IPv6 (IPng)

1) Warum IPv6 ?

IPv4 leistet zwar bis heute hervorragende Dienste, aber trotzdem bringt dieses Protokoll einige Probleme mit sich (bzw. wird es mit sich bringen). Die Wichtigsten sind folgende:

- Ineffizientes Routing: Die Berechnung unnötiger Headerfields ist zeitraubend.
- 32-bit Adressraum (ca. 4 Mrd. Adressen) ist zu knapp: Experten schätzen, dass der Adressraum in den Jahren 2008 bis 2018 aufgebraucht sein wird. Grund dafür ist unser Informationszeitalter, das mit zunehmender Technisierung auch für Autos, Handys, PDAs, Fernseher, Videospielkonsolen, Alarmsysteme im Haus, usw. Internetzugänge bietet bzw. bieten will.

Mit IPv6 hat man hauptsächlich folgende Verbesserungen durchgeführt, um obige Probleme zu lösen:

- Vereinfachung des Headers: Der IPv6-Header besteht nur noch aus 7 Feldern, statt aus 13. Die Router können Pakete schneller verarbeiten und erhöhen somit den Durchsatz.
- 128-bit Adressraum: Dieser 4-fach verlängerte Adressraum liefert nun 2^{128} Adressen (entspricht ca. $3x10^{38}$).

2) IPv6 Adresskonzept:

- **Adressaufbau:**
  Die IPv6-Adresse ist mit 128 bit 4-mal länger als in IPv4.
  Diese 128 bit werden dargestellt in 8 Gruppen von jeweils 16-bit Zahlen in Hexadezimal-Darstellung, jeweils durch ':' getrennt.
  Dadurch ergibt sich ein Wertebereich von

  0000:0000:0000:0000:0000:0000:0000:0000
  bis
  FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF

  Die Darstellung im Hex-Format liefert also einen „besseren Überblick“ !?

- **Kurzschriftregeln:**
  Um die Adressdarstellung etwas abzukürzen und noch übersichtlicher zu gestalten, hat man sich auf folgende Kürzungsregeln geeinigt:

  - Abkürzung der führenden Nullen (0000):

Beispiel: 1060:0000:0000:0000:0000:0600:002C:326B
⇓
1060:~~000~~0:~~000~~0:~~000~~0:~~000~~0:~~0~~600:~~00~~2C:326B
⇓
1060:0:0:0:0:600:2C:326B

- Abkürzung durch zweifachen Doppelpunkt (::):
  Dabei wird eine Folge von Nullen und Doppelpunkten durch '::' ersetzt.

  !!! Abkürzung darf in einer Adresse nur einmal verwendet werden !!!

  Beispiel: 1060:0:0:0:0:600:2C:326B
  ⇓
  1060~~:0:0:0:0:~~600:2C:326B
  ⇓
  1060**::**600:2C:326B

  Für die Rückerweiterung muss man nur herausfinden, wie viele Doppelpunkte fehlen und an welcher Stelle. Folgende Adressschablone könnte u.U. Helfen:

  ****:****:****:****:****:****:****:****

- **IPv4→IPv6 Adresskonvertierung:**
  Da der IPv4-Adressraum eine Teilmenge vom IPv6-Adressraum ist, passen alle IPv4-Adressen in folgendes Schema:

  0000:0000:0000:0000:0000:0000:****:**** bzw. : :****:****

  Beispiel: 130.103.40.5 (Ipv4)
  ⇓
  : :130.103.40.5 (Hybrid-Notation, auch zulässig)
  ⇓
  : :8267:2805 (Ipv6)

- **Spezielle IPv6 -Adressen:**
  - Die unspezifizierte Adresse: 0:0:0:0:0:0:0:0 ⇔ : :
    Diese Adresse wird bei DHCP verwendet.
  - Loopback -Adresse: 0:0:0:0:0:0:0:1 ⇔ : :1
    Zu Testzwecken verwendet man diese Adresse.
  - Site-lokale Adressen: FEC0:****:****:****:****:****:****:****
    Dabei handelt es sich um Adressen im Intranet einer Organisation, welche vom Internet aus nicht zugänglich sind.
  - Link-lokale Adressen: FE80:****:****:****:****:****:****:****
    Diese Adressen werden nur in Netzwerksegmenten gebraucht, und werden deshalb nicht an Router weitergeleitet.
  - Multicast -Adressen: FF**:****:****:****:****:****:****:****
    Diese Adresse bezeichnet nur eine bestimmte Gruppe.

