

IPv6

Adressaufbau IPv6

IPv6-Adressen bestehen aus 128 Bit und werden üblicherweise in acht Gruppen zu jeweils 16 Bit (4 hexadezimale Zeichen) dargestellt. Das Format sieht so aus:

2001:0db8:85a3:0000:0000:8a2e:0370:7334

BLOCK	BEDEUTUNG
2001	Global Routing Prefix
0db8	Dokumentationsnetz (Beispieladresse)
85a3	Subnetzerkennung
0000:0000	Reservierte Felder
8a2e:0370:7334	Interface Identifier (z.B. MAC-basiert)

Länge:

- 128 Bit → 8 Blöcke zu je 16 Bit (4 Hex-Zeichen)
- Hexadezimale Darstellung mit Doppelpunkten (:) als Trennzeichen

Abkürzungen:

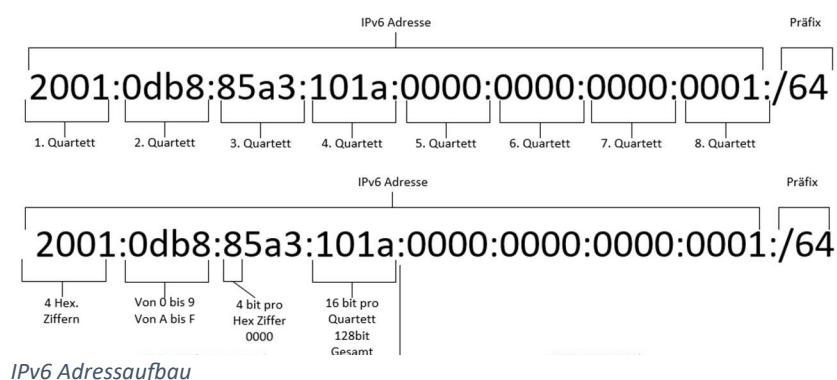
- Führende Nullen in einem Block können weggelassen werden:
 - 2001:db8:85a3:0:8a2e:370:7334
- Längere Folgen von Blöcken mit 0000 können einmalig durch :: ersetzt werden:
 - 2001:db8:85a3::8a2e:370:7334

Typische Struktur:

- Netzwerkpräfix (z. B. erste 64 Bit): Definiert das Netzsegment
- Interface Identifier (letzte 64 Bit): Identifiziert ein Interface eindeutig im Netz (oft automatisch generiert)

Adressarten:

- Unicast: Eindeutige Adresse für ein einzelnes Interface
- Multicast: Kommunikation an eine Gruppe von Interfaces
- Anycast: Eine Adresse, die mehreren Interfaces zugewiesen ist, aber Daten werden nur zum „nächsten“ Knoten geschickt



Adressbereiche

Global Unicast (öffentlich routbar)

- Bereich: **2000::/3**
- Verwendung: Öffentlich erreichbare Adressen im Internet
- Beispiel: **2001:0db8::/32**
- Besonderheit: Entspricht den „normalen“ öffentlichen IPv4-Adressen

Link-Local Adressen

- Bereich: **fe80::/10**
- Verwendung: Kommunikation innerhalb eines lokalen Netzsegments (Layer 2)
- Beispiel: **fe80::1**
- Besonderheit: Wird automatisch auf Interfaces generiert, keine Weiterleitung über Router

Unique Local Addresses (ULA)

- Bereich: **fc00::/7 (effektiv verwendet: fd00::/8)**
- Verwendung: Private Netzwerke (vergleichbar mit IPv4 10.0.0.0/8)
- Beispiel: **fd12:3456:789a::/64**
- Besonderheit: Nicht im Internet routbar, oft für interne Kommunikation

Multicast

- Bereich: **ff00::/8**
- Verwendung: Eine Nachricht an eine Gruppe von Interfaces
- Beispiel: **ff02::1** (alle Nodes im Link)
- Besonderheit: Kein Broadcast in IPv6 → Multicast wird stattdessen verwendet

Loopback-Adresse

- Adresse: **::1**
- Verwendung: Kommunikation mit sich selbst (entspricht IPv4 127.0.0.1)
- Besonderheit: Nur gültig auf dem lokalen Host

