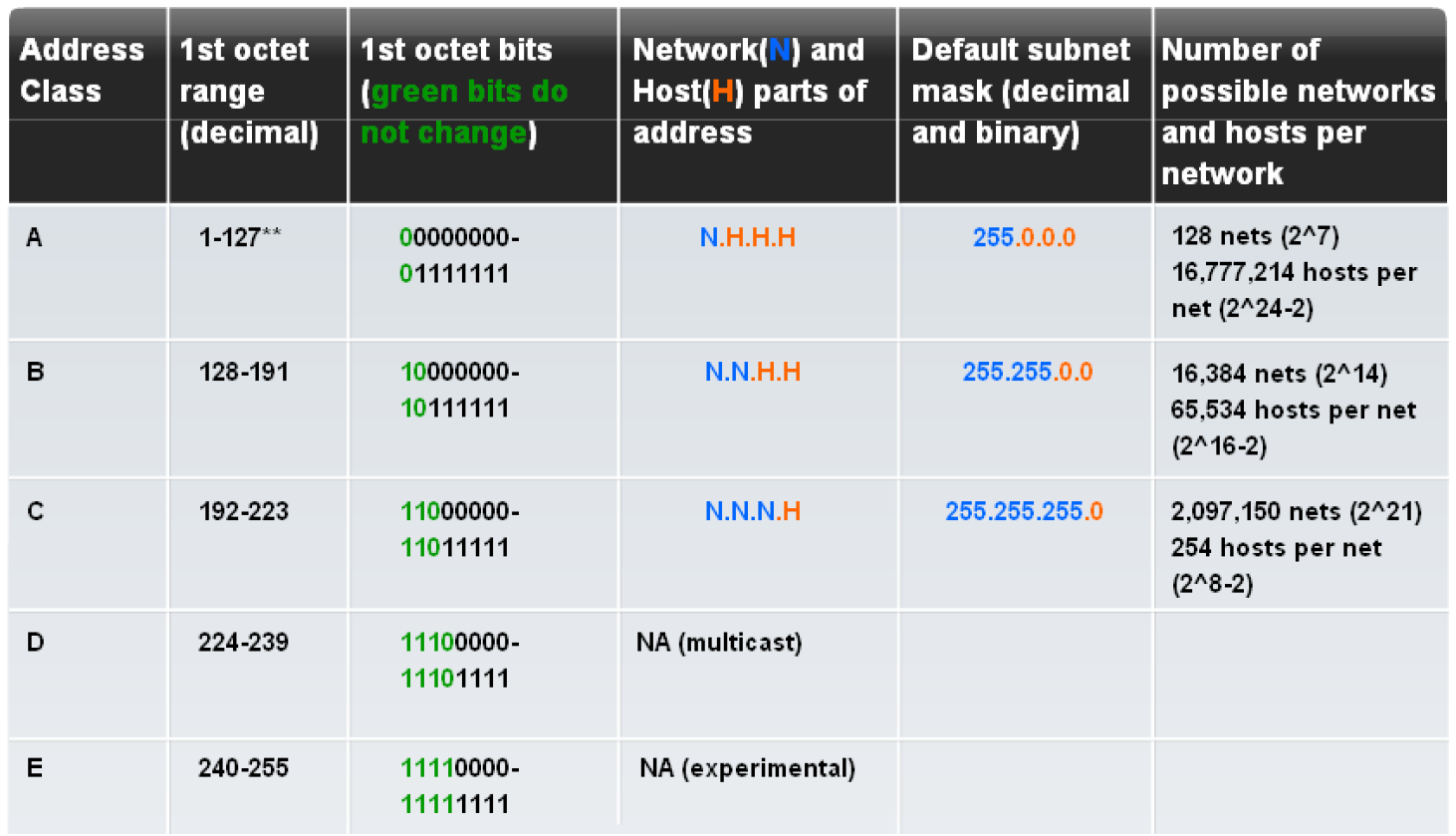
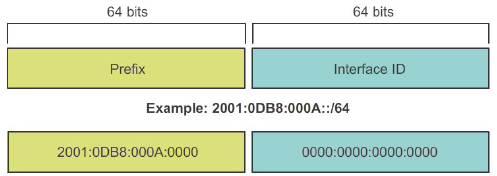
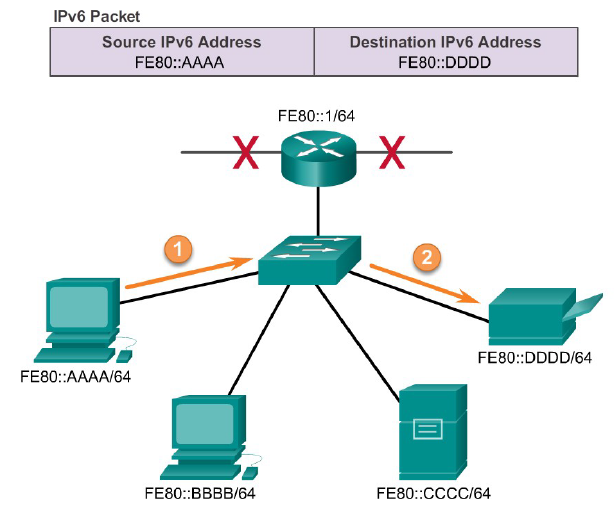
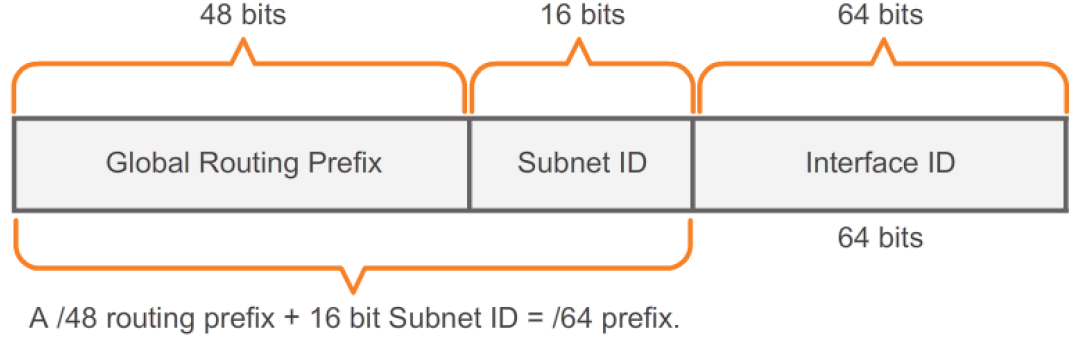
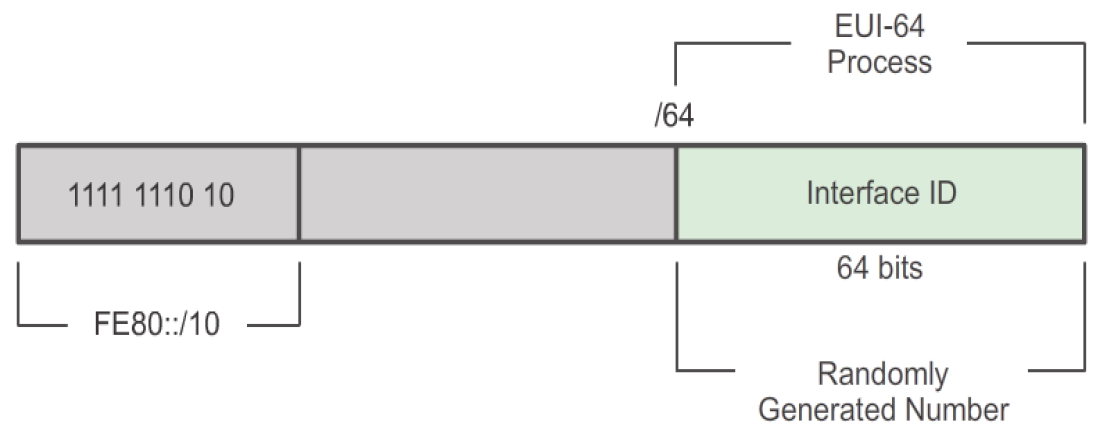
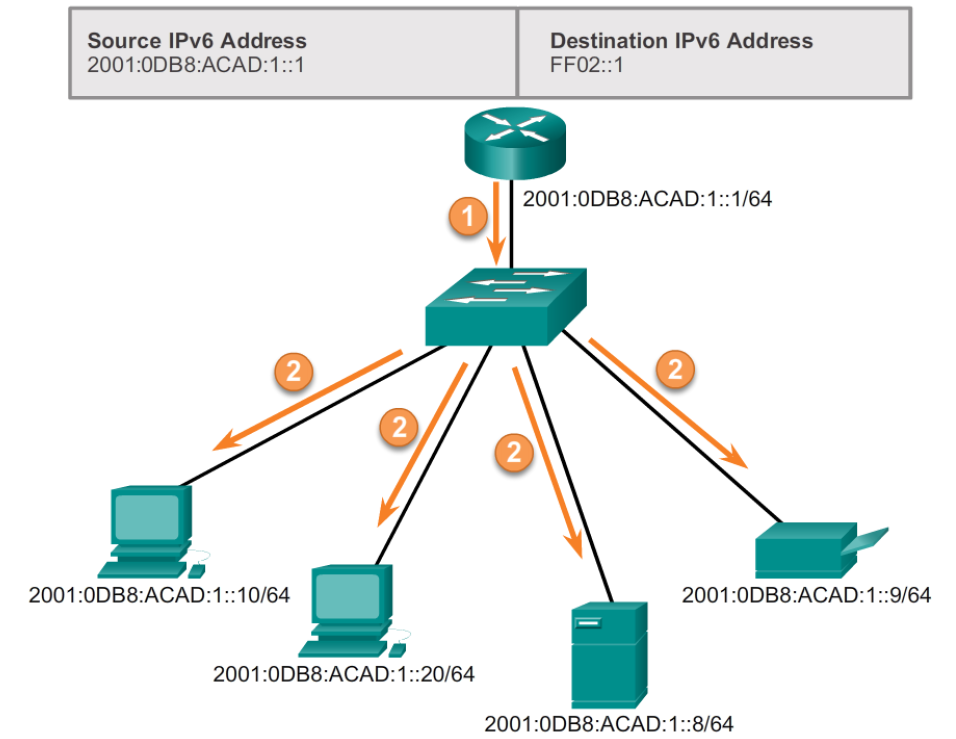
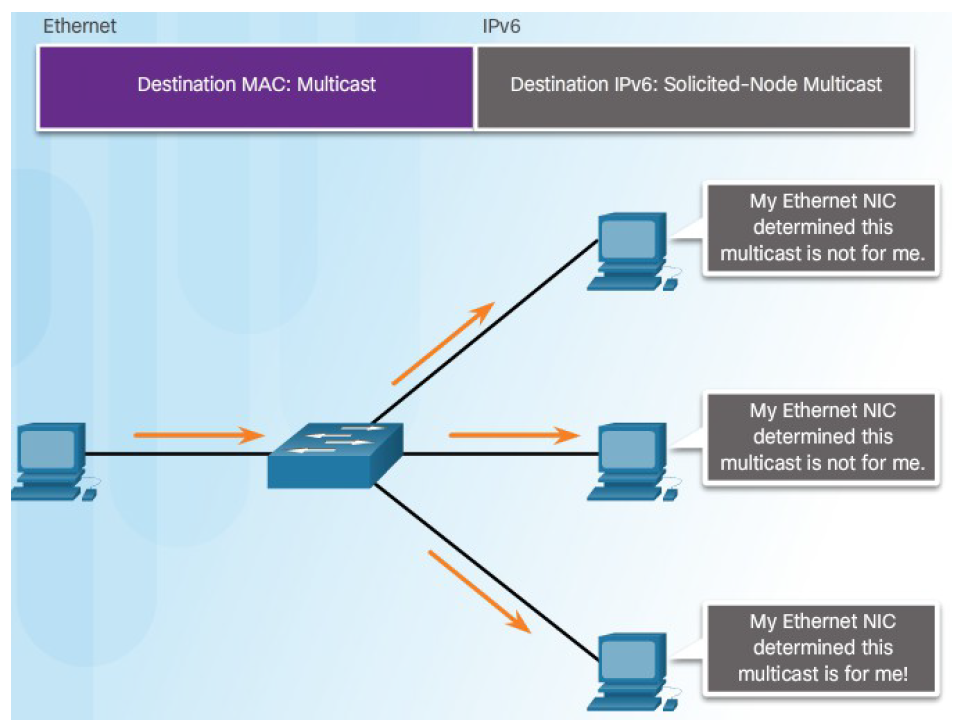
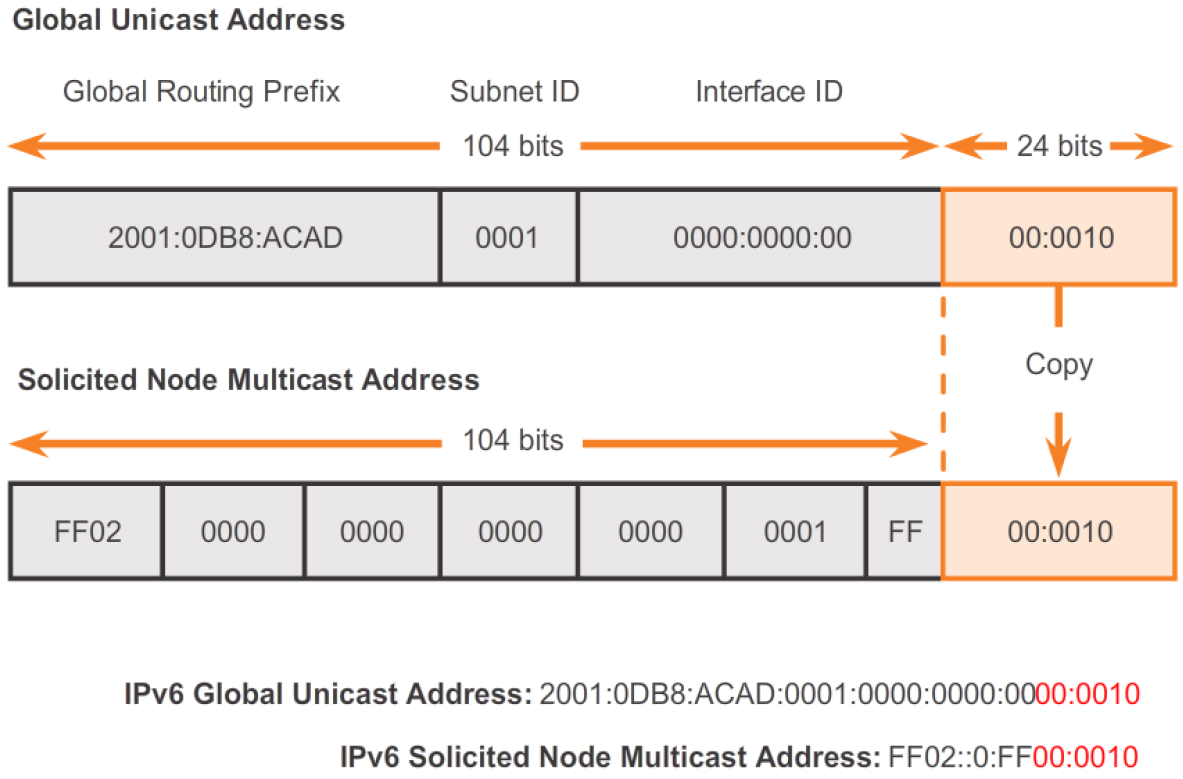
## Kapitel 5: Ethernet

* Protokollübersicht
  + Ethernet deckt die Schichten 1 und 2 des OSI Layers ab
    - Schicht 1
      * Definition der Signalpegel und des Timings
      * Definition der Kodierung
      * Stecker und Kabel
      * Verschiedene Ausführungsvarianten für verschiedene Medien
    - Schicht 2, gemäss IEEE 802 in zwei Teilschichten aufgeteilt
      * LLC (Logical Link Layer)
      * MAC (Medium Access Control)
  + Aufgaben der MAC Subschicht
    - Kapselung der Daten
      * Markierung von Beginn und Ende eines Rahmens
      * Adressierung
      * Fehlerdetektion
    - Kontrolle des Kanalzugangs
      * Platzierung der Rahmen auf einem Kanal
      * Fehlerbehandlung bei Kollisionen
  + Aufgaben der LLC Subschicht
    - Zuweisung des Rahmeninhaltes an die richtige Protokollinstanz der Schicht 3 mittels eines Service Access Points
  + Entwicklung und Ablauf
    - 1973: Entwicklung von Ethernet 1 durch Xerox
    - 1980: Ethernet 2 via Coax durch DIX
    - 1983: IEEE 802.3 mit 10 Mbps
    - 1995: IEEE 802.3u mit 100 Mbps
    - 1998: IEEE 802.3z mit 1 Gbps
    - 2002: IEEE 802.3ae mit 10 Gbps
    - 2015: IEEE mit 100 Gbps
  + Erfolgsfaktoren für Ethernet
    - Einfachheit, einfacher Unterhalt, Zuverlässigkeit
    - Integration neuer Technologien ohne Verzicht auf alte
    - Günstige Installation und Aufrüsten
* Ethernet Rahmen
  + 
  + Ethernet 1 und 2 wurden durch DIX entwickelt und später durch die IEEE als 802.3 spezifiziert. Im LAN kommen sowohl Ethernet 1 und 2 als auch IEEE Rahmen (Spanning Tree Protocol) vor
  + Felder
    - Preamble (DIX) und Preamble + Start of Frame Delimiter (IEEE) kommen auf dasselbe heraus. Es ist eine 1010.. Folge, markiert den Rahmenanfang und dient bei 10 Mbps Leitungen zum Aufsynchronisieren des Empfängers auf das Eingangssignal. Bei einer Analyse mit Wireshark wird die Präambel weder mitgezählt noch aufgezeichnet 🡪 Die Aufzeichnung beginnt immer mit der Destination MAC Adresse
    - Destination und Source: MAC Adresse à 6 Byte
    - Type (DIX): Falls der Inhalt zwischen 0x0600 und 0xFFFF liegt, so handelt es sich um einen Potokollcode, welcher angibt, welchem Schicht 3 Protokoll der Inhalt übergeben werden soll
    - Length (IEEE): Falls der Inhalt kleiner als 0x05EA ist, so handelt es sich um die Länge des Playload im Ethernet Rahmen 🡪 Es ist ein Rahmen nach IEEE Norm
  + Beim IEEE Frahmen folgt auf das Geld Length/Type drei Byte LLC (802.2 Header) welche angeben, an welches Schicht 3 Protokoll die Daten übergeben werden. Erst dann folgen die Daten-Bytes
  + Unterscheidung ob Ethernet 2 oder IEEE
    - Wenn Type/Length mindestens 0x0600 ist: Ethernet 2
    - Wenn Type/Length kleiner als 0x05EA ist: IEEE
    - Dazwischen: Undefiniert
* Ethernet MAC Adresse
  + In einem Multi Access Netz teilen sich viele Teilnehmer den Kanal
  + Aufbau der MAC Adresse à 6 Bytes
    - Organizational Unique Identifier (OUI): 24 Bits oder 6 Hex
    - Vendor Assigned: 24 Bits oder 6 Hex
  + Es warden drei Adressarten von Paketen unterschieden
    - Broadcast: Ziel sind alle Netzwerk-Interfaces in einem Netz. Die MAC Adresse ist FF:FF:FF:FF:FF:FF
    - Unicast: Ziel ist ein Rechner. In der MAC Adresse ist das LSB des ersten linken Bytes gleich 0 (Beispiel Ethernet/WLAN Interface). Beispiel: 10:08:b1:3e:81:3f
    - Multicast: Ziel ist eine Gruppe von Rechnern oder Netzwerk-Interfaces. In der MAC Adresse ist das LSB des ersten linken Bytes gleich 1. Die zweite Hex Zahl ist eine 1 oder falls lokal administriert eine 3. Falls das zweite Bit gesetzt ist, handelt es sich um eine private Adresse (Wird fast nie verwendet). Beispiel 01:00:5E:00:00:0A (Dabei ist 01:00:5E der erste MAC Teil für eine Multicast Adresse). Aus den untersten, rechten 23 Bit wird die IP Multicast Adresse gebaut, wobei das 24. Bit immer 1 ist. Die Zuordnung IP Multicast zu MAC Multicast ist also nicht eindeutig
* Medium Access Control
