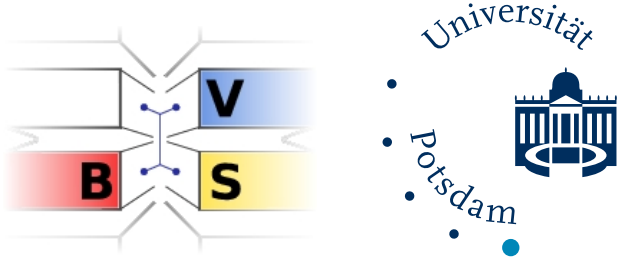
IPv6 – Lehrerfortbildung

Prof. Bettina Schnor

Universität Potsdam
Institut für Informatik
Professur Betriebssysteme und Verteilte Systeme



9.3.2010

Ablauf

I. Theorieteil: Grundlagen (Prof. Dr. Bettina Schnor)

10:00 - 11:30 : Einführung in das IPv6 Protokoll
11:30 - 12:15 : Mittagspause
12:15 - 13:45 : Netzwerksicherheit mit IPv6?

II. Praxisteil: (Jörg Zinke, Klemens Kittan)

14:00 - 15:15 : Mit IPv6 in die weite Welt?
15:15 - 15:30 : Pause
15:30 - 16:00 : IPv6-Programmierung

IPv6–Aktivitäten an der UP

2002: Lehrveranstaltung **IPv6 Showcase**
Prof. Kalkbrenner, Prof. Rebensburg, Prof. Schnor

2004/06: Sven Friedrich, Sebastian Krahmer, Lars Schneidenbach, Bettina Schnor: *Loaded: Server Load Balancing for IPv6*, Proceedings of the International Conference on Networking and Services, Santa Clara, USA.

2005: Lars Schneidenbach, Bettina Schnor: *Migration of MPI Applications to IPv6 Networks*, Proceedings of the International Conference on Parallel and Distributed Computing and Networks, Insbruck.

2008: Adrian Knoth, Christian Kauhaus, Dietmar Fey, Lars Schneidenbach and Bettina Schnor: *Challenges of MPI over IPv6*, Proceedings of the International Conference on Networking and Services 2 (ICNS), (MPICH2/IPv6 und OpenMPI/IPv6).

Was ist eigentlich mit IPv5?

0	Reserved
1	Reserved
2	Unassigned
3	Unassigned
4	Internet Protocol
5	ST Datagram Mode
6	Internet Protocol version 6

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

IPv6 – Motivation

- RFC 1883 (1995), RFC 1887 (1995), RFC 2460 (1998) obsoletes 1883
  Mittlerweile gibt es mehr als 200 RFCs zu IPv6!
- Motivation: "Adreßkrise"
- 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 zwischen verschiedenen Rechner über das Internet ausgetauscht.

In Japan sind Waschmaschinen und Kühlschränke IPv6-fähig.

Aktuelle Bedeutung von IPv6 in Europa

- 27.Mai 2008: **Aktionsplan für die Einführung des neuen Internet-Protokolls IPv6 in Europa**, Kommission der Europäischen Gemeinschaft
- Deutscher IPv6 Rat, gegründet 6.12.2007
- Bundesland Sachsen erprobt IPv6
- DSL Router-Hersteller (e.g. AVM Fritzbox) bieten IPv6-fähige Geräte an.
  CeBIT 2009/10: AVM Fritz!Box (Modelle 7270 und 7390) baut 6to4-Tunnel auf.
- Im Dezember 2009 verkündet der Webhoster Strato, daß er intern auf IPv6 umgestellt hat und wirbt mit IPv6 ready für „Dedicated Server“.
- EU Projekt: „IPv6 security models and dual-stack (IPv6/IPv4) implications“
  1. Workshop am 23.2.2010 in Brüssel diskutiert *„10 promising business and private user scenarios“*

Meinungen zu IPv6

Jens Linke - BLIT'09

Früher oder später wird IPv6 kommen, es ist besser sich in Ruhe in das Thema einzuarbeiten und jetzt schon passende Entscheidungen beim Netzdesign zu treffen.

Jens Linke - BLIT'09

Erst einmal sind IPv4-Adressen noch nicht wirklich knapp. Sie werden nur teurer. Es wurden schon erste kleine ISPs aufgekauft, um an zusätzliche Adressen zu kommen. Der Handel mit IPv4 Adressen hat begonnen. Irgendwann wird es einfach günstiger sein IPv6 einzusetzen.

Bernhard Schmidt - LRZ

Last but not least: Der Imagegewinn für „Early Adopters"!

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 werden in Blöcken von 2 Bytes zusammengefaßt und hexadezimal geschrieben ($8 * 4 = 32$ Hexadezimal-Ziffern):
  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

Beispiel:
2001:DB8:0:0:8:800:200C: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

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.