Unspecified Adresse

- Adresse: **::**
- Verwendung: Platzhalter, z. B. bei noch nicht konfigurierten Interfaces
- Besonderheit: Dient oft als „keine Adresse vorhanden“

Embedded IPv4 (IPv4-Mapped)

- Bereich: **::ffff:0:0/96**
- Verwendung: Darstellung von IPv4-Adressen in IPv6-Systemen (Transition)
- Beispiel: **::ffff:192.168.1.1**

Reserved / Future Use

- Beispiel: **0000::/8, 100::/64** etc.
- Verwendung: Für zukünftige Zwecke reserviert, teilweise noch ungenutzt

Übersichtstabelle:

ADRESSEBEREICH	PRÄFIX	VERWENDUNG
GLOBAL-UNICAST	2000::/3	Öffentlich routbar
LINK-LOCAL	fe80::/10	Lokales Segment (nicht routbar)
UNIQUE-LOCAL (ULA)	fd00::/8	Privates Netzwerk
MULTICAST	ff00::/8	Gruppenkommunikation
LOOPBACK	::1	Selbstreferenz (localhost)
UNSPECIFIED	::	Keine Adresse vorhanden
IPv-4-MAPPED	::ffff:0:0/96	IPv4-Kompatibilität

Präfixe

IPv6-Prefix-Tabelle:

PRÄFIX	BEREICH / CIDR	BESCHREIBUNG	BEISPIELADRESSE
::/128	1 Adresse	Unspecified Address (noch nicht gesetzt)	::
::1/128	1 Adresse	Loopback Address	::1
::ffff:0:0/96	/96	IPv4-mapped IPv6	::ffff:192.168.1.1
100::/64	/64	Discard-Only Prefix (RFC 6666)	100::
2000::/3	/3	Global Unicast	2001:db8::/32
fc00::/7	/7	Unique Local Address (ULA)	fd12:3456:789a::/64
fe80::/10	/10	Link-Local Address	fe80::1
ff00::/8	/32	Dokumentation/Testnetz (nicht routbar)	2001:db8::1

Präfix-Längen im Routing/Subnetting:

PRÄFIXLÄNGE	BESCHREIBUNG
/128	Einzelne Adresse
/64	Standard für Interface-Identifier / Subnetze
/48	Typisch für größere Kundennetze
/32	Provider- oder ISP-Zuweisung
/56	Kleinere Kundennetze (z.B. Heimnetz)

End-to-End Prinzip

Das End-to-End-Prinzip ist ein zentrales Designprinzip der Netzwerkarchitektur, besonders im Kontext des Internets und Protokollen wie TCP/IP oder IPv6. Es besagt:

Funktionen sollen möglichst in den Endsystemen (Clients, Server) realisiert werden – nicht im Netzwerk selbst (Router, Firewalls, Gateways).

Kernidee:

Nur die Endpunkte der Kommunikation (also z. B. Client und Server) wissen genau, was die Kommunikation bedeutet, und sind daher am besten geeignet, zur Durchführung von Funktionen wie:

- Fehlererkennung und -korrektur
- Datenverschlüsselung
- Datenvollständigkeit
- Wiederherstellung bei Verbindungsabbrüchen

Beispiel:

Dateiübertragung über TCP zwischen 2 Rechnern:

- End-to-End-Prinzip:
Die Endsysteme prüfen, ob alle Daten korrekt angekommen sind (z. B. durch Checksummen, ACKs).
- Nicht im Netzwerk:
Router auf dem Weg kümmern sich nicht darum, ob das Paket vollständig oder korrekt ist – sie leiten es nur weiter.

Warum ist das wichtig?

- Einfachheit im Netzwerk: Router bleiben „dumm“ und schnell.
- Skalierbarkeit: Neue Dienste oder Protokolle müssen nur auf Endsystemen angepasst werden.
- Transparenz: Das Netz kennt keine Details über die Applikationen.
- Endgeräte sind verantwortlich: Fehlerbehandlung, Verschlüsselung etc. erfolgt dort, wo sie gebraucht wird.

Einschränkungen / Herausforderungen

- Firewalls und NAT (v. a. bei IPv4) unterbrechen das End-to-End-Prinzip, da sie Pakete inspizieren oder verändern.
- Sicherheitsanforderungen führen oft dazu, dass Funktionen ins Netzwerk verlagert werden (z. B. DPI, IDS/IPS).
- QoS oder Traffic Shaping widersprechen dem Prinzip in Teilen.

