IPv6

Was ist IPv6 und warum brauchen wir es?

IPv6 (Internet Protocol Version 6) ist ein auf Layer 3 stattfindendes Protokoll für die Übertragung und Vermittlung von Datenpaketen in einem paketorientiert arbeitenden Netzwerk wie dem Internet. Es soll das bisher verwendete IP-Protokoll Version 4 (IPv4) ablösen.

Das Internetprotokoll der Version 4 ist in vielen Bereichen veraltet und kann die Anforderungen moderner Netzwerke und netzwerkfähiger Applikationen nicht mehr im gewünschten Maß erfüllen. Es vereinfacht die Einrichtung und den Betrieb und ist direkt nach dem Start eines netzwerktauglichen Gerätes verfügbar. Zustands behaftete Verfahren zur Adressvergabe wie DHCP, die bei IP der Version 4 zum Einsatz kommen, werden überflüssig.

Im Vergleich zu den IP-Adressen der Version 4 mit 32 Bit Länge sind IPv6-Adressen 128 Bit lang. Sie bieten damit einen wesentlich größeren Adressraum und eine Lösung für die Adressknappheit von IPv4-Adressen im Internet.

Beispiel einer IPv6 Adresse

`2001:0000:0000:0000:0080:ACDE:02CE:1234`

- **Acht Gruppen** mit je **16 Bit**, separiert mit Doppelpunkten
- Jede Gruppe hat **vier Hexadezimalzeichen** zu je **4 Bit**

> Jede in einer Gruppe vorausführende Null kann weggelassen werden

Somit würde die IPv6 Adresse wie folgt aussehen:

`2001:0:0:0:80:ACDE:2CE:1234`

> Gruppen aus Nullen können wiederum durch zwei Doppelpunkte dargestellt werden. Dies darf aber nur ein mal angewendet werden. Es können also keine doppelten Paare aus Doppelpunkten verwendet werden!

Schlussendlich sieht unsere IPv6 Adresse dann wie folgt aus:

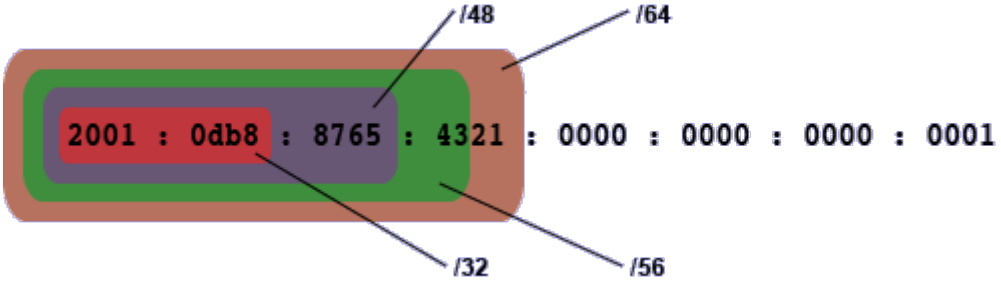
`2001::80:ACDE:2CE:1234`

Unterteilung der Gruppen

2001:0000:0000:0000:0080:ACDE:02CE:1234

2001:0000:0000:0000	Network Prefix (Präfix oder Netz-ID) – Wobei dieses Modell weiter unterteilt werden kann. So können die letzten 8 Bits der Network Prefix die Subnet Prefix angeben.
0080:ACDE:02CE:1234	Interface Identifier (Suffix, IID oder EUI)

Segmentierung: Präfix und Präfixlänge



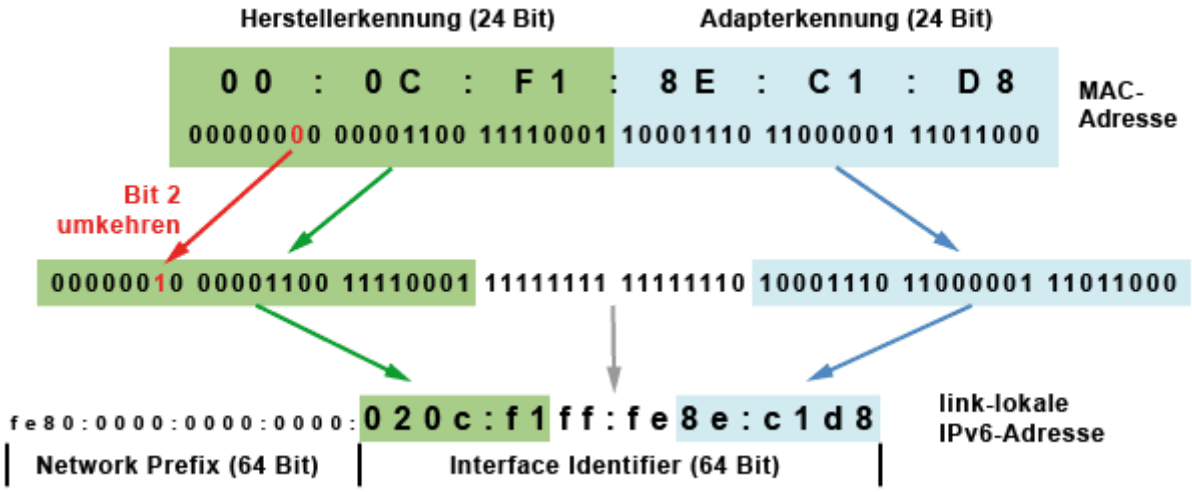
Die von IPv4 bekannte Netzmaske bzw. Subnetzmaske fällt bei IPv6 ersatzlos weg. Um trotzdem eine Segmentierung und Aufteilung von Adressbereichen bzw. Subnetzen vornehmen zu können, wird die Präfixlänge definiert und mit einem / an die eigentliche IPv6-Adresse angehängt. Der hierarchische Aufbau des Präfixes soll das Routing mit IPv6 vereinfachen.
Standardmäßig ist /64 die Präfixlänge. Es gibt jedoch weitere typische Präfixe, die 32, 48 und 56 Bit lang sind.

