Datenkommunikation

Internet-Steuerprotokolle und IPv6

Wintersemester 2011/2012

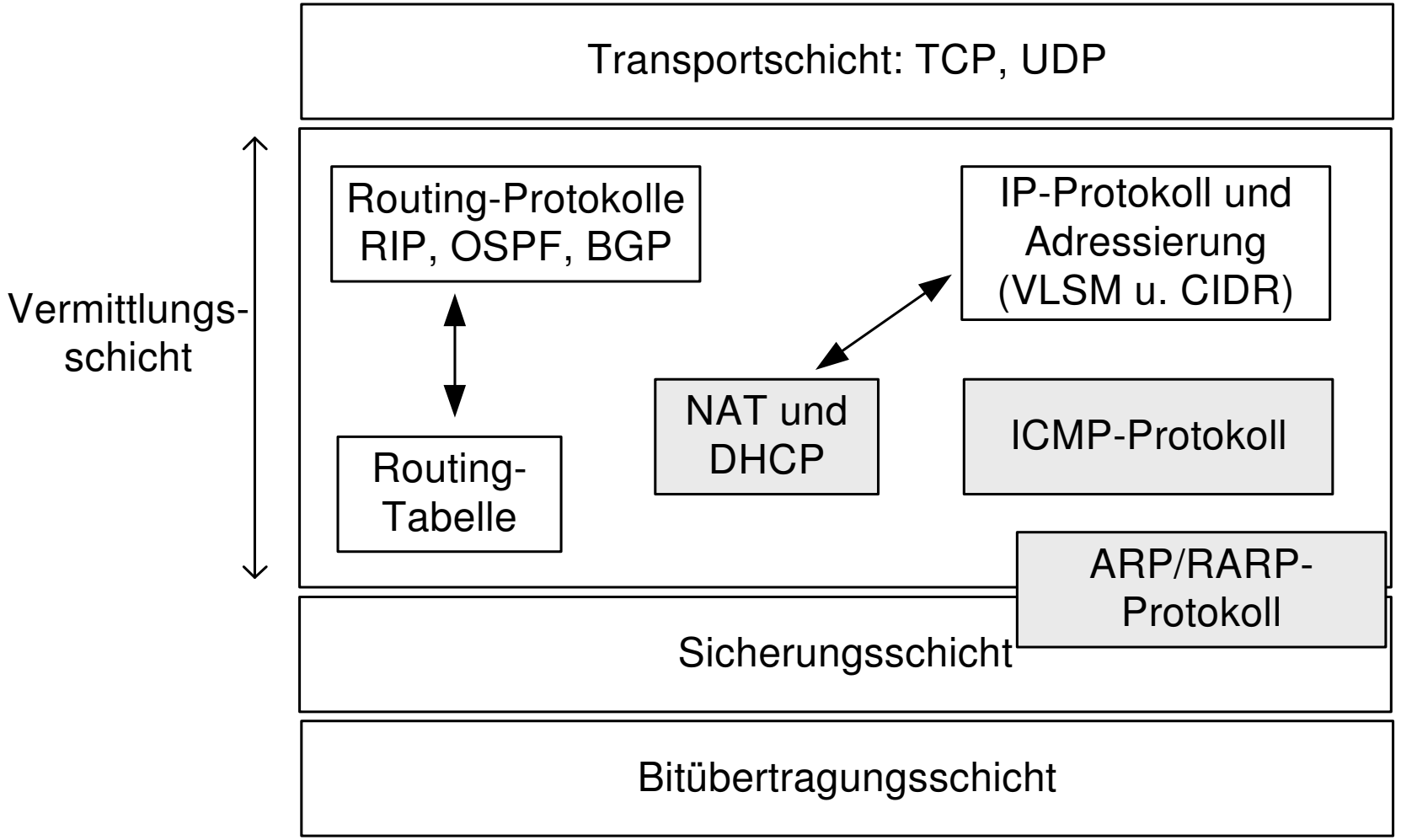
Überblick

1	Grundlagen von Rechnernetzen, Teil 1
2	Grundlagen von Rechnernetzen, Teil 2
3	Transportzugriff
4	Transportschicht, Grundlagen
5	Transportschicht, TCP (1)
6	Transportschicht, TCP (2) und UDP
7	Vermittlungsschicht, Grundlagen
8	Vermittlungsschicht, Internet
9	Vermittlungsschicht, Routing
10	Vermittlungsschicht, Steuerprotokolle und IPv6
11	Anwendungsschicht, Fallstudien
12	Mobile IP und TCP

Überblick

1. Steuerprotokolle
   - **ICMP**
   - ARP und RARP
   - NAT
   - DHCP
2. IPv6
   - Grundlagen und Adressierung
   - IPv6-PDU
   - Automatismen, Neighbor Discovery

Einordnung
Die Internet-Vermittlungsschicht

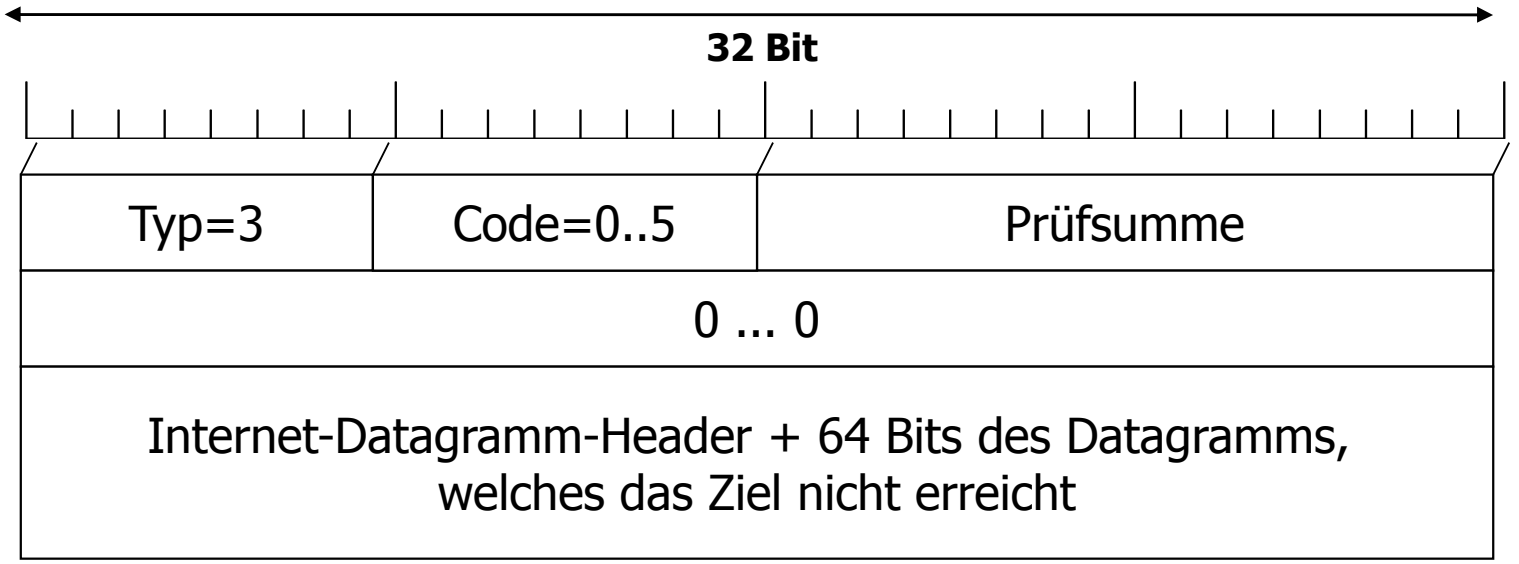


ICMP: Einführung

- ICMP (Internet Control Message Protocol, RFC 792)
  - Dient der Übertragung von unerwarteten Ereignissen und für Testzwecke
  - Beispiel 1: Ein Netzwerk ist nicht erreichbar: Ein IP-Router sendet in diesem Fall die ICMP-PDU „Network Unreachable“
  - Beispiel 2: Das ping-Kommando verwendet z.B. ICMP-PDUs (Echo Request, Echo Reply)
  - Beispiel 3: Das Kommando traceroute (tracert) nutzt ICMP (Typ=11, Time-to-live exceeded)
- ICMP-Nachrichten werden in IP-Datagrammen versendet

ICMP: PDU

- ICMP-Beispiel: **Destination unreachable** → Ein Router kann ein Datagramm nicht ausliefern



- Router sendet ICMP-Nachricht an den Absender
- Code: 0 = Netzwerk nicht erreichbar, 1 = Rechner nicht erreichbar,...

Überblick

1. Steuerprotokolle
   - ICMP
   - **ARP und RARP**
   - NAT
   - DHCP
2. IPv6
   - Grundlagen und Adressierung
   - IPv6-PDU
   - Automatismen, Neighbor Discovery

ARP

- ARP (Address Resolution Protocol), RFC 826
  - ARP dient dem **dynamischen Mapping** von IP-Adressen auf Schicht-2-Adressen (MAC-Adressen)
  - Jeder Host kennt seine eigene Schicht-2-Adresse, nicht aber die Adressen der anderen Hosts
  - Jeder Host führt einen **ARP-Cache** und merkt sich darin Schicht-2-Adressen, die über ARP im **IP-Broadcasting** erfragt werden können → **Periodisches Löschen vermeidet Inkonsistenz!**
  - Ist der Zielhost nicht gespeichert, wird ein **ARP-Broadcast** mit der IP-Zieladresse als Parameter versendet
  - Der Zielrechner antwortet mit einem **ARP-Reply** (MAC-Adresse)
  - IP-Router übernehmen Rolle des **ARP-Proxy**