  + Kanalzugriffsverfahren Carrier Sense Multiple Access with Collision Detection (CSMA/DC)
    - Jede Station hört zuerst, ob der Kanal belegt ist (Listen before transmit)
    - Nur wenn der Kanal frei ist, beginnt die Station zu senden
    - Stellt der Sender eine Kollision fest, sendet er vorerst ein Jam Signal mit einer Länge von 32 Bit Perioden weiter, bis alle anderen Stationen von der Kollision Bescheid wissen
    - Alle Station verfallen dann in einen Backoff Zustand und gehen nach einer generierten Zufallszeit wieder in den regulären Modus über
  + Die Slot-Time gibt die minimale Länge an, die ein Rahmen haben muss, damit eine Kollision immer von allen Stationen detektiert wird. Wenn die Station Device 1 aufhört zu senden bevor das Signal überhaupt bei Device 2 angelangt ist, so kann es passieren, dass Device 1 die Kollision gar nicht bemerkt. Damit eine Kollision von Device 1 in jedem Fall entdeckt wird, muss er solange senden, wie das Signal benötigt, sich bis ans entfernte Ende auszubreiten und wieder zurück. Daraus errechnete man die minimale Länge, die ein Ethernet-Rahmen haben muss. Die Abbildung berücksichtigt, dass in einem Ethernet gemäss Norm maximal vier Repeater eingesetzt werden dürfen. Ein Repeater regeneriert ein abgeschwächtes elektrisches Signal. Damit kann die räumliche Länge eines Ethernets maximal 500m (5 mal maximal 100 m) werden
  + Slot-Time Mindestlängen (Wenn der Payload kürzer ist, muss er mit Nullen aufgefüllt werden)
    - 10 Mbps: 64 Byte Rahmen mit 46 Byte Payload in 51.2 Microseconds
    - 100 Mbps: 64 Byte Rahmen mit 46 Byte Payload in 5.12 Microseconds
    - 1 Gbps: 512 Byte Rahmen mit 494 Byte Payload in 4.1 Microseconds
  + Mindester zeitlicher Abstand zwischen zwei aufeinanderfolgenden Rahmen
    - 10 Mbps: 96 Bit time mit 9.6 Microseconds
    - 100 Mbps: 96 Bit time mit 0.96 Microseconds
    - 1 Gbps: 96 Bit time mit 0.096 Microseconds
    - 10 Gbps: 96 Bit time mit 0.0096 Microseconds
* Entwicklung des Ethernets
  + Früher würde über ein Buskabel mit ansteckbaren Adaptern gesendet. Das Hinzufügen neuer Adapter war sehr schwierig
    - Erster Schritt: Legacy Ethernet via Hub
      * Logische Struktur: Weiterhin eine Multiaccess Bus
      * Physikalische Struktur: Stern, welcher viel praktischer ist
      * Hinweis: Jedoch kann weiterhin nur eine Station gleichzeitig senden, da der Hub intern alle Anschlüsse durchreicht
    - Zweiter Schritt: Switch
      * Logische Struktur: Mehre Buse, wo jede Station individuell senden kann
      * Physikalische Struktur: Weiterhin ein Stern
* LAN Switches
  + Repeater: Ein Repeater verbindet zwei Ethernet Segmente miteinander und arbeitet wie ein Verstärker. Er nimmt eigehende Rahmen, verstärkt sie und reicht sie am anderen Ende weiter. Es existiert also eine Kollisionsdomäne
  + Hub: Ein Hub ist ein Multiport-Repeater und verfügt folglich auch nur über eine Kollisionsdomäne
  + Bridge: Eine Bridge verbindet zwei Ethernet Segmente miteinander, macht aber eine Zwischenspeicherung der Rahmen und analysiert den Ethernet-Header. Falls sich die Zieladresse im anderen Segment befindet, wird der Rahmen am anderen Port ausgegeben, sonst nicht. Zentraler Bestandteil ist also eine Table mit Spalten für die Ports und einer Spalte für die angeschlossenen MAC Adressen. Folglich existieren zwei Kollisionsdomänen
  + Switch: Ein Switch ist eine Multi Port Bridge und hat so viele Kollisionsdomänen wie Ports
    - Da ein Switch eine Mikrosegmentierung betreibt, können mehrere Stationen gleichzeitig senden und eine Station kann gleichzeitig senden und empfangen, da je ein Aderpaar dafür existiert (Full Duplex)
    - Da an einen Switch jedoch auch ein Hub angeschlossen werden kann, braucht es aus Kompatibilitätsgründen auch einen Half Duplex Modus
    - Ein Switch betreibt folgende Operationen
      * Learning: Auffüllen der MAC Adresse, indem er sich die Quelladresse eingehender Rahmen merkt und diese in der MAC Tabelle ablegt
      * Aging: Wenn eine MAC Adresse in MAC Tabelle geschrieben wird, dann wird ein Zeitstempel hinzugefügt. Der Eintrag wird beispielsweise nach 2 Minuten gelöscht
      * Flooding: Wenn eine MAC Zieladresse nicht in der MAC Tabelle gefunden wird, wird das Rahmen an alle anderen Ports weitergeleitet
