Systeme II

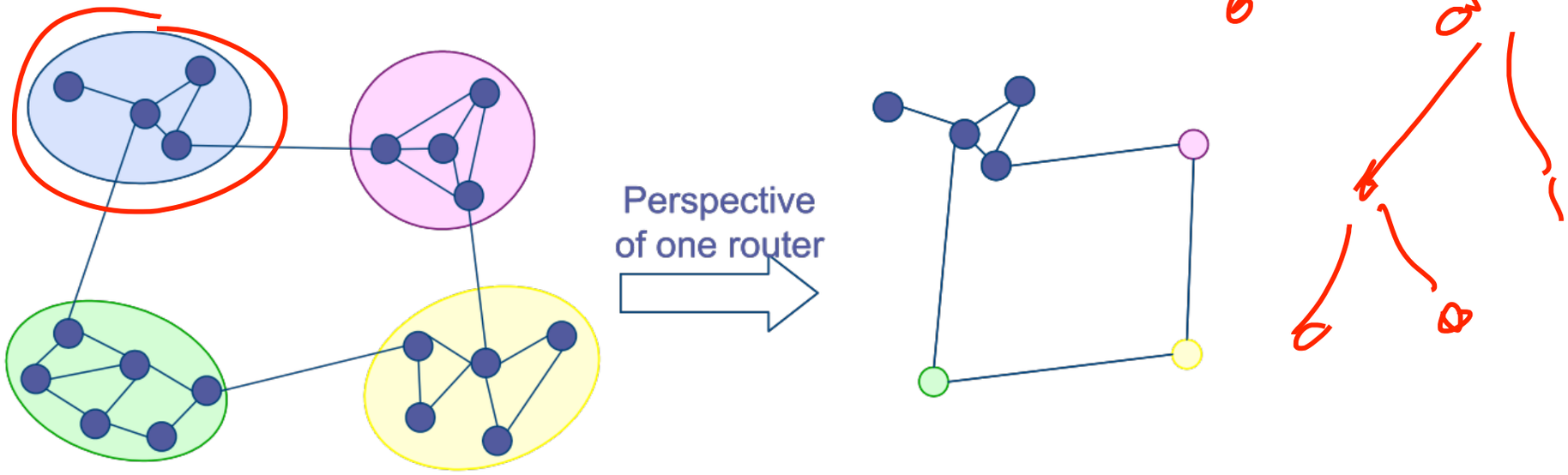
4. Die Vermittlungsschicht

Christian Schindelhauer
Technische Fakultät
Rechnernetze und Telematik
Albert-Ludwigs-Universität Freiburg

Version 07.06.2016

Adressierung und Hierarchisches Routing

- Flache (MAC-) Adressen haben keine Strukturinformation



- Hierarchische Adressen
  - Routing wird vereinfacht wenn Adressen hierarchische Routing-Struktur abbilden
  - Group-ID_n:Group-ID_{n-1}:…:Group-ID_1:Device-ID

