**Inhaltsverzeichnis**

[1 Geschichte und Entstehung 2](#_Toc497656493)

[2 Vergleich IPv4 und IPv6 2](#_Toc497656494)

[2.1 Gründe für IPv6 2](#_Toc497656495)

[2.2 Schreibweise und Adressaufbau 2](#_Toc497656496)

[2.2.1 Komatible und abgebildete IPv6 Adressen 4](#_Toc497656497)

[2.2.2 MAC zu IPv6 5](#_Toc497656498)

[2.3 Adresszuweisung und Adressstrukturen 5](#_Toc497656499)

[3 Der IPv6 Header 6](#_Toc497656500)

[3.1 Extension Headers 6](#_Toc497656501)

[3.2 Routing Header 7](#_Toc497656502)

[3.3 Fragmentierungsheader 7](#_Toc497656503)

[4 Sicherheit 7](#_Toc497656504)

[4.1 Security Architecture for IP (IPsec) 7](#_Toc497656505)

[4.2 Encapsulating Security Payload (ESP) 7](#_Toc497656506)

[4.3 Authentification Header (AH) 7](#_Toc497656507)

[5 IPv6 Autokonfiguration (SLAAC) 7](#_Toc497656508)

[6 Mobile IP 8](#_Toc497656509)

# 1 Geschichte und Entstehung

IPv6 befindet sich in Schicht 3 des OSI-Schichtenmodells. Es ist für die Vermittlung von

Datenpakete, Adressierung von Netzknoten und -stationen, sowie die Weiterleitung von

Datenpakete zwischen Teilnetzen zuständig.

Seit 1998 steht IPv6 bereit und wurde hauptsächlich wegen der Adressknappheit und

verschiedener Unzulänglichkeiten von IPv4 entwickelt. Es wurde von der Internet Engineering

Taskforce (IETF) eingeführt und war früher auch unter Internet Protocol next Generation (IPng)

bekannt.

Es gab ein experimentelles IPv5 (ST-2, Internet Stream Protocol Version 2), welches für

Echtzeitdatenströme genutzt werden sollte. ST-2 ist nun durchs RSVP (Resource Reservation

Protocol) zur Bandbeirtenanforderung bei Routern ersetzt worden.

# 2 Vergleich IPv4 und IPv6

Eine IPv6-Adresse hat eine Länge von 128 Bit. Diese Adresslänge erlaubt eine unvorstellbare Menge von 2128 IPv6-Adressen. Das sind rund 340 Sextillionen Adressen. Bei IPv4 spricht man von rund 4,3 Milliarden Adressen.

Der Adressraum von IPv6 reicht aus, um umgerechnet jeden Quadratmillimeter der Erdoberfläche inklusive der Ozeane mit rund 600 Billiarden Adressen zu pflastern. Weil man mit dieser großen Menge an Adressen verschwenderisch umgehen darf, spart man sich eine aufwendige Verwaltung, wie es bei IPv4-Adressen notwendig ist. Damit ist genügend Raum, um möglichst viele Netzwerk-Topologien abzubilden. Außerdem entfällt die Subnetzmaske

## 2.1 Gründe für IPv6

* größerer Adressraum (Adressknappheit bei IPv4, ausgeschöpft seit 2011)

*Wichtig für die Wahrung des Ende-zu-Ende Prinzips (NAT=Verletzung)*

*Der Anwender erhält bei IPv6 nicht nur einen einzige IP-Adresse, sondern einen global eindeutigen IP-Adressraum für ein ganzes Teilnetz*

* mehrere IPv6 Adressen pro Host (unterschieldliche Gültigkeitsbereiche)
* Autokonfiguration möglich

*Zustandsbehaftetes DHCP Verfahren wird überflüssig (jetzt zustandslos)*

* IPsec Verschlüsselung

*Verschlüsselung und Authentizität von IP-Paketen wird ermöglicht*

* Quality of Service und Multicast Unterstützung
* Vereinfachung der Protokollrahmens

*Entlastet Router von Rechenaufwand, Kopfdaten optimiert*

* Versendung von bis zu 4GB Paketen möglich (Jumbograms)
* Mobile IP

## 2.2 Schreibweise und Adressaufbau

Im Gegensatz zu anderen Adressen hat ein IPv6-Host mehrere IPv6-Adressen, die

unterschiedliche Gültigkeitsbereiche haben. Die verbindungslokale IPv6-Adresse ist nur im lokalen Netzwerk gültig und wird nicht geroutet. Die globale IPv6-Adresse ist über das lokale Netzwerk hinaus im Internet gültig.