      * Selective Forwarding: Wenn eine MAC Zieladresse gefunden wird, wird der Rahmen selektiv an den entsprechenden Port weitergeleitet
      * Filtering: Ein Switch kann bestimmte Rahmen herausfiltern, beispielsweise wenn die FCS nicht stimmt
* Weiterleitungsmethoden
  + Store and forward: Ein ankommendes Rahmen wird ganz empfangen und gespeichert. Die FCS wird ausgewertet und der Rahmen wird weitergeleitet, falls diese stimmt – sonst verworfen
  + Cut through switching: Der Rahmen wird weitergeleitet, bevor er ganz empfangen wurde
    - Fragment free: Es werden 64 Bytes abgewartet, damit keine Kollisionsfragmente weitergeleitet werden. Nach 64 Byte wird mit der Weiterleitung begonnen
    - Fast forwarding: Sobald die Zieladresse gelesen wurde, wird der Rahmen weitergeleitet. Es kann vorkommen, dass Fragmente weitergeleitet werden
* Zwischenspeicherung der Rahmen auf einem Switch
  + Port based memory: Jeder Port hat seinen eigenen Speicher
  + Shared memory: Alle Rahmen werden in einem gemeinsamen Speicher abgelegt
* Einstellungen auf Switch Ports
  + Switch und angehängtes Gerät handeln Duplex und Datenrate automatisch aus (Autonegotiation). Stimmt sie nicht an beiden Orten überein, geht der Port down
  + Je nach Gerät benötigt man für ältere Geräte ohne Auto MDX Funktion noch ein gekreuztes Kabel
    - Rechner zu Switch: Gerade
    - Rechner zu Router: Gekreuzt
    - Switch zu Router: Gerade
    - Switch zu Switch: Gerade
* Bedeutung von ARP
  + Problematik: Ein Host kennt eine Ziel IP Adresse eines Pakets, aber im Allgemeinen nicht die nächste Ziel MAC Adresse des «next hop»
  + Funktionen des Address Resolution Protocol (ARP)
    - Es findet die MAC Adresse zu einer IP Adresse
    - Es unterhält die ARP Tabelle des Rechners, um das Auffinden zu beschleunigen und das Netzwerk zu entlasten
  + Ablauf
    - Wenn ein Paket an eine Ziel IP Adresse gesendet werden soll, wird nachgeschaut, ob dafür schon eine MAC Adresse im ARP Cache liegt
    - Falls ja, wird die betreffende MAC Adresse im Ethernet Header als Destination angegeben
    - Falls nein, wird eine WHOIS Anfrage als Broadcast durch das Netzwerk versendet. Der betreffende Rechner oder aber das Default Gateway werden antworten und die MAC Adresse wird in den Cache aufgenommen
* Probleme mit ARP
  + Zu viel Broadcastverkehr in einem LAN
  + Sicherheitsrisiko, da via ARP Spoofing ein Rechner vorgeben kann, er hätte die entsprechende IP Adresse. Aller verkehrt geht dann bei ihm vorbei und kann abgehört werden
  + Bei IPv6 hat man deshalb versucht, die Zuordnung einer Schicht 2 Adresse zu einer Schicht 3 Adresse besser zu gestalten (Neighbor Discovery NS)

## Kapitel 6: Die Netzwerkschicht

* Die Netzwerkschicht in Kommunikationssystemen
  + Aufgaben der Netzwerkschicht
    - Auf dem Endsystem (Senderichtung): Das Protokoll der Netzwerkschicht nimmt Segmente von der Transportschicht entgegen und packt sie in Pakete ein
    - Bildung des Headers mit allerlei Overhead Informationen
    - Adressierung (Quelladresse, Zieladresse, private Adressierung oder öffentliche Adressierung)
    - Netzelemente der Schicht 3 (Router); Wegleitung der Pakete von einem Netz ins nächste (Routing)
    - Auf dem Endgerät in Empfangsrichtung: Auspacken von ankommenden IP Paketen und Auswertung des IP Headers, Übergabe des Segmentes an die Transportschicht
  + Regeln
    - Eine Maschine die an ein Netz angeschlossen ist und über eine IP Adresse verfügt, wird Host genannt
    - Eine Maschine die über verschiedene Interfaces an mehrere Netze angeschlossen ist und Pakete von einem Netz in ein anderes Netz weiterleiten kann wird Router genannt
    - Hinweis: Ein Router hat nur eine Schnittstelle in ein Netz. An einem Netz können aber mehrere Router angeschlossen sein
  + Layer 3 Protokille
    - IPv4 und IPv6
    - IPX (Novell)
    - AppleTalk
    - CLNS
* Charakteristika des IP Protokolls
  + Verbindungslos: Ein Sender schickt dem Empfänger etwas, ohne dass dieser es schon weiss. Der Sender weiss nicht, ob der Empfänger bereit ist, ob das Paket ankommt oder ob der Empfänger es lesen kann. Der Empfänger weiss nicht, wann ein Paket ankommen soll
  + Best effort: Das Netz leitet soviele Pakete wie möglich weiter. Sind zu viele Pakete unterwegs, werden die gepuffert und bei einem Überlauf weggeworfen
