Einführung in das IPv6 Protokoll

Prof. Bettina Schnor

Universität Potsdam
Institut für Informatik
Professur Betriebssysteme und Verteilte Systeme

BLIT 2011, 5.11.2011

IDSv6-Projekt

- IPv6 honeypot
- IPv6 extensions for the intrusion detection system snort
- firewall test suites
- `www.ipv6-ids.de`

funded by

Bundesministerium
für Bildung
und Forschung

IPv6 – Workshop auf dem BLIT 2011

- Einführung in das IPv6 Protokoll - Bettina Schnor
- IPv6 Hands on - Klemens Kittan, Paul Szameitpreiks
- Methoden und Techniken für den Test von IPv6 Netzwerken - Thomas Scheffler
- IPv6 Intrusion Detection - Martin Schütte, Bettina Schnor, Thomas Scheffler
- IPv6 Netzwerkprogrammierung - Oliver Eggert

IPv6–Aktivitäten an der UP

2002: IPv6 Showcase
Labor- und Lehrbetrieb in Kooperation mit T-Systems u.a.
Webseite: www.ipv6-showcase.de

2004: IPv6 Server Load Balancer
Präsentation auf der CeBIT 2004

2005: IPv6 Cluster Computing
Portierung von MPICH1 nach IPv6

2008: IPv6 Grid Computing
Portierung von MPICH2 und OpenMPI nach IPv6 (Koop. Uni Jena)

2011: IPv6 Intrusion Detection System
BMBF gefördertes Projekt zur Angriffsprävention und validierten Absicherung von IPv6-Netzen
Webseite: www.ipv6-ids.de

Was ist eigentlich mit IPv5?

IP Version Numbers:

0	Reserved
1	Reserved
2	Unassigned
3	Unassigned
4	Internet Protocol
5	Experimental Internet Stream Protocol, Version 2, RFC 1819 (1995), obsol
6	Internet Protocol version 6

Quelle: `http://www.iana.org/assignments/version-numbers`

IPv6 – Motivation

Vinton Cerf, einer der Väter des Internets, im Vortrag an der Universität Potsdam, 26.5.2011:

"How could we make open standards? It was the time of the cold war! We did it and nobody noticed.

If you want to blame someone for the 32 bit IPv4 addresses, blame me! – I had to decide, and we expected the network to be *experimental*."

IPv6 – Motivation

- IPv4-Adressraum ausgeschöpft (32-Bit-Adressen)
- IPv6 stellt größeren Adressraum zur Verfügung (128-Bit-Adressen)
  $\Longrightarrow$ Adressierung von Mobiltelefonen, Heizung, Kühlschrank möglich (Internet of Things)

Testnetz 6Bone (1995-2006)
Das 6Bone war ein IPv6 Testbett. Dabei handelte es sich um ein virtuelles Netzwerk: Mittels IPv6-in-IPv4-Tunneling wurden IPv6-Pakete über das Internet ausgetauscht.

"World IPv6 Day" am 8.6.2011: Google, Yahoo, Facebook, ... sowohl IPv4 als auch IPv6 erreichbar!

Gashinsky (Yahoo's Chefnetzwerkarchitekt): „Das war eine Menge Arbeit für 0,229 % IPv6-Nutzer."

IPv6 Addressierung

- IPv6 Adressen sind 128 Bit lang!
- $2^{128} = 340282366920938463374607431768211456$
- Das entspricht 665 Milliarden Adressen pro mm^2 Erdoberfläche

Schreibweise von IPv6-Adressen

- IPv6 Adressen als 32 Hexadezimal-Ziffern dargestellt, geschrieben als 8 Blöcke von jeweils 4 Hexadezimal-Ziffern durch Doppelpunkte getrennt:
  Beispiel:
  2001:0DB8:0000:0000:0008:0800:200C:417A eine Unicast-Adresse
- Führende Nullen können weggelassen werden:
  Beispiel:
  2001:DB8:0:0:8:800:200C:417A
- Genau 1 Folge von Nullen kann durch "::" ersetzt werden:
  Beispiel:
  2001:DB8::8:800:200C:417A eine Unicast-Adresse

IPv6 benutzt 3 Adresstypen:

- Unicast: Punkt-zu-Punkt-Kommunikation:
  - global
  - link-local
- Multicast: 1-zu-n-Kommunikation: Jedes Gruppenmitglied erhält eine Kopie der Nachricht.
- Anycast (Vormals Cluster-Adresse genannt): Adresse einer Gruppe von Rechnern mit gleichem Präfix. Ein an diese Adresse gesendetes Datagram wird genau einem der Rechner zugestellt.

Es gibt keine Broadcast-Adressen mehr, aber eine Multicast-Adresse ff02::1 für alle Knoten im lokalen Netz.

Ein Interface hat immer

- eine link-local Unicast-Adresse.
- eine oder mehrere Multicast-Adressen.
- kann eine oder mehrere globale Unicast-Adressen haben.

(Site Local Unicast-Adressen sind obsolet.)

Beispiel:
2001:DB8:0:0:8:0800:200C:417A a unicast address
FF01:0:0:0:0:0:0:101 a multicast address
0:0:0:0:0:0:0:1 the loopback address

in Kurzschreibweise:
2001:DB8::8:800:200C:417A a unicast address
FF01::101 a multicast address
::1 the loopback address

aber: 2001:0DB8:0000:0000:0008:0000:0000:417A
in Kurzschreibweise: 2001:DB8::0008:0:0:417A
nicht: 2001:DB8::0008::417A