ARP-Cache

C:\>**arp -a**

Schnittstelle: 192.168.2.116 --- 0x2

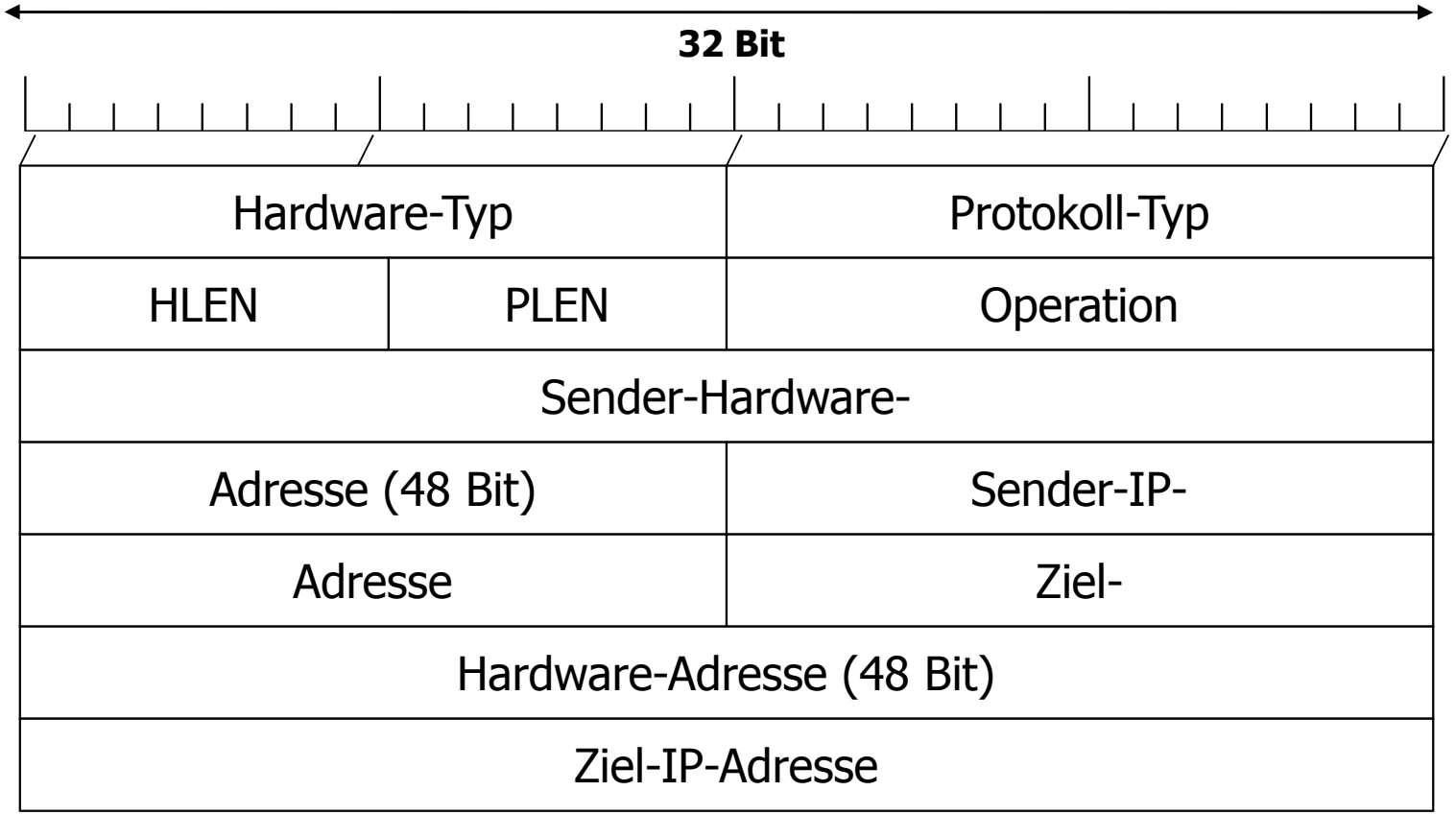
Internetadresse	Physikal. Adresse	Typ
192.168.2.1	00-50-fc-cb-7e-da	dynamisch
192.168.2.14	00-e0-4c-10-17-32	dynamisch
192.168.2.250	08-00-37-31-de-ae	dynamisch

RARP

- RARP = Reverse ARP
  - RARP wird verwendet, wenn die eigene IP-Adresse eines Hosts nicht bekannt ist, aber benötigt wird
  - RARP sendet RARP-Request mit der eigenen MAC-Adresse als Broadcast
  - Anwendungsfall:
    - Plattenlose Desktop-Arbeitsplätze, die beim Booten Ihre IP-Adresse ermitteln wollen

ARP-PDU

- Nachrichtenformat eines ARP/RARP-Pakets

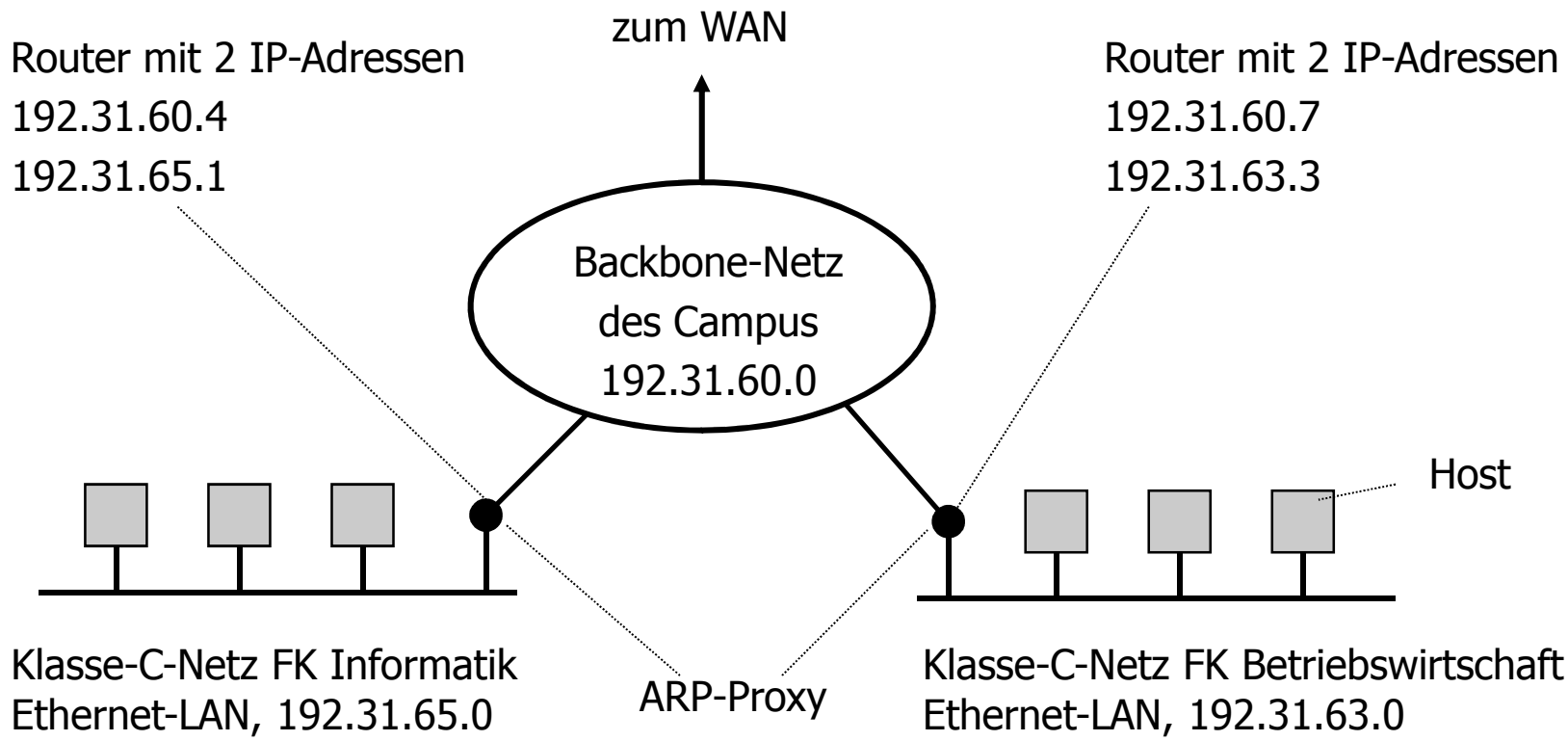


ARP-PDU

- **Hardware-Typ:**
  - Hardware-Typ, 1 = Ethernet
- **Protokoll-Typ:**
  - Typ des High-Level-Protokolls, X`0800` = IP
- **HLEN:**
  - Hardware-Adressenlänge
- **PLEN:**
  - IP-Adressenlänge
- **Operation**:
  - 1 = ARP-Request
  - 2 = ARP-Response
  - 3 = RARP-Request
  - 4 = RARP-Response
- **...**