Die vorderen 64 Bit sind der Präfix bzw. Network-ID. Vereinfacht ausgedrückt, ist das die IPv6-Adresse des Subnetzes, in dem sich ein Host befindet. Die hinteren 64 Bit werden als Interface Identifier (IID) bezeichnet. Das ist der Host-Adressanteil einer IPv6-Adresse.

C:\Users\Pascal\Documents\SYP\Referat_IPv6\ipv6 adressnotation.gif

Für den Interface Identifier der IPv6-Adresse wird typischerweise die MAC-Adresse des Netzwerk-Interfaces herangezogen. Da MAC-Adressen weltweit eindeutig sind, entsteht somit eine weltweit eindeutiger Interface Identifier.

Um die Bedenken bezüglich Datenschutz und Privatsphäre zu zerstreuen hat man Privacy Extensions eingeführt. **Privacy Extensions** erzeugen regelmäßig einen zufälligen Interface Identifier, der keinen Rückschluss auf die MAC-Adresse und damit den Host zulässt.

Die textuelle Notation von IPv6-Adressen ist in Abschnitt 2.2 von RFC 4291 (= Standard von IETF) beschrieben:

*Die folgenden Schreibweisen sind Repräsentationen der gleichen IPv6-Adresse.*

2001 : 0db8 : 0000 : 0000 : 0001 : 0000 : 0000 : 0001

2001 : db8 : 0 : 0 : 1 : 0 : 0 : 1

2001 : 0db8 : 0000 : 000 : 1 : 00 : 0 : 1

2001 : db8 : : 0 : 1 : 0 : 0 : 1

2001 : db8 : 0 : 0 : 1 : : 1-

2001 : DB8 : 0 : 0 : 1 : : 1

2001 : db8 : : 1 : 0 : 0 : 1

Die einzige korrekte Schreibweise nach den verbindlichen Notationsregeln in RFC 5952 ist die letzte. Um zu viele unterschiedliche Schreibweise zu vermeiden wurden folgende verbindliche Notationsregeln in RFC 5952 definiert:

* Alle alphabetischen Zeichen werden grundsätzlich klein geschrieben.
* Alle führenden Nullen eines Blocks werden grundsätzlich weggelassen.
* Ein einzelner 4er Nullerblock wird zu einer "0" zusammengefasst.
* Aufeinanderfolgende 4er Nullerblöcke werden durch zwei Doppelpunkte ("::") gekürzt.
* Sind mehrere gleichwertige Kürzungen möglich, ist die erste von Links beginnend zu wählen.

Beispiel der Adressstruktur für eine globale Unicast Adresse:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 3 Bit | 13 Bit | 8 Bit | 24 Bit | 16 Bit | 64 Bit |
| FP (001) | TLA | Res. | NLA | SLA | Interface |

**FP**  Identifiziert das Protokoll.

**TLA Top Level Aggregation**

werden benutzt, um auf höchster Ebene der Routing-Hierarchie Organisationen unterscheiden zu können, die dauerhafte Transit-Dienste im Internet anbieten.

Haupttransferrouten im Internet.

**Res** Reserviert für eventuell spätere Verwendung.

**NLA Next Level Aggregation**

identifiziert Provider, welche Adressen den Endverbrauchern zur Verfügung stellen.