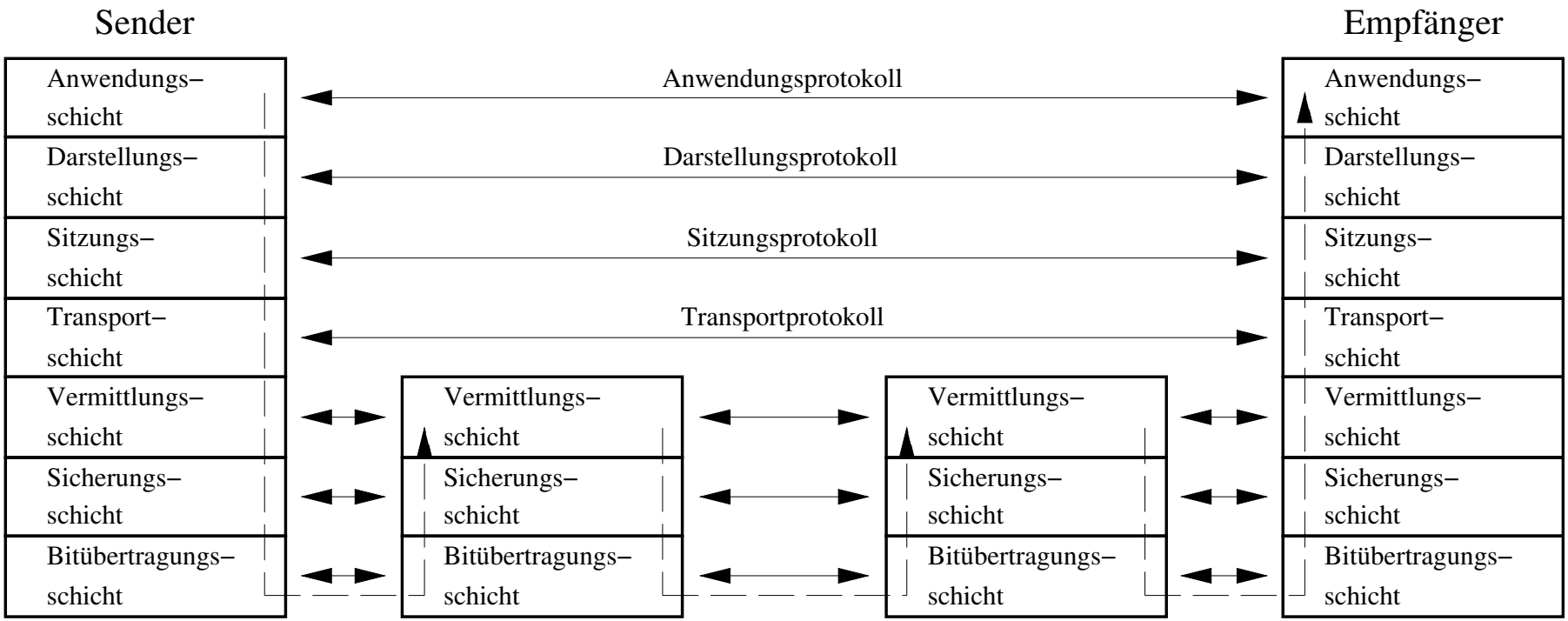
Ein IPv6 address prefix wird wie folgt dargestellt:
ipv6-address/prefix-length

Der Typ einer IPv6-Adresse wird durch die high-order Bits bestimmt:

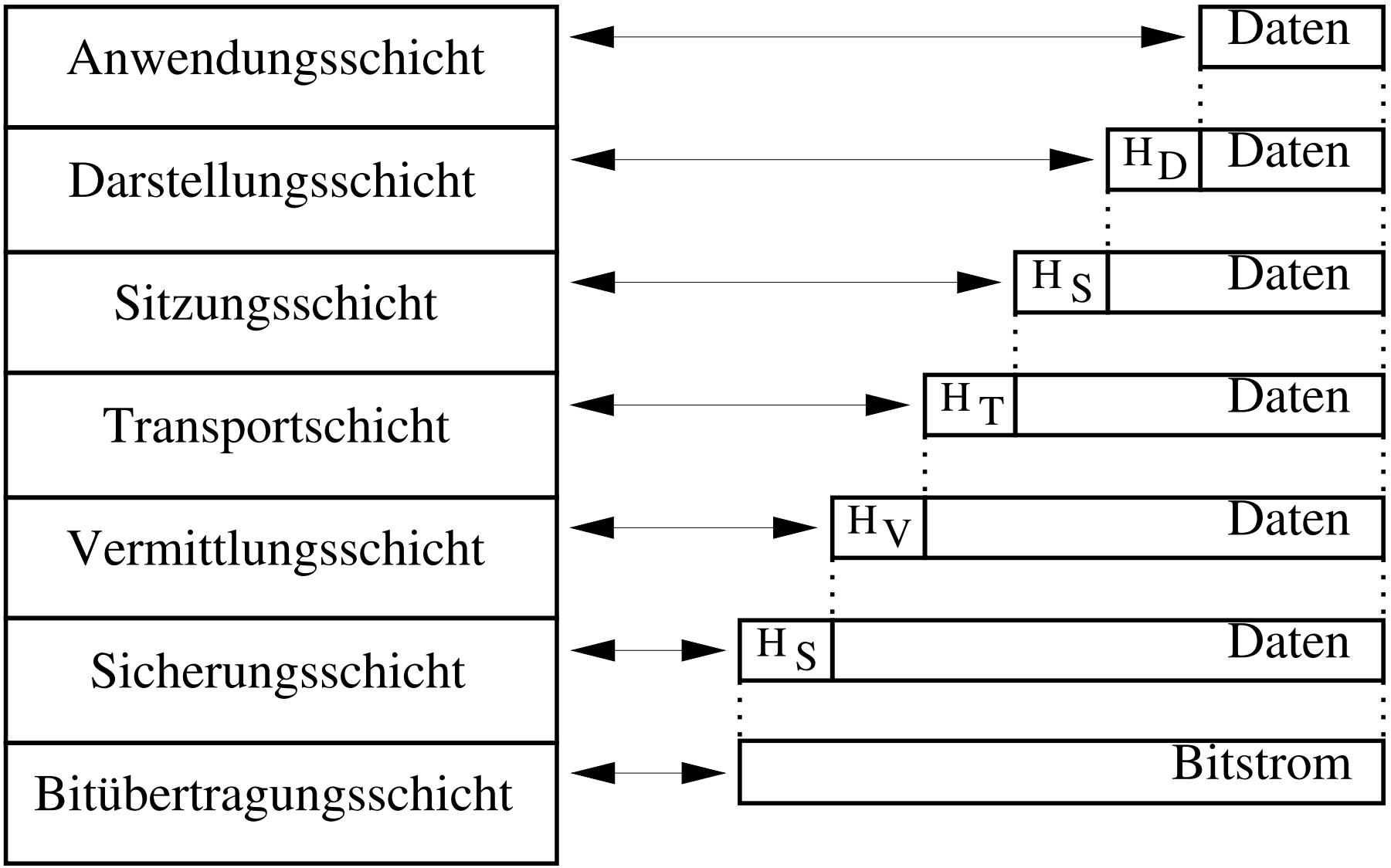
Address type	Binary prefix	IPv6 notation
Unspecified	00...0 (128 bits)	::/128
Loopback	00...1 (128 bits)	::1/128
Multicast	11111111	FF00::/8
Link-Local unicast	1111111010	FE80::/10
Global Unicast	(everything else)	