Ein Interface hat immer

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

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

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

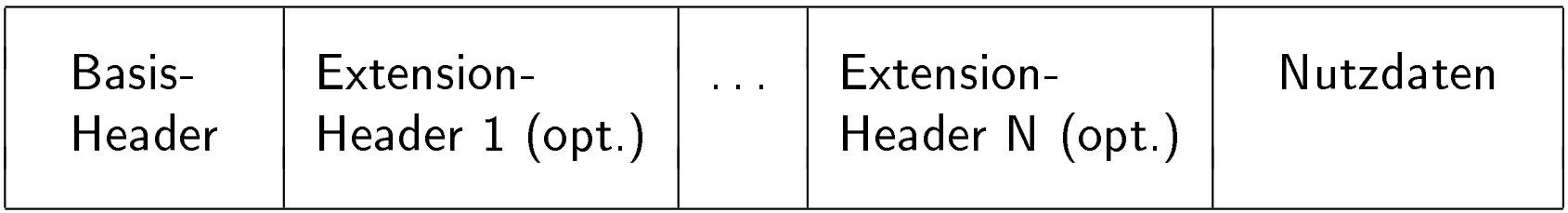
Address type	Binary prefix	IPv6 notation
Unspecified	00...0 (128 bits)	::/128
Loopback	00...1 (128 bits)	::1/128
Multicast	11111111	FF00::/8
Link-Local unicast	1111111010	FE80::/10
Global Unicast	(everything else)	

The address 0:0:0:0:0:0:0:0 is called the unspecified address. It must never be assigned to any node. It indicates the absence of an address. One example of its use is in the Source Address field of any IPv6 packets sent by an initializing host before it has learned its own address.

Es ist vorgesehen, daß jede Site ein /48 bekommt.