CoNe Freiburg

IP-Adressen und Domain Name System

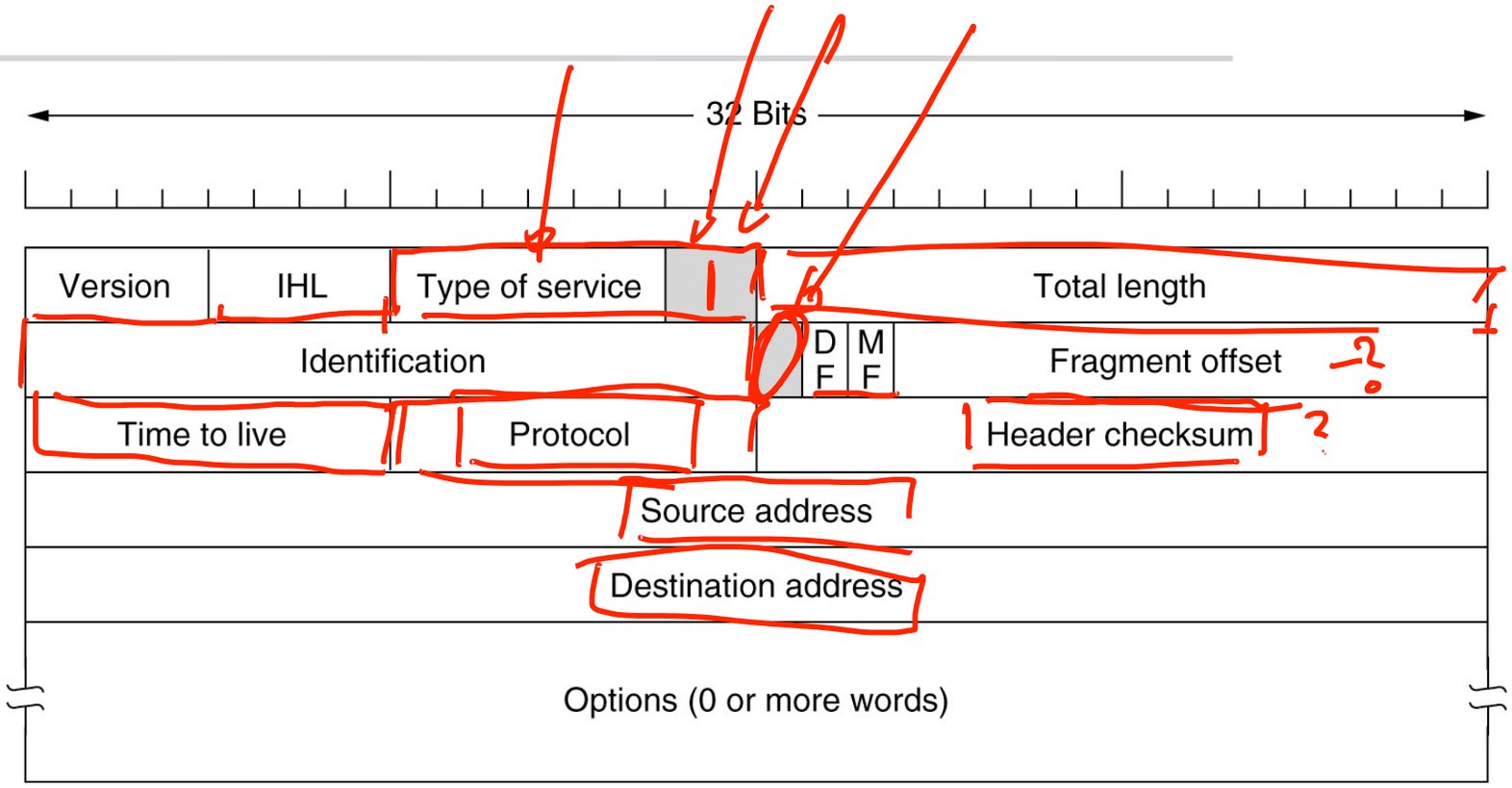
$4 \cdot 1024 \cdot 1024 \cdot 1024$

$2^{32} = 2^2 \cdot 2^{10} \cdot 2^{10} \cdot 2^{10}$

- IP-Adressen
  - Jedes Interface in einem Netzwerk hat weltweit eindeutige IP-Adresse
  - 32 Bits unterteilt in Net-ID und Host-ID
  - Net-ID vergeben durch Internet Network Information Center
  - Host-ID durch lokale Netzwerkadministration
- Domain Name System (DNS)
  - Ersetzt IP-Adressen wie z.B. 132.230.105.133durch Namen wie z.B. falcon.informatik.uni-freiburg.de und umgekehrt
  - Verteilte robuste Datenbank

IPv4-Header (RFC 791)

- Version: 4 = IPv4
- IHL: IP Headerlänge
  - in 32 Bit-Wörtern (>5)
- Type of Service
  - Optimiere delay, throughput, reliability, monetary cost



- Checksum (nur für IP-Header)
- Source and destination IP-address
- Protocol, identifiziert passendes Protokoll
  - Z.B. TCP, UDP, ICMP, IGMP .....
- Time to Live:
  - maximale Anzahl Hops