Es ist üblich /64-Netze zu vergeben: Also 2^{64} frei verfügbare Adressen

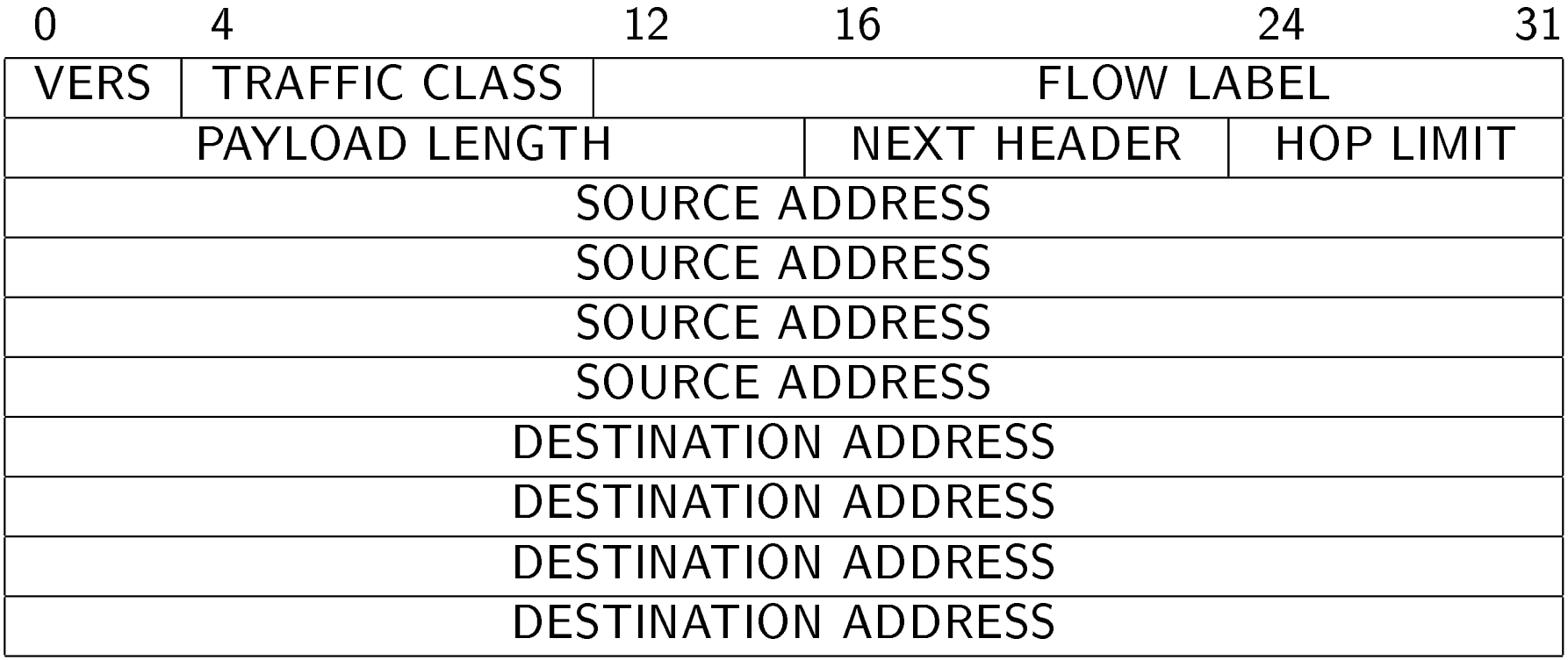
Hauptaufgabe von IP: Wegwahl



Das Notizbuch: Der Protokollheader

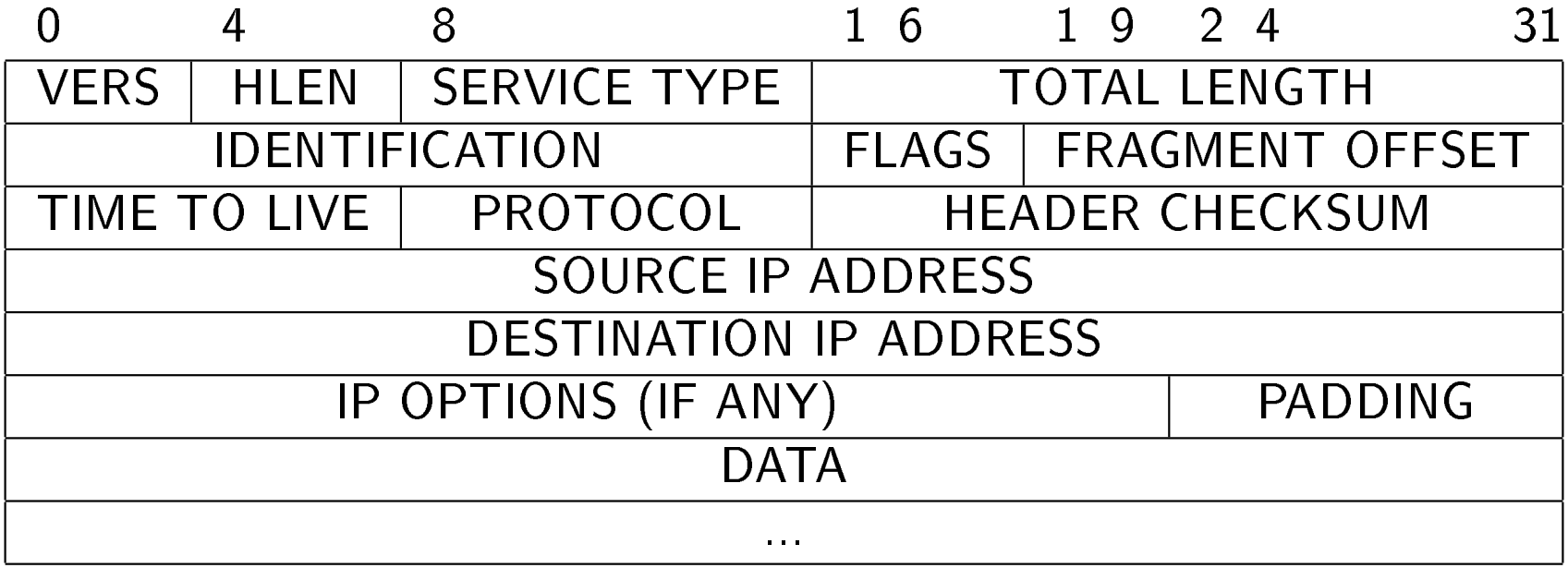


IPv6-Basis-Header



Der IPv6-Basis-Header umfasst weniger Felder als der IPv4-Header.