ARP: Beispiel

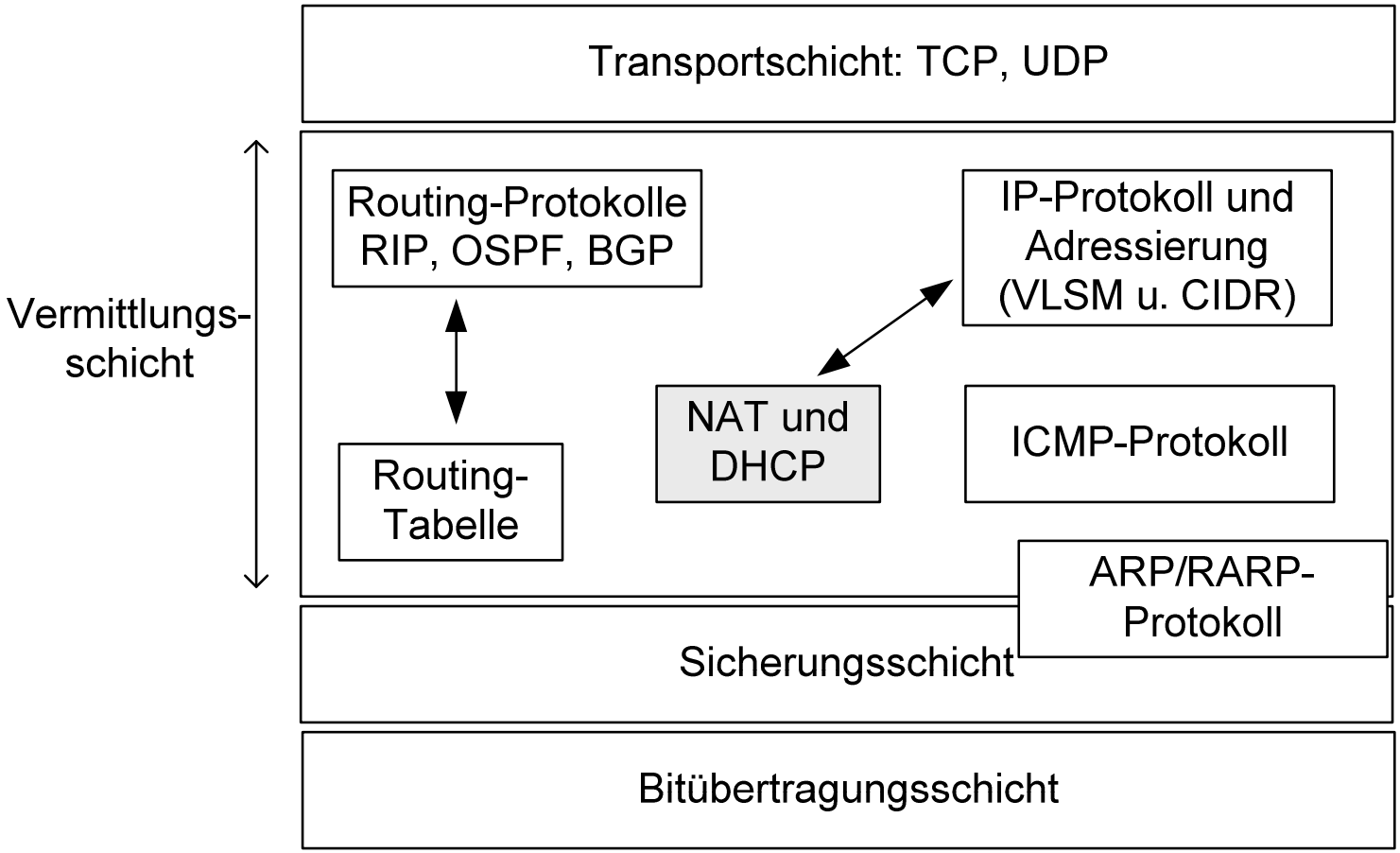
- Typisches Netzbeispiel: Campusnetz (nach Tanenbaum)



Überblick

1. Steuerprotokolle
   - ICMP
   - ARP und RARP
   - **NAT**
   - DHCP
2. IPv6
   - Grundlagen und Adressierung
   - IPv6-PDU
   - Automatismen, Neighbor Discovery

Einordnung
Die Internet-Vermittlungsschicht



Network Address Translation (NAT): Einführung

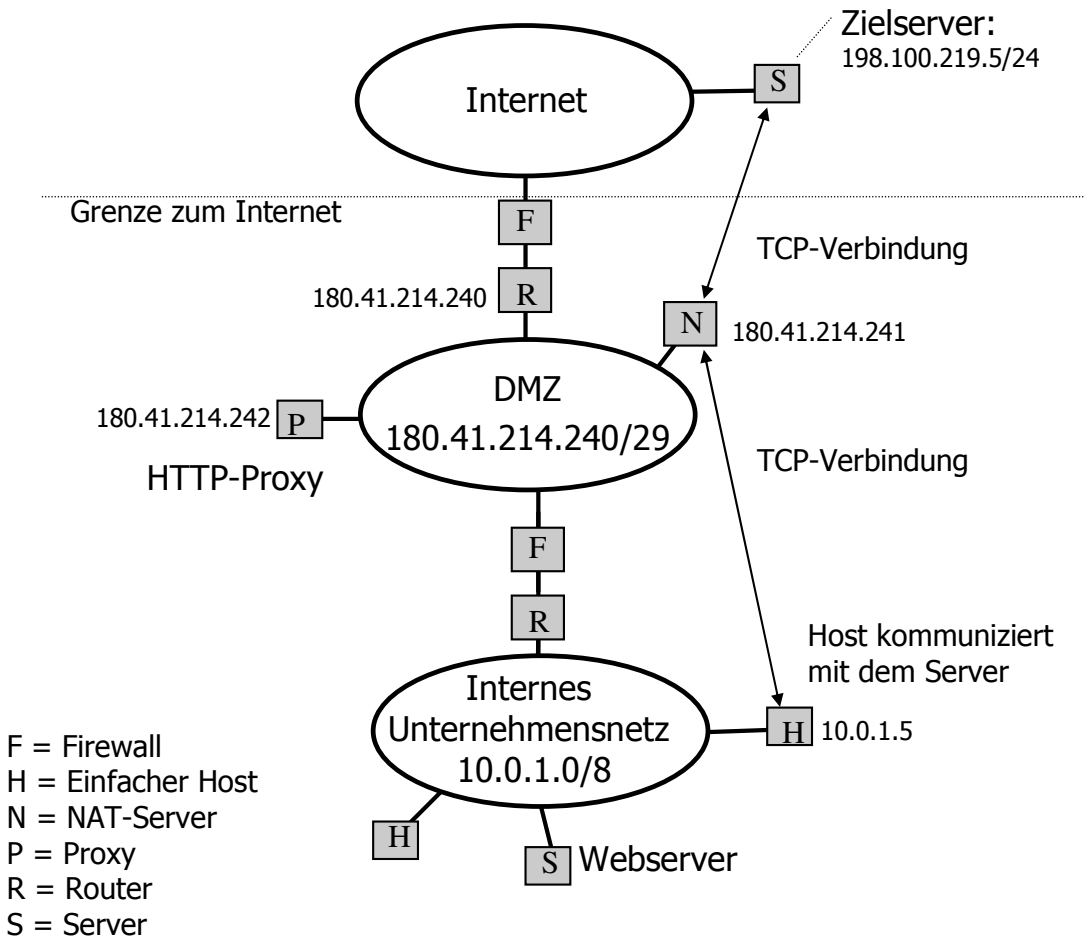
- Bei NAT handelt sich vorwiegend um eine Möglichkeit, die **Sicherheit** im Unternehmensnetz zu erhöhen
- NAT dient auch dazu, Netzwerkadressen einzusparen
- Für ein Netz (Unternehmensnetz) benötigt man **nur noch eine bzw. wenige offizielle IP-Adresse**
- Intern kann dann eine beliebige, nach außen nicht sichtbare, Netzwerknummer verwendet werden

  → Private IP-Adressen!

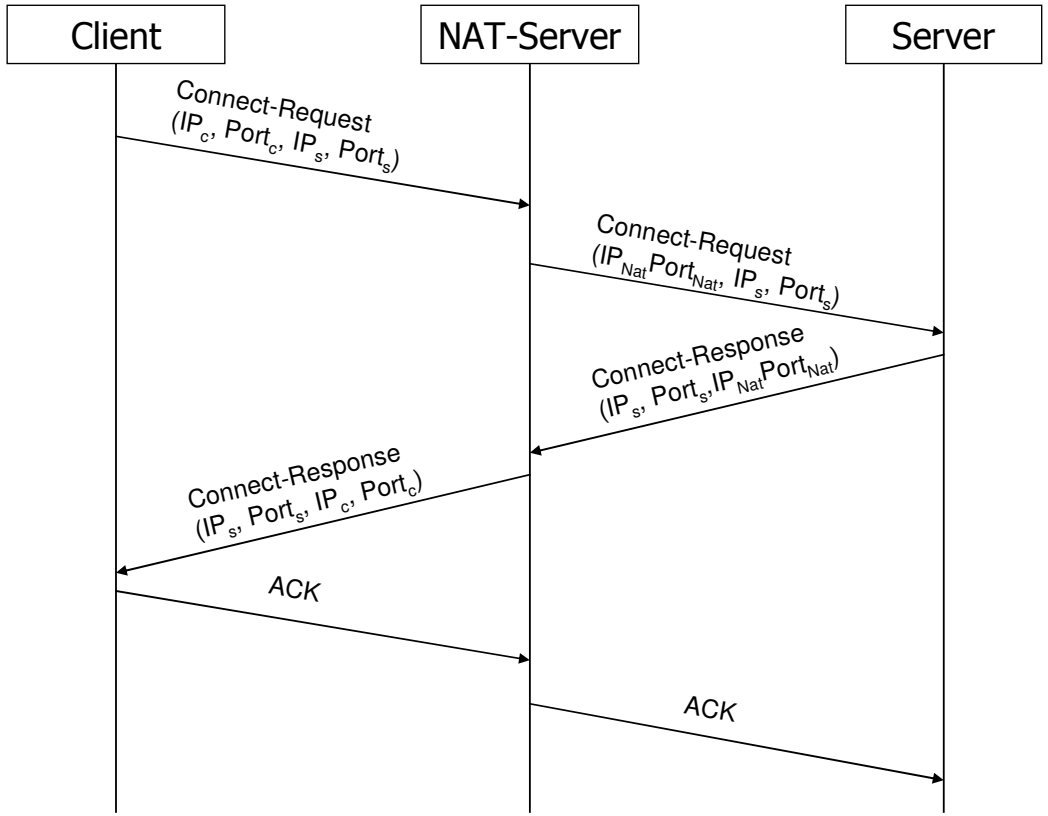
NAT, NAPT

- IP-Router bzw. NAT-Server „**mappen**" bei NAT ankommende Pakete auf interne Hostadressen und umgekehrt
- IP-Router arbeiten nach außen als **Stellvertreter** (Proxies) für alle internen Hosts
- Verschiedene Varianten von NAT verfügbar, auch NAPT = Network Address **Port** Translation