→ IPv6 hop count

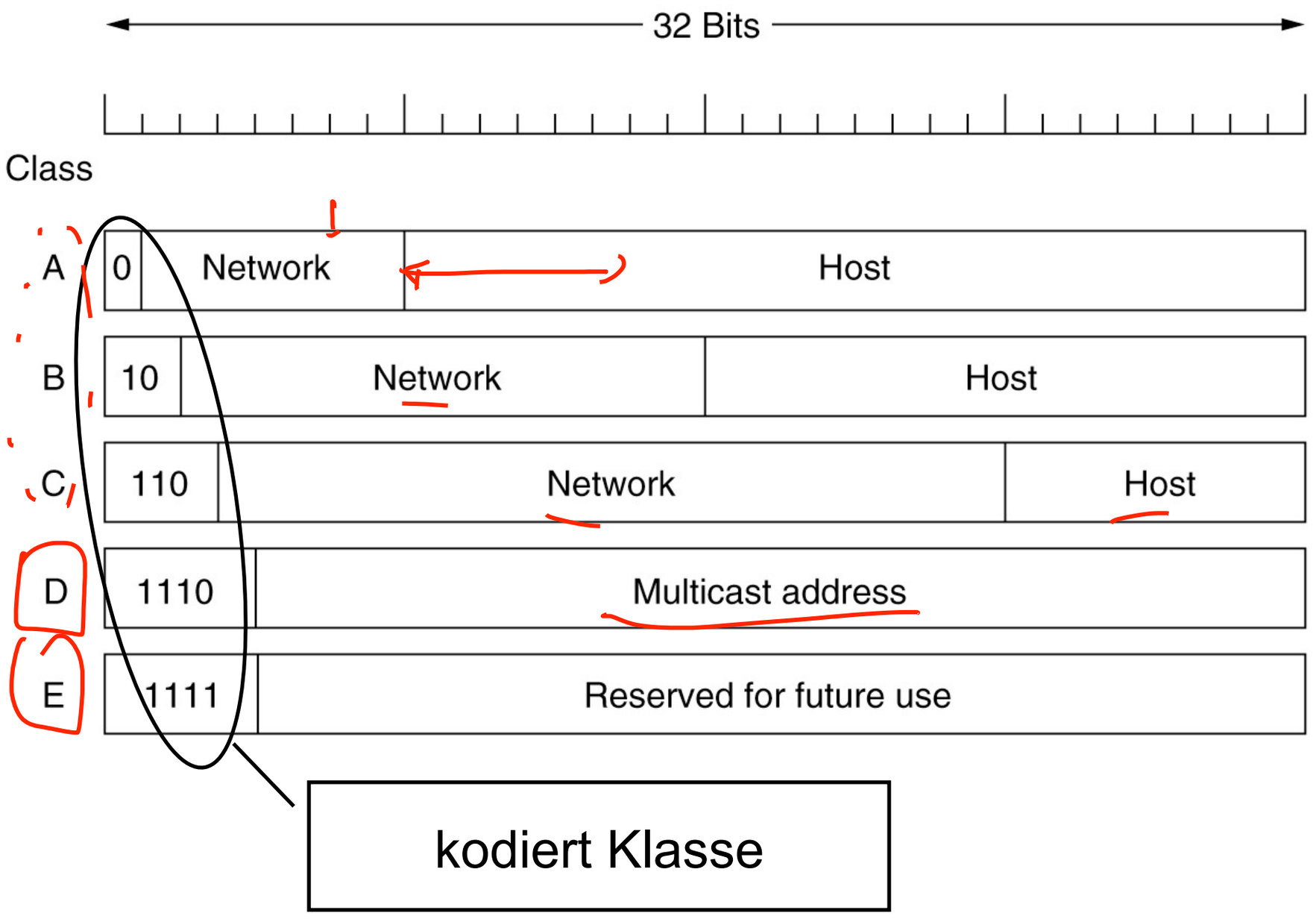
CoNe Freiburg

Internet IP Adressen bis 1993

- IP-Adressen unterscheiden zwei Hierarchien
  - Netzwerk-Interfaces
  - Netzwerke
    - Verschiedene Netzwerkgrößen
    - Netzwerkklassen:
      - Groß - mittel - klein (Klasse A, B, and C)
- Eine IP-Adresse hat 32 Bits
  - Erster Teil: Netzwerkadresse
  - Zweiter Teil: Interface

