IPv6
Workbook
Grundlagen und Adressierung

Einführung:

IPv4 bietet einen Adressraum von etwas über vier Milliarden IP-Adressen (2^{32} = 256^4 = 4.294.967.296), von denen 3.707.764.736 verwendet werden können, um Computer und andere Geräte direkt anzusprechen[1]. In den Anfangstagen des Internets, als es nur wenige Rechner gab, die eine IP-Adresse brauchten, galt dies als weit mehr als ausreichend. Aufgrund des unvorhergesehenen Wachstums des Internets herrscht heute aber Adressenknappheit. Im Januar 2011 teilte die IANA der asiatischen Regional Internet Registry APNIC die letzten zwei frei zu vergebenden Netze zu[2]. Gemäß einer Vereinbarung aus dem Jahr 2009[3] wurde am 3. Februar 2011 schließlich der verbleibende Adressraum gleichmäßig auf die regionalen Adressvergabestellen verteilt[4]. Darüber hinaus steht den regionalen Adressvergabestellen kein weiterer IPv4-Adressraum mehr zur Verfügung. Am 15. April 2011 teilte APNIC die letzten frei zu vergebenden Adressen für die Region Südostasien zu[5]; am 14. September 2012 folgte dann RIPE NCC mit der letzten freien Zuteilung in der Region Europa/Naher Osten[6]. Seitdem haben APNIC- und RIPE NCC-Mitglieder jeweils nur noch Anspruch auf eine einzelne Zuteilung von IPv4-Adressraum der minimalen Zuteilungsgröße[7].

Die historische Entwicklung des Internets wirft ein weiteres Problem auf: Durch die mit der Zeit mehrmals geänderte Vergabepraxis von Adressen des IPv4-Adressraums ist dieser inzwischen stark fragmentiert, d. h., häufig gehören mehrere nicht zusammenhängende Adressbereiche zur gleichen organisatorischen Instanz. Dies führt in Verbindung mit der heutigen Routingstrategie (Classless Inter-Domain Routing) zu langen Routingtabellen, auf welche Speicher und Prozessoren der Router im Kernbereich des Internets ausgelegt werden müssen. Zudem erfordert IPv4 von Routern, Prüfsummen jedes weitergeleiteten Pakets neu zu berechnen, was eine weitere Prozessorbelastung darstellt.

Aus diesen Gründen begann die IETF bereits 1995 die Arbeiten an IPv6. Im Dezember 1998 wurde IPv6 mit der Publikation von RFC 2460 auf dem Standards Track offiziell zum Nachfolger von IPv4 gekürt.

[1] Heise.de Datenschützer besorgt über IPv6; ↑ [a] [b] IANA:

[2] APNIC: Two /8s allocated to APNIC from IANA Meldung vom 1. Febr. 2011

[3] ICANN: Global Policy for the Allocation of the Remaining IPv4 Address Space

[4] Twitter-Verlautbarung der IANA zum Ende des IPv4-Adressraums

[5] APNIC: APNIC IPv4 Address Pool Reaches Final /8

[6] RIPE NCC:

[7] APNIC: Policies for IPv4 address space management in the Asia Pacific region, Abschnitt 9.10.1

RIPE NCC:

Die wesentlichen neuen Eigenschaften von IPv6 umfassen:

- Vergrößerung des Adressraums von IPv4 mit 2^{32} (≈ 4,3 Milliarden) Adressen auf 2^{128}(≈ 340 Sextillionen) Adressen bei IPv6, d. h. Vergrößerung um den Faktor 2^{96}.
- Vereinfachung und Verbesserung des Protokollrahmens (Kopfdaten); dies entlastet Router von Rechenaufwand.
- Zustandslose automatische Konfiguration von IPv6-Adressen; zustandsbehaftete Verfahren wie DHCP werden beim Einsatz von IPv6 damit in vielen Anwendungsfällen überflüssig
- Mobile IP sowie Vereinfachung von Umnummerierung und Multihoming
- Implementierung von IPSec innerhalb des IPv6-Standards[8]. Dadurch wird die Verschlüsselung und die Überprüfung der Authentizität von IP-Paketen ermöglicht[9].
- Unterstützung von Netztechniken wie Quality of Service und Multicast

Aufgabe 1: Größe IPv6 Netz

2001:0DB8:9696:0000:0000:0000:0000:0000/64 ist ein typisches IPv6-Netz. Wie oft passt das gesamte IPv4-Internet hinein?