**SLA Site Level Aggregation**

Identifiziert das Sub-Netzwerk, welches der Nutzer erhält

**II** Host Adresse für Gerät (Handy, Laptop, …) oder eindeutig zugewiesen

**Adressnotation:**

1. Hexadezimale Notation in Blöcken zu jeweils 16 Bit (4 Ziffern), welche mit Doppelpunkten unterteilt werden: **2001:0db8:85a3:08d3:1319:8a2e:0370:7344**

2. Führende Nullen innerhalb eines Blockes dürfen ausgelassen werden:

**2001:0db8:0000:08d3:0000:8a2e:0070:7344 = 2001:db8:0:8d3:0:8a2e:70:7344**

3. Ein oder mehrere aufeinander folgende Blöcke, deren Wert 0 (bzw. 0000) beträgt, dürfen

ausgelassen werden. Dies wird durch zwei aufeinander folgende Doppelpunkte angezeigt:

**2001:0db8:0:0:0:0:1428:57ab = 2001:db8::1428:57ab**

4. Die Reduktion durch Regel 3 darf nur einmal durchgeführt werden, das heißt, es darf

höchstens eine zusammenhängende Gruppe aus Null-Blöcken in der Adresse ersetzt werden. Die Adresse **2001:0db8:0:0:8d3:0:0**:0 darf demnach entweder zu **2001:db8:0:0:8d3::** oder **2001:db8::8d3:0:0:0** gekürzt werden; **2001:db8::8d3::** ist unzulässig, da dies mehrdeutig ist und fälschlicherweise z. B. auch als **2001:db8:0:0:0:8d3:0:0** interpretiert werden könnte. Es empfiehlt sich den Block mit den meisten Null-Blöcken zu kürzen.

5. Ebenfalls darf für die letzten vier Bytes (also 32 Bits) der Adresse die herkömmliche dezimale Notation verwendet werden. So ist **::ffff:127.0.0.1** eine alternative Schreibweise für **::ffff:7f00:1.** Diese Schreibweise wird vor allem bei Einbettung des IPv4-Adressraums in den IPv6-Adressraum verwendet.

URL-Notation von IPv6-Adressen:

In einer URL wird die IPv6-Adresse in eckige Klammern eingeschlossen, z. B.:

<http://[2001:0db8:85a3:08d3:1319:8a2e:0370:7344]/>

Netz-Notation von IPv6-Adressen:

Dazu werden die erste Adresse (bzw. die Netzadresse) und die Länge des Präfixes in Bits getrennt durch einen Schrägstrich notiert. Subnetzgröße muss einer 2er Potenz entsprechen.

**2001:0db8:1234::/48** für das Netzwerk mit den Adressen **2001:0db8:1234:0000:0000:0000:0000:0000** bis **2001:0db8:1234:ffff:ffff:ffff:ffff:ffff**

### 2.2.1 Komatible und abgebildete IPv6 Adressen

Die ersten 6 Blöcke (96 Bits) müssen immer 0 sein. Deshalb sieht eine kompatible Adresse so

aus: **0:0:0:0:0:0:212.204.101.210 bzw. ::212.204.101.210**

Kompatible Adressen werden dazu verwendet, um auszudrücken, ob ein Interface sowohl über IPv4 als auch über IPv6 kommunizieren kann. Der Switch schneidet die 6-0-Blöcke ab für IPv4 oder fügt sie für IPv6 hinzu.

Die ersten 5 Blöcke (80 Bits) müssen immer 0 sein. Der 6. Block (16 Bits) muss FFFF entsprechen. Deshalb sieht eine abgebildete Adresse so aus:

**0:0:0:0:0:FFFF:212.204.101.210 bzw. ::FFFF:212.204.101.210**

Werden verwendet um in einem Netzwerk, in dem sowohl das IPv4 als auch das IPv6-Protokoll genutzt wird, die Interfaces zu identifizieren, die das IPv4-Protokoll nutzen können.

Diese Methode ist aber nur beschränkt möglich. Sie funktioniert nur bei Tunnelverbindungen.

