IP - Header

Netzwerkgrundlagen (NWG2)

Markus Zeilinger[1]

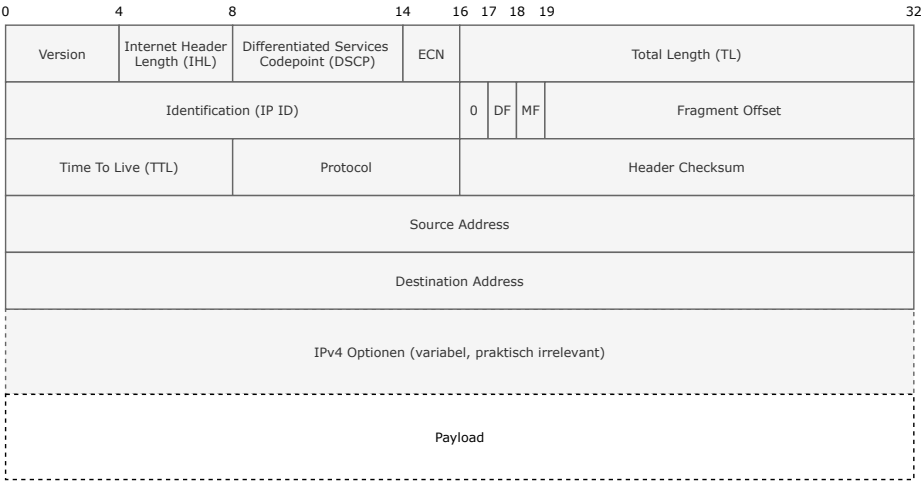
[1]FH Oberösterreich
Department Sichere Informationssysteme

Sommersemester 2022

Wichtiger Hinweis

Alle Materialien, die im Rahmen dieser LVA durch den LVA-Leiter zur Verfügung gestellt werden, wie zum Beispiel Foliensätze, Audio-Aufnahmen, Übungszettel, Musterlösungen, ... dürfen ohne explizite Genehmigung durch den LVA-Leiter NICHT weitergegeben werden!

IPv4 Header I



IPv4 Header II

- Version
  - IP Version: IPv4 = $4_{10} = 0100_2$
- Internet Header Length (IHL)
  - Länge IPv4 Header in 32-Bit Worten → max. IPv4 Header Länge = $(2^4 - 1) \cdot 32$ Bit = 60 Byte (Minimum: Header ohne Option, 20 Byte → $5_{10} = 0101_2$).
- Differentiated Services Code Point (RFC 2474) für QoS Features, Explicit Congestion Notification (RFC 3168) für Congestion Control.
- Total Length
  - Gesamtlänge des IPv4 Pakets inkl. Header in Bytes → max. Länge eines IPv4 Pakets = $2^{16} - 1 = 65535$ Bytes → 65515 Bytes Nutzdaten bei 20 Bytes Header.

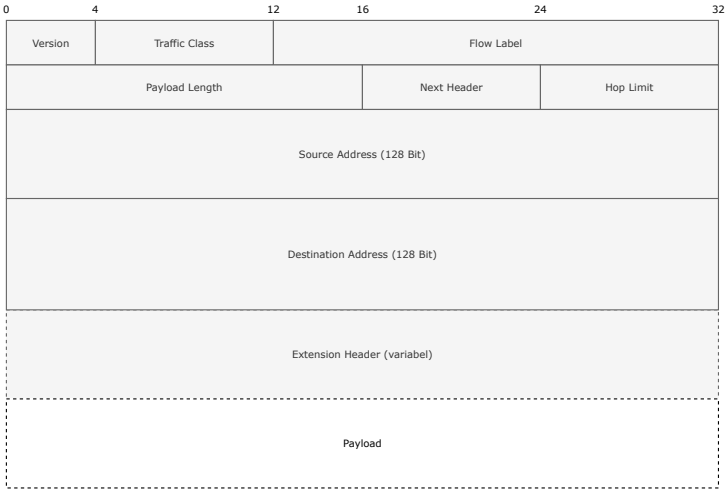
IPv4 Header III - Fragmentation & Reassembly