NAT: Beispiel



NAT: Nachrichtenfluss



- Diskussion: End-to-End-Beziehung

Überblick

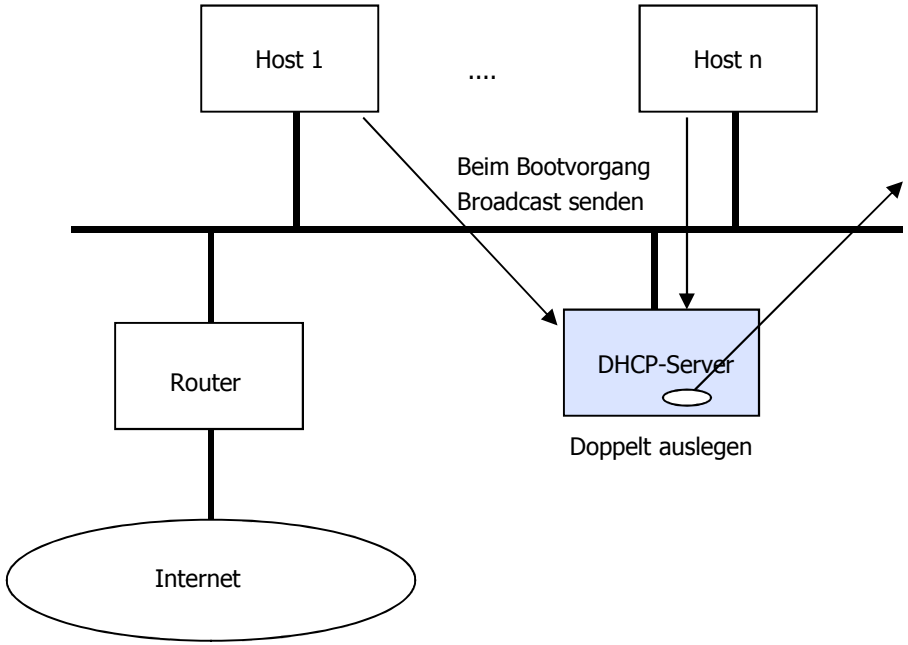
1. Steuerprotokolle
   - ICMP
   - ARP und RARP
   - NAT
   - **DHCP**
2. IPv6
   - Grundlagen und Adressierung
   - IPv6-PDU
   - Automatismen, Neighbor Discovery

DHCP: Einführung

- Manuelle Netzwerkkonfiguration ist schon bei kleinen Netzen ein Problem
- Dynamic Host Configuration Protocol schafft Abhilfe
  - Hosts müssen Adressen nicht mehr kennen, sie werden dynamisch beim Booten besorgt
- Dynamische Vergabe von IP-Adressen und weiteren Netzwerk-Parametern über einen DHCP-Server:
  - Subnetzmaske
  - DNS-Server-Adresse
  - IP-Router-Adresse
  - ...

DHCP: Beispielnetz

- Meist beziehen nur Arbeitsplatzrechner Ihre IP-Adresse vom DHCP-Server



Konfigurationsdatei z.B.: /etc/dhcpd.conf

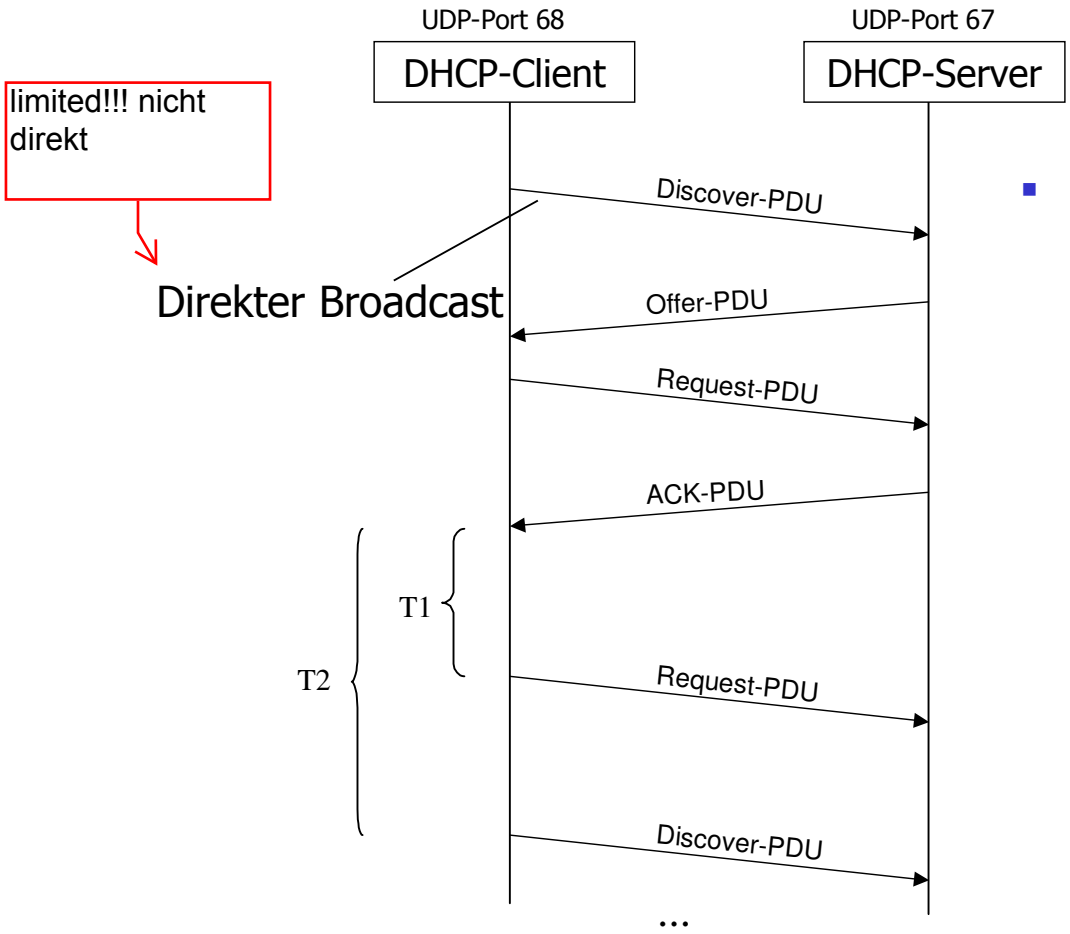
default-lease-time 600; # 10 Minuten
max-lease-time 7200; # 2 Stunden

option **domain-name** “isys.com”;
option **domain-name-servers** 192.168.1.1 192.168.1.2;
option **broadcast-address** 192.168.1.255;
option **routers** 192.168.1.254;
option **subnet-mask** 255.255.255.0;

subnet 192.168.1.0 netmask 255.255.255.0
{
    range 192.168.1.10 192.168.1.20;
    range 192.168.1.100 192.168.1.200;
}

host mandl
    hardware ethernet 00:00:45:12:EE:E4;
    fixed-address 192.168.1.21;

DHCP: Kommunikation beim Bootvorgang



- IP-Ranges (Adressbereiche) oder direkte Zuordnung von IP-Adressen zu Hosts möglich
  → Zuordnung über MAC-Adresse

T1 = Timer für 50 % der Lease-Zeit
T2 = Timer für 87,5 % der Lease-Zeit

DHCP: Leases

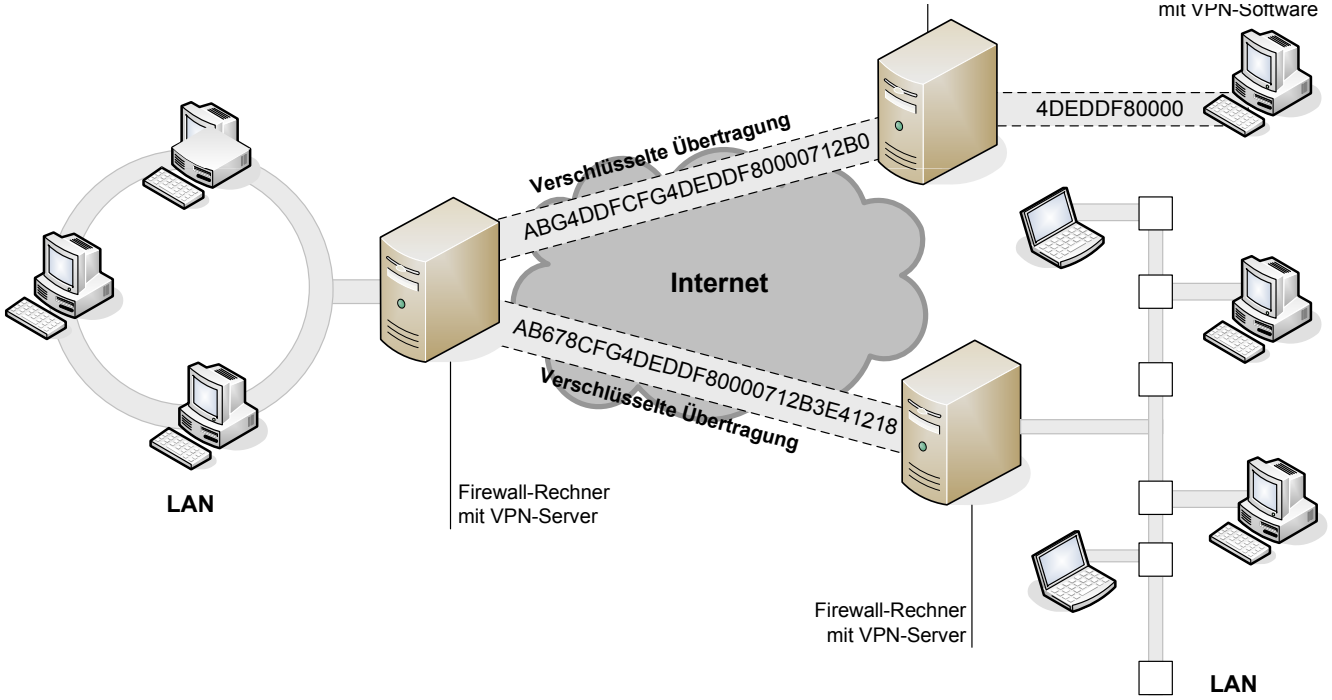
- Lease-Zeit = Nutzungszeit für IP-Adresse
  - Parameter (Timer) werden beim dyn. Konfigurieren an den Client gesendet
  - Parameter T1 gibt standardmäßig 50 % der Lease-Zeit an
    - Client sendet erneut einen DHCP-Request
  - Parameter T2 87,5 % der Lease-Zeit
    - Wenn kein ACK vom Server kommt, dann erneutes DHCP-Discovery durch Client