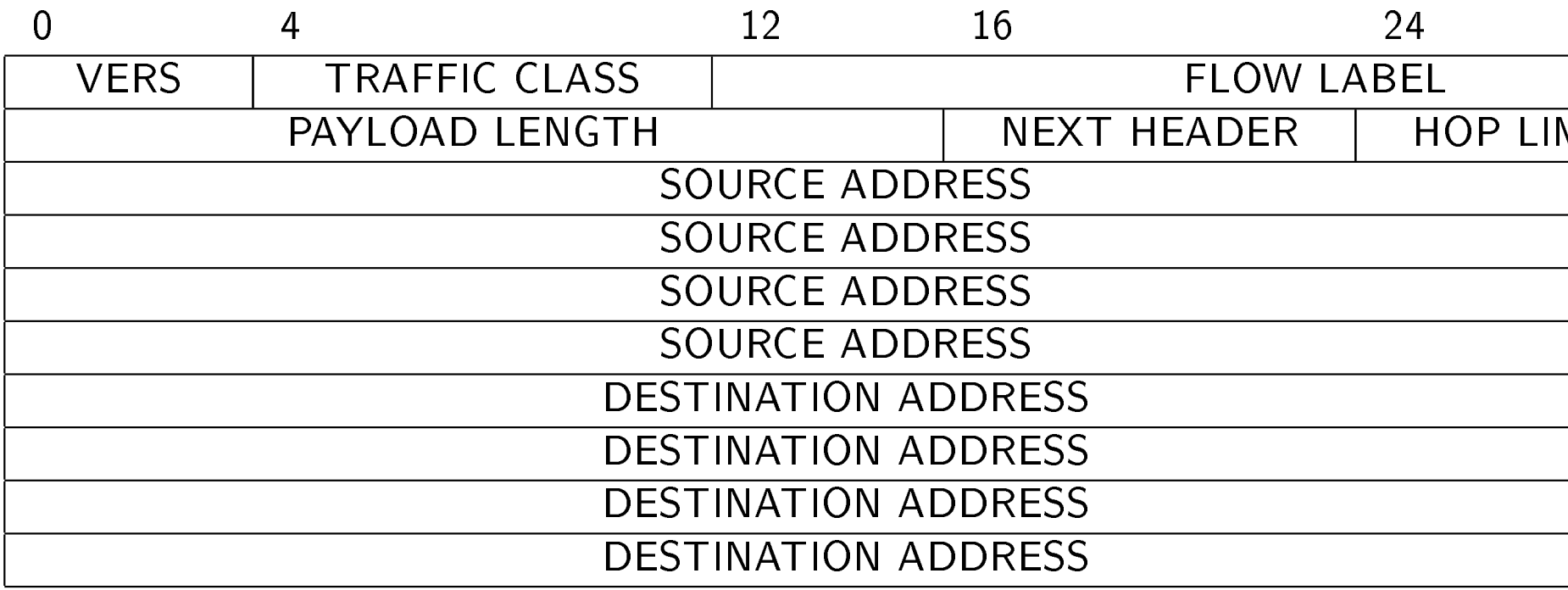
Header-Format

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

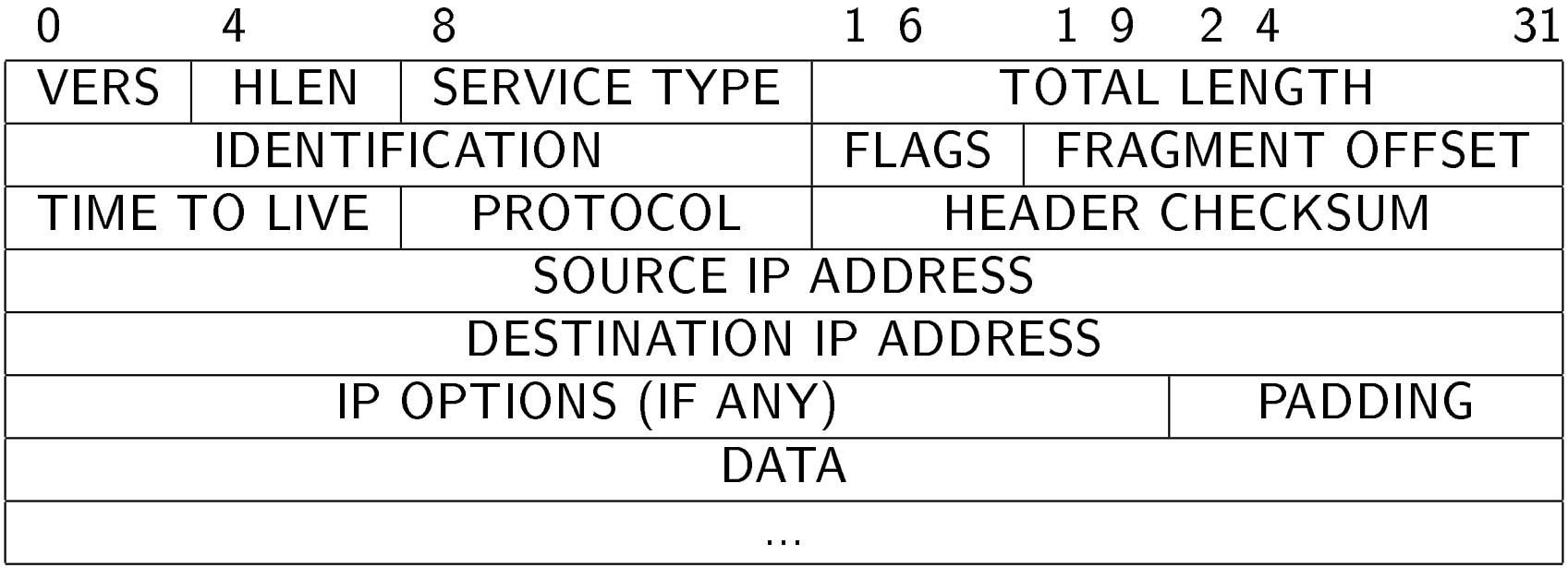


Basis-Header

Der 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: Versionsnummer

TRAFFIC CLASS: Angabe für QoS-Routing

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

NEXT HEADER: Spezifiziert die hinter dem aktuellen Header folgenden Datenart. Dies können Nutzdaten sein oder weitere Header.

HOP LIMIT: ehemals TTL

Zitate aus RFC 2460

Flow Labels:

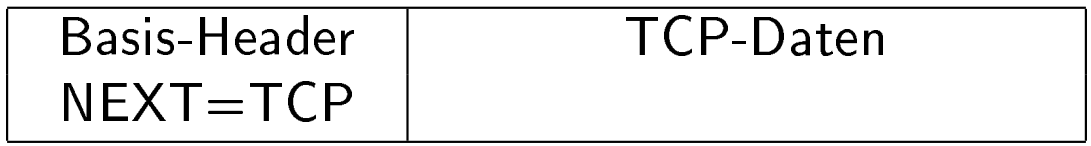
..... This aspect of IPv6 is, at the time of writing, still experimental and subject to change as the requirements for flow support in the Internet become clearer. Hosts or routers that do not support the functions of the Flow Label field are required to set the field to zero when originating a packet, pass the field on unchanged when forwarding a packet, and ignore the field when receiving a packet.

Traffic Classes

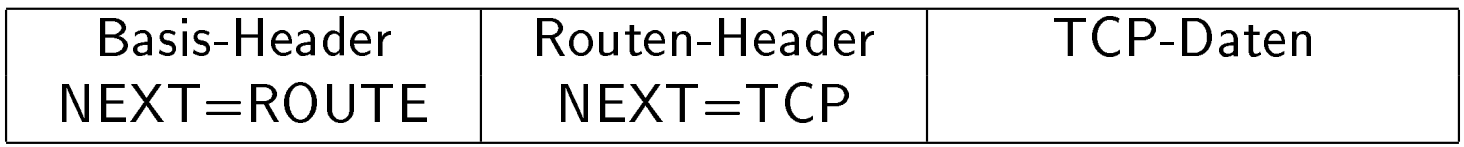
The 8-bit Traffic Class field in the IPv6 header is available for use by originating nodes and/or forwarding routers to identify and distinguish between different classes or priorities of IPv6 packets. At the point in time at which this specification is being written, there are a number of experiments underway in the use of the IPv4 Type of Service and/or Precedence bits to provide various forms of "differentiated service" for IP packets, other than through the use of explicit flow set-up.

Zwei Beispiele für ein IPv6-Datagramms

(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.