- ☐ Gar nicht, das IPv6-Netz ist kleiner als das IPv4-Internet.
- ☐ Es passt genau einmal hinein.
- ☐ Rund 4,2 Billionen mal.
- ☐ Rund 4,2 Milliarden mal.

Die hauptsächliche Motivation zur Vergrößerung des Adressraums besteht in der Wahrung des Ende-zu-Ende-Prinzips[10], das ein zentrales Designprinzip des Internets ist[11]: Nur die Endknoten des Netzes sollen aktive Protokolloperationen ausführen, das Netz zwischen den Endknoten ist nur für die Weiterleitung der Datenpakete zuständig. Dazu ist es notwendig, dass jeder Netzknoten global eindeutig adressierbar ist[12].

Heute übliche Verfahren wie Network Address Translation (NAT), welche derzeit die IPv4-Adressknappheit umgehen, verletzen das Ende-zu-Ende-Prinzip[13]. Sie ermöglichen den so angebundenen Rechnern nur ausgehende Verbindungen aufzubauen. Aus dem Internet können diese hingegen nicht ohne weiteres kontaktiert werden. Auch verlassen sich IPSec oder Protokolle auf höheren Schichten wie z. B. FTP und SIP teilweise auf das Ende-zu-Ende-Prinzip und sind mit NAT nur eingeschränkt oder mittels Zusatzlösungen funktionsfähig[14]. Besonders für Heimanwender bedeutet IPv6 damit einen Paradigmenwechsel: Anstatt vom Provider nur eine einzige IP-Adresse zugewiesen zu bekommen und über NAT mehrere Geräte ans Internet anzubinden, bekommt der Anwender

[8] RFC 6434, Abschnitt 11

[9] IPsec wurde zusätzlich auch für IPv4 spezifiziert, dort ist die Umsetzung aber optional, während sie für IPv6 zunächst in RFC 4294 vorgeschrieben war. Diese Vorschrift wurde aber mit RFC 6434 zurückgenommen.

[10] siehe etwa RFC 2775, Abschnitt 5.1

[11] RFC 3724, Abschnitt 2

[12] siehe etwa RFC 2775, Abschnitt 5.1

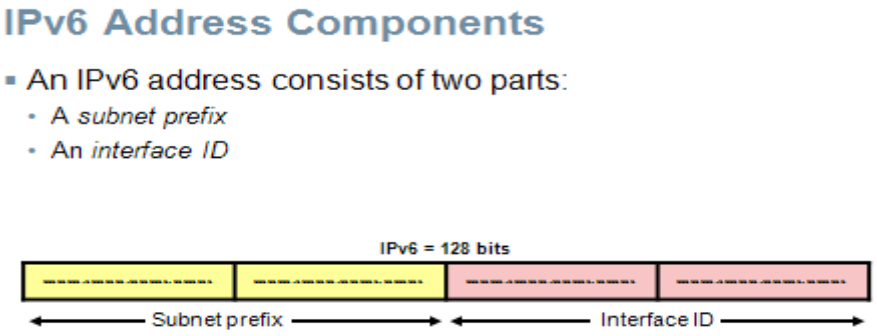
[13] RFC 2993, Abschnitt 6

[14] Stefan Wintermeyer: Asterisk 1.4 + 1.6. Addison-Wesley, München; 1. Auflage 2009. Kapitel 8.

global eindeutigen IP-Adressraum für ein ganzes Teilnetz zur Verfügung gestellt, so dass jedes seiner Geräte eine IP-Adresse aus diesem erhalten kann. Damit wird es für Endbenutzer einfacher, durch das Anbieten von Diensten aktiv am Netz teilzunehmen. Zudem entfallen die Probleme, die bei NAT durch die Adressumschreibung entstehen.