  + Media independant: Das Protokoll läuft über alle möglichen Layer 2 Protokolle (Ethernet, PPP, ATM etc.) und alle Schicht 1 Medien (Glas, Kupfer, Luft)
  + Hinweis: Kapselung bedeutet so viel wie das Abpacken einer Layer 4 PDU zu einem Layer 3 Datensatz mit Layer 3 Header davor (also eine neue Layer 3 PDU)
* IPv4 Header
  + 
  + Version (4 Bit): 4
  + IP Header Length: Der Header hat nicht immer die Länge von 20 Bytes, deshalb wird im Internet Header Length die Anzahl Zeilen \* 4 Bytes angegeben
  + Differentiated Services: Früherer Versuch, gewisse Kategorien von Verkehr zu unterscheiden (Netzneutralität), deshalb heute meist genullt. Die ersten sechs Bits bezeichnen dabei den Differentiated Service Code Point (DSCP) für den QoS Mechanismus, z.B. für Priority Queue in privaten Netzwerken. Die letzten zwei Bits sind für Explicit Congestion Notification (ECN), als Stauhinweise, registriert
  + Die zweite Zeile wird nur gebraucht, wenn ein Schicht 2 Rahmen grösser als die maximale Länge von 1500 Bytes ist und fragmentiert werden muss. Dies kommt aber heute faktisch nicht mehr vor
  + Time to Live (TTL). Dieses Feld wird vom Sender z.B. auf 128 oder maximal 255 gesetzt und wird von jedem Router um 1 dekrementiert bis es bei 0 weggeworfen wird und der Absender eine ICMP Fehlernachricht bekommt. Dies verhindert, dass Pakete endlos herumkreisen können
  + Protocol: Gibt an, welchem Protokoll ein angekommenes IP Paket übergeben werden soll, z.B. 0x06 für TCP
  + Source- und Destinationaddress zu je 4 Bytes (Heute viel zu kurz)
  + In mehr als 99% der Pakete werden keine Optionen mitgegeben und der Header beträgt in der Regel 20 Bytes. Werden Optionen mitgegeben, müssen diese auf Zeilen \* 4 Bytes aufgepaddet werden
* IPv6 Header
  + 
  + Hinweis: Der IPv4 Adressraum ist mit 32 Bit und 3.7 Milliarden möglichen Adressen heute viel zu klein. Hinzu kommt, dass mit der Einführung von NAT und dem daraus resultierenden Einsparen von Adressen neue Probleme aufgetreten sind (Nicht direkt erreichbar)
  + Vorteile von IPv6
    - Vervielfachung des Adressraums
    - Vereinfachung der Paketweiterleitung dank eines einfacheren Headers
    - Verzicht auf NAT
    - Sicherheit ist im Protokoll eingebaut
  + Version (4 Bit): 6
  + Traffic Class: Ist equivalent zum Feld «Differentiated Services» von IPv4
  + Flow Label (20 Bit): Spezialdienst für Echtzeitanwendungen. Informationen an die Router, für diesen Strom denselben Weg beizubehalten, damit die ankommenden Pakete nicht mehr geordnet werden müssen
  + Payload Length (16 Bit): Länge des gesamten IP Paketes inklusive Header und Extension-Header
  + Next Header (8 Bit): Entspricht dem Feld Protocol bei IPv5. Es gibt das Protokoll an, was auf IPv6 folgt. Anstatt Optionen mitzuführen, kann ein IPv6 Header auf Extension Header als nächstes Protokoll hinweisen
  + Hop Limit (8 Bit): TTL bei IPv4, aber mit ICMPv6 Meldung an den Absender
  + Source- und Destinationaddress zu je 16 Bytes
* Routing auf einem Rechner
  + Beim Senden eines IP Paketes wird zwischen zwei Fällen unterschieden
    - Der Zielrechner ist im lokalen Netz (Local Host)
    - Der Zielrechner ist in einem entfernten Netz (Remote Host)
  + Für einen Local Host holt sich der Rechner die MAC Adresse via ARP oder ARP Cache und schickt dann direkt ein Schicht 2 Frame mit dem IP Paket als Payload
  + Für einen Remote Host muss er mittels IP und Subnetzmaske herausfinden, dass die IP nicht im gleichen Fall liegt. Jetzt muss der kürzeste Weg zum Ziel gefunden werde, was Routing genannt wird
* Rechner: Routing Table mit drei Teilen
  + Teil 1: Netzwerk Interfaces: mit physikalischen und logischen Adaptern Komische Nummer, dann Bezeichnung (Mindestens 1 Loopback Interface)
  + Teil 2: IPv4 Routing Table
    - 
    - Zu unterscheidende Gruppen anhand des Netzwerkziels
      * 0.0.0.0: Default Route, wenn keine andere Route zutrifft. Das Paket wird über das eigene Interface 192.168.10.11 an das lokale Netzwerk Interface mit der Adresse 192.168.10.1 weitergeleitet
      * 127.0.0.1 – 127.255.255.255: Adressen für Dienste auf dem eigenen System. Sie werden an das Loopback Interface des Rechners weitergeleitet
      * 192.168.10.0 – 192.168.10.255: Adressen im lokalen Netz