IP-Klassen bis 1993

- Klassen A, B, and C
- D für multicast; E: “reserved”



128 NWs; 16 M hosts

16K NWs; 64K hosts

2M NWs; 256 hosts

IPv4-Adressen

- Bis 1993 (heutzutage veraltet)
  - 5 Klassen gekennzeichnet durch Präfix
  - Dann Subnetzpräfix fester Länge und Host-ID (Geräteteil)
- Seit 1993
  - Classless Inter-Domain-Routing (CIDR)
  - Die Netzwerk-Adresse und die Host-ID (Geräteteil) werden variabel durch die Netzwerkmaske aufgeteilt.
    - Z.B.:
      - Die Netzwerkmaske 11111111.11111111.11111111.00000000
      - Besagt, dass die IP-Adresse
        - 10000100. 11100110. 10010110. 11110011
        - Aus dem Netzwerk 10000100. 11100110. 10010110
        - den Host 11110011 bezeichnet
- Route aggregation
  - Die Routing-Protokolle BGP, RIP v2 und OSPF können verschiedene Netzwerke unter einer ID anbieten
    - Z.B. alle Netzwerke mit Präfix 10010101010* werden über Host X erreicht

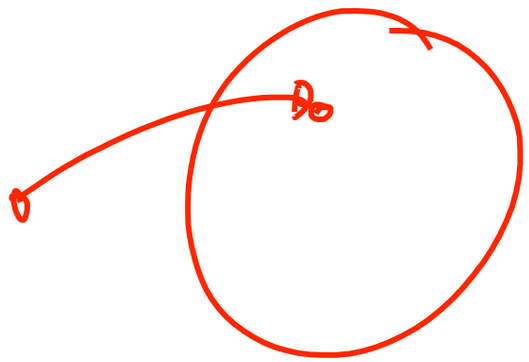
Umwandlung in MAC-Adressen: ARP

- Address Resolution Protocol (ARP)
- Umwandlung: IP-Adresse in MAC-Adresse
  - Broadcast im LAN, um nach Rechner mit passender IP-Adresse zu fragen
  - Knoten antwortet mit MAC-Adresse
  - Router kann dann das Paket dorthin ausliefern
- IPv6:
  - Funktionalität durch Neighbor Discovery Protocol (NDP)
  - Informationen werden per ICMPv6 ausgetauscht

CoNe Freiburg

IPv6

- Wozu IPv6?
- Freie IPv4-Adressen sind seit 31.01.2011 nicht mehr vorhanden
  - Zwar gibt es 4 Milliarden in IPv4 (32 Bit)
  - Diese sind aber statisch organisiert in Netzwerk- und Host-ID
    - Adressen für Funktelefone, Kühlschränke, Autos, Tastaturen, etc...
- Autokonfiguration
  - DHCP, Mobile IP, Umnummerierung
- Neue Dienste
  - Sicherheit (IPSec)
  - Qualitätssicherung (QoS)
  - Multicast
  - Anycast
- Vereinfachungen für Router
  - keine IP-Prüfsummen
  - Keine Partitionierung von IP-Paketen



