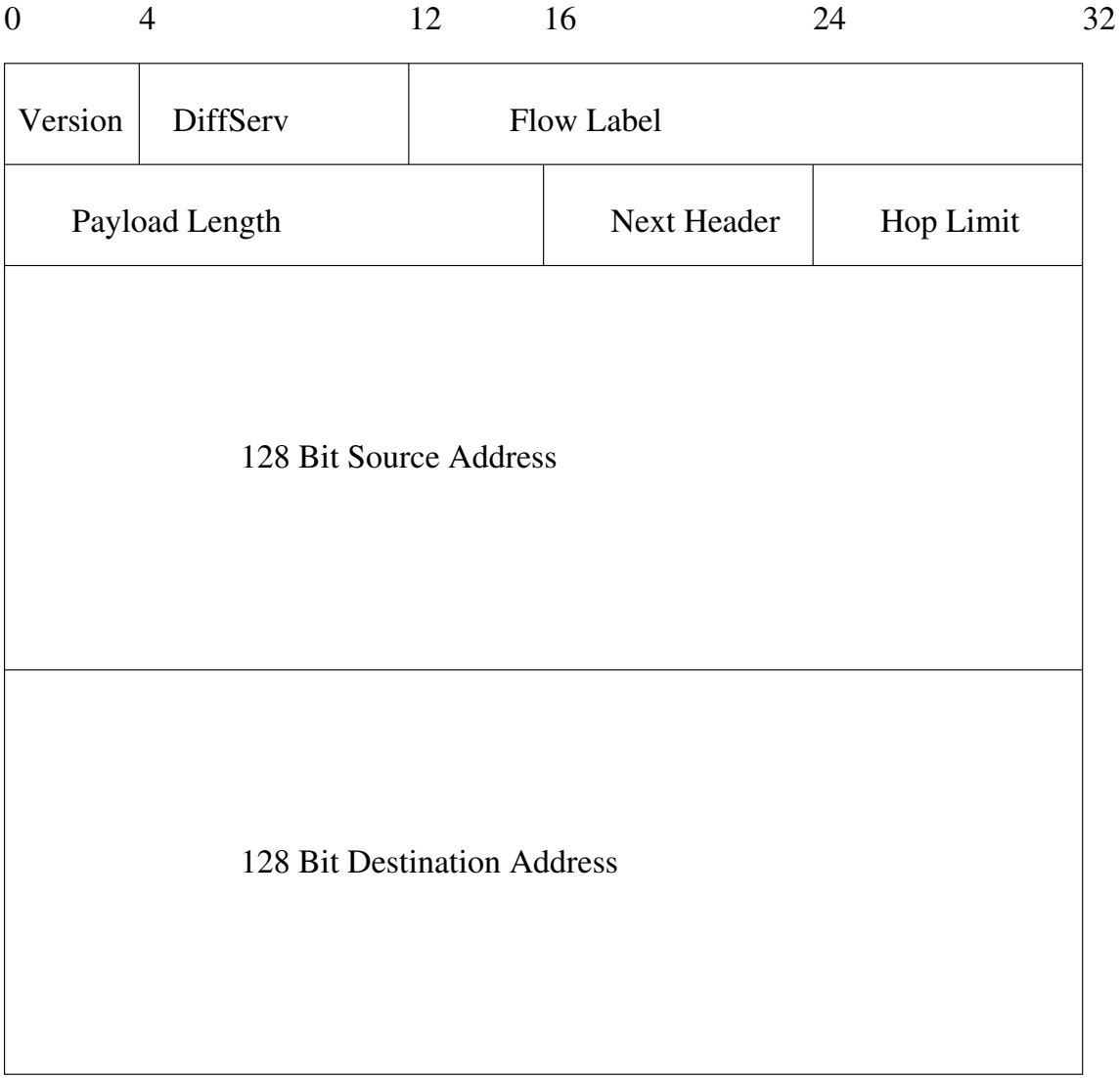
Zustand IPv4

- Router im Internet haben > 200000 Einträge in der Routingtabelle
- IP Adressen sind eine extrem knappe Resource
- Viele Dienste sind nur mit Hilfe neuer und komplizierter Protokolle möglich, z.B.:
  - MMS, vgl. www.openmobilealliance.org
  - Mobile E-Mail
- Temporäre Adressvergabe mittels DHCP, private Adressbereiche und NAT helfen, die vorhandenen Adressen effizient zu nutzen.