- Anycast -Adressen:
  Wie Multicast, aber es wird immer nur an das am nächsten liegende Mitglied gesendet.

3) IPv6 -Header:

Der Header von IPv6 besitzt das Format wie in Abb. 3.1 gezeigt:

- ***Version (4 bit):*** Enthält die Nummer der IP-Version (hier: 6).
- ***Traffic class (8 bit):*** Gibt die Priorität der zu übermittelnden Daten an.
- ***Flow label (20 bit):*** Benennt einen Datenstrom. Alle Datagramme desselben Datenstroms tragen in diesem Feld den gleichen Wert.
- ***Payload length (16 bit):*** Bezeichnet die Länge des Datenpakets nach dem ersten Header.
- ***Next header (8 bit):*** Bestimmt den Typ des nächsten Header (z.B.: Routing Header, TCP, UDP, usw.)
- ***Hop limit (8 bit):*** Dieser Wert wird bei jedem Router-Durchgang um 1 dekrementiert. Ist der Wert Null, wird das Datagramm verworfen. Dies dient zur Vermeidung von Schleifen.
- ***Source Address (128 bit):*** Absenderadresse
- ***Destination Address (128 bit):*** Empfängeradresse

Anschließend folgen die eigentlichen Daten (Payload).

IPv6 hat also eine **feste** Header-Size von **40 Bytes**!

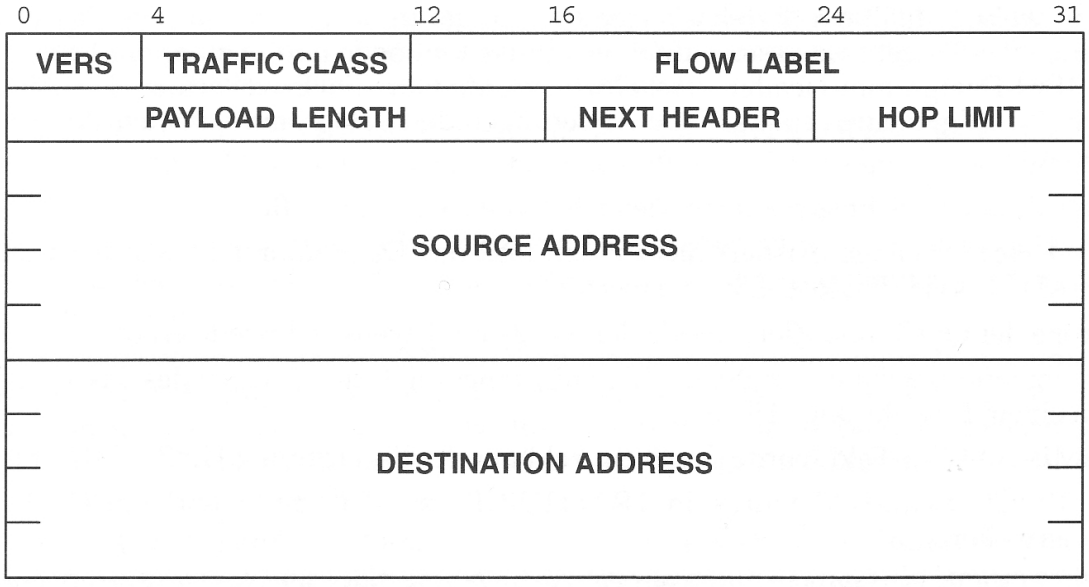

Abb. 3/1: *IPv6 Basis-Header*

- **Fehlende Felder bezüglich IPv4:**
  Folgende Felder bezüglich IPv4 hat man in IPv6 weggelassen:
  - *Header length:* IPv6 hat sowieso eine feste Header-Länge von 40 Bytes
  - Alle Felder im Bezug auf *Fragmentation:* Alle Hosts und Router müssen minimale MTU-Pakete unterstützen. Ist das Paket zu lang, wird eine Nachricht an den Host