        + 192.168.10.0: Bedeutet das ganze lokale Netz 192.168.10.x
        + 192.168.10.11: Bedeutet das Interface des eigenen Rechners
        + 192.168.10.255: Bedeutet die Broadcast Adresse des Netzes. Alle Interfaces im Netz hören auf diese Adresse
      * 224.0.0: Multicast Adressen
      * 255.255.255.255: Broadcast Adressen für alle Rechner im Netz
  + Teil 3: IPv6 Routing Table: Analog zu IPv4 Routing Table
* Routing Tabelle auf einem Router
  + Ein Router hat drei Arten von Routing Einträgen
    - Direkt angeschlossene Netze
    - Entfernte Netze, bekannt gemacht mittels
      * Statischen Einträgen
      * Dynamischen Routingprotokollen
    - Default Route
  + Beispiel
    - 
    - 
  + Es erscheinen automatisch alle direkt angeschlossenen und laufende Netze. Kriterium dabei ist, dass das Schicht 2 Protokoll auf dem entsprechenden Interface läuft oder nicht
  + Bezeichnungen
    - C: Direkt angeschlossene Netze («Connected»)
    - L: Lokale Interface Adresse
    - S: Statische Routen
    - O: Routen, die durch OSPF kennengelernt wurden
    - D: Routen, die durch EIGRP kennengelernt wurden
    - R: Routen, die durch RIP kennengelernt wurden
  + Erklärung
    - D 10.1.1.0/24 [90/2170112] via 209.165.200.226, 00:26:45, Serial0/0/0
    - D: Herkunft des Netzes
    - 10.1.1.0/24: Identifikation des Zielnetzes
    - [90: Administrative Distanz des Routing-Protokolls
    - 2170112]: Die Metrik, die das Routing-Protokoll dem Netz zuordnet
    - 209.165.200.226: Next-Hop IP-Adresse
    - 00:26:45: Wie viel Zeit ist seit der letzten Bestätigung der Route abgelaufen
    - Serial0/0/0: Das Ausgangs-IF für das Zielnetz
* Aufbau eines Routers
  + Ein Router leitet Pakete von einem Netz ins andere weiter und benötigt mindestens zwei Netzwerkinterfaces. Man unterscheidet zwischen
    - LAN-Interfaces wie Fast-Ethernet und Gigabit-Ethernet
    - WAN-Interfaces wie Serial
    - Management-Interfaces wie RS232 oder USB/AUX
  + Bestandteile und Aufgaben eines Routers
    - CPU
      * Macht die Weiterleitung der Pakete
      * Rechnet den Routing Algorithmus
    - RAM
      * Das Betriebssystem wird beim Aufstarten vom Flash ins RAM geladen
      * Enthält die running configuration
      * Enthält die Routing Tabelle
      * Enthält den ARP Cache
      * Enthält Warteschlangen als Paketspeicher
    - ROM
      * Diagnostic Software für Tests beim Aufstarten (POST)
      * Speichert die bootstrap Befehle
      * Enthält ein minimales IOS (ROM Monitor) für das Laden eines neuen IOS falls das laufende defekt wird
    - Flash
      * Permanente Speicherung des Betriebssystem IOS
      * Optional: Einige andere kleine Dateien
    - NVRAM
      * Nichtflüchtiger Speicher für die startup configuration
* Aufstartvorgang eines Routers
  + Laden des Betriebssystems
    - Perform POST aus ROM
    - Execute Bootstrap Loader aus ROM
    - Loacate the IOS aus Flash/TFTP Server
    - Load the IOS
  + Laden der Konfiguration
    - Load the configuration aus NVRAM/TFTP Server/Console
  + Hinweis: Findet das IOS keine Konfiguration im NVRAM und ist ein Netzwerkkabel mit Layer 3 Verbindung angeschlossen und konfiguriert, wird IOS automatisch per Broadcast prüfen, ob ein TFTP Server erreichbar ist. Dies kann im Labor mühsam sein, wenn man zuerst verkabelt und erst dann die Systeme startet
* Grundkonfiguration eines Routers: Siehe Cheatsheet
* Konfiguration der Interfaces: Siehe Cheatsheet
* Konfiguration des Default Gateways: Siehe Cheatsheet

## Kapitel 7: IP Adressierung

* Struktur einer IPv4 Adresse
  + Eine IPv4 Adresse besteht aus vier Bytes, wobei jedes Byte durch einen Punkt abgetrennt ist. Teilweise ist es sinnvoll, die Dezimalwerte von 0 bis 255 binär auszuschreiben
* IPv4 Subnetzmasken
  + Eine IPv4 Adresse besitzt einen Netzteil (Network Portion) und einen Hostteil (Host Portion). Der Netzteil kann variable sein und seine Länge wird durch die Subnetzmaske definiert
  + Verknüpft man die binäre Subnetzmaske mit der IPv4 Adresse, entsteht daraus der Netzteil
  + Der Netzteil zeichnet sich durch eine zusammenhängende Folge von Einsen ab, der Hostteil durch eine von Nullen
  + 
  + Netzadresse: IP Adresse mit lauter Nullen im Hostteil bezeichnet das ganze Netz
  + Broadcast-Adresse: IP mit lauter Einsen im Hostteil ist die Broadcast Adresse für das ganze Netz