Neuerungen durch IPv6

- 128Bit für Adressen, nicht 32Bit
- Hierarchische Netzstruktur durch gezielte Adresszuweisung
- Minimaler Basisheader mit flexibler Erweiterungsmöglichkeit
- Differentiated Services sind Standard
- Automatische Konfiguration ist ohne Zusatzprotokolle möglich.
- Dienste für mobile Terminals werden unterstützt
- Sicherheitsdienste werden von der Vermittlungsschicht transparent angeboten.
- Multicast Dienste sind besser integriert

IPv6 Header


0
4
12
16
24
32
Version
DiffServ
Flow Label
Payload Length
Next Header
Hop Limit
128 Bit Source Address
128 Bit Destination Address

IPv6 Header

- **Version:** 4 Bit Version, 6 für IPv6
- **DiffServ:** Differentiated Services Kennung, entspricht IPv4
- **Flow Label:** Kennung zusammengehöriger Pakete, vgl. RFC3697
- **Payload Length:** 16 Bit Länge der Daten in Byte
- **Next Header:** Typ des nächsten Headers, entweder Protocol (RFC1700) wie in IPv4, oder einer der standardisierten Erweiterungsheader
- **Hop Limit:** Max. Anzahl Hops, vgl. IPv4 TTL
- **Source Address:** 128 Bit Quelladresse
- **Destination Address:** 128 Bit Zieladresse

IPv6 Adressen (vgl. RFC3513)

Adressen identifizieren Schnittstellen (Interfaces, vgl. RFC2460, Section 2), mit denen Knoten mit dem Netzwerk verbunden sind.

In IPv6 werden drei Typen von Adressen unterschieden:

- **Unicast:** Adresse einer Schnittstelle, Pakete werden zu genau dieser Schnittstelle weitergeleitet.
- **Anycast:** Adresse für eine Gruppe von Schnittstellen, ein Paket wird zu einer dieser Schnittstellen weitergeleitet.
- **Multicast:** Adresse für eine Gruppe von Schnittstellen, Pakete werden zu allen Schnittstellen der Gruppe ausgeliefert.

Schreibweise für IPv6 Adressen

- Die 16 Byte einer Adresse in Network Byte Order werden geschrieben als 8 Segmente von je 2 Byte in hexadezimaler Darstellung, durch Doppelpunkte getrennt.
- Führende Nullen in Segmenten können weggelassen werden.
  Beispiel: 00 01 02 03 04 05 06 07 18 19 1A 1B 1C 1D 1E 1F
  geschrieben: 1:203:405:607:1819:1A1B:1C1D:1E1F
- Eine Gruppe von aufeinanderfolgenden, leeren Segmenten kann durch zwei Doppelpunkte abgekürzt werden:
  Beispiel: 00 01 00 00 00 00 00 00 00 00 1A 1B 1C 1D 1E 1F
  geschrieben: 1::1A1B:1C1D:1E1F
- Alternative Schreibweise: Die letzten 4 Byte können als “Dotted Notation” geschrieben werden:
  Beispiel: 00 01 00 00 00 00 00 00 00 00 1A 1B 01 02 03 04
  geschrieben: 1::1A1B:1.2.3.4