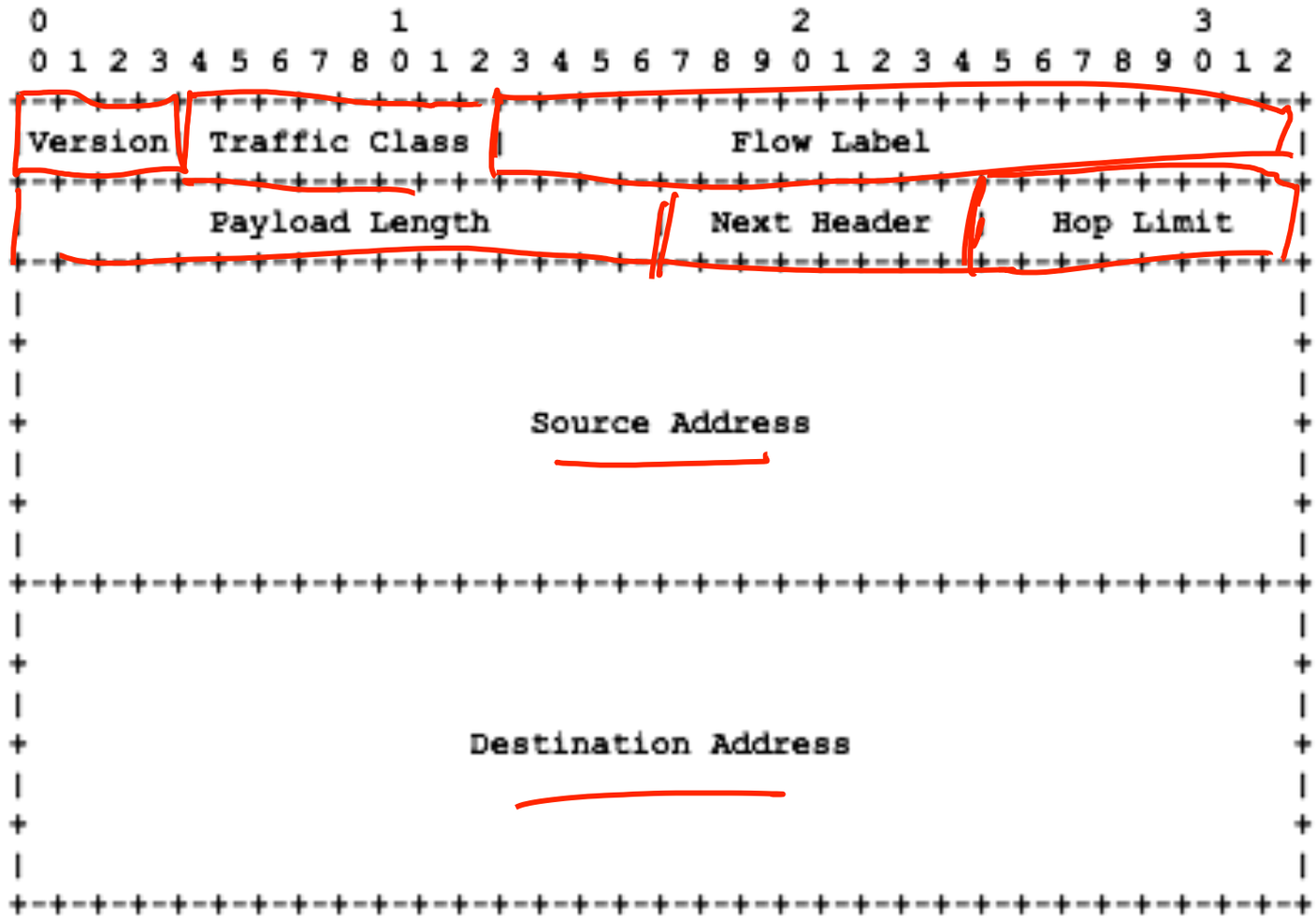
CoNe Freiburg

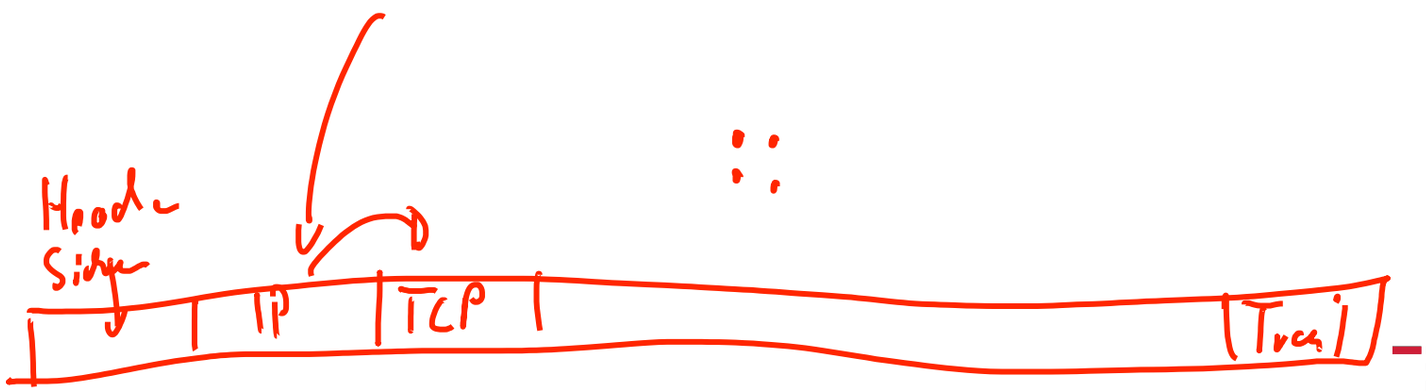
Lösung der Adressenknappheit: DHCP

- DHCP (Dynamic Host Configuration Protocol)
  - Manuelle Zuordnung (Bindung an die MAC-Adresse, z.B. für Server)
  - Automatische Zuordnung (feste Zuordnung, nicht voreingestellt)
  - Dynamische Zuordnung (Neuvergabe möglich)
- Einbindung neuer Rechner ohne Konfiguration
  - Rechner „holt“ sich die IP-Adresse von einem DHCP-Server
  - Dieser weist dem Rechner die IP-Adressen dynamisch zu
  - Nachdem der Rechner das Netzwerk verlässt, kann die IP-Adresse wieder vergeben werden
  - Bei dynamischer Zuordnung, müssen IP-Adressen auch „aufgefrischt“ werden
  - Versucht ein Rechner eine alte IP-Adresse zu verwenden,
    - die abgelaufen ist oder
    - schon neu vergeben ist
  - Dann werden entsprechende Anfragen zurückgewiesen
  - Problem: Stehlen von IP-Adressen

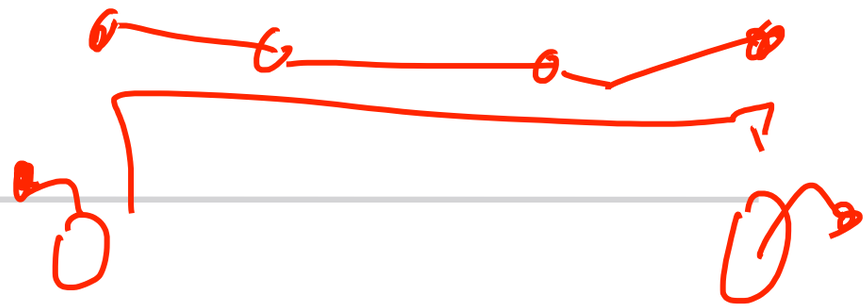
IPv6-Header (RFC 2460)

- Version: 6 = IPv6
- Traffic Class
  - Für QoS (Prioritätsvergabe)
- Flow Label
  - Für QoS oder Echtzeitanwendungen
- Payload Length