Zum Vergleich: Das IPv4-Datagrammformat



- VERS: Versionsnummer des benutzten IP-Protokolls
- PROTOCOL: Bestimmt das Transportprotokoll, das die Daten erzeugt hat, z.B. welche TCP-/UDP-Version

Felder im IPv6-Header:

VERS: Internet Protocol Versionsnummer (hier: 6)

TRAFFIC CLASS: Angabe für QoS-Routing: identifiziert und unterscheidet verschiedene Klassen und Prioritäten bei IPv6-Paketen. Mögliche Werte:
0-7 - Datenverkehr bei Überlastung verlangsamen
8-15 - konstante Übertragungsrate (z.B. Echtzeit-Anwendungen)

FLOW LABEL: Das Feld dient für QoS-Routing: Wird für eine Anwendung eine bestimmte Dienstqualität gewünscht (siehe Traffic Class), so kann ein entsprechender Netzwerkpfad ermittelt werden, der diese Dienstqualität erfüllt. Dieser Netzwerkpfad wird mit einer bestimmten ID gekennzeichnet, die im Flow Label gemerkt wird.

PAYLOAD LENGTH: Länge des Datenfeldes in Bytes

HOP LIMIT:
- entspricht TTL in IPv4
- Überlebensdauer eines Pakets
- Wert wird von jedem weiterleitenden Router dekrementiert.
- bei Wert 0 - Paket wird verworfen.

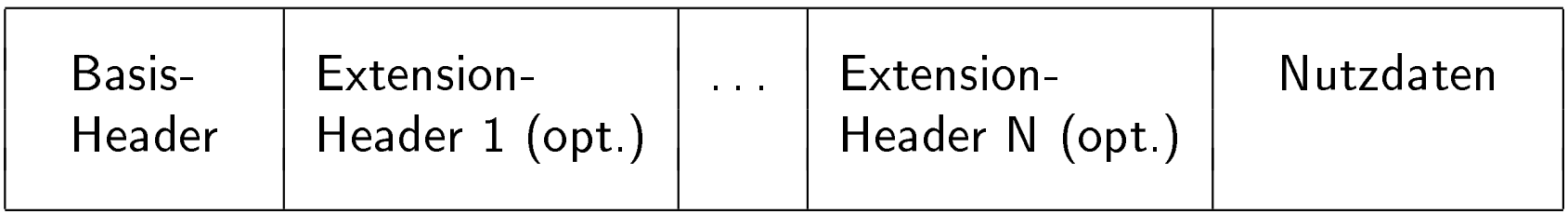
Fragmentierung

IPv6 requires that every link in the internet have an Maximum Transfer Unit (MTU) of 1280 octets or greater. On any link that cannot convey a 1280-octet packet in one piece, link-specific fragmentation and reassembly must be provided at a layer below IPv6.
It is strongly recommended that IPv6 nodes implement Path MTU Discovery [RFC-1981], in order to discover and take advantage of path MTUs greater than 1280 octets. However, a minimal IPv6 implementation (e.g., in a boot ROM) may simply restrict itself to sending packets no larger than 1280 octets, and omit implementation of Path MTU Discovery.

Extension-Header

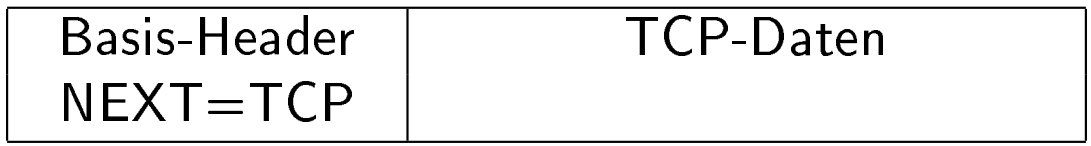
NEXT HEADER: Spezifiziert die hinter dem aktuellen Header folgenden Datenart (Nutzdaten, Extension Header)
Jeder Extension-Header hat ebenfalls ein Next-Header-Feld. Der letzte Extension-Header verweist auf das Transportprotokoll (z.B. TCP,UDP)

Der Basis Header ist zwingend, während Extension-Header wahlfrei nach Bedarf benutzt werden können.

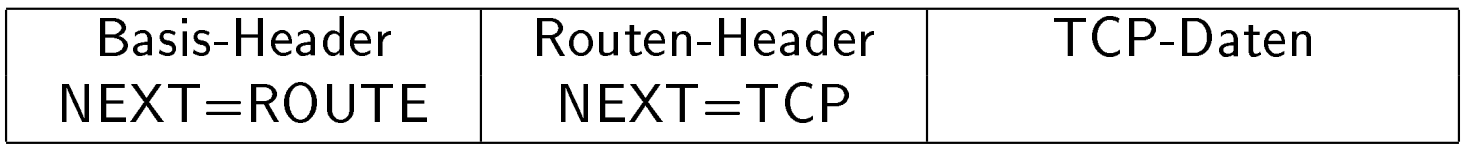


Zwei Beispiele für ein IPv6-Datagramm

(a) mit Basis-Header und Nutzdaten



(b) mit Basis-Header, einem Extension-Header für die Route und dem Nutzdatenbereich. Das Feld NEXT HEADER in beiden Headern spezifiziert das danach folgende Element.