Extension-Header

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

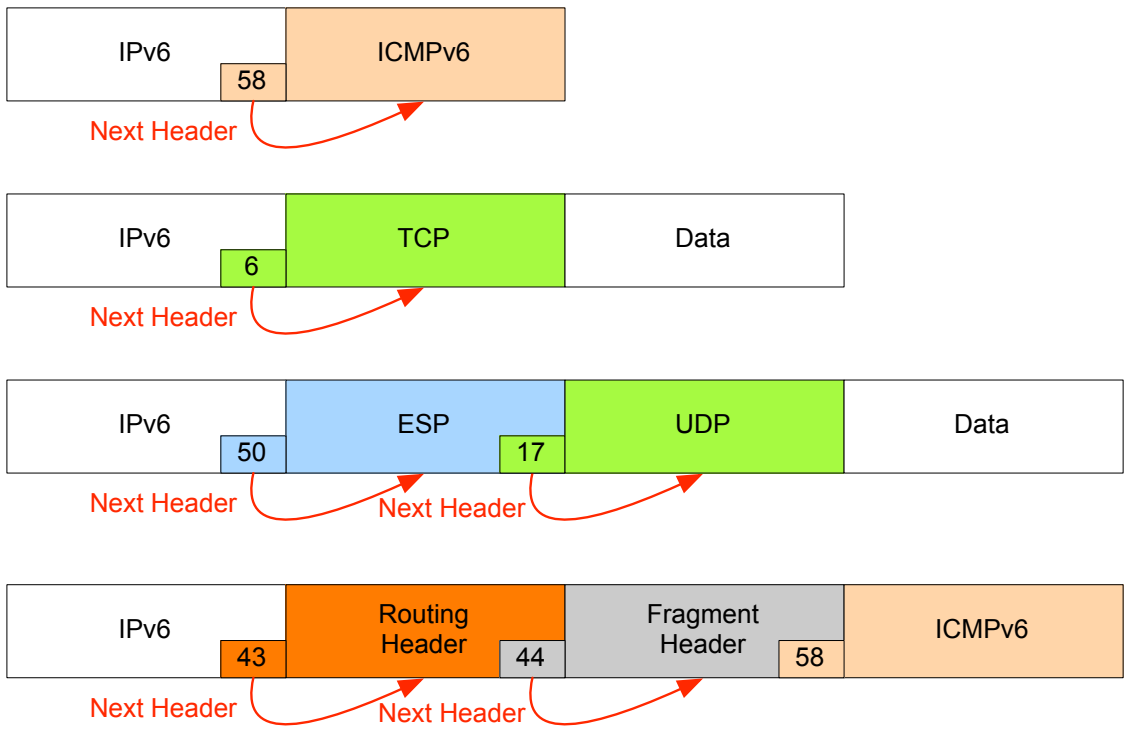
The first four are specified in RFC-2460; the next two are specified in RFC-2402 and RFC-2406 (IPsec), respectively.
Each extension header should occur at most once, except for the Destination Options header which should occur at most twice (once before a Routing header and once before the upper-layer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

Hop-by-Hop Options header: The Hop-by-Hop Options header is used to carry optional information that must be examined by every node along a packet's delivery path. The only hop-by-hop options defined in RFC 2460 are the Pad1 and PadN options for padding.

Routing header: The Routing header is used by an IPv6 source to list one or more intermediate nodes to be "visited" on the way to a packet's destination. This function is very similar to IPv4's Loose Source and Record Route option.

Fragment header: The Fragment header is used by an IPv6 source to send a packet larger than would fit in the path MTU to its destination. Unlike IPv4, fragmentation in IPv6 is performed only by source nodes, not by routers along a packet's delivery path.

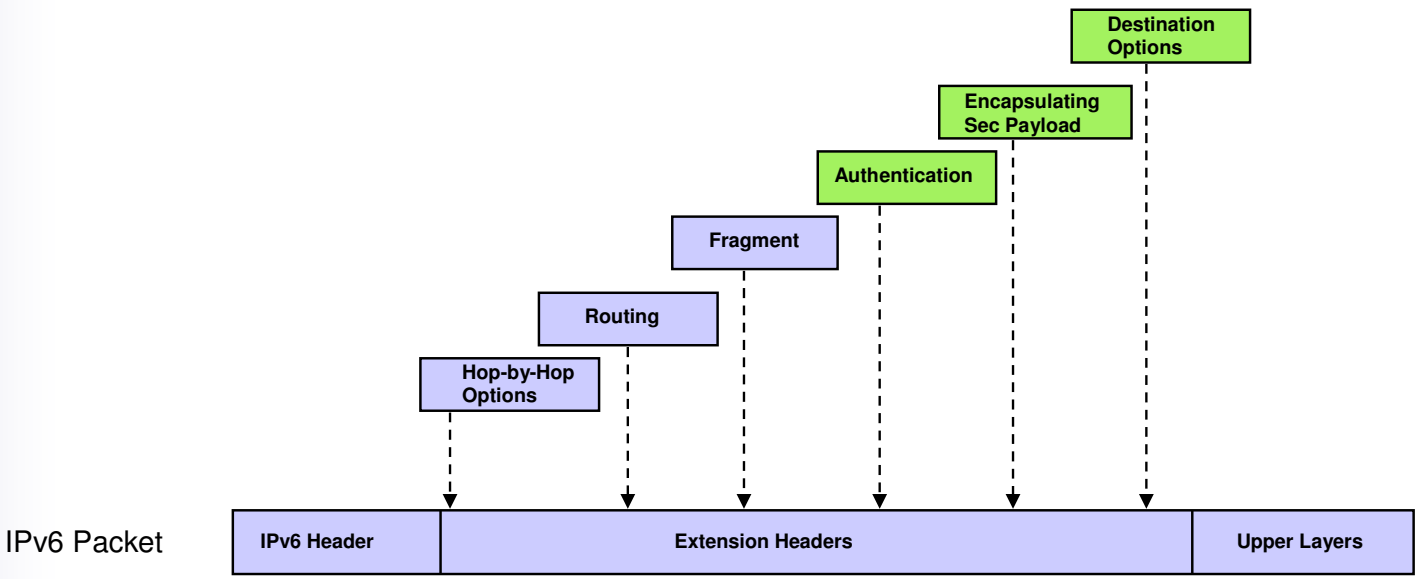
IPv6 Extension Header



Netzwerksicherheit IPv6 - IPsec

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



Extension Header Order

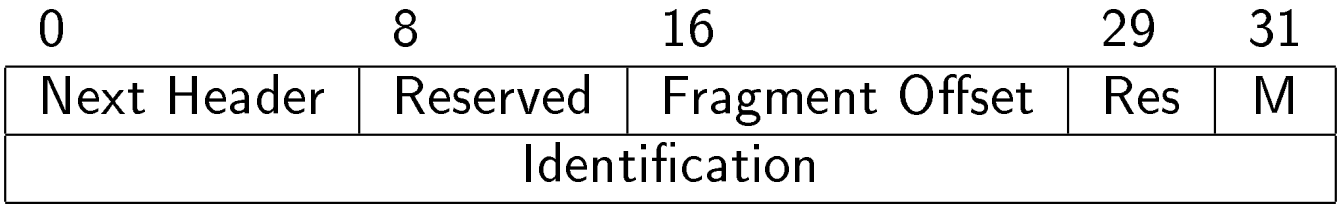
When more than one extension header is used in the same packet, it is recommended that those headers appear in the following order:

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.