Bezug zu IPv6

IPv6 wurde u. a. entwickelt, um das End-to-End-Prinzip wieder zu stärken:

- Keine NAT nötig (dank global eindeutiger Adressen)
- Direkte Erreichbarkeit der Geräte wird gefördert
- Bessere Voraussetzungen für Peer-to-Peer und VoIP

Adressvergabe

Die Adressvergabe bei IPv6 unterscheidet sich grundlegend von IPv4 und bietet mehrere automatische und manuelle Methoden. Hier ist ein Überblick über die wichtigsten Verfahren:

Manuelle Adressvergabe (Static Configuration)

- Die Adresse wird fest auf dem Gerät konfiguriert.
- Verwendung in Servern, Routern oder wenn feste IPs notwendig sind.

Stateless Address Autoconfiguration (SLAAC)

Am weitesten verbreitet

- Host generiert seine Adresse automatisch, basierend auf:
 - dem vom Router angekündigten Prefix
 - und seiner eigenen MAC-Adresse oder einem zufälligen Wert (Privacy Extensions)
- Kein DHCP nötig

Ablauf:

1. Host hört auf Router Advertisements (RA) via ICMPv6
2. Nimmt z. B. das Präfix 2001:db8:1::/64
3. Fügt seine Interface-ID hinzu → z. B. 2001:db8:1::1234:abcd:5678:9abc

Stateful Address Configuration (DHCPv6)

- Wie bei IPv4: Ein DHCPv6-Server weist Adressen und weitere Netzwerkinfos zu
- Wird verwendet, wenn:
 - vollständige Kontrolle über Adressvergabe nötig ist
 - zusätzliche Konfigurationsinformationen (DNS etc.) verteilt werden sollen
- Typisch in Enterprise-Umgebungen

Temporary Addresses (Privacy Extensions)

- Optionaler Mechanismus zur Wahrung der Privatsphäre
- SLAAC-Adresse wird nicht dauerhaft verwendet, sondern dynamisch generiert
- Reduziert die Rückverfolgbarkeit von Endgeräten

Zusatzfunktionen durch ICMPv6:

- Router Solicitation (RS): Host fragt aktiv nach einem Router
- Router Advertisement (RA): Router teilt Prefixe und Konfigurationshinweise mit

Vergleich der Methoden:

VERFAHREN	AUTOMATISCH	DHCP NÖTIG	GEEIGNET FÜR
MANUELL	✗	✗	Server, statische Netze
SLAAC	✓	✗	Heim- & Unternehmensnetze
DHCPV6	✓	✓	Enterprise-Umgebungen
PRIVACY EXT.	✓	✗	Mobile/Client-Geräte

IPv6 Header

Der IPv6-Header wurde im Vergleich zu IPv4 vereinfacht und optimiert, um effizienteres Routing, bessere Erweiterbarkeit und geringere Verarbeitungszeiten zu ermöglichen.

Aufbau des IPv6-Headers (Fixed Header, 40 Byte)

FELD	GRÖÙE (BITS)	BESCHREIBUNG
VERSION	4	Protokollversion, bei IPv6 immer 0110 (6)
TRAFFIC CLASS	8	Priorisierung von Paketen (QoS, ähnlich wie TOS in IPv4)
FLOW LABEL	20	Markierung für zusammengehörige Pakete (z. B. VoIP-Flows)
PAYLOAD LENGTH	16	Länge des Nutzdatenbereichs (ohne Header) in Byte
NEXT HEADER	8	Gibt das nächste Protokoll an (TCP=6, UDP=17, ICMPv6=58, Extension Header...)
HOP LIMIT	8	Maximale Anzahl Hops (wie TTL bei IPv4)
SOURCE ADDRESS	128	IPv6-Adresse des Absenders
DESTINATION ADDRESS	128	IPv6-Adresse des Empfängers

Was fehlt im Vergleich zu IPv4?