A full implementation of IPv6 includes implementation of the following extension headers:

NEXT HEADER	Beschreibung
0	Hop-by-Hop Options
43	Routing (Type 0)
44	Fragment
60	Destination Options
51	Authentication
50	Encapsulating Security Payload
59	No next header

The first four are specified in RFC-2460; the next two are specified in RFC-2402 and RFC-2406 (IPsec), respectively.
Each extension header should occur at most once, except for the Destination Options header which should occur at most twice (once before a Routing header and once before the upper-layer header).

Hop-by-Hop Options header:
- optionale Informationen für Hops auf dem Pfad zum Ziel-Host
- müssen von allen Zwischenstationen untersucht werden
- Beispiele: Jumbo Payload Option (RFC 2675), Padding Options: Pad1 (RFC 2460), PadN (RFC2460)

Routing header:
- Beeinflussung der Route eines IPv6-Pakets
- Auflistung von Systemen, die auf dem Weg zum Ziel besucht werden müssen
- Sicherheitskritisch $\Longrightarrow$ obsolet

Fragment header:
- Fragmentierung von großen Datenpakten (größer als MTU)
- IPv6: Fragmentierung wird von Endpunkten durchgeführt

Destination Options Header:
- spezielle Informationen für den Zielrechner
- werden ausschließlich von diesem ausgewertet

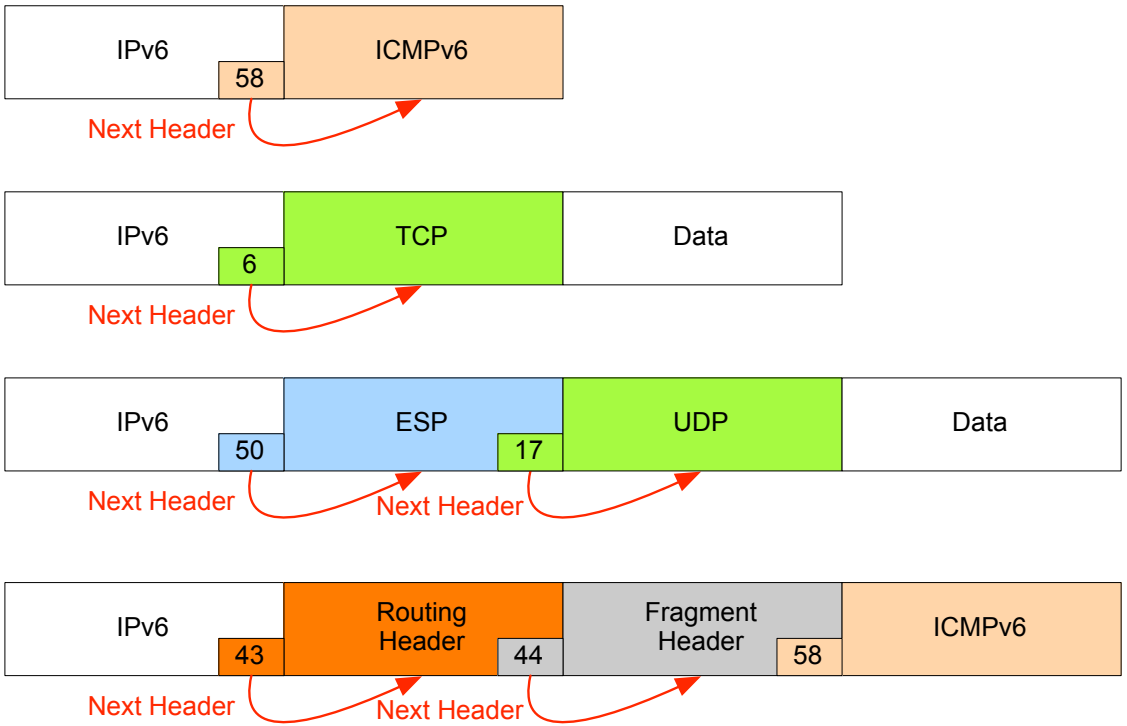
Authentication Header (IPsec):
- Empfänger kann vorgegebenen Absender des Pakets Überprüfen
- Überprüfung auf evtl. Veränderungen des Pakets während der Übertragung

Encapsulating Security Payload Header (IPsec):
- Verschlüsselung des Pakets

No Next Header:
- keine weiteren Header folgen

IPsec ist **zwingend** vorgeschrieben für IPv6 und optional für IPv4.

IPv6 Extension Header



(entnommen: Philippe Biondi: *Scapy and IPv6 Networking*, Hack in the Box Security Conference, 2006)

Extension Header Order

When more than one extension header is used in the same packet, it is recommended that those headers appear in the following order:

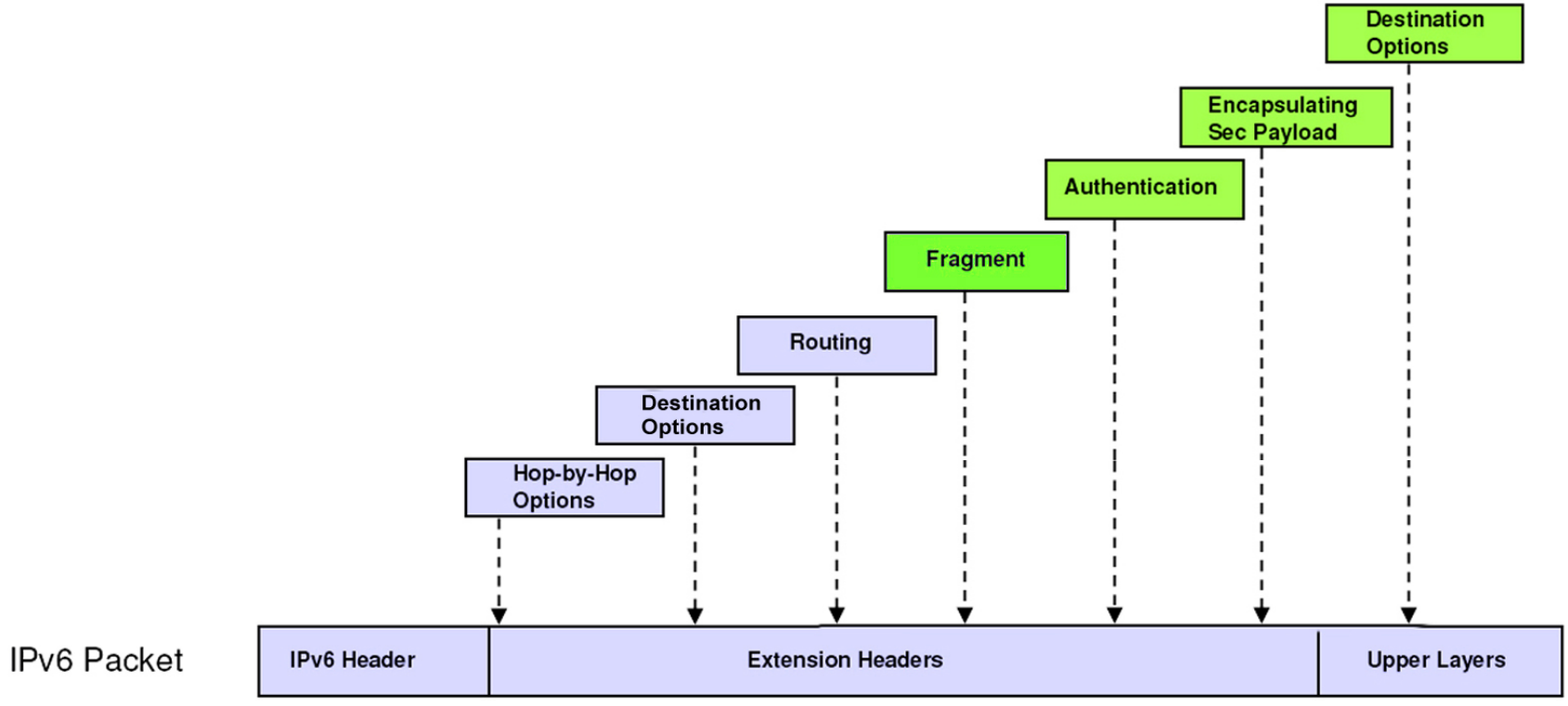
IPv6 header
Hop-by-Hop Options header
Destination Options header (note 1)
Routing header
Fragment header
Authentication header
Encapsulating Security Payload header
Destination Options header (note 2)
upper-layer header

note 1: for options to be processed by the first destination that appears in the IPv6 Destination Address field plus subsequent destinations listed in the Routing header.

note 2: for options to be processed only by the final destination of the packet.

Prinzip der optionalen Extension-Header von IPv6

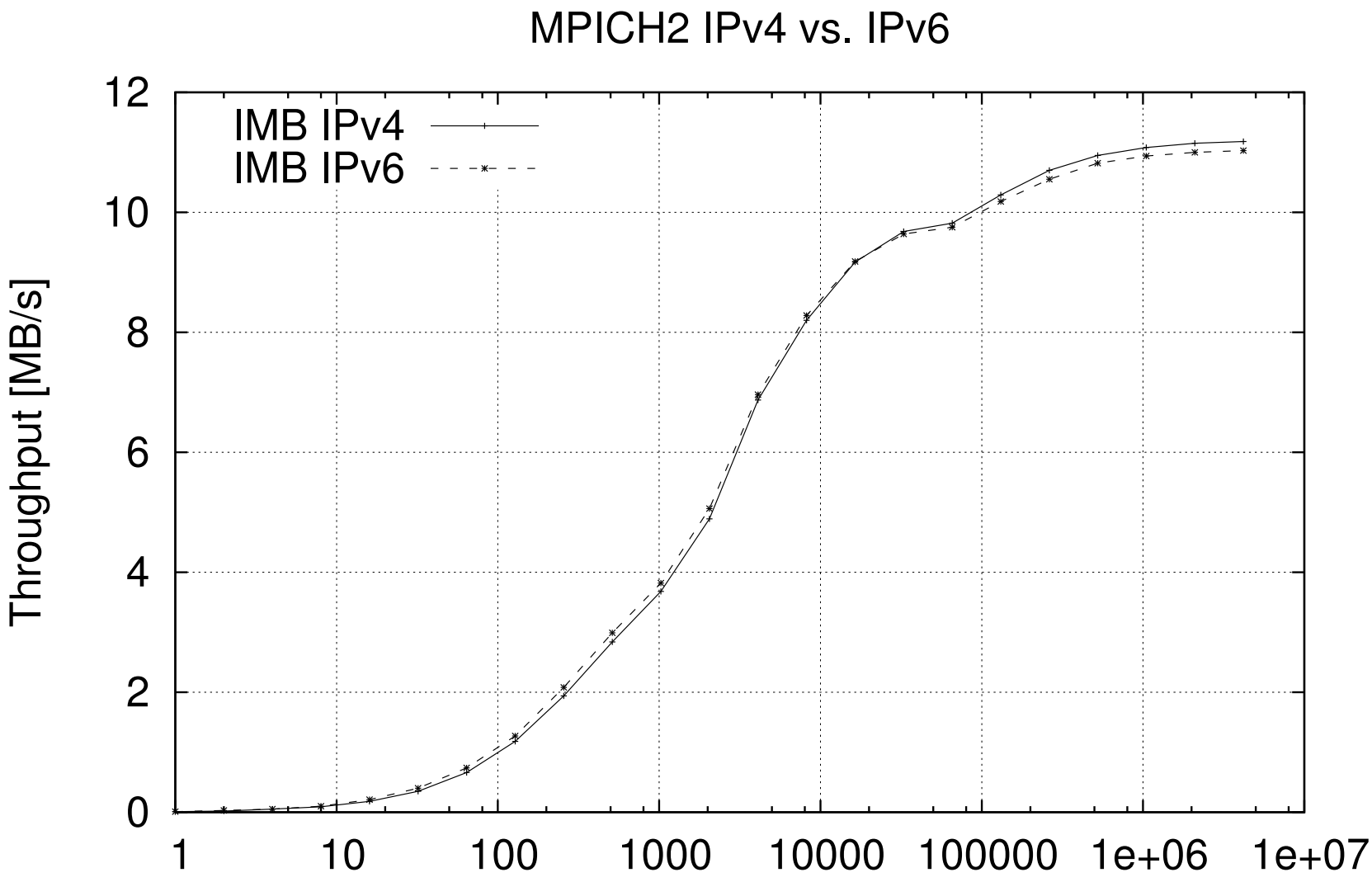
- Ermöglicht zukünftige Protokollerweiterungen
- Standard IPv6 Header ist von fester Länge (40 Byte)
  - Ermöglicht effektive Paketbehandlung beim Routing
- End-to-End [ ] und Hop-by-Hop Header [ ] je nach Funktionalität eingebracht und von den entsprechenden Systemen (Endsystemen bzw. Router) behandelt