Bei der Wahl der Adresslänge und damit der Größe des zur Verfügung stehenden Adressraums waren mehrere Faktoren zu berücksichtigen. Zum einen müssen pro Datenpaket auch Quell- und Ziel-IP-Adresse übertragen werden. Längere IP-Adressen führen damit zu erhöhtem Protokoll-Overhead, d. h. das Verhältnis zwischen tatsächlichen Nutzdaten und der zur Vermittlung notwendigen Protokolldaten sinkt[15]. Auf der anderen Seite sollte dem zukünftigen Wachstum des Internets Rechnung getragen werden. Zudem sollte es zur Verhinderung der Fragmentierung des Adressraums möglich sein, einer Organisation nur ein einziges Mal Adressraum zuweisen zu müssen. Um den Prozess der Autokonfiguration sowie Umnummerierung und Multihoming zu vereinfachen, war es außerdem wünschenswert, einen festen Teil der Adresse zur netzunabhängigen eindeutigen Identifikation eines Netzknotens zu reservieren. Die letzten 64 Bit der Adresse bestehen daher in der Regel aus der EUI-64 der Netzwerkschnittstelle des Knotens.

IPv6-Adressen sind 128 Bit lang (IPv4: 32 Bit). Die letzten 64 Bit bilden bis auf Sonderfälle einen für die Netzwerkschnittstelle (engl. Interface) eindeutigen Interface Identifier. Eine Netzwerkschnittstelle kann unter mehreren IP-Adressen erreichbar sein; in der Regel ist sie dies mittels ihrer link-lokalen Adresse und einer global eindeutigen Adresse. Derselbe Interface Identifier kann damit Teil mehrerer IPv6-Adressen sein, welche mit verschiedenen Präfixen auf dieselbe Netzwerkkarte gebunden sind. Insbesondere gilt dies auch für Präfixe möglicherweise verschiedener Provider; dies vereinfacht Multihoming-Verfahren.



[16]

Da die Erzeugung des Interface Identifiers aus der global eindeutigen MAC-Adresse die Nachverfolgung von Benutzern ermöglicht, wurden die Privacy Extensions (RFC 4941) entwickelt, um diese permanente Kopplung der Benutzeridentität an die IPv6-Adressen aufzuheben. Indem der Interface Identifier zufällig generiert wird und regelmäßig wechselt, soll ein Teil der Anonymität von IPv4 wiederhergestellt werden.

---

[15] Eine Diskussion des Problems findet sich in einem Internet-Draft von W. Eddy, Comparison of IPv4 and IPv6 Header Overhead.

[16] IPv6-Part21-Addr-Types, 2006, Cisco Systems

Da im Privatbereich in der IPv6-Adresse aber sowohl der Interface Identifier als auch das Präfix allein recht sicher auf einen Nutzer schließen lassen können, ist aus Datenschutzgründen in Verbindung mit den Privacy Extensions ein vom Provider dynamisch zugewiesenes, z. B. täglich wechselndes, Präfix wünschenswert. (Mit einer statischen Adresszuteilung geht in der Regel insbesondere ein Eintrag in der öffentlichen Whois-Datenbank einher.) Dabei ist es wie oben beschrieben grundsätzlich möglich, auf derselben Netzwerkkarte sowohl IPv6-Adressen aus dynamischen als auch aus fest zugewiesenen Präfixen parallel zu verwenden. In Deutschland hat der Deutsche IPv6-Rat Datenschutzleitlinien formuliert, die auch eine dynamische Zuweisung von IPv6-Präfixen vorsehen.[17]

Aufgabe 2: Unterschiede IPv4 vs. IPv6

IPv6-Adressen sind länger als IPv4-Adressen. Was ist bei IPv6 noch anders?

- Netzwerkklassen (Class A, B, C) werden abgeschafft.
- Der IPv6-Header enthält keine Checksumme mehr.
- Router fragmentieren IPv6-Pakete nicht.
- IPv6-Adressen bleiben lebenslang persönlich zugeordnet.
- Network Address Translation (NAT) ist nicht mehr möglich.