  + Netzadresse und Broadcast-Adresse dürfen an keine Interfaces vergeben werden
  + Adressen mit Einsen und Nullen im Hostteil bezeichnen Hosts
  + Ein und dieselbe IP Adresse 10.1.1.0 kann mit unterschiedlicher Subnetzmaske unterschiedliche Netzbereiche darstellen (24/25/26 Bit Netzteil mit 254, 126 und 62 Hosts)
* IPv4 Unicast-, Broadcast- und Multicast-Adressen: Es gibt drei Typen von Zieladressen
  + Unicast Adresse: Ein IP Paket geht genau an ein Interface im Netzwerk. In einem /24er Netz sind dies die Adressen 1 bis 254
  + Broadcast Adresse: Ein Rechner stellt eine Anfrage an alle anderen Rechner im Netz. Er ersetzt dabei den Hostteil mit lauter Einsen
  + Multicast Adresse: Sollen Pakete an eine Gruppe von Rechnern gesendet werden, so werden Multicast Adressen verwendet: 224.0.0.0 – 239.255.255.255. Die Adressen 224.0.0.0 – 224.0.0.255 haben nur link-local Bedeutung und werden nicht geroutet. Der Bereich 224.0.1.0 – 238.255.255.255 sind globale Multicast Adressen
* Verschiedene Typen von IPv4 Adressen: Unterscheidung öffentlicher und privater Adressen. Dabei gibt es drei Adressräume, reserviert für die private Benutzung
  + 10.0.0.0 – 10.255.255.255 (10.0.0.0/8)
  + 172.16.0.0 – 172.31.255.255 (172.16.0.0/12)
  + 192.168.0.0 – 192.168.255.255 (172.16.0.0/16)
  + Hinweis: Eine private Adresse muss zwar im Netz eindeutig sein, kann aber in anderen Netzen erneut verwendet werden. Um eine Verbindung mit dem Internet aufzubauen, ist eine Netzwerk-Address Übersetzung erforderlich
* Spezielle Adressen
  + Loopback Adresse: 127.0.0.1 ist die Adresse des lokalen IP Stack. Der Adressraum 127.0.0.0/8 ist reserviert
  + Link lokale Adressen: 169.254.0.0/16 können automatisch dem Local Host zugewiesen werden
  + 192.0.2.0/24 sind für Unterricht und Dokumentation reserviert
  + Der Adressraum 240.0.0.0 – 255.255.255.254 ist reserviert und darf nicht frei verwendet werden
* Klassenbezogene Adressierung: Diese ist zwar veraltet, aber für das Verständnis immer noch wichtig. In vielen Fällen kann für eine Klasse die Netzmaske weggelassen werden. Für A Netze wurde ein /8, für B ein /16 und für C ein /24 Netzteil genommen
  + 
  + 
  + Klassenbezogene Adressierung benötigt kein Setzen der Subnetmaske, nutzt den Adressraum aber sehr schlecht aus, da A und B Netzte hostmässig nie ausgelastet werden können. Man ist deshalb zu einer klassenlosen Adressierung übergegangen, wo die Subnetzmaske explizit, dafür frei wählbar gesetzt werden kann
* Mängel von IPv4
  + Im Februar 2011 wurden die letzten freien IPv4 Blöcke durch die IANA an die ISP vergeben
  + Hinzu kommt, dass NAT viele Anwendungen wie IP Telefonie erschwert
  + IPv6 unterstützt eine hierarchische Vergabe von Adressen, die die Geografie berücksichtigt, was bei IPv4 nicht möglich ist. Das Internet kann aber nicht über Nacht von IPv4 auf IPv6 wechseln
  + Ansatz 1: Dual Stack: Man geht davon aus, dass IPv4 und IPv6 noch mehrere Jahre nebeneinander existieren werden und verwendet beide Stacks gleichzeitig. Wo beide Enden IPv6 unterstützen, wird dieses verwendet, allenfalls wird auf IPv4 zurückgegriffen. Dieser Ansatz hat sich im Großen und Ganzen durchgesetzt
  + Ansatz 2: Tunneling IPv6 in IPv4: Möchte jemand auf IPv6 umstellen, sein ISP unterstützt dies aber nicht kann IPv6 in IPv4 verpackt und regulär durchs Internet gesendet werden. Auf der anderen Seite kann dann das IPv6 Packet aus dem IPv4 Packet entpackt werden
  + Ansatz 3: Adress-Translation: IPv6 Adressen werden via NAT64 in IPv4 Adressen übersetzt. Dieser Ansatz wird heute aber nicht mehr verwendet.
* IPv6 Adressierung
  + IPv4: 32 Bits mit Dezimalzahlen von 0 bis 256
  + IPv6: 128 Bits mit Hexadezimalen Zweierzahlen als Hex
  + Eigentlich wären 64 Bit ausreichend gewesen, doch hat man 128 Bit bewusst gewählt
    - Die MAC Adresse kann komplett in die IPv6 Adresse dargestellt werden
    - Mehr Flexibilität bei einer Translation einer IPv4 in eine IPv6 Adresse
  + Führende Nullen können weggelassen werden
    - Lang: 2001:0DB8:0000:1111:0000:0000:0000:0200
    - Kurz: 2011: DB8 0:1111 0: 0: 0: 200
  + Die längste Nullfolge kann durch zwei Doppelpunkte ersetzt werden
    - Lang: 2001:0DB8:0000:1111:0000:0000:0000:0200
    - Kurz: 2011:DB8:0:1111::200