Ergänzung:
Wichtige Administrations-Kommandos

- Diagnose- und Konfigurationskommandos im TCP/IP-Umfeld, die man öfter mal braucht:
  - ping
  - hostname
  - netstat
  - nslookup (kommt später bei DNS)
  - arp
  - traceroute (Windows: tracert)
  - ifconfig
  - route
  - ipconfig (Windows)
  - nbtstat (Windows)

Ergänzung:
Virtual Private Networks (VPN)

- Sicherheitsprotokolle:
  - IPSec und IKE (Key Exchange Protocol)
  - IPSec-Tunnel



Überblick

1. Steuerprotokolle
   - ICMP
   - ARP und RARP
   - NAT
   - DHCP
2. IPv6
   - **Grundlagen und Adressierung**
   - IPv6-PDU
   - Automatismen, Neighbor Discovery

Grundlegendes

- CIDR reicht nicht für alle Zeit, daher wurde eine neue Version von IP konzipiert (seit 1990)
- Zukunftsszenarien:
  - **Jeder Fernseher ist möglicherweise bald ein Internet-Knoten** (Video-on-Demand)
  - **Millionen von drahtlosen** Systemen im Internet
- Hauptziel von IPv6 (IPnG) ist es, die **Adress-problematik** umfassend und langfristig zu lösen
- Koexistenz mit IPv4 erforderlich und angestrebt

Weitere Ziele

- **Vereinfachung** des Protokolls zur schnelleren Bearbeitung von Paketen in Routern
- Umfang der **Routing-Tabellen reduzieren**
- **Anwendungstypen** wie Multimedia-Anwendungen (Echtzeitanwendungen) unterstützen

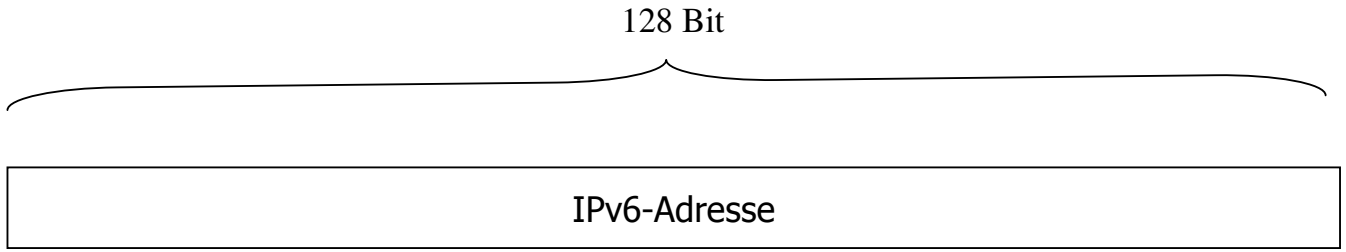
  → Unterstützung von **Flussmarken**
- Höhere **Sicherheit** (Datenschutz, Authentifikation)
- **Multicasting** besser unterstützen
- **Mobile IP-Adressen**: Möglichkeit schaffen, dass Hosts ihr Heimatnetz verlassen können
- Möglichkeiten der **Weiterentwicklung** schaffen

IPv6-Adressen

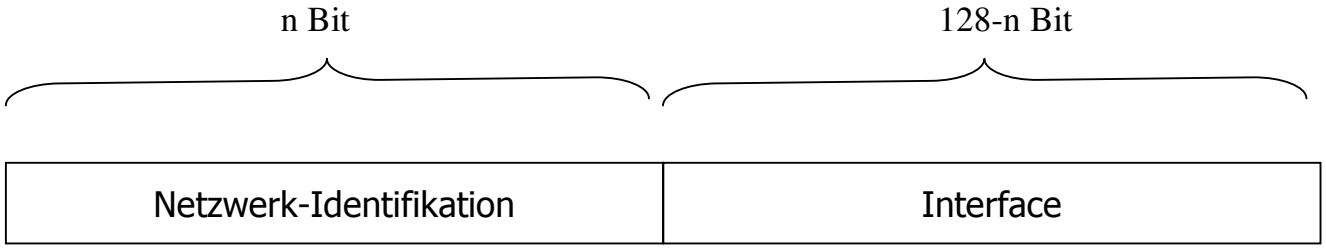
- **16-Byte-Adressen** (128 Bits) mit neuer Notation
- Analogie zur Anzahl der vorhandenen Adressen (2^{128}):
  - Wäre die ganze Welt mit Computern bedeckt, könnte man mit IPv6 **$7*10^{23}$** IP-Adressen pro m^2 ermöglichen
- Verschiedene Klassen von Adressen
  - **Unicast**-Adressen
    - Der traditionelle Adresstyp
    - Adressieren einen Netzanschluss eines Hosts oder Routers
  - **Anycast**-Adressen
    - Adressierung einer Gruppe von Interfaces
    - Aber nur ein Mitglied der Gruppe bekommt das Paket
    - Auswahl übernimmt der zuständige Router
    - Nutzung innerhalb von Teilnetzen, kein Routing außerhalb
  - **Multicast**-Adressen
    - Adressierung einer Gruppe von Interfaces
  - **Keine** Broadcast-Adresse mehr in IPv6!!
- Aufteilung des IPv6-Adressraums in **RFC 4291** geregelt

IPv6-Adressaufbau: Struktur

- Unstrukturierte IPv6-Adresse

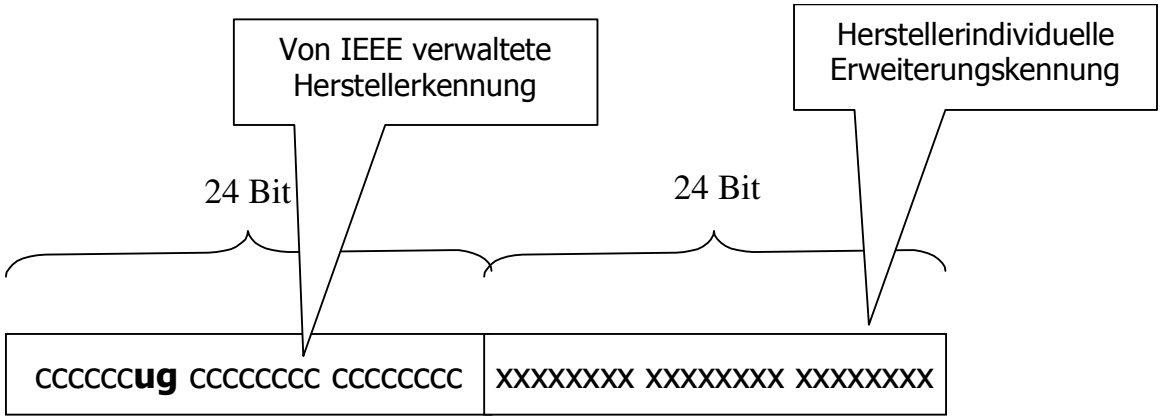


- Strukturierte IPv6-Adresse
  - Netzwerkanteil über CIDR-Notation (x/y) kennzeichnen, ISP erhält /32-Adressen von NIC oder DENIC usw. und gibt meist /64-Adressen weiter



Einschub: IEEE 802.3-Adresse (Schicht 2)

- 48-Bit-MAC-Adresse, als IEEE 802.3-Adresse bezeichnet
  - 24-Bit-Firmenkennung
  - 24-Bit-Erweiterungskennung (Platinenkennung)
  - Wird bei der Herstellung zugewiesen und ist global eindeutig
  - Dies ist die bekannte MAC-Adresse (Media Access Control)



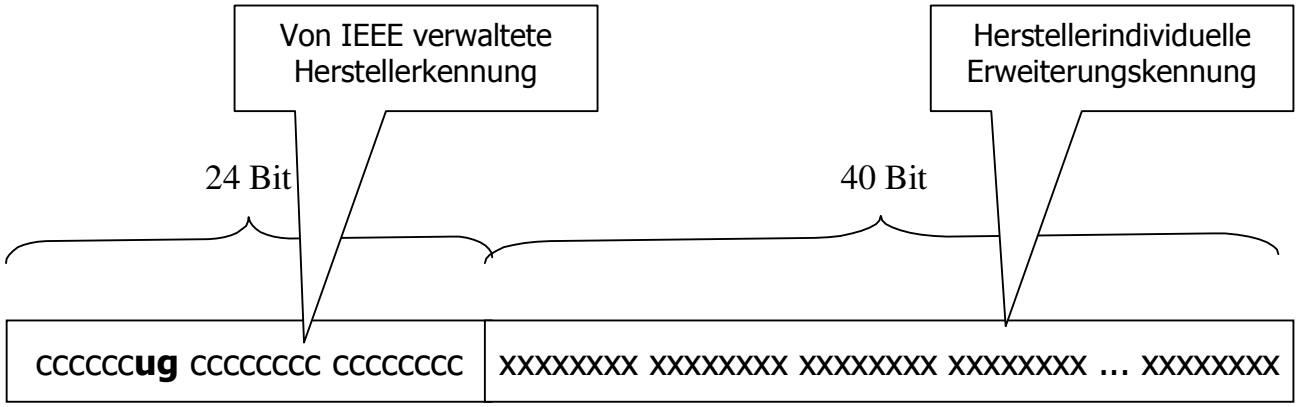
c = Company-Bit
x = Bit vom Interface-Hersteller vergeben
u = universal oder local
g = group oder individual

Einschub: IEEE 802.3-Adresse (Schicht 2)

- U/L (Universal/Local)
  - Das U/L-Bit ist das siebte Bit des ersten Byte und wird zur Bestimmung, ob es sich um eine universell oder eine lokal verwaltete Adresse handelt, verwendet.
    - U/L-Bit = 0 → Adresse von IEEE verwaltet
    - U/L-Bit = 1 → Netzwerkadministrator verwaltet Adresse lokal
- I/G (Individual/Group)
  - Das I/G-Bit ist das Bit mit niedrigster Priorität des ersten Byte
  - Dient zur Festlegung, ob es sich um eine individuelle Adresse (Unicast) oder eine Gruppenadresse (Multicast) ist
    - I/G-Bit = 0 → Unicastadresse
    - I/G-Bit = 1 → Multicastadresse
- Bei einer 802.x-Standard-Netzwerkadapteradresse gilt:
  - U/L-Bit = I/G-Bit = 0 → universell verwaltete MAC-Unicastadresse