  - Größe des Rests des IP-Pakets (Datagramms)
- Next Header (wie bei IPv4: protocol)
  - Z.B. ICMP, IGMP, TCP, EGP, UDP, Multiplexing, ...
- Hop Limit (Time to Live)
  - maximale Anzahl Hops
- Source Address
- Destination Address
  - 128 Bit IPv6-Adresse





IPsec (RFC 2401)



- Schutz vor Replay-Attacken
- IKE (Internet Key Exchange) Protokoll
  - Vereinbarung einer Security Association
    - Identifikation, Festlegung von Schlüsseln, Netzwerke, Erneuerungszeiträume für Authentifizierung und IPsec Schlüssel
  - Erzeugung einer SA im Schnellmodus (nach Etablierung)
- Encapsulating Security Payload (ESP)
  - IP-Kopf unverschlüsselt, Nutzdaten verschlüsselt, mit Authentifizierung
- IPsec im Transportmodus (für direkte Verbindungen)
  - IPsec Header zwischen IP-Header und Nutzdaten
  - Überprüfung in den IP-Routern (dort muss IPsec vorhanden sein)
- IPsec im Tunnelmodus (falls mindestens ein Router dazwischen ist)
  - Das komplette IP-Paket wird verschlüsselt und mit dem IPsec-Header in einen neuen IP-Header verpackt
  - Nur an den Enden muss IPsec vorhanden sein.
- IPsec ist Bestandteil von IPv6
- Rückportierung nach IPv4