* Verschiedene Typen von IPv6 Adressen
  + Unicast: Ein Empfänger
  + Multicast: Eine Gruppe von Empfängern
  + Anycast: Eine Unicast Adresse, die Gruppen von Network Interfaces zugeordnet werden kann. Das Paket wird an das nächste Interface weitergeleitet (At least one out of any)
  + Hinweis: Es gibt bei IPv6 kein Broadcast mehr
  + Hinweis: Es gibt bei IPv6 keine Subnetzmaske mehr. Stattdessen wird am Schluss /n angefügt, wobei n im Bereich 0 bis 128 liegen muss – in der Regel gilt /64
  + 
* IPv6 Unicast Adressen: Es gibt 6 Arten
  + Global Unicast Adressen: Weltweit eindeutig. Sie werden im öffentlichen Internet geroutet und können statisch konfiguriert oder dynamisch zugewiesen werden
  + Link lokale Unicast Adressen: Sie werden für Kommunikation im lokalen Netz benützt und werden im öffentlichen Netz nicht geroutet. Jedes IPv6 Interface muss eine link-lokale Adresse haben, damit über den lokalen Link immer kommuniziert werden kann. Link lokale Adressen werden automatisch generiert, können aber händisch überschrieben werden. Adressraum FE80::/10
  + 
  + Loopback: Logisches Interface zum eigenen IPv6 Stack mit ::1/128
  + Unspecified Address (Any) ::/128, wird nur als Quelladresse gebraucht, wenn diese irrelevant ist
  + Unique local oder site local: Adressraum FC00::/7. Es sind Adressen für Kommunikation ausschliesslich innerhalb eines Firmennetzes. Für Kommunikation ins Internet sollten keine unique local Adressen verwendet werden. Insbesondere soll bei IPv6 auf NAT verzichtet werden. Nur Geräte, die keinen Anschluss ans Internet haben sollen, dürfen eine site local Adresse bekommen
  + IPv4 kompatible Adressen oder «IPv4 embedded»: Adressen, die eine Translation zwischen IPv4 und IPv6 ermöglichen (Thema zu komplex, wird folglich nicht behandelt)
* IPv6 Multicast Adressen (Spezifikation in der RFC 3587)
  + Global Routing Prefix: Eine Regional Internet Registry (RIR) vergibt heute Adressen aus dem Adressraum 2000::/3. Eine ISP erhält /32er Adressbereiche
  + Die ISPs geben ihren Kunden /48er Netze. Nur die ersten 48 Bit werden für das Routing im öffentlichen Internet berücksichtigt. Der Adress-Teil heisst Global Routing Prefix
  + Subnet ID: Der Adress-Teil vom 49. bis zum 64. Bit ist die Subnet ID. Ein Kunde, der einen 48 Bit Prefix erhält, kann also 16 Bit für Subnetze einsetzen, ist aber für das Routing dieser Subnetze selber verantwortlich
  + Die Interface ID, das heisst die letzten 64 Bit, entsprechen dem Host Teil bei IPv4. Im Gegensatz zu IPv4 kann ein Rechner auf einem physikalischen Interface aber mehrere IPv6 Adressen haben
  + 
* Autokonfiguration mittels Stateless Address Autoconfiguration (SLAAC)
  + Bei IPv6 ist es möglich, die Interfaces automatisch zu konfigurieren. Konkret heisst das, ein Rechner kann ohne Vorhandensein eines DHCP Servers zu kommunizieren beginnen, wobei es sich um eine zustandslose Kommunikation handelt
  + Ein IPv6 Router sendet auf seinen Interfaces in regelmässigen Abständen (Circa 200s) ICMPv6 Router Advertisment (RA) Nachrichten mit folgendem Inhalt
    - Prefix
    - Prefixlänge
    - Default Gateway Address
  + Ein Rechner muss nicht auf ein Router Advertisement warten, sondern kann selber via Router Solicitation (RS) eine Nachricht an die Multicastgruppe FF02::2 (Alle Routers) schicken und erhält dann eine Antwort. Wenn ein Rechner den v6 Prefix hat, so kanner aus der MAC Adresse des Interface eine eindeutige Interface ID generieren und jat dann eine vollständige IPv6 Adresse
  + Wann soll SLAAC oder DHCP gewählt werden
    - Option 1: SLAAC Only. Ein Client soll sich selber Autokonfigurieren – er kennt dann aber die Adresse des DNS Servers nicht
    - Option 2: SLAAC und DHCPv6. Der Client soll sich zusätzlich zur Autokonfiguration noch statische Parameter beim DHCPv6 abholen (zustandsloser DHCP)
    - Option 3: Nur DHCPv6: Der Client soll alle Parameter, auch die Adresse, beim DHCP Server abholen (stateful DHCPv6)
* Generieren der Interface ID: Zwei Wege
  + Gemäss IEEE RFC 5342 kann aus der MAC Adresse ziemlich schnell eine Interface ID, auch EUI-64-Adresse genannt, generiert werden – diese enthält aber eben die MAC Adresse (Datenschutz)
  + In einem zweiten Verfahren wird eine Interface ID gebaut, in welcher die echte MAC Adresse nicht mehr vorkommt