Schreibweise für Netzwerke

- Netzwerkpräfixe werden in CIDR Notation (Adresse/Länge) geschrieben.
- Segmente, die außerhalb der Maske liegen, brauchen nicht aufgeführt zu werden.
  Beispiel: das 60 Bit Präfix `12AB 0000 0000 CD3` kann geschrieben werden als:
  - 12AB:0:0:CD30/60
  - 12AB:0:0:CD30:0:0:0:0/60
  - 12AB:0:0:CD30::/60
- Alle möglichen Mehrdeutigkeiten sind **nicht** erlaubt, z.B.:
  - 12AB:0:0:CD3/60, Segment vier kann auch 0CD3 sein.
  - 12AB::CD30/60, Würde interpretiert als 12AB 0000 0000 000

Adresstypen

Die unterschiedlichen Adresstypen und Adressbereiche sind Subnetze des IPv6 Adressraumes:

Type	Prefix
Unspecified	::/128
Loopback	::1/128
Multicast/Anycast	FF00::/8
Link-local unicast	FE80::/10
Site-local unicast	FEC0::/10
Global unicast	everything else

Aufbau von Global Unicast Adressen

Adressen, die nicht mit ::/12 beginnen, enden in einer 64 Bit Schnittstellenadresse gemäß IEEE EUI-64.

Beispiel: Die 48 Bit Ethernetadresse einer Schnittstelle wird zu einer 64 Bit Schnittstellenadresse expandiert, indem Bit 1 des ersten Bytes auf 1 gesetzt wird (ist in der Ethernetadresse immer 0, da OUI), Byte 2 und 3 unverändert übernommen werden, dann wird 0xFFFE eingefügt, dann folgen die letzten 3 Byte der Ethernetadresse:

Beispiel: Aus der Ethernetadresse 08:00:46:9E:92:0E wird . . .:0A00:46FF:FE9E:920E

Für andere Interfacetypen finden sich entsprechende Abbildungsregeln in den RFCs, die die Übertragung von IPv6 über den Link spezifizieren.

Mapping von IPv4 Adressen

Schnittstellen, die sowohl IPv4 als auf IPv6 bedienen können, können spezielle IPv6 Adressen bekommen (**IPv4 compatible address**), die die IPv4 Adresse als letzte 4 Bytes enthalten. Diese Adressen werden heute kaum noch verwendet:

Beispiel: IPv6 fähige Schnittstelle mit IPv4 Adresse 1.2.3.4 hat IPv6 Adresse ::1.2.3.4

Soll eine Anwendung sowohl mit IPv4 als auch IPv6 funktionieren, wird oft IPv6 als Obermenge verwendet. Adressen einer Schnittstelle werden dann als sogenannte **IPv4 mapped address** vom Stack geliefert, wenn es sich um eine IPv4 Adresse handelt.

Beispiel: Schnittstelle mit IPv4 Adresse 1.2.3.4 hat IPv4 mapped address ::FFFF:1.2.3.4

Diese Adressen unterliegen den IPv4 Einschränkungen.

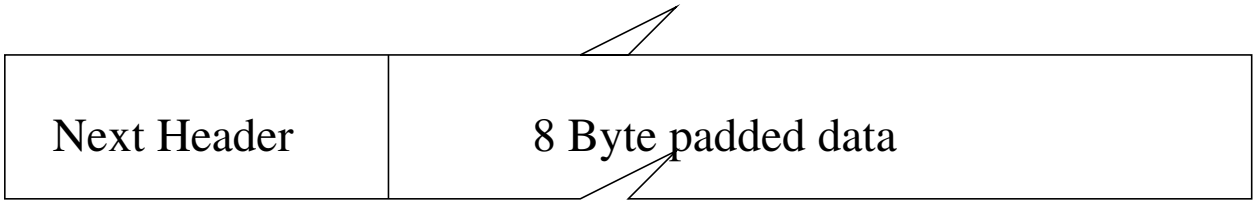
IPv6 Erweiterungsheader

Erweiterungsheader beginnen auf 8 Byte Grenzen, die folgende Reihenfolge muß eingehalten werden:

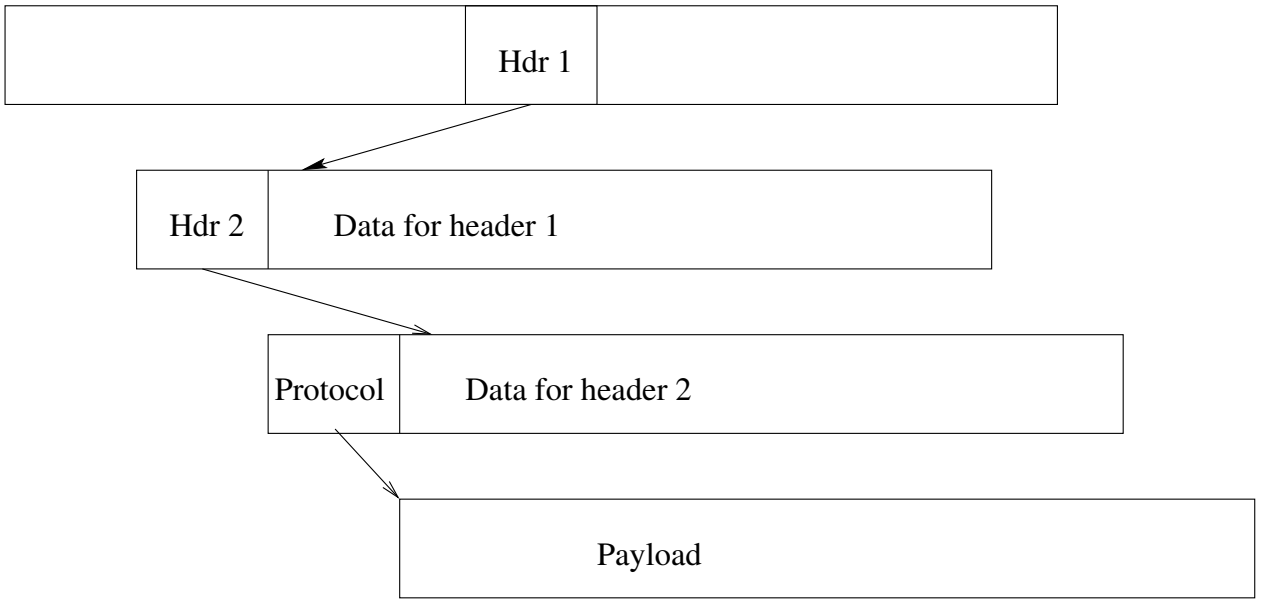
0	Hop-By-Hop Option (RFC1883)
60	Destination Option
43	Routing Header
44	Fragment Header
51	Authentication Header (RFC2402)
50	Encrypted Security Payload (RFC2406)
59	No Next Header
60	Destination Option
135	Mobility Header

Erweiterungsheader: Format und Verkettung

Format eines Erweiterungsheaders:



Headerfolge, ähnlich IPv4 Optionen:



Hop-By-Hop Option

- Alle Optionen, die von jedem Router ausgewertet werden müssen, werden in Hop-By-Hop Headern übertragen.
- Der Header hat immer die Felder
  1. Next Header
  2. Length, gezählt in Bytes ab Byte 8
  3. Parameter
- Parameter sine Typ/Länge/Wert kodiert, bis auf Typ 0, der keine Paramter besitzt.
- Type 0 und 1 dienen als Füller
- Typ 194 (Jumbo Payload) signalisiert Pakete bis 4GByte
- Weitere Typen sind in der Standardisierung

Destination Option

- Die Destintion Option ist von jedem Router auszuwerten, sofern sie vor dem Routing Header auftritt, sonst nur vom Zielhost.
- Der Aufbau entspricht den Hop-By-Hop Headern.
- Einige Optionen sind standardisiert, z.B.:
  - ein Header, der die Zahl geschachtelter IPv6 Tunnel limitiert.
  - Home Address bei Mobile IP
- Optionen können aus Anwendungen gesetzt werden.