### 2.2.2 MAC zu IPv6

Mac Adresse: **00:80:41:ae:fd:7e**

1111 1111 1111 1110 (Hexadezimal: FFFE) einfügen

**00:80:41:ff:fe:ae:fd:7e**

**0080:41ff:feae:fd7e** *(in Notation gebracht)*

Ersten beiden Zahlen (00) in binär = 00000000

7. Bit von links invertieren = 00000010 = 2

Einsetzen: **280:41ff:feae:7d7e**

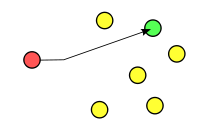
Formatpräfix: **fe80::280:41ff:feae:7d7e**

... Formatpräfix für Link-Local-Adressen (Adressierung von Knoten in abgeschlossenen

Systemen)

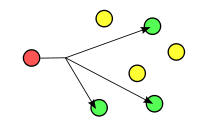
## 2.3 Adresszuweisung und Adressstrukturen

Unicast

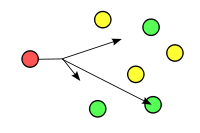
Daten werden von einem Endpunkt über einen Knoten zu

genau einem Endpunkt transportiert (one to one).

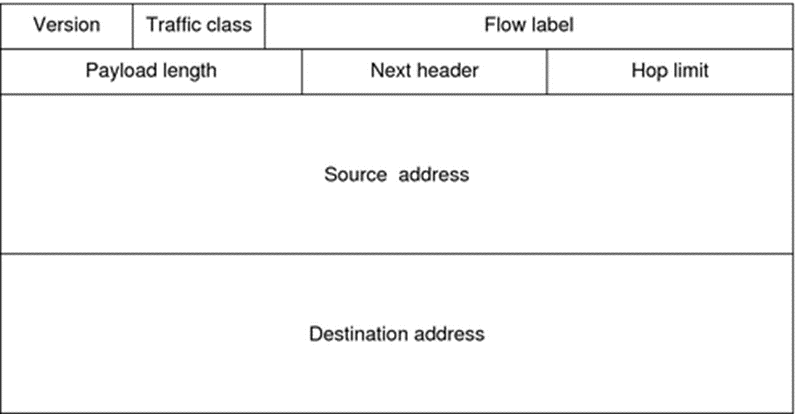
Multicast

Daten werden von einem Endpunkt über einen Knoten zu beliebig vielen Endpunkten in einem Netzwerk oder -segment (Multicast-Domain) transportiert. Der Knoten übernimmt die Verteilung/Duplikation und Weiterleitung der Daten an die interessierten Endpunkte (Empfänger). Der Knoten kennt üblicherweise die interessierten Empfänger anhand der Multicast-Adresse der Endpunkte.

Anycast

Daten werden von einem Endpunkt über einen Knoten zum topologisch am nächsten liegenden Endpunkt transportiert. Der Knoten übernimmt diese Aufgabe.

# 3 Der IPv6 Header



**Version (4 Bit)** = IP-Versionsnummer (6)

**Traffic Class (8 Bit)**

Eine Art Prioritätsvergabe; Das Feld Traffic Class wird zum Unterscheiden der verschiedenen Übermittlungsanforderungen von Paketen benutzt. Zum Bsp. benötigt man für die Übertragung von digitaler Sprache mehr Schnelligkeit und weniger Genauigkeit, im Gegensatz zur Übertragung von Dateien, wo die Genauigkeit wichtiger ist als die Geschwindigkeit.

**Flow Label (20 Bit)**

Ist ein für z.B. Echtzeitanwendungen verwendeter Wert. Pakete, die dasselbe Flow Label tragen, werden gleich behandelt. Kommt ein Paket mit einem anderen Wert als 0 an, können alle Router in ihren Tabellen nachsehen welche spezielle Behandlung gewünscht wird. Systeme die diese Funktion nicht unterstützen müssen dieses Feld auf 0 setzen.

**Payload Length (16 Bit)** Länge des IPv6-Paketinhaltes (ohne Header).

**Next Header (8 Bit)**

Identifiziert den Typ des übergeordneten Headers, dieser kann entweder einen Extension Header oder ein Protokoll höherer Schicht bezeichnen, wie z. B. TCP oder UDP.