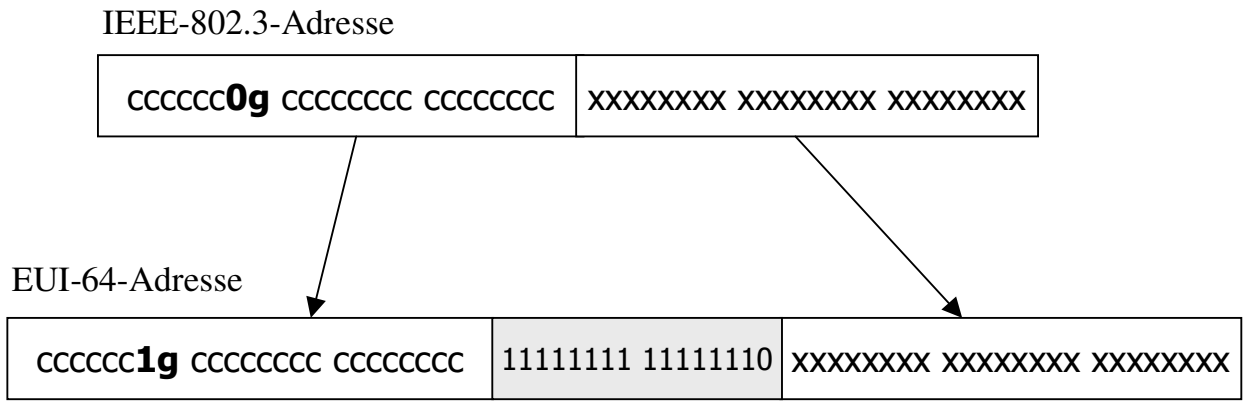
Einschub: EUI-64-Adresse (Schicht 2)

- IEEE EUI-64-Adresse (Extended Unique Identifier) ist ein neuer Standard in der Adressierung von Netzwerkschnittstellen. Zwei Adressteile:
  - Firmenkennung ist 24 Bit lang
  - Erweiterungskennung ist 40 Bit → größerer Adressbereich für Hersteller von Netzwerkadaptern
- Die IEEE EUI-64-Adresse verwendet die U/L- und I/G-Bits auf dieselbe Art wie die IEEE 802.3-Adresse



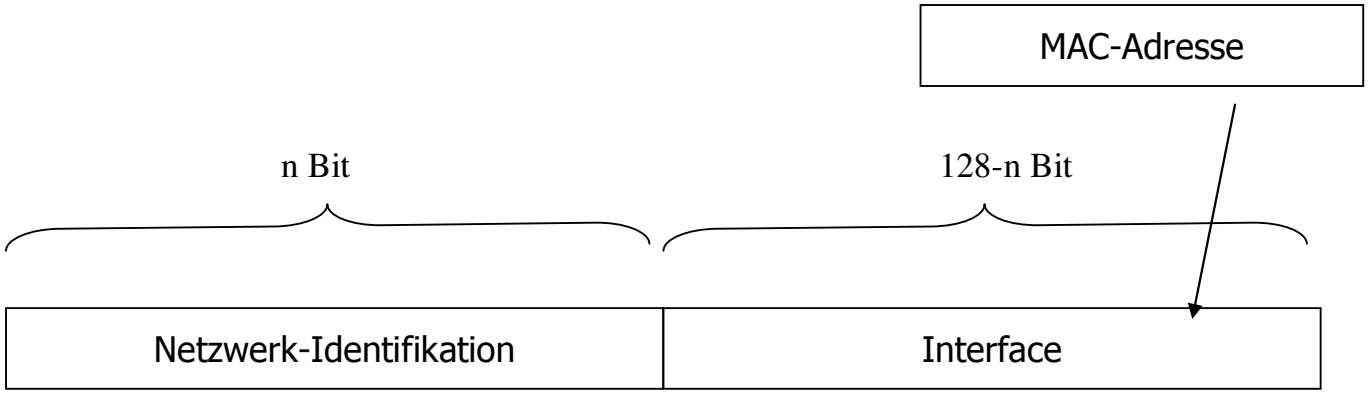
Einschub: Mapping IEEE 802.3-Adresse → EUI-64-Adresse (Schicht 2)

- IEEE EUI-64-Adresse ist länger, also nicht direkt abbildbar
- 16 Bit 0b1111111111111110 = 0xFFFE werden zwischen der Firmenkennung und der Erweiterungskennung in die IEEE 802.3-Adresse eingefügt
- u-Bit wurde für IPv6 wegen einfacherer Schreibweise einer link-lokalen Adresse invertiert :
  - Beispiel: FE80::124 einfacher als FE80::200:0:0:124



IPv6-Adressaufbau: Netzwerk-Id

- MAC-Adresse wird als Interface-Identifikation übernommen
  - →Sicherheitsproblem, konnte man leicht manipulieren
  - →Umfangreiche Diskussionen dazu
  - →Daher RFC 4941 (privacy Extensions), um zufällige Interface Identifier zu erzeugen
- Abbildung IEEE-803.3-Adresse auf IEEE EUI-64-Adresse



IPv6-Adressaufbau und Regeln

- Adressen-Notation mit 8 Gruppen zu je vier Hex-Zahlen abgetrennt durch Doppelpunkte, CIDR-Notation (x/y) auch zulässig

  Beispiel:

  8000:0000:0000:0000:**0**123:5555:89AB:CDEF

- Führende Nullen können in jeder Gruppe weggelassen werden und Gruppen mit lauter Nullen können durch einen Doppelpunkt ersetzt werden, aber „::" nur an einer Stelle möglich:

  8000::123:5555:89AB:CDEF

- IPv4-Adressen können mit speziellen Unicast-Adressen (Präfix ::FFFF/96) abgebildet werden (Mapping-Adressen)

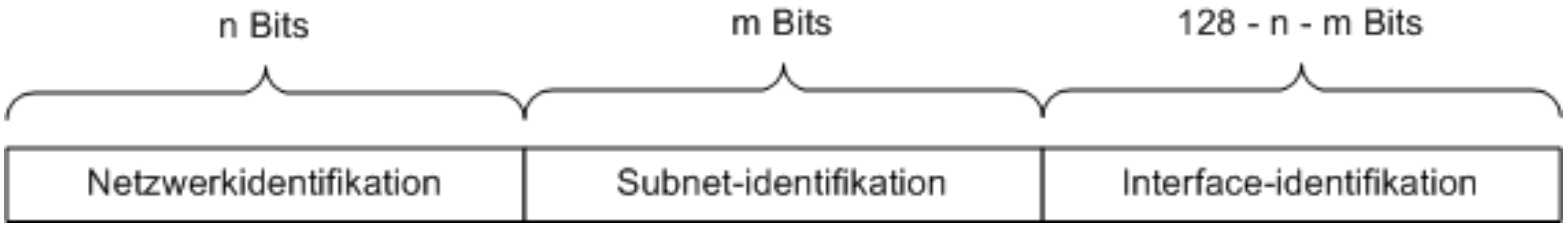
Beispiel: 192.168.0.1 ➔ ::FFFF:C0A8:1

Besondere IPv6-Adressen, Sonderformen

- ::0 entspricht 0.0.0.0 in IPv4 (undefinierte Adresse)
  - Synonym: 0:0:0:0:0:0:0:0 oder ::/128
- ::1 entspricht der Loopback-Adresse 127.0.0.1 in IPv4
  - Synonym: 0:0:0:0:0:0:0:1 oder ::1/128
- FF00::/8 weist auf eine Multicast-Adresse hin
- FE80::/10 weist auf eine Link-Lokal-Adresse hin

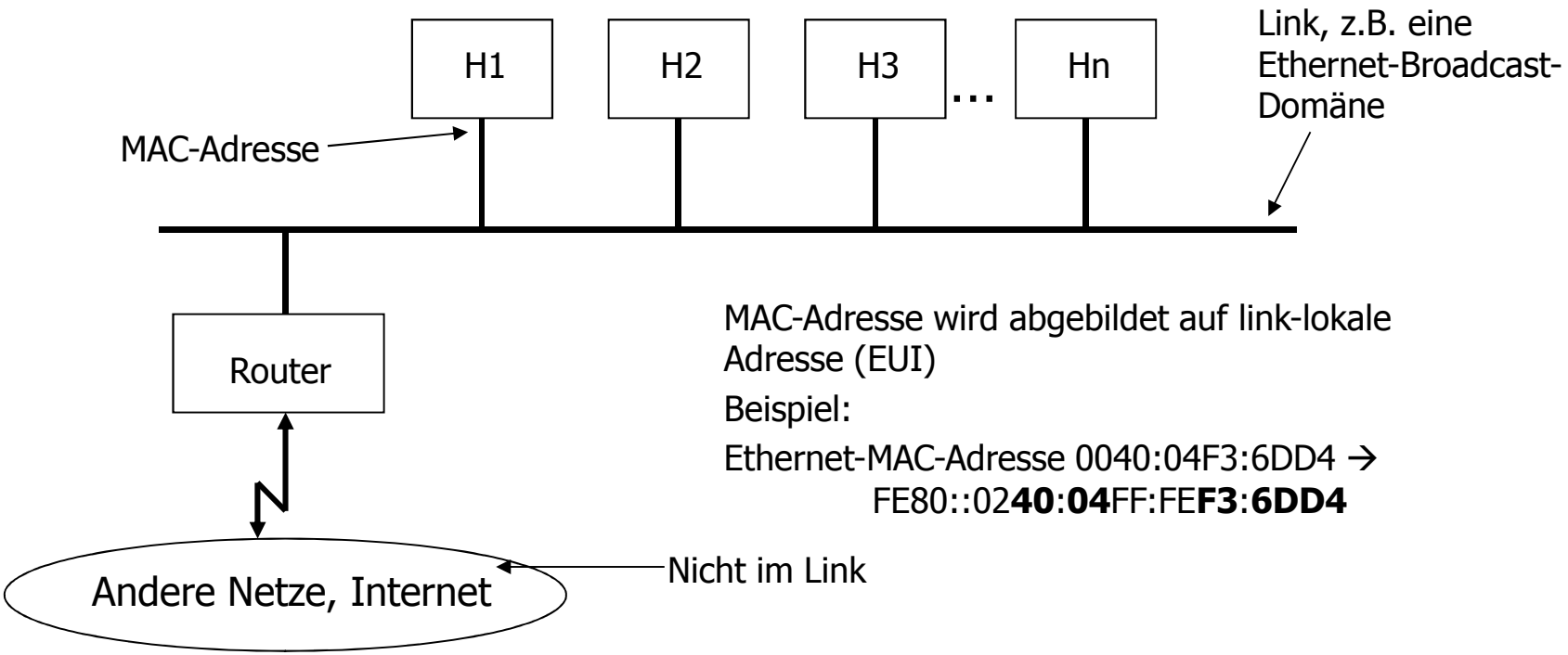
Globale Unicast-Adressen: Aufbau, Struktur