Zusammenfassung IPv6

1. **Wieviel Platz braucht man für eine IPv6-Adresse?**
   128 Bit Adressen
2. **Welcher Adresstyp ist neu**
   Anycast
3. **Wie lautet der Präfix von Multicast-Adressen?**
   FF
4. **Wie groß ist der Overhead bei der Verwendung von IPv6 verglichen mit IPv4, wenn Sie die minimalen Paketgrößen betrachten?**
   IPv4: 20 Byte minimaler Header
   IPv6: 40 Byte Basis-Header
5. **Welchen Design-Vorteil besitzt IPv6?**
   erweiterbares Protokoll dank flexibler Extension-Header
6. **Was bedeutet „IPv6 unterstützt Sicherheitsziele von Haus aus“?**
   IPsec ist zwingend vorgeschrieben.
7. **Welche Unterschiede gibt es zwischen IPv4 und IPv6?**
   128 Bit-Adressen, Fragmentierung ist Ende-zu-Ende, MTU von 1280 Bytes

Vergleich: Bandbreite IPv4 und IPv6



Bandbreite von MPICH2 über IPv4 und IPv6.

Subnetzgröße für IPv6 beträgt mindestens: $2^{64}(1,8 \times 10^{18}$ **Hosts) – Größe durch die Interface ID abgesteckten Host-Anteils der IP-Adresse**

- Derzeitige Wurmattacken verwenden z.B. Hostscans, um mögliche Angriffsziele zu identifizieren.

Hostscan in einem IPv6 Subnetz:

- Bei angenommener Gleichverteilung von 10.000 Hosts in diesem Adressraum und 1 Million Anfragen pro Sekunde dauert es durchschnittlich 17 Jahre bis der erste Host gefunden wird.

Aber Angriff wird erleichtert, falls:

- Host-ID auf Basis MAC-Adresse
- Manuell konfigurierte Host-ID, die leicht zu erinnern ist (::10, ::20, eingebettete IPv4-Adresse usw.)
- IPv6 unterstützt well-known Multicast Adresses (RFC 2375): all routers (FF05::2), all DHCP Server (FF05::3)
- Namensauflösung über DNS

Angriffe werden trivial, falls der Angreifer lokalen Zugriff hat:

- IPv6 unterstützt well-known Multicast Adressen (RFC 2375): All-Nodes (FF02::1), All-Routers (FF05::2), All-DHCP Server (FF05::3)
- Absetzen eines gefälschten Routing Advertisements und Sniffen der Anfragen zur Duplicate Address Detection (DAD)

R. Hinden, S. Deering: *IP Version 6 Addressing Architecture* RFC 4291 (Obsoletes: 3513), February 2006

Link-lokale Adressen FE80::/10

- Jeder Link benötigt mindestens eine Link-lokale Adresse!
- werden nicht geroutet!
- Aktueller Ansatz: 64-Bit Präfix und eindeutiger Anteil aus MAC Adresse (IEEE 802.3) konstruiert.

10	54	64
1111 1110 10	00 : 0000 :: 0000	Eindeutiger Anteil

Wie bekomme ich diese unhandlich langen Adressen konfiguriert?

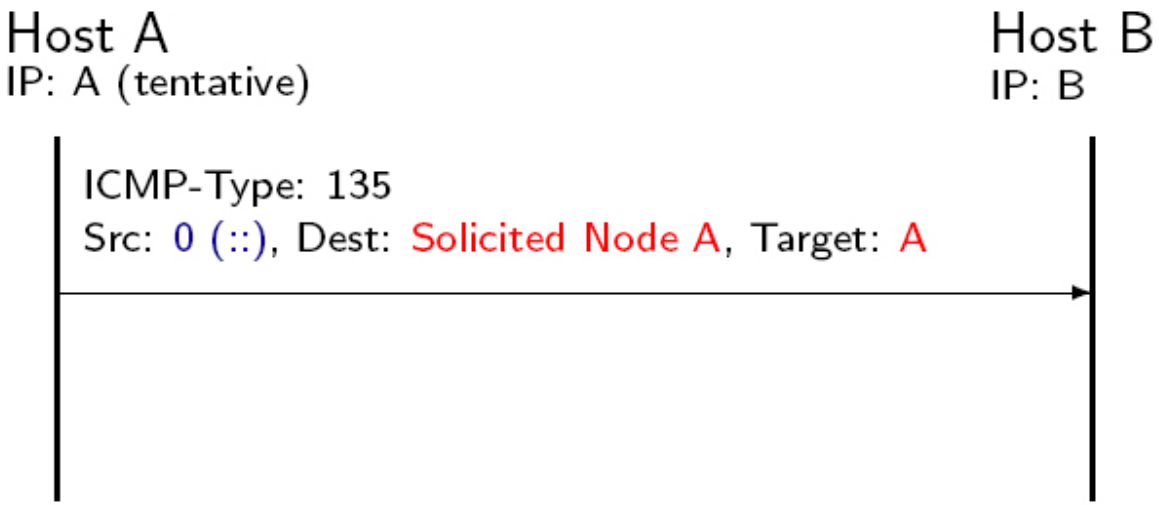
1. statische Adressen
2. Dynamic Host Configuration Protocol (DHCPv6): zentrales Adressmanagement beim DHCP-Server, kann auch Adressen von Diensten wie DNS-Servern bekannt machen
3. Stateless Address Autokonfiguration:
   Ein Rechner erzeugt sich eine IPv6 Adresse aus einer Prefix-Information, die er in der Router Discovery Phase erhalten hat. Dann testet er die erzeugte Adresse im Netzwerk auf Eindeutigkeit.
   $\Longrightarrow$ neu in ICMPv6

ICMPv6

The ICMPv6 protocol is a central protocol for the deployment and use of IPv6. It provides a number of functions that, either did not exist in IPv4, or where provided through other protocols:

- Stateless Address Autoconfiguration and Router Discovery
- L2-address resolution through the ICMPv6 Neighbour Discovery Protocol (NDP). IPv4 uses the ARP protocol on Layer 2.
- Determination of reachability and parameters of the transmission path: Echo Request/Response, Path MTU Discovery.
- Management of multicast group membership through the Multicast Listener Discovery und Multicast Router Discovery. IPv4 uses here the IGMP protocol.