**Hop Limit (8 Bit)**

Dieses Feld enthält die Anzahl der verbleibenden weiterleitenden Stationen, bevor das IP-Paket verfällt. Es entspricht dem TTL-Feld von IPv4. Jede Station, die ein IP-Paket weiterleitet, muss von diesem Wert 1 abziehen.**Source Address (128 Bit)** Adresse des Senders

**Destination Address (128 Bit)** Adresse des Empfängers

## 3.1 Extension Headers

Optionale Header-Informationen sind in den sogenannten Extension Headers zwischen Header und Payload untergebracht. Das hat den Vorteil, dass es keine Größenbeschränkung für Optionen gibt und neue Optionen eingeführt werden können ohne den Header zu verändern. Die einzige Grenze liegt darin, dass ein Extension Header im Datenpaket Platz finden muss, was unter Umständen den Platz für den Payload reduziert, weil das IPv6-Paket in seiner Gesamtheit nur eine bestimmte Größe haben darf. Das heißt, Extension Headers verkürzen den Platz für die Nutzdaten.

## 3.2 Routing Header

Routing bedeutet Datenpakete von einem System über verschiedene Netzwerke hinweg zu

einem anderen System zu vermitteln. Der Routingheader wird verwendet um ein Paket, bevor es am Ziel ankommen soll, zu vordefinierten Zwischenknoten zu schicken.

## 3.3 Fragmentierungsheader

Der Fragmentierungsheader wird verwendet, um ein großes Paket in mehrere kleine Pakete

aufzuspalten, über die Leitung zu schicken und am Ende wieder zusammenzufassen.

# 4 Sicherheit

Mit IPv6 ließe sich jedem mit dem Internet verbundenen Gerät eine eigene, dauerhafte und damit unverwechselbare Adresse zuweisen. Und über diese Adresse ließe sich prinzipiell auch Jahre später noch der Nutzer ermitteln und damit feststellen, wann er mit welchem seiner Geräte auf welcher Website zu Besuch war.

In der IPv4-Welt bekam der Nutzer dagegen eine einzige Adresse pro Internetverbindung, die mit jeder neuen Sitzung wechselte. Der deutsche IPv6-Rat will entsprechende Leitlinien zum Datenschutz aufstellen.

## 4.1 Security Architecture for IP (IPsec)

IPsec ist eine Erweiterung des Internet-Protokolls (IP) für Verschlüsselungs- und Authentifizierungsmechanismen. Als Standard auf Netzwerkebene kann IPsec applikationsunabhängig eingesetzt werden (VPN).

Die zentralen Funktionen in der IPsec-Architektur sind das AH-Protokoll (Authentification Header), das ESP-Protokoll (Encapsulating Security Payload) und die Schlüsselverwaltung (Key Management). Authentizität, Vertraulichkeit und Integrität erfüllt IPsec durch AH und ESP.

## 4.2 Encapsulating Security Payload (ESP)

Der "Encapsulating Security Payload"-Header (ESP) sichert in erster Linie die Geheimhaltung, aber mit gewissen Algorithmen kann er zusätzlich auch Integrität und Echtheit der Daten sichern. ESP wird also zu Verschlüsselung des Pakets benötigt.

## 4.3 Authentification Header (AH)

Der Authentification Header (AH) stellt die Datenintegrität von den IP-Protokollen IPv6 und IP Security Protocol (IPsec) durch die Prüfsumme sicher und sorgt für die Authentifizierung des Datenursprungs. Mit AH lässt sich also feststellen, ob die Nachricht von dem angenommenen Absender stammt und ob ihr Inhalt unverändert ist. Der AH schützt den gesamten Nachrichteninhalt durch Verschlüsselung des IP-Paketes.

# 5 IPv6 Autokonfiguration (SLAAC)

Die globale IPv6-Adresse ist mit einer öffentlichen IPv4-Adresse vergleichbar, weil ein Host nur damit über das lokale Netz hinaus eine Verbindungen ins Internet aufbauen kann. Um eine globale IPv6-Adresse zu bekommen, benötigt der IPv6-Host die link-lokale IPv6-Adresse. Der hintere Teil der Adresse besteht aus dem Interface-Identifier und ist somit bei beiden Adressen gleich. Nur der vordere Teil, der Präfix, der muss für die globale Adresse noch ermittelt werden.

IPv6 kennt drei Wege, wie ein Host an eine globale IPv6-Adresse kommen kann. Entweder wird sie manuell konfiguriert, per *Stateless Address Autoconfiguration* (SLAAC) oder wie bei IPv4 per DHCP (DHCPv6) vergeben.