- Dienen dazu, einen Host (Knoten) im Internet **global** eindeutig zu identifizieren → **öffentliche** Adressen (wie Klasse A, B, C aus IPv4)!
- Hierarchiebildung möglich → Provider-/Netzbetreiberzuordnung
- Adresspräfix binär: 001 -> Hex: 20 .. 3F
- Eine Unicast-Adresse hat z.B. folgenden Aufbau:



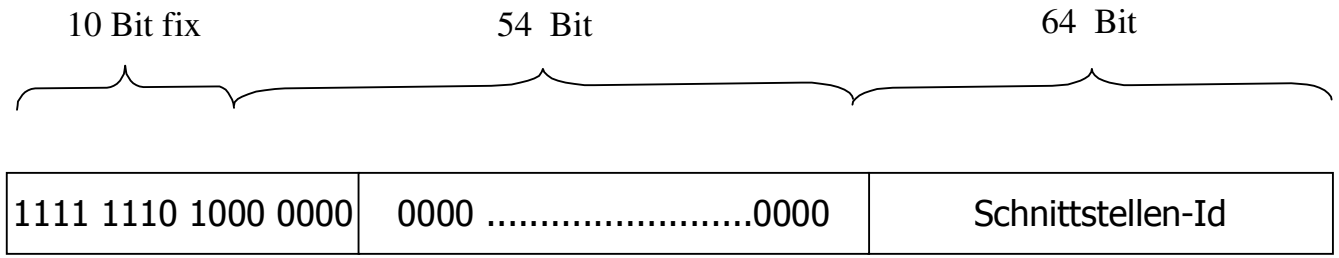
Verbindungslokale Adressbereiche (link-lokal)

- Link-Lokal bezieht sich auf das lokale Netz
- Ausbreitung nur in einem Teilnetz (Subnetz)
- Präfix der Adressen: 1111 1110 10 → FE80::/10 – FEBF::/10



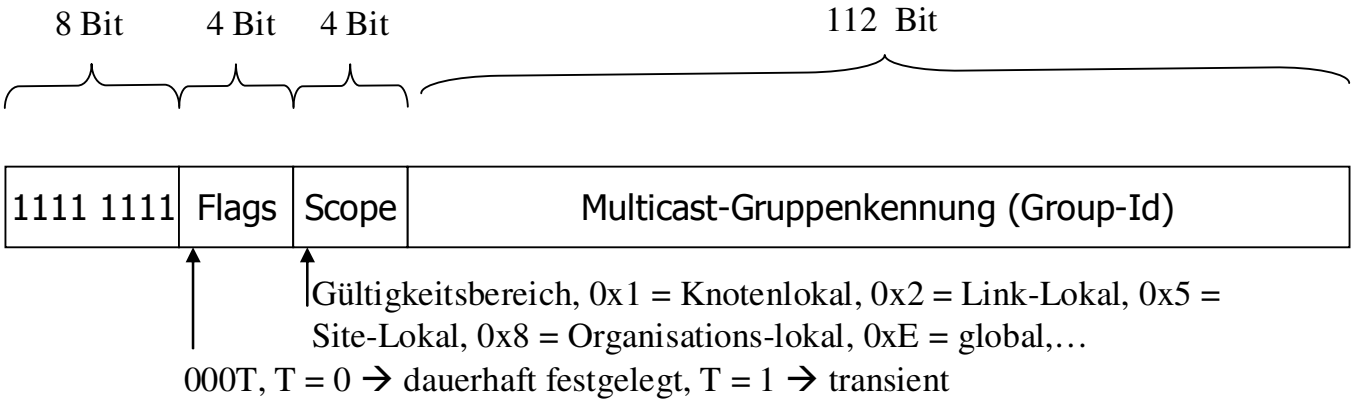
Besondere IPv6-Adressen, Link-lokale Adresse

- **Aufbau einer link-lokalen Adresse**



Besondere IPv6-Adressen, Sonderformen

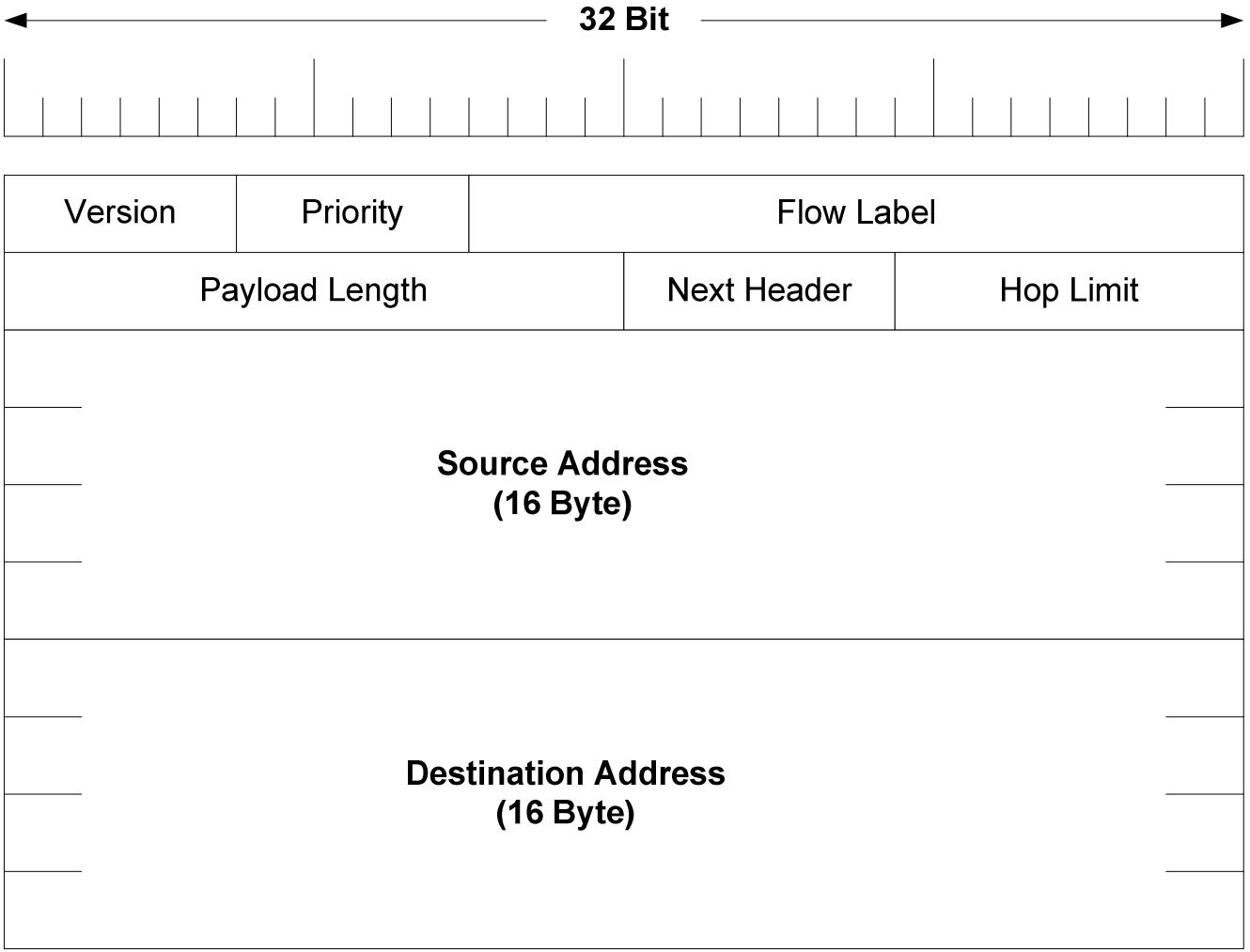
- **Multicast-Adressen**
  - Multicast-Adressen beginnen mit 0xFF
  - Knotenlokale Adresse **FF01**:... → knotenlokal, Nachricht verlässt Knoten nicht
  - Für das gleiche Link-Segment **FF02**:... → Nachricht verlässt Knoten, bleibt aber im Subnetz
  - **FF0E**: Entspricht der IPv4-Broadcast-Adresse (limited)
  - ...