zurückgeschickt, mit der Aufforderung das Paket zu verkleinern.
- *Header checksum:* Die Berechnung der Checksumme hat einen nachteiligen Einfluss auf die Leistung. Dieser Leistungsverlust summiert sich, wenn die Checksumme bei jedem Routerdurchgang überprüft werden muss.
- *Options:* Auf ein optionales Erweiterungsfeld hat man auch verzichtet. Stattdessen bietet IPv6 so genannte Erweiterungs-Header.

➢ **Erweiterungs-Header:**
In manchen Situationen sind fehlende Felder trotzdem notwendig.
IPv6 bietet hier ein Konzept der optionalen Erweiterungs-Header an. Diese Header werden benutzt um zusätzliche Informationen bereitzustellen.
Derzeit sind 6 Erweiterungs-Header gebräuchlich:

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

Die Erweiterungs-Header werden einfach an den IPv6-Basis-Header angehängt (siehe Abb. 3/2).

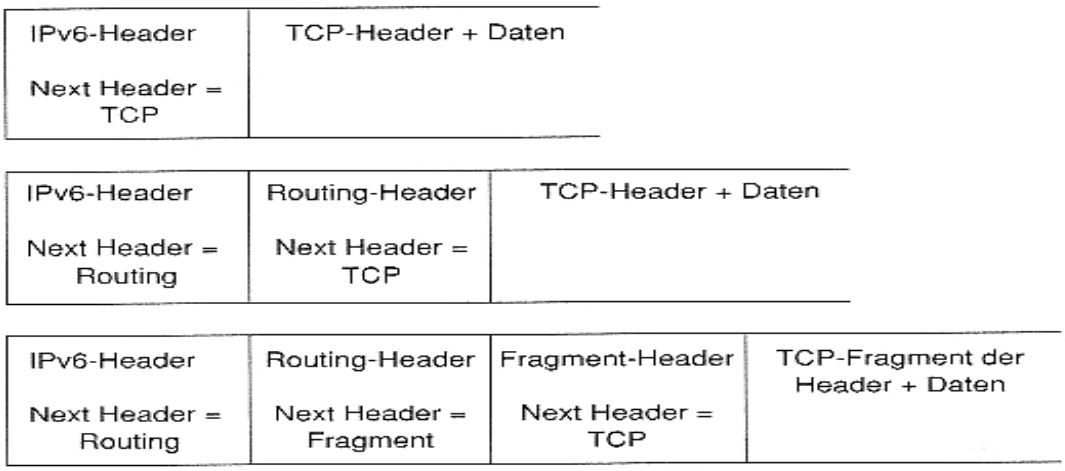

Abb. 3/2: *Mögliche Erweiterungs-Header*

4) IPv6 Services:

Zu den Serviceleistungen von IPv6 zählen unter anderen folgende:

- **Autodiscovery:**
  In IPv6 sind Hosts in der Lage ihr eigenes Netzwerksegment kennen zu lernen, sprich Informationen zu sammeln. Hierbei werden die bereits erwähnten Linklokalen Addressen und das NDP (*Neighbour Discovery Protocol*), das über ICMPv6 läuft, verwendet.

  Router hingegen nutzen RA (*Router Advertisement*) -Packete um ...
  - ... ihre Existenz im Netzwerk bekannt zu geben,
  - ... den Netzwerk-Part einer IPv6-Adresse bekannt zu machen, und
  - ... den Hosts zu signalisieren, ob sie eine stateless oder eine stateful Autokonfiguration durchführen sollen.