Fragmentation Header Format

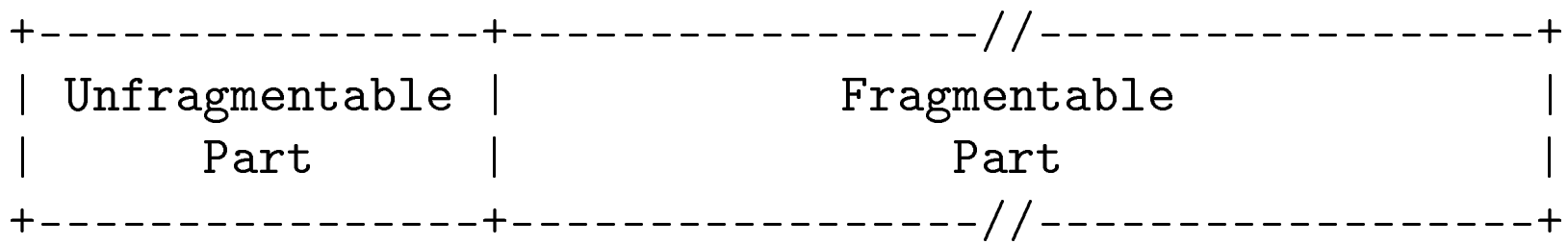


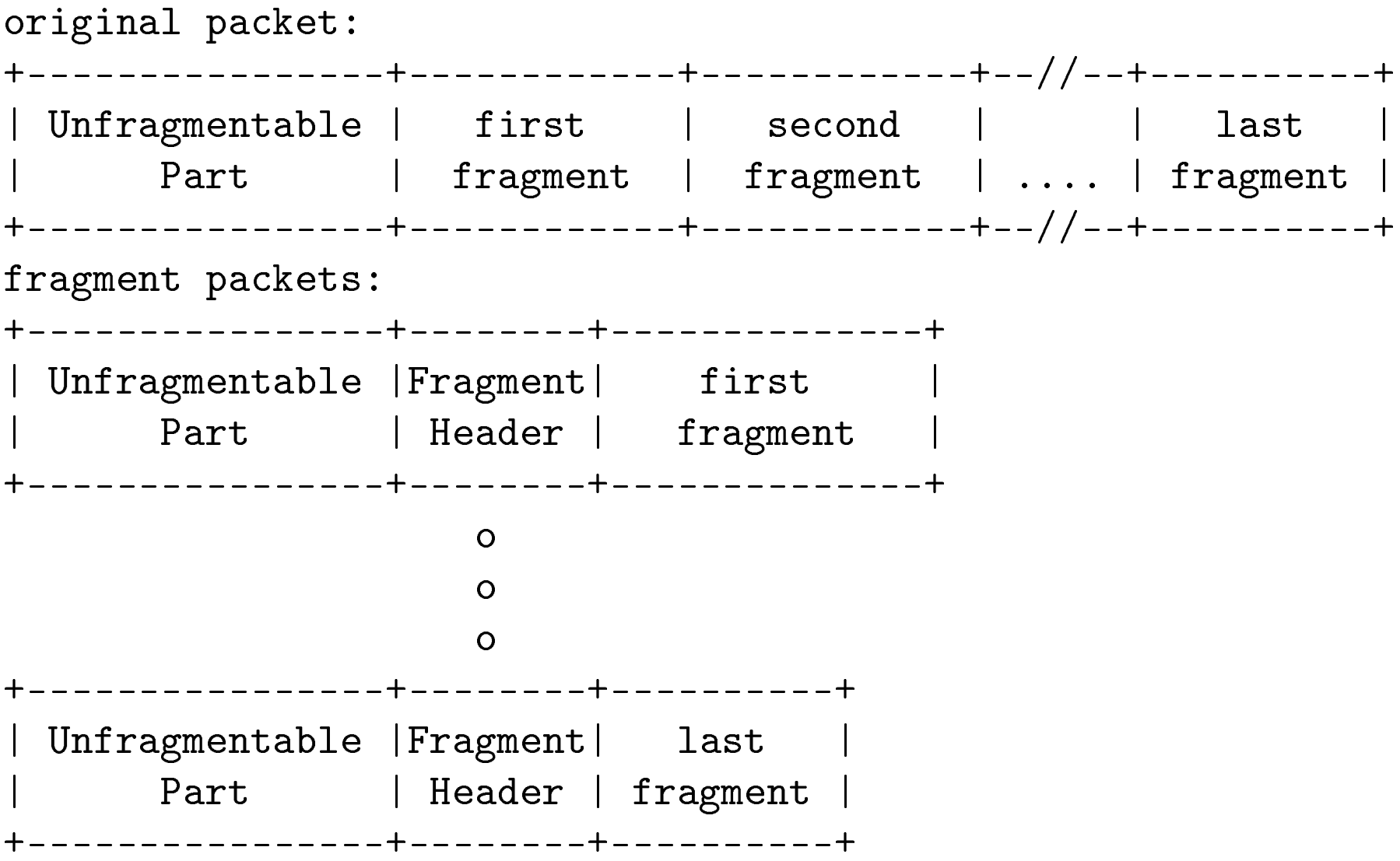
Reserved, Res: 8-bit resp. 2-bit reserved field. Initialized to zero for transmission.