Überblick

1. Steuerprotokolle
   - ICMP
   - ARP und RARP
   - NAT
   - DHCP
2. IPv6
   - Grundlagen und Adressierung
   - **IPv6-PDU**
   - Automatismen, Neighbor Discovery

IPv6-Header

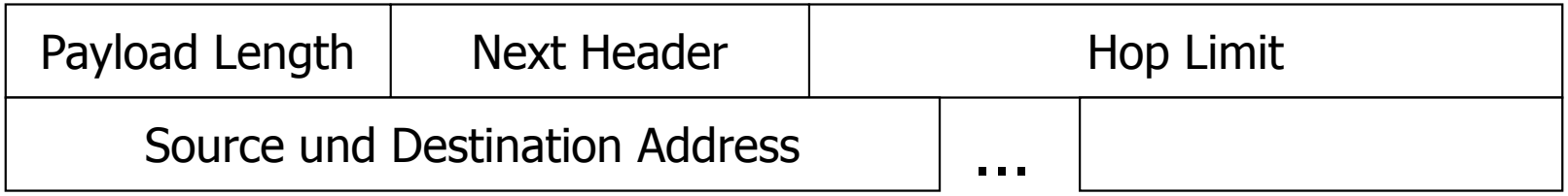

32 Bit
Version
Priority
Flow Label
Payload Length
Next Header
Hop Limit
Source Address
(16 Byte)
Destination Address
(16 Byte)

IPv6-Header

Version	Priorität	Flow Label (Flussmarke)

- **Version** Versionsnummer des Internet-Protokolls (6)
- **Priorität**: auch **Traffic Class** / **DS** = Differenciated Service Field (neu) mit neuen Werten (RFC 2474, 2478)
  - Information für Router, interessant bei Überlastsituationen
    - stoßartiger Verkehr (ftp, NFS) → hoher Durchsatz
    - interaktiver Verkehr (telnet) → geringe Verzögerung
    - Verkehrsarten ohne Staukontrolle (z.B. für Videoanwendungen)
- **Flussmarke**: Identifikation des Flusses, falls ungleich 0
  - Zweck: Zusammengehörige Datenflüsse (Video/Audio) auf Netzebene speziell behandeln
  - Quelladresse+Zieladresse+Flussmarke kennzeichnen einen Fluss
  - Flussmarken werden im Quellknoten in die IPv6-PDU eingetragen

IPv6-Header



- **Payload Length:** Nutzdatenlänge **ohne** die 40 Bytes des IPv6-Headers, es gibt aber auch Jumbo-Pakete
- **Next Header**: Verweis auf ersten Erweiterungs-Header
  - Letzter Header verweist auf Protokolltyp der nächst höheren Schicht (siehe IPv4-Feld **Protokoll**)
- **Hop Limit**: Verbleibende Lebenszeit des Pakets in Hops
  - Jeder Router zählt Hop Limit um 1 herunter
  - Entspricht dem TTL-Feld in IPv4
  - Name entspricht jetzt der eigentlichen Nutzung im Internet
- **Source und Destination Adresse**: IPv6-Adressen der Quelle und des Ziels

IPv6-Header, Erweiterungs-Header

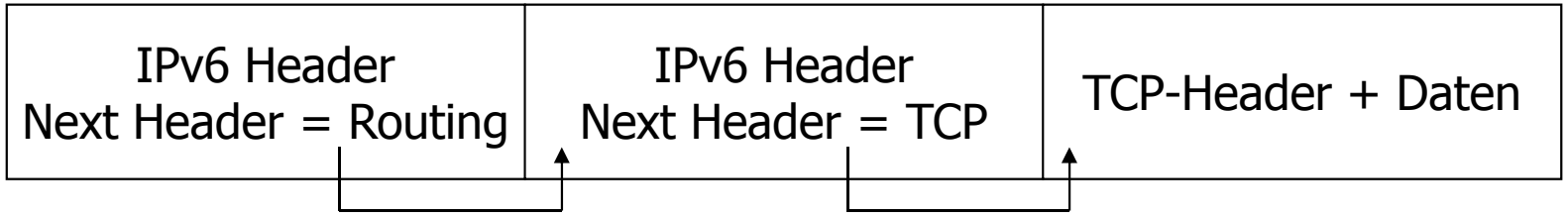
- Kodierung im Next-Header-Feld
  - EGP = 0x08
  - Routing = 0x2B
  - Fragment = 0x44
  - TCP = 0x06 …

Erweiterungs-Header	Beschreibung
Optionen für Teilstrecken (Hop-by-Hop)	Verschiedene Informationen für Router
Routing	Definition einer vollen oder teilweisen Route
Fragmentierung	Verwaltung von Datengrammfragmenten
Authentifikation	Echtheitsüberprüfung des Senders
Verschlüsselte Sicherheitsdaten	Informationen über den verschlüsselten Inhalt
Optionen für Ziele	Zusätzliche Informationen für das Ziel

IPv6-Header, Erweiterungs-Header

- Header und Erweiterungs-Header sind miteinander **verkettet,** jeder Typ **max. einmal**
- Die Erweiterungen werden **nicht** in den Routern bearbeitet, nur in den Endsystemen
- Eine **Ausnahme**: Routing-Erweiterungs-Header
- Reihenfolge der Header ist festgelegt

- Beispiel eines IPv6-Headers mit einem Erweiterungs-Header und einer anschließenden TCP-PDU



IPv6-Header, Erweiterungs-Header

- Der **Routing-Header** dient der Quelle zur Festlegung des Weges bis zum Ziel

Next Header	Header Ext. Länge	Routing Typ	Verbl. Segmente
1-24 Adressen			

...

- **Next Header**: siehe vorne
- **Header Ext. Länge:** Länge des Routing-Headers
- **Routing Typ:** Gibt den Typ der Routing-Headers an
- **Verbleibende Segmente:** Anzahl der folgenden Adressen, die besucht werden müssen

IPv6-Header, Erweiterungs-Header

- Der **Fragmentierungs-Header** wird verwendet, um größere Dateneinheiten zu senden, als zugelassen
  - PDU-Länge > MTU des Pfades (MTU = Maximum Transmission Unit)
  - Minimum auch in IPv6 576 Bytes
- Fragmentierung erfolgt bei IPv6 nur im Quellknoten, Router fragmentieren nicht → geringe Routerbelastung

Next Header	reserviert	Fragment Offset	00M
Identifikation			

- **Fragment Offset:** Position der Nutzdaten relativ zum Beginn der PDU (Ursprungs-Dateneinheit) → 13 Bit (wie IPv4)
- **Identifikation:** Id der PDU (wie IPv4)
- **M:** More-Flag, M=1 → weitere Fragmente folgen (wie IPv4)

IPv6, Sicherheitsaspekte

- Im Gegensatz zu IPv4 sind in IPv6 schon Sicherheitsmechanismen im Protokoll spezifiziert (siehe IPv4+**IPsec**)
  - Authentifizierung
  - Verschlüsselung
- **MD5-Algorithmus** (Message Digest) kann zur Authentifizierung der Partner verwendet werden
- Verschlüsselung des Nutzdatenteils wird mit einer Variante des **DES- oder AES-Verschlüsselungsalgorithmus** unterstützt
  - DES = Data Encryption Standard
  - AES = Advanced Encryption Standard
  - Symmetrisches Verschlüsselungsverfahren

IPv6, Flussmarken

- Ziel: Aufbau von **Pseudoverbindungen** zwischen Quelle und Ziel mit QS-Merkmalen wie Verzögerung und Bandbreite
  - Ressourcenreservierung
  - Datenströme für Echtzeitanwendungen
- Flexibilität von Datagramm-Netzen kombiniert mit virtuellen Verbindungen
- Ein „Fluss" wird durch Quell- und Zieladresse sowie einer Flussnummer identifiziert
- Router führen eine Sonderbehandlung durch
- Noch in der Experimentierphase!

Überblick

1. Steuerprotokolle
   - ICMP
   - ARP und RARP
   - NAT
   - DHCP
2. IPv6
   - Grundlagen und Adressierung
   - IPv6-PDU
   - **Automatismen, Neighbor Discovery**

Autokonfiguration: Einige wichtige Features

- **Selbstkonfiguration:** Host konfiguriert seine eigene Adresse dynamisch (kein ARP mehr notwendig):
  - Die **dynamische Adress-Auflösung** für Layer-2-Adressen wie es heute im **ARP-Protokoll** abgewickelt wird
- **Router Discovery:** Das Auffinden von Routern im gleichen Link (Subnetz)
- **Parameter Discovery:** Die dynamische Zuordnung von Konfigurationsparametern wie der maximalen MTU und dem Hop-Limit an IPv6-Endsysteme
- Die automatische **IP-Adress-Konfiguration** für Interfaces zur Laufzeit
- Die Suche nach dem optimalen MTU zwischen Sender und Empfänger (**Path MTU Discovery**)

Einige wichtige Features
Beispiel: Router-Discovery

- Wenn ein Endsystem seinen nächsten Router sucht, sendet es eine ***Router-Solicitation*-Nachricht** über Multicast an die Adresse **FF02::2**
- Router antworten mit einer ***Router-Advertisement*-Nachricht**
- Damit unterstützt das ND-Protokoll das Auffinden des verantwortlichen Routers zur Laufzeit → DHCP kann auch wegfallen
- Mehrere Router können aktiv sein
- Das ND-Protokoll nutzt zur Abwicklung seiner Aufgaben einige ICMPv6-Nachrichten

Einige wichtige Features
Beispiel: Parameter-Discovery

- Netzwerkparameter werden vom Host zum Startzeitpunkt auch über ***Router-Solicitation*-Nachricht** besorgt (DHCP-Aufgaben)
- Nachricht geht an Multicast-Adresse **FF02::2**
- Ein Router antwortet mit einer ***Router-Advertisement*-Nachricht** an die Link-Adresse des Endsystems
- Folgende Parameter kann eine *Router-Advertisement*-Nachricht u.a. übertragen:
  - *Max-Hop-Limit*: Dies ist der Wert „Hop-Limit" der in die IPv6-PDUs eingetragen wird
  - *Retransmission-Timer*: Zeit in Millisekunden, die seit dem Absenden der *Solicitation*-Nachricht ablaufen darf, bevor wiederholt wird
  - *...*
  - Über ein *Optionsfeld* wird z.B. vom Router auch die *MTU-Size* übermittelt

Rückblick und Weiterführendes

1. Steuerprotokolle
   - ICMP
   - ARP und RARP
   - NAT
   - DHCP
2. IPv6
   - Grundlagen und Adressierung
   - IPv6-PDU
   - Automatismen, Neighbor Discovery

Was ist noch interessant:

- RSVP, IGMP, ...
- Mobiles Routing
- Sicherheit: IPsec-Protokolle und VPNs,...
- Migration IPv4 → IPv6, ...