IPv6-Address-Scopes (Gültigkeitsbereiche)

Unicast	Link-Local-Adressen (Verbindungslokale Unicast-Adressen) sind nur innerhalb von geschlossenen Netzsegmenten gültig. Router dürfen Datenpakete mit Link-Local Adressen als Quelle oder Ziel nicht an andere Links weiterleiten. Präfix: **fe80::/10**
Multicast-Adressen	Eine Multicast-Adresse ist ein Identifier für eine Gruppe von Geräten. Jedes Gerät kann zu beliebig vielen Multicast-Gruppen gehören. Präfix: **ff00::/8**
Anycast-Adressen	Im IPv6 wurde ein neuer Adresstyp "Anycast" definiert. Dieser Adresstyp erlaubt es, dass Datenpakete zu einem oder mehreren Geräten mit gleicher Adresse geroutet werden. Anycast-Adressen können einem oder mehreren, typischerweise an unterschiedlichen Geräten befindlichen, Netzwerk-Interfaces zugewiesen werden. Die Routing-Protokolle liefern jedes Paket zum nächsten Interface.

SLAAC und DAD

Stateless Address Autoconfiguration (SLAAC) ist ein Verfahren zur zustandslosen und automatischen Konfiguration von IPv6-Adressen an einem Netzwerk-Interface. Mit „stateless“ bzw. „zustandslos“ ist gemeint, dass die jeweilige IPv6-Adresse nicht zentral vergeben und gespeichert wird. Demnach erzeugt sich der Host seine IPv6-Adresse unter Zuhilfenahme zusätzlicher Informationen selbst.



Eine link-lokale IPv6-Adresse wird aus einem Präfix (64 Bit) und einem Suffix (64 Bit) gebildet. Der Präfix für alle link-lokalen IPv6-Adressen ist immer "fe80:0000:0000:0000". Das Suffix (Interface Identifier) ist der EUI-64-Identifier oder IEEE-Identifier, der aus der MAC-Adresse (Hardware-Adresse des Netzwerkadapters) gebildet wird.
In der Mitte der 48-Bit-MAC-Adresse (zwischen dem dritten und dem vierten Byte) werden mit **"ff:fe"** zwei feste Bytes eingefügt, damit es 64 Bit werden. **Zusätzlich wird noch das zweite Bit im ersten Byte der MAC-Adresse invertiert.** Das heißt, aus "1" wird "0" und aus "0" wird "1".

Auf diese Weise wird zum Beispiel die MAC-Adresse "00:0C:F1:8E:C1:D8" zum Interface Identifier "020c:f1ff:fe8e:c1d8". Und der Host bildet sich so die link-lokale Adresse "fe80:0000:0000:0000:020c:f1ff:fe8e:c1d8".

Um Adresskollisionen zu vermeiden sollte der Host bei einer neu generierten IPv6-Adresse eine **Duplicate Address Detection (DAD)** durchführen.

1. **Neighbor Solicitation**: Dazu schickt der Host eine Anfrage an die generierte Adresse ins lokale Netz. Als Antwort-Adresse dient eine Multicast-Adresse.
2. **Neighbor Advertisement**: Falls eine andere Station die IPv6-Adresse bereits nutzt, kommt eine Antwort zurück.

Erst wenn keine Antwort von dieser Adresse zurückkommt bindet sich das Interface an diese Adresse und kann sie für die Kommunikation nutzen.

Weil es keine Pflicht gibt eine DAD durchzuführen, sind Adresskollisionen durchaus möglich. Aufgrund des sehr großzügigen Adressraums und der weltweit eindeutigen MAC-Adressen aber eher unwahrscheinlich.
Sollte es doch einmal zu einer Kollision kommen und die IPv6-Adresse tatsächlich schon existieren, dann muss die IPv6-Adresse vom Anwender manuell geändert werden.

Dann sollte man gleich das ganze Netzwerk überprüfen. Es könnte dann sein, dass jemand eine MAC-Adresse gekapert hat und per MAC-Spoofing ins Netzwerk eingedrungen ist.

Created 2022-03-07 08:54:05 UTC by Joshua Lieder
Updated 2022-04-02 16:22:55 UTC by Joshua Lieder