- Identification (IP ID)
  - Eindeutige Identifikation eines IP Pakets (typischerweise einfach inkrementiert (bei 16 Bit $\rightarrow$ max. $2^{16} = 65535$ Paket vor Wiederholung.
  - Wird zur Fragmentierung/Reassembly benötigt, um alle Fragmente dem richtigen IPv4 Paket zuordnen zu können (alle Fragmente haben gleiche IP ID).
- Don't Fragment Flag (DF)
  - Wenn gesetzt, darf das IPv4 Paket nicht fragmentiert werden ($\rightarrow$ ICMP Destination Unreachable, Fragmentation Needed but DF set).
- More Fragments Flag (MF)
  - Wenn gesetzt, ist das Fragment nicht das letzte im IPv4 Paket.
- Fragment Offset
  - Position des Fragments innerhalb des IPv4 Pakets in 64 Bit (8 Byte) Blöcken.
  - $\rightarrow$ z. B. IPv4 Paket mit 800 Bytes in max. 100 Fragmente zerlegbar.

IPv4 Header IV

- Time to Live (TTL) (eigentlich Hop Count)
  - Max. Anzahl an Routern, die ein IPv4 Paket am Weg von Quelle zum Ziel passieren darf (Lebensdauer).
  - Jeder Router muss bei Weiterleitung eines IPv4 Pakets den Wert im TTL-Feld um 1 verringern.
  - Wird dabei der Wert von 0 erreicht, wird das IPv4 Paket verworfen ($\rightarrow$ ICMP Time Exceeded, TTL Expired in Transit).
- Protocol
  - Identifiziert das im IPv4 Paket enthaltene nächst höhere Protokoll (normalerweise das Transportprotokoll).
  - IANA Protocol Numbers, z. B. TCP = 6, UDP = 17, OSPF = 89
- Source/Destination Address: IPv4 Quell- und Zieladresse
- IPv4 Options sind in der Praxis irrelevant.

IPv6 Main Header I



IPv6 Main Header II

- Version
  - IP Version: IPv6 $= 6_{10} = 0110_2$
- Differentiated Services Code Point (RFC 2474) für QoS Features, Explicit Congestion Notification (RFC 3168) für Congestion Control.
- Flow Label
  - Identifikation eines zusammenhängenden Datenstroms (z. B. einer TCP Verbindung) (RFC 6437)
- Payload Length
  - Länge des IPv6 Pakets ohne Main Header aber inkl. Extension Headern in Bytes $\rightarrow$ max. Länge eines IPv6 Pakets $= 2^{16} - 1 = 65535$ Bytes inkl. Extension Header.

IPv6 Main Header III

- Next Header
  - Identifiziert das im IPv6 Paket enthaltene nächst höhere Protokoll (normalerweise das Transportprotokoll) oder den ersten Extension Header.
  - IANA Protocol Numbers, z. B. TCP = 6, UDP = 17, OSPF = 89, 44 = Fragment Extension Header
- Hop Limit
  - Max. Anzahl an Routern, die ein IPv6 Paket am Weg von Quelle zum Ziel passieren darf (Lebensdauer).
  - Jeder Router muss bei Weiterleitung eines IPv6 Pakets den Wert im TTL-Feld um 1 verringern.
  - Wird dabei der Wert von 0 erreicht, wird das IPv6 Paket verworfen ($\rightarrow$ ICMPv6 Time Exceeded, Hop Limit exceeded in Transit).
- Source/Destination Address: IPv6 Quell- und Zieladresse

IPv6 Extension Header

- Auf den IPv6 Main Header kann eine beliebige Anzahl an Extension Headern folgen.
- Alle Funktionalitäten, die nicht in jedem IPv6 Paket gebraucht werden, wurden in Extension Header ausgelagert (z. B. Fragmentierung).
- Wichtige Extension Header
  - Fragment (Next Header = 44)
  - Authentication Header (AH) (Next Header = 51, → NWS, IPsec)
  - Encapsulating Security Payload (ESP) (Next Header = 50, → NWS, IPsec)
- Die Extension Header enthalten jeweils ein Next-Header-Feld worüber Main Header, Extension Header und die Payload miteinander verknüpft werden.


Fragen
Ceisteanna
Domande
Froen
Vragen
Pitanja
Questions
Quaestiones
Kysymykset
Cwestiynau
Vprašanja
Kérdések
Galderak
Spørgsmål
Spurningar
Preguntas
Mistoqsijiet
Frågor