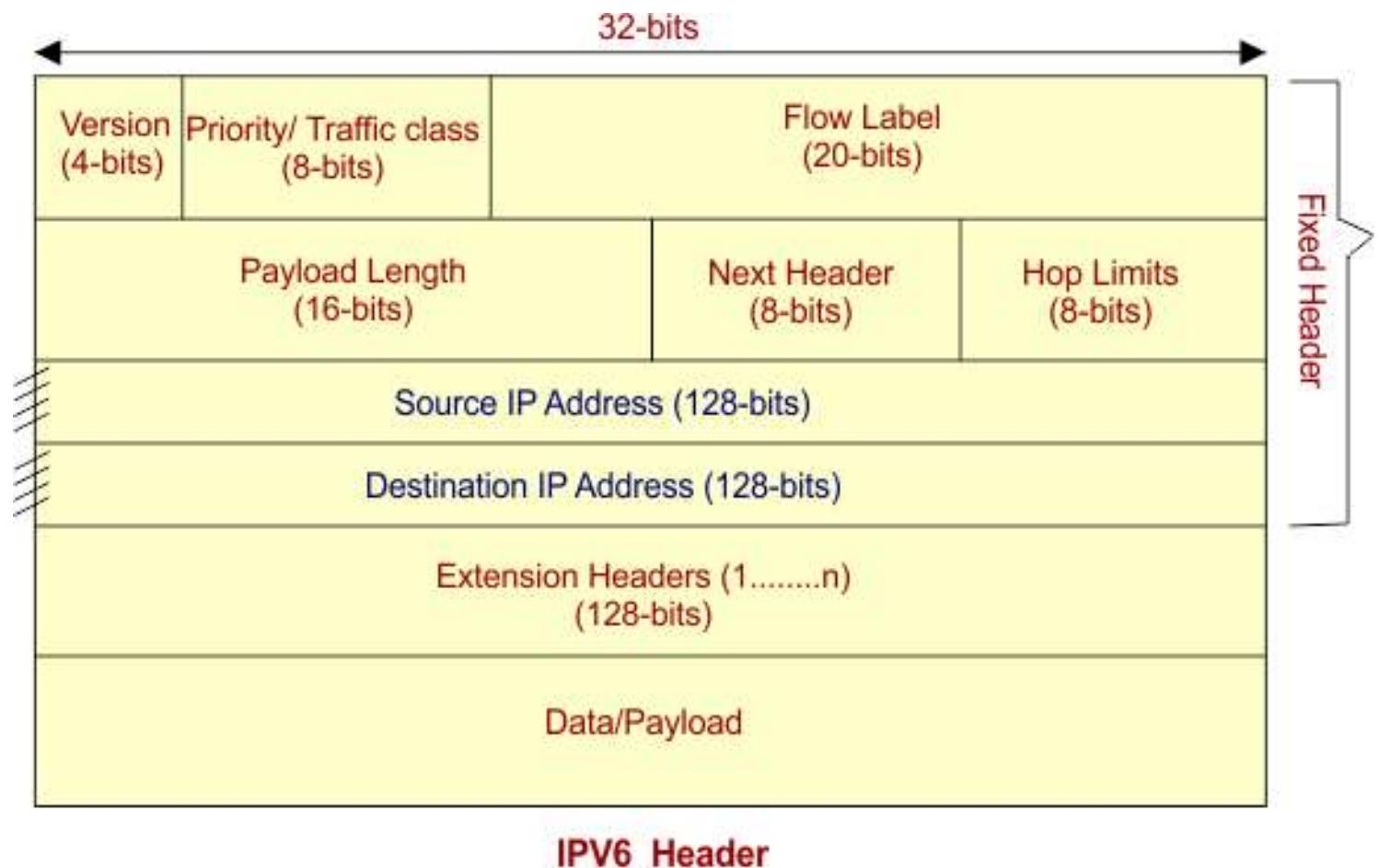
FUNKTION	IPV4	IPV6
FRAGMENTIERUNG	Router & Host	Nur Endsysteme (per Extension Header)
PRÜFSUMMEN IM HEADER	Ja	Nein (Entlastung der Router)
OPTIONEN	Im Header	Über separate Extension Headers

Extension Header Konzept

- IPv6 nutzt optionale Erweiterungs-Header zwischen dem festen Header und dem Nutzdatenprotokoll.
- Beispiele:
 - Routing Header
 - Fragment Header
 - Authentication Header
 - Destination Options Header

Diese Erweiterungen erlauben Flexibilität, ohne den Haupt-Header zu überladen.

Grafische Darstellung eines IPv6-Headers



IPV6 Header