Routing Header

- Der Routing Header hat im wesentlichen dieselbe Funktion, wie Loose Source Routing bei IPv4, allerdings ohne deren Limitierungen.
- Ein Äquivalent zu Strict Source Routing wird in IPv6 bisher nicht angeboten.
- Der Header besteht wie bei IPv4 aus einer Länge (8 Bit gezählt in 8 Byte Einheiten), einer Liste von Adressen und einem Zeiger in diese Liste, damit die Router das nächste Ziel erkennen können.
- Ein 8 Bit Typ Feld sowie 4 Byte Padding sichern Erweiterbarkeit.

Fragment Header

- Bei IPv6 fragmentiert nur der sendende Endpunkt einer Kommunikationsbeziehung, keine Router im Pfad.
- Die MTU wird mit dem Path MTU Discovery Protocol (RFC1981) bestimt.
- Der Fragment Header entspricht weitgehend den IPv4 Headerfeldern, die zur Fragmentierung genutzt werden, d.h. er enthält:
  - 13 Bit Offset in 8 Byte Einheiten
  - 32 Bit Identification
  - 1 Bit More Fragments
  - Mit 8 Bit Next Header und 10 Bit Padding erhält man 64 Bit
- Daten des IP Headers bis zum Fragment Header können nicht fragmentiert werden.

Authentication Header (AH)

- AH ist eines der Protokolle, die unter dem Namen IPSec transparente Sicherheitsdienste auf Ebene der Vermittlungsschicht anbieten.
- IPSec ist integraler Bestandteil von IPv6.
- Es gibt inzwischen viele Implementationen von IPSec auf Basis von IPv4.
- Authentizität wird von AH durch gegenseitige Authentifizierung gesichert.
- Integrität wird durch Signatur der Header und Daten sichergestellt.
- Sicherung gegen Mehrfacheinspielung (Replay Attack) von Daten ist optional.
- Vertraulichkeit ist **nicht** Bestandteil von AH

Encrypted Security Payload (ESP)

- ESP bietet gegenüber AH erweiterte Sicherheitsdienste
- ESP kann in Verbindung mit AH verwendet werden.
- Es werden Tunnel Modus und Transport Modus unterschieden.
- Vertraulichkeit wird durch Verschlüsselung der Daten und im Tunnel Modus durch Aggregierung von Datenströmen erreicht.
- Gegenseitige Authentifizierung der Endpunkte (Host oder Router/Security Gateway) ist möglich.
- Verhinderung von Mehrfacheinspielung ist möglich.

Mobility Header

- Der Mobility Header wird benutzt, um Assoziationen zwischen mobilem Endgerät und Home-Agent herzustellen, aufzulösen oder zu testen.
- Folgende Nachrichtentypen sind spezifiziert:
  1. Binding Refresh Request Message, erzeugt Assoziation im Home-Agent
  2. Home Test Init Message, Care-of Test Init Message: Teil der “Return Routability Procedure”, die die Erreichbarkeit des Endgerätes sicherstellt
  3. Home Test Message: Antwort zur Home Test Init Message
  4. Care-of Test Message: Antwort zur Care-of Test Init Message
  5. Binding Update Message: Setzen einer neuen Care-Of-Address
  6. Binding Acknowledgement Message: Antwort auf den Binding Update Message

Migration zu IPv6

- Aktuelle Betriebssysteme (Windows, Unix Derivate, Symbian, IOS, ...) unterstützen IPv6
- Server und Infrastruktur im Internet sind inzwischen auf IPv6 eingerichtet, Protokolle angepasst, z.B.:
  - RIPng
  - BGP4+
  - DNS
- Viele Programme sind nicht fähig, IPv6 zu nutzen und werden es niemals sein.
- Know How für IPv6 ist kaum verfügbar, Erfahrungen gibt es kaum.
- Die “IPng Transition (ngtrans) working group” erklärt am 14.8.2002: **v6 considered operational**
- vgl. D.J. Bernstein: The IPv6 Mess, `http://cr.yp.to/djbdns/ipv6mess.html`