- **Autokonfiguration:**
  Die Autokonfiguration geschieht mit Hilfe der oben erwähnten RA-Pakete.
  Man unterscheidet dabei zwei Arten der Konfiguration:

  - Stateless Konfiguration:
    Dabei erzeugt sich das System zunächst selbst eine IP-Adresse. An diese selbsterzeugte Adresse schickt das System nun eine NS (*Neighbour Solicitation*) -Anfrage. Antwortet auf diese Anfrage ein anderes System mit einem NA (*Neighbour Advertisement*), so ist die Adresse bereits an das antwortende System vergeben und ein weiterer Versuch wird gestartet (d.h.: Wieder Adresse selbst erzeugen, NS-Anfrage, warten auf Antwort).

  - Stateful Konfiguration:
    Das System bekommt dabei eine IP-Adresse von einem DHCP-Server zugewiesen.

- **Autoregistration (speziell für Server):**
  Dieser Service registriert Dienstleistungssysteme automatisch im DNS.

- **Sicherheit:**
  IPv6 unterstützt zum einen die *Authentifikation* von Datagrammen, d.h. das Protokoll kann überprüfen, ob das empfangene Paket auch vom tatsächlich genannten Absender stammt.

  Mit Hilfe der *Datenintegrität* wird sichergestellt, dass das Datagramm während der Übertragung nicht geändert werden kann.

  Schließlich sorgt IPv6 noch für die *Vertraulichkeit* der Daten, sprich, das Datagramm kann von Hackern nicht eingesehen werden.

5) IPv4 -IPv6 -Koexistenz:

Der letzte Punkt befasst sich noch mit der Frage, wie man am besten von IPv4 nach IPv6 umrüsten soll?
Drei Möglichkeiten haben sich dabei etabliert:

- **Flag day:**
  Bei diesem Lösungsansatz werden alle Internetsysteme an einem bestimmten Tag zu einer bestimmten Zeit abgeschaltet, auf das neue IPv6 aufgerüstet und schließlich wieder in Betrieb

genommen. Bei den heutigen Ausmaßen ist ein *Flag day* allerdings unmöglich und könnte sich sogar zu einer Katastrophe entwickeln!

- **Dualstack Approach:**
  Heißt, dass auf den Netzwerkknoten (Hosts, Routers) beide Implementationen komplett, sowohl für IPv4 als auch für IPv6 vorhanden sind. Die Datagramme können somit wahlweise, je nach Kompatibilität, von den Systemen als IPv4- oder als IPv6-Pakete weitergeleitet werden.

- **Tunneling:**
  Bei der dritten Möglichkeit wird ein IPv6-Datagramm in ein IPv4-Datagramm eingebettet, wenn IPv6 bei der Kommunikation zwischen 2 Netzwerkknoten nicht unterstützt wird, und wieder herausgefiltert und im Originalzustand weitergeleitet, falls wieder eine IPv6-Kompatibilität vorhanden ist.

6) Quellenangaben:

- **Literatur:**

  - [Kurose, Ross] *Computer Networking – A Top-Down Approach Featuring the Internet* (2. Auflage, Addison-Wesley, 2003)
  - [Hein] *TCP/IP Internetprotokolle im professionellen Einsatz* (4. Auflage, International Thompson Publishing, 1998)
  - [Leiden, Wilensky] *TCP/IP für Dummies* (1. Auflage, International Thomson Publishing, 1998)
  - [Comer] *TCP/IP – Konzepte, Protokolle und Architekturen* (1. Auflage, mitp, 2003)

- **Bilder:**
  - Abb. 3/1: Aus [Comer] *TCP/IP – Konzepte, Protokolle und Architekturen* (1. Auflage, mitp, 2003)
  - Abb. 3/2: Aus [Hein] *TCP/IP Internetprotokolle im professionellen Einsatz* (4. Auflage, International Thompson Publishing, 1998)