* Link lokale Adressen
  + Auf jedem IPv6 Interface wird automatisch eine link lokale IPv6 Adresse mit dem Prefix FF80:: wie folgt generiert
  + 
  + Oft kann man aus Faulheit einfach link lokal Adressen generieren, um mit diesen einfacher zu kommunizieren
* IPv6 Multicast Adressen: Zwei Arten, um Pakete an eine oder mehrere Zielrechner zu senden und unnötig redundanten Verkehr einzusparen
  + Assigned MC für vordefinierte Gruppen von Interfaces
    - FF02::1: Alle IPv6 Interfaces. Jedes Interface muss diese Pakete verarbeiten
    - FF02::2: Alle Router Interfaces verarbeiten diese Pakete
    - 
    - Mit einer Adresse werden also mehrere Rechner erreicht, die einen bestimmten Dienst bereitstellen
      * Die «all nodes» MC Adresse FF02::1 wird bei den ICMPv6 Router Advertisments (RA) als Zieladresse verwendet und entsprechen einem Broadcast bei IPv4
      * Die MC Adresse FF02::2 wird als Zieladresse für die ICMPv6 Router Solicitation Pakete (RS) verwendet. Die Autokonfiguration der Clients bei IPv6 wird also mit ICMPv6 und mit «assigned» MC Adressen gemacht
  + Solicitated Node MC
    - Eine Solicitated Node MC hat eine ähnliche Funktion wie die «all nodes» MC Adresse, ist aber effizienter und wird auf einem Interface automatisch generiert, wenn eine IPv6 Unicast oder link lokale Adresse konfiguriert wird. Der Vorteil besteht darin, dass ein Ethernet Interface die für den Rechner relevanten Rahmen gleich auf Layer 2 herausfiltern und nicht die Layer 3 Informationen extrahieren muss
    - 
    - Eine Solicitated Node MC Adresse wird wie folgt gebildet: Die in den letzten 24 Bit der MC Adresse stimmen mit der Interface ID überein
    - 
    - Anwendungen die Packete an an MC Adressen senden, verwenden das Schicht 4 Protokoll UDP, da eine Verbindung zu Gruppen von Rechnern nicht möglich ist
* Das Protokoll ICMP
  + Mit dem Internet Control Message Protocol (ICMP) kann das Routing im Netz und die Erreichbarkeit von Systemen getestet werden. Die wichtigsten ICMP Meldungen
    - Host confirmation mit echo request und echo response
    - Destination or service unreachable
    - Time exceeded
    - Route redirection
  + Die Werkzeuge ping, traceroute oder tracert arbeiten auf dem ICMP Protokol
  + Erhält ein Router ein Paket das er nicht weiterleiten kann, kann er es via «Destination or service unreachable» dem Sender mitteilen. Auch kann das Ablaufen eines TTL Feldes dem Sender mitgeteilt werden. Mit «Route Redirection» kann ICMP dem Router eine kürzere, angebundene Route mitteilen
  + ICMP ist ein Schicht 3 Protokoll und benutzt Schicht 3 Funktionalität, nicht aber höhere Layer
* Prüfen der Erreichbarkeit
  + Befehl ping: Sendet eine Reihe von Echo Requests als ICMP an einen Zielhost. Erhält dieser die Pakete, antwortet er mit einem Echo Reply. Die vergangene Zeit für den Hin- und Rückweg wird gemessen. Es kann vorkommen, dass der Echo Request ankommt, die Antwort aber ausbleibt. Dies ist meist auf ein Routing Problem zurückzuführen, das den Rückweg blockiert. Häufig werden ICMP Pakete auch durch eine Firewall blockiert
  + Befehl traceroute/tracert: Zeigt den Weg zum Zielsystem an. Dabei wird mit einer TTL von 1 begonnen, sodass man eine «Time exceeded» Fehlermeldung vom Router erhält. Man erhöht die TTL dann immer weiter, um den ganzen Weg ablaufen zu können
  + Das ICMP Protokoll verfügt gegenüber ICMPv4 zudem über die Features des Router Advertisments und der Router Solicitation Meldungen
* ICMPv6
  + ICMPv6 verfügt auch über Neighbor Solicitation (NS) und Neighbor Advertisment Meldungen, welche für Address Resolution und Duplicate Address Detection (DAD) verwendet werden
  + Soll eine MAC Adresse zu einer IPv6 Adresse gefunden werden, so sendet die Station eine ICMP NS Meldung, auf welche die gesuchte Station antwortet
  + Soll ein Interface eine IPv6 Adresse konfigurieren, so soll auf diese Adresse zuerst ein ICMP NS gesendet werden. Erhält man keine Antwort, ist die Adresse frei und kann verwendet werden 🡪 Die Adresse ist eindeutig. Die Verwendung von DAD ist empfohlen
  + Interessant ist, dass die Anfrage an eine NS MC Adresse gesendet wird. Damit können Interfaces bereits auf Layer 2 bestimmen, ob die Anfrage an sie gerichtet ist und so CPU Zeit durch Broadcasts sparen