Fragment Offset: The offset, in 8-octet units, of the data following this header.

M flag: 1 = more fragments; 0 = last fragment.

The initial, large, unfragmented packet is referred to as the "original packet", and it is considered to consist of two parts, as illustrated:




original packet:
Unfragmentable Part
first fragment
second fragment
....
last fragment
fragment packets:
Unfragmentable Part
Fragment Header
first fragment
Unfragmentable Part
Fragment Header
last fragment

IPv6 requires that every link in the internet have an 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.

- Wieviel Platz braucht man für eine IPv6-Adresse?
- Welcher Adresstyp ist neu, wird aber noch nicht unterstützt?
- Wie lautet der Präfix von Multicast-Adressen?
- Wie groß ist der Overhead bei der Verwendung von IPv6 verglichen mit IPv4, wenn Sie die minimalen Paketgrößen betrachten?
- Welchen Design-Vorteil besitzt IPv6?
- Wieso unterstützt IPv6 Sicherheitsziele „von Haus aus“?
- Welche Unterschiede gibt es zwischen IPv4 und IPv6?

Zusammenfassung IPv6

- **Wieviel Platz braucht man für eine IPv6-Adresse?**
  128 Bit Adressen
- **Welcher Adresstyp ist neu, wird aber noch nicht unterstützt?**
  Anycast
- **Wie lautet der Präfix von Multicast-Adressen?**
  FF
- **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
- **Welchen Design-Vorteil besitzt IPv6?**
  erweiterbares Protokoll dank flexibler Extension-Header
- **Wieso unterstützt IPv6 Sicherheitsziele „von Haus aus“?**
  IPsec zwingend vorgeschrieben
- **Welche Unterschiede gibt es zwischen IPv4 und IPv6?**
  128 Bit-Adressen, Fragmentierung ist Ende-zu-Ende, MTU von 1280 Bytes

Aufgabe: Migration von IPv4 zu IPv6

aktuelle Dual-Stack-Lösungen

Anwendungsszenarien

EU Projekt: „IPv6 security models and dual-stack (IPv6/IPv4) implications“
1. Workshop am 23.2.2010 in Brüssel diskutiert ***„10 promising business and private user scenarios“***

- **E-Government:** Voting, tax declaration, car registration, Petition for a Referendum, ...
  + IPv6 removes the need for several NAT levels: This could faster the development and deployment of e-government applications on a large scale.
- **Mobile User:** The user is on a trip and is roaming between different access networks and service providers. He is interested in session continuity using Mobile IPv6.
  + The secure bootstrapping process of the mobility service and the required interfaces and messages (e.g. between the Home Agent, Network Access Server, and Authentication and Authorization Server) are only standardized for Mobile IPv6. With IPv4 inflexible and inefficient manual configuration would be rquired.

- **Public Safety:** Public Safety organizations call for advanced communication possibilities, e.g. exchange of videos, pictures, documents, messages, etc.
  + With IPv4, NAT boxes hinder the internetworking between different organizations and the deployment of end-to-end protocols, e.g. security protocols and real-time applications (e.g. VoIP and video streaming)
- **Direct secure end-to-end communication:** Extend the Mobile phone experience (voice and SMS) to all IP services
  + end-to-end communication may be of interest for phone operators
  ... provided some billing model
  + Mobile IPv6 (MIPv6) support
- **Corporate networks:** Corporate networks are evolving from border-protected sets of internal resources and users to an extended enterprise architecture with mobile users. ...

- **Personal Area Networks (PAN):** Users carry several devices (phone, laptop, sensors, input devices) with short range communication capabilities (Bluetooth, 802.15.4), one of the devices may provide acess to the Internet (via WLAN).
  + IPv6 provides a natural solution for mobile networks via Mobile IPv6
- **Access Security:** Deployment of Secure Neighbor Discovery can provide authentication of infrastructure elements and additional trust in the neighboring environment.

Der Standard IEEE 802.15.4 beschreibt ein Übertragungsprotokoll für Wireless Personal Area Networks (WPAN).
Charakteristisch für die Knoten eines IEEE 802.15.4 Netzes sind die langen Ruhephasen, wodurch ein Knoten die meiste Zeit in einem energiesparenden Betriebszustand verweilen kann. Sobald er Daten senden oder empfangen möchte, kann er in lediglich 15 ms aufwachen, anschließend die Kommunikation abwickeln und sich wieder schlafen legen. Dadurch können batteriebetriebene Netzknoten typische Laufzeiten von sechs Monaten bis zu zwei Jahren erreichen.

- **Car-to-Car communication:** e.g. exchange of sensor measurements to avoid traffic jam nad accidents, communication with Internet for infotainment, communication with car manufacturer for maintenance
  + car 2 car communication consortium (C2C-CC) considers only IPv6
  + End-to-end transparency for security protocols (e.g. IPsec) and applications without the requirement for deploying NAT traversal technology.
- **Home network connectivity and Networked gaming**
  + IPv6 comes with IPsec
- **Collective Transport:** Collective transport (e.g. plane) provide Internet connection to passengers, airplane applications and aircraft applications using NEMO.
  + planning reliability: extended lifetime compared to IPv4

Network Mobility (NEMO)

The growing use of IP devices in portable applications has created the demand for mobility support for entire networks of IP devices. Network Mobility (NEMO) solves this problem by extending Mobile IP.
Devices on a mobile network are provided with uninterrupted Internet access even when the network changes its attachment point to the Internet. The Internet Engineering Task Force (IETF) has already created a set of NEMO protocols to provide basic NEMO functionality on both IPv4 and IPv6. The first set of NEMO implementations are available on several platforms including BSD variants, Linux, and Cisco Systems routing equipment.
NEMO works through the use of a Home Agent and Mobile Router. MRs bind themselves to a HA when away from their home networks. HAs then forward all packets destined to a mobile network to that network's MR through a tunnel. Reverse traffic is tunneled back to the HA for delivery to a Correspondent Node. IETF defined this protocol as the NEMO Basic Support Protocol in RFC 3963 (2005).