Mit SLAAC bezieht ein IPv6-Host nur den globalen Präfix per Router Advertisement und bildet sich zusammen mit dem bekannten Interface Identifier die globale IPv6-Adresse selber.

Sofern ein DHCPv6-Server eingerichtet ist, kann ein Host die globale IPv6-Adresse auch von dort beziehen, wie man es von IPv4 kennt.

DHCPv6 läuft unter der Bezeichnung Stateful Address Autoconfiguration. Hierbei wird an zentraler Stelle festgelegt, welcher Host, welche IPv6-Adresse bekommt/hat.

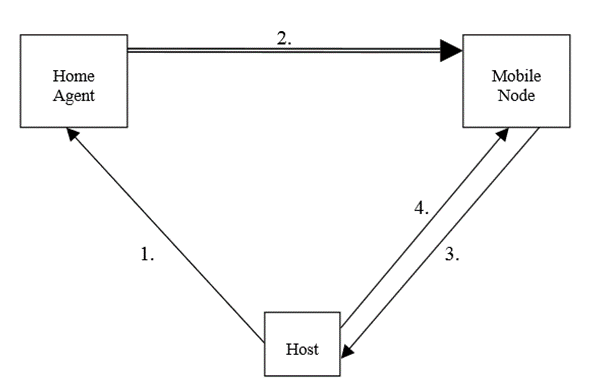
Grundsätzlich gilt, dass ein IPv6-Host seine Adressen per SLAAC selber bilden kann. Er ist dabei nicht auf DHCPv6 angewiesen.

* Zuerst erzeugt sich ein Host eine link-lokale Adresse mit "fe80:..." und dem Interface Identifier, der in der Regel aus der MAC-Adresse gebildet wird.
* Damit ist der Host in der Lage im lokalen Netzwerk zu kommunizieren und besorgt sich damit einen globalen Präfix und bildet sich zusammen mit dem Interface Identifier eine globale IPv6-Adresse. Über diese globale IPv6-Adresse kann ein Host global kommunizieren und auch aus dem Internet erreichbar.
* Ist Privacy Extensions aktiviert, dann wird regelmäßig eine neue, temporär globale IPv6-Adresse mit dem globalen Präfix und einem zufälligen Interface Identifier für ausgehende Verbindungen erzeugt.

# 6 Mobile IP

IPv6 ermöglicht es, sich von einem Netzwerk zu einem anderen zu bewegen, ohne seine TCP/IP-Verbindungen zu verlieren.

Eine Verbindung wird zwischen zwei Knoten hergestellt und basiert auf deren IP-Adresse. Wenn sich ein Knoten in ein anderes Netzwerk bewegt, so ändert sich auch seine IP-Adresse. Ohne Mobile IP würde deshalb die Verbindung abgebrochen, der Knoten wäre nicht mehr über seine ursprüngliche Adresse erreichbar.



1. Host sendet Paket an Heimatadresse des mobilen Knotens.

2. Home Agent (Router im Heimnetzwerk des mobilen Konten) fängt Paket ab und tunnelt es an

Care-of-Adresse (temporäre Adresse, durch die

der Rechner im Fremdnetz ansprechbar ist) des mobilen Knotens.

3. Mobiler Knoten entpackt das Paket und kann Host direkt antworten. (Care-of-Adresse) als

Absender

4. Host speichert Adresse des mobilen Knotens, nachfolgende Kommunikation kann direkt

erfolgen.

# Quellenverzeichnis

<https://www.elektronik-kompendium.de/sites/net/1902131.htm>

<https://www.elektronik-kompendium.de/sites/net/0812201.htm>

<https://www.elektronik-kompendium.de/sites/net/1902111.htm>

<https://www.elektronik-kompendium.de/sites/net/2003011.htm>

<https://de.wikipedia.org/wiki/IPv6>

<https://www.1und1.at/digitalguide/server/knowhow/ipsec-sicherheitsarchitektur-fuer-ipv4-und-ipv6/>

<https://aseith.com/display/KB/Unterschiede+zwischen+Unicast%2C+Broadcast%2C+Multicast+und+Anycast>