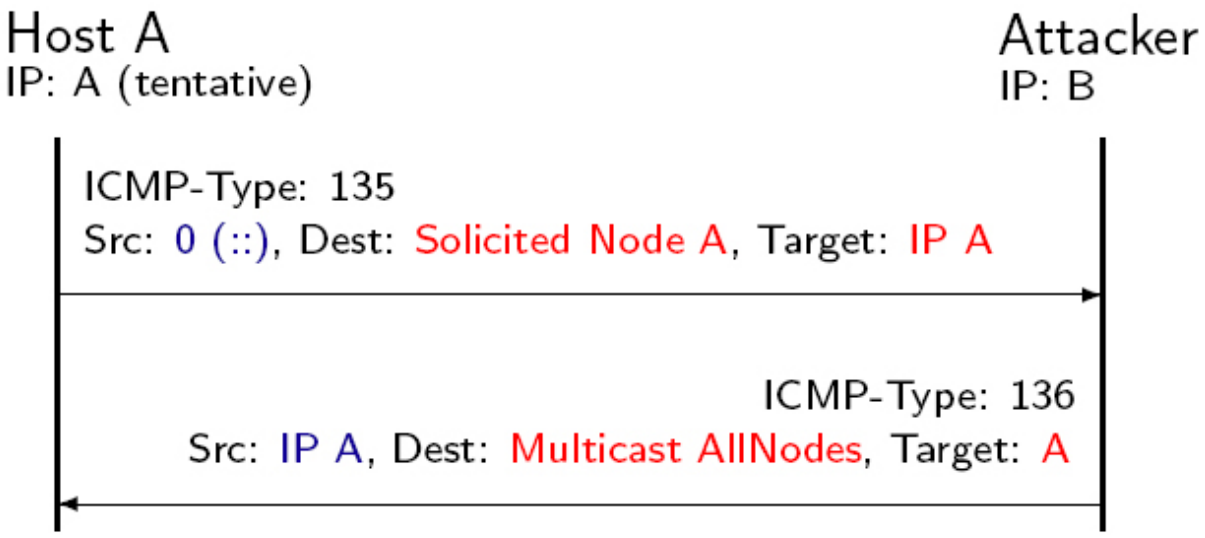
Duplicate Address Detection



- If the IPv6-Address generated by Host A is already used on the link, it can not be assigned to the interface.
- Given the large address space and the particular address generation mechanism this is a very unlikely event.

Duplicate Address Detection - DOS

DoS-Attack against Duplicate Address Detection



An attacker falsely and repeatedly answers the DAD-Request from Host A. The attacker effectively denies Host A the configuration of a valid IPv6 address.

Abhilfe: Authentifizierte Neighbour Discovery Message (AH-Header gemäß RFC 2402)

Problem: Tracable Internet-Users

Da die MAC-Adresse global eindeutig ist, folgt:
$\Rightarrow$ Die Interface ID ist global eindeutig.
$\Rightarrow$ Endsystem kann im gesamten Internet "getract" werden!
$\Rightarrow$ Verletzung der Privatsphäre des Nutzers, der mit dem Endsystem identifiziert wird. Mobilität und Aktivität des Nutzers können erfaßt werden.

RFC3041 "Privacy Extensions for Stateless Autoconfiguration"

- Pseudo-zufallsbasiertes Erzeugen der Interface ID (via MD5) mit temporärer Gültigkeit
- Auswirkungen auf DNS und Fehlerverfolgung
- Bereits in neueren Betriebssystem-Versionen integriert (z.B. bei Windows Default-Einstellung)
- Die Anwendung der Privacy Extensions ist besonders im Fall der Netzmobilität sinnvoll, um die Verfolgung von Endsystemen bei Providerwechsel und nomadischer Nutzung zu erschweren.

Zusammenfassung: Sicherheitsrisiken von IPv6

- **Was ist ein Sicherheitsvorteil des großen Adreßraums?**
  Hostscans sind ggf. erschwert.
- **Was sind neue Features von ICMPv6?**
  Stateless Address Autoconfiguration, Router Discovery, Path MTU Discovery, ...
- **Welche wesentliche Netzwerkkomponente ist von diesen Veränderungen betroffen?**
  Firewalls müssen neu konfiguriert werden.
- **Welchen Angriff ermöglicht die Stateless Address Autoconfiguration?**
  DOS-Attacke durch falsches Beantworten der Duplicate Address Detection Nachricht.
- **Wieso ist der Einsatz von IKE und IPv6 (bisher noch) mangelhaft?**
  IKE unterstützt keine Multicast-Nachrichten.
- **Wieso war in der ursprünglichen IPv6-Spezifikation ein Routing Header vorgesehen?**
  Nostalgie.

Zusammenfassung

+ IPv6 bringt einen größeren Adressraum
+ Extension-Header-Konzept ermöglicht Protokollerweiterungen
+ Ende-zu-Ende-Fragmentierung
+/- Fehler bei der Spezifikation (Routing Header, Verwendung der MAC-Adresse als Teil der IPv6-Adresse) sind mittlerweile ausgebügelt
+/- vergleichbare Performance von IPv4 und IPv6
+/- IPv6 ist nicht sicherer als IPv4!
- Längere IPv6-Adressen bleiben unhandlich!

Herausforderungen

- Aktualisieren bzw. Ersetzen aktueller Hardware wie z.B. Netzrouter, Drucker
- Training der Systemadministratoren
- Defizite bei IPv6-fähigen Netzwerkmanagement-Tools
- Firewallkonfigurationen müssen angepaßt werden (siehe ICMPv6, RFC 4890, 2007)
- ICMPv6 ist wesentlich von ICMPv4 verschieden. Neue Ansätze bergen neue Sicherheitsrisiken.
- Während der Transition von IPv4 zu IPv6 muß IPv4 und IPv6 unterstützt werden $\Longrightarrow$ erweiterte Angriffsfläche :-(
- Aufwand, um Anwendungen IPv6-fähig zu machen

Vinton Cerf, IPv6 Forum Honorary Chairman:

"Take the internet where no other network has been before."