Ein Blick auf IP Security (IPsec)

- IPsec ist zwingend vorgeschrieben für IPv6 und optional für IPv4.
- Ein spezielles IP-Komprimierungsprotokoll erlaubt die Komprimierung der Daten vor der Verschlüsselung.
- Sämtliche kryptographischen Algorithmen können ausgehandelt werden.
- Die Schlüsselverteilung und das Aushandeln der kryptographischen Verfahren erfolgt durch ein externes Protokoll. Derzeit wird das Internet Key Exchange (IKE) Protokoll für diesen Zweck favorisiert.
- IPsec wird derzeit hauptsächlich zum Aufbau von sicheren Tunneln eingesetzt, mit denen virtuelle private Netze (VPNs) realisiert werden.

Literatur: Ralf Spenneberg: *VPN mit Linux*, Addison-Wesley, 2004.
(Grundlagen + praktische Umsetzung mit `racoon` und `isakmpd`)

IPsec stellt zwei Betriebsarten zur Verfügung:

1. Im Transport Mode werden IP Pakete zwischen zwei Rechnern durch IPsec gesichert. Daten werden als Klartext von der IPsec Implementation entgegengenommen und gesichert über das Internet zum Zielsystem übertragen. Dort werden die Daten wieder als Klartext den Applikationen zugänglich gemacht.
2. Im Tunnel Mode wird zwischen zwei Gateways ein sicherer Tunnel aufgebaut, über den beliebiger Datenverkehr durch IPsec gesichert übertragen werden kann.

Die IPsec-Dienste werden von zwei Protokollen zur Verfügung gestellt:
Das ESP-Protokoll (Encapsulating Security Payload) dient der

- Verschlüsselung der Nutzdaten,
- Datenintegrität,
- (Authentifikation des Absenders) und
- dem Schutz gegen Replay-Attacks.

Das AH-Protokoll (Authentication Header) dient nur der

- Datenintegrität,
- Authentifikation des Absenders und
- dem Schutz gegen Replay-Attacks.

Datenintegrität wird durch einen Message Authentication Code (MAC) geprüft.

Jedem IP-Paket werden ein oder mehrere IPsec-Header (AH- oder ESP-Header) hinzugefügt.

AH-Protokoll (Authentication Header)

- RFC 2402 (November 1998) schreibt HMAC-MD5 und HMAC-SHA-1 vor.
  (HMAC := Der Initialwert für die Kompression wird durch den Schlüssel verändert.)
- Port 51
- Der Sender berechnet den MAC-Wert für das gesamte Paket, d.h. für die Daten des IP- und AH-Headers sowie für die Nutzdaten des IP-Pakets; ausgenommen sind Felder, die sich während der Übertragung ändern. Diese werden bei der Berechnung auf Null gesetzt.
- IP-Fragmentierung erfolgt nach der MAC-Berechnung. $\Longrightarrow$ Fragmente müssen vor der Überprüfung wieder zusammengesetzt werden.

ESP (Encapsulating Security Payload)

- RFC 2406 (November 1998) schreibt vor, daß jede Implementation
  - HMAC-MD5 und HMAC-SHA-1
  - DES und Tripel-DES im CBC-Modus

  unterstützen muß.
- Port 50
- Im Gegensatz zum AH-Header erstreckt sich die MAC-Berechnung nur auf den ESP-Header, die Nutzdaten und einen Teil des ESP-Trailors (IP-Header wird nicht geprüft).

Jedes IPsec-Endsystem bzw. IPsec-Gateway verwaltet die Informationen über die anzuwendenden Verfahren und Schlüssel in einer Security Association (SA) genannten Datenstruktur.

SAs werden pro Zielknoten bzw. Zielnetz vergeben und durch einen 32-Bit Security Parameter Index (SPI) zusammen mit der IP-Adresse des Zielknotens eindeutig identifiziert. SAs werden in der Security Association Database (SAD) gespeichert.

Eine Security Association (SA) enthält folgende Informationen:

- die Authentifikationsverfahren und Schlüssel für das AH-Protokoll,
- die Verschlüsselungsverfahren und Schlüssel für das ESP-Protokoll,
- Die Angaben über den potentiell erforderlichen Initialisierungsvektor IV, diese Information wird nur für das ESP benötigt,
- die Lebensdauer der Schlüssel bzw. der ganzen SA sowie
- die IP-Adresse desjenigen Endsystems bzw. Subsystems, auf das sich die Vereinbarungen der SA beziehen. Gelten die SA-Festlegungen für mehrere Empfänger, so kann dies auch die Adresse eines ganzen Netzes oder Teilnetzes sein.
- Falls die Kommunikationspartner eine Multi-Level Sicherheitsstrategie implementieren, enthält die SA auch die Sicherheitsklassifikation (confidential, secret, unclassified) der zu schützenden Daten

Granularitätsstufen für Schlüsselvergabe:

1. Host-oriented: Es wird ein einziger Schlüssel für alle Verbindungen zu einem Zielknoten benutzt.
2. User-oriented: Es wird ein Schlüssel pro Benutzer benutzt, d. h. zwischen den verschiedenen Anwendungen eines Benutzers wird nicht unterschieden.
3. Verbindungsorientiert: Für jede logische Verbindung des Benutzers wird ein eigener Schlüssel benutzt.