Damit ein Host nicht anhand seiner IPv6-Adresse identifiziert werden kann, gibt es die "Privacy Extensions". Wie funktionieren sie?

- Alle Pakete werden über Privacy-Server im Internet umgeleitet.
- Der Router ersetzt die wiedererkennbaren IPv6-Adressen der Hosts durch seine eigene (NAT).
- Der Host wechselt regelmäßig und zufällig seine Adresse.
- Der Router setzt den "Lokal Part" der Adresse auf 0 und füllt ihn bei den Antwortpaketen wieder aus.

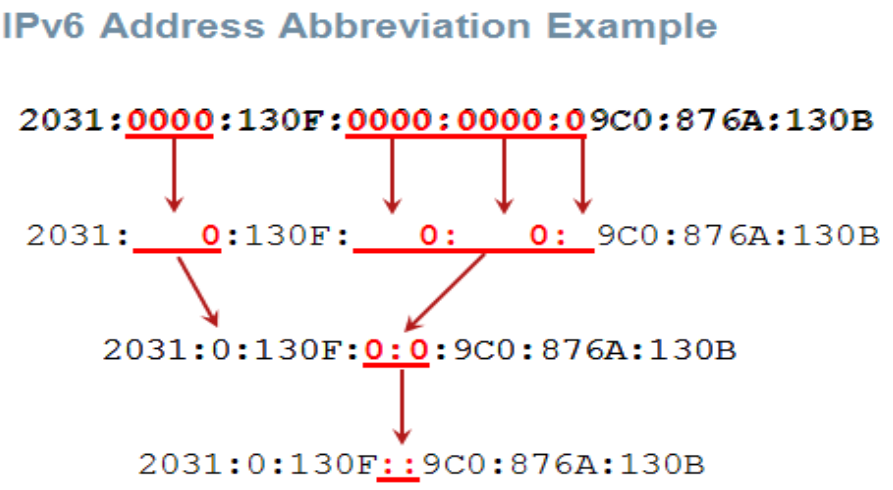
[17] German IPv6 Council: Leitlinien IPv6 und Datenschutz

Adressnotation

Die textuelle Notation von IPv6-Adressen ist in Abschnitt 2.2 von RFC 4291 beschrieben:

1. IPv6-Adressen werden gewöhnlicherweise hexadezimal (IPv4: dezimal) notiert, wobei die Zahl in acht Blöcke zu jeweils 16 Bit (4 Hexadezimalstellen) unterteilt wird. Diese Blöcke werden durch Doppelpunkte (IPv4: Punkte) getrennt notiert: 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 ist gleichbedeutend mit 2001:db8:0:8d3:0:8a2e:70:7344.
3. 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 ist gleichbedeutend mit 2001:db8::1428:57ab. Ein einzelner Block, dessen Wert 0 beträgt, darf jedoch nicht ausgelassen werden[18].

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.



19

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.

---

[18] RFC 5952, A Recommendation for IPv6 Address Text Representation, S. Kawamura (August 2010), Abschnitt 4.2.2: http://tools.ietf.org/html/rfc5952#section-4.2.2

[19] IPv6-Part21-Addr-Types, 2006, Cisco Systems

Aufgabe 3: Reduzierte Schreibweise von IPv6 Adressen

Welches sind gültige IPv6-Adressen?

- ☐ ::
- ☐ 2001:DB8::abf:1:7
- ☐ ::ffff:192.0.2.128
- ☐ 2001:DB8::abf:1::7
- ☐ 2001:0DB8:0000:0000:0abf:0001:0007

Aufgabe 4: Vergleich von IPv6 Adressen

a) Handelt es sich bei der IPv6-Adressen

1. 2001:0db8::1428:57ab
2. 2001:db8::28:b

um die gleiche Adresse wie

a. 2001:0db8:0000:0000:0000:0000:1428:57ab
b. 2001:0db8::0028:000b?

b) Geben Sie die IPv6-Adresse in verkürzter Schreibweise an:

2001:0db0:85a3:0000:1319:0000:0000:0044

Aufgabe 5: Aufbau von IPv6 Adressen

Welcher Fehler ist bei der Angabe der IPv6-Adresse 2001::25de::cade gemacht worden?