Aushandeln der SA und benötigte Schlüssel:

- statisch
- manuell
- z. B. IKE

SAs werden gemäß einer festgelegten Sicherheitsstrategie erzeugt.
Die Security Policy Database (SPD) verwaltet die Strategiespezifikation,
d. h. Regeln für kommende und gehende Pakete.

Internet Key Exchange (IKE)

- Allgemeines Protokoll zum Aushandeln von Sicherheitsverfahren
- RFC 2409 (November 1998)
- RFC 2407 definiert, welche Bedeutung die Sicherheitsattribute und Datentypen haben, die in IKE-Nachrichten ausgetauscht werden.
- RFC 4306 (Dezember 2005) IKE Version 2:
  nicht kompatibel mit IKE Version 1, bisher nicht weit verbreitet
- IKE wird benutzt, falls für ein abzusendendes Paket keine SA existiert, aber es einen SPD-Eintrag gibt, der die Anwendung von IPsec fordert.
- Zur Berechnung gemeinsamer geheimer Schlüssel wird das Diffie-Hellman Verfahren eingesetzt.

IKE arbeitet in 2 Phasen:

- IKE stellt in einem ersten Schritt einen sicheren Kanal zwischen zwei IKE Implementation her, d.h. es werden SAs für die IKE-Nachrichten ausgehandelt.
  - Aggressive Mode: (3 Nachrichten) - Identität wird preisgegeben, keine Aushandlung der Schutzklassen
  - Main Mode: (6 Nachrichten) - Identität wird geschützt, verschiedene Schutzklassen aushandelbar
- Dieser sichere Kanal wird in der zweiten Phase für den vertraulichen und authentifizierten Austausch von Informationen zur Erzeugung von SAs benutzt.

- Wie kann man mittels IPsec Masquerade-Angriffe verhindern?
- Ist IPsec ein Vorteil von IPv6?
- Sollten ESP- bzw. AH-Header Hop-by-Hop oder Ende-zu-Ende angewandt werden?
- Welche Gefahr geht von Replay-Attacken aus, die Pakete mit IPsec-Headern benutzen?
- Für welche Betriebsart (Transport Mode oder Tunnel Mode) ist die Schlüsselverteilung weniger aufwendig?
- Was ist Voraussetzung für den Aufbau einer sicheren Verbindung zwischen 2 IKE-Instanzen?

Zusammenfassung

- **Wie kann man mittels IPsec Masquerade-Angriffe verhindern?**
  Bei einem Masquerade-Angriff schickt der Angreifer ein Paket mit gefälschter IP-Adresse. Dies kann durch das AH-Protokoll verhindert werden, da damit das gesamte IP-Paket geprüft wird inklusive IP-Header mit IP-Adressen.
- **Ist IPsec ein Vorteil von IPv6?**
  Nein, die IPsec-Protokolle funktionieren auch mit IPv4.
- **Sollten ESP- bzw. AH-Header Hop-by-Hop oder Ende-zu-Ende angewandt werden?**
  Beides sind Ende-zu-Ende-Protokolle, ansonsten wären sie angreifbar für Man-in-the-Middle-Attacken. Im Tunnel Mode sind die Endpunkte aber die Gateways.
- **Welche Gefahr geht von Replay-Attacken aus, die Pakete mit IPsec-Headern benutzen?**
  Kann zu einer DOS-Attacke (Denial of Service) werden, da sowohl das Berechnen der Prüfsummen als auch das Entschlüsseln der Nachricht rechenaufwendig ist.
  Daher enthalten die IPsec-Header ein Feld Sequenznummer. Die Verwendung ist aber optional!

- **Für welche Betriebsart (Transport Mode oder Tunnel Mode) ist die Schlüsselverteilung weniger aufwendig?**
  Tunnel Mode
- **Was ist Voraussetzung für den Aufbau einer sicheren Verbindung zwischen 2 IKE-Instanzen?**
  Pre-Shared Keys oder eine PKI für die IKE-Instanzen.

Das war bisher nur die halbe Wahrheit!

Zusammenfassung: Sicherheitsrisiken von IPv6

- **Was ist ein Sicherheitsvorteil des großen Adreßraums?**
- **Was sind neue Features von ICMPv6?**
- **Welche wesentliche Netzwerkkomponente ist von diesen Veränderungen betroffen?**
- **Welchen Angriff ermöglicht die Stateless Address Autoconfiguration?**
- **Wieso ist der Einsatz von IKE und IPv6 (bisher noch) mangelhaft?**
- **Wieso war in der ursprünglichen IPv6-Spezifikation ein Routing Header vorgesehen?**

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.

Herausforderungen

- Aktualisieren bzw. Ersetzen aktueller Hardware wie z.B. Netzrouter, Drucker
- Aufwand, um Anwendungen IPv6-fähig zu machen
- Defizite bei IPv6-fähigen Netzwerkmanagement-Tools
- Training der Systemadministratoren
- Firewallkonfigurationen müssen angepaßt werden (siehe ICMPv6)
- 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 :-(

„Never change a running system!?“