URL-Notation von IPv6-Adressen

In einer URL wird die IPv6-Adresse in eckige Klammern eingeschlossen[20], z. B.:

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

Diese Notation verhindert die fälschliche Interpretation von Portnummern als Teil der IPv6-Adresse:

-
- http://[2001:0db8:85a3:08d3:1319:8a2e:0370:7344]:8080/

Aufgabe 6: Browser und IPv6 Adressen

Wie wählt man beim Internet-Surfen im Browser eine IPv6-Verbindung zum Server www.example.com aus?

- ☐ http6://www.example.com
- ☐ http://www.example.com:6
- ☐ Gar nicht, der Browser trifft die Entscheidung automatisch.
- ☐ http://[www.example.com]

[20] RFC 3986, Abschnitt 3.2.2

Netznotation

IPv6 verwendet eine andere Netzmaske als IPv4. Die wesentlichen Unterschiede sind in RFC 5942 (IPv6 Subnet Model) zusammengefasst.

Bei der Präfixlänge für IPv6 wird schlicht wie im CIDR die Anzahl der Bits im Netzwerkteil getrennt durch „/“ hinter die IPv6-Adresse geschrieben. Dazu werden die erste Adresse (bzw. die Netzadresse) und die Länge des Präfixes in Bits getrennt durch einen Schrägstrich notiert.

Zum Beispiel steht 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.

Die Größe eines IPv6-Netzwerkes (oder Subnetzwerkes) im Sinne der Anzahl der vergebbaren Adressen in diesem Netz muss also eine Zweierpotenz sein. Da ein einzelner Host auch als Netzwerk mit einem 128 Bit langen Präfix betrachtet werden kann, werden Host-Adressen manchmal mit einem angehängten „/128“ geschrieben.

Beispiel:

- 2001:0db8:85a3:08d3:1319:8a2e:0370:7347/64.

Die Präfixlänge ist in diesem Falle	/64,
das Netz	2001:0db8:85a3:08d3:0000:0000:0000:0000/64
der Geräteteil oder Interface Identifier	1319:8a2e:0370:7347.

Aufgabe 7: IPv6 Subnetze.

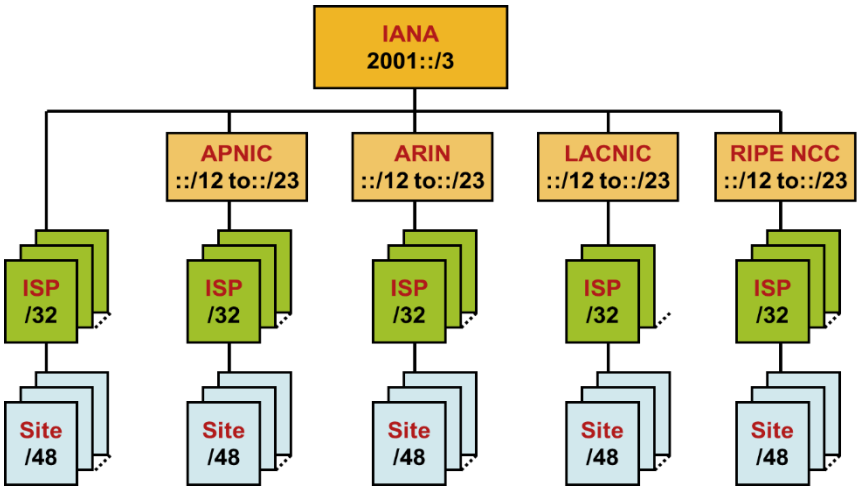
In welchem Subnetz befindet sich der Host mit der IPv6-Adresse 2001:0db8:85a3:08d3:1319:8a2e:0370:7344/64?

Aufgabe 8: IPv6 Subnetting.

Befindet sich der Host mit der IPv6-Adresse 2001:0db8:85a3:08d3:1319:8a2e:0370:7344/64 im Subnetz 2001:0db8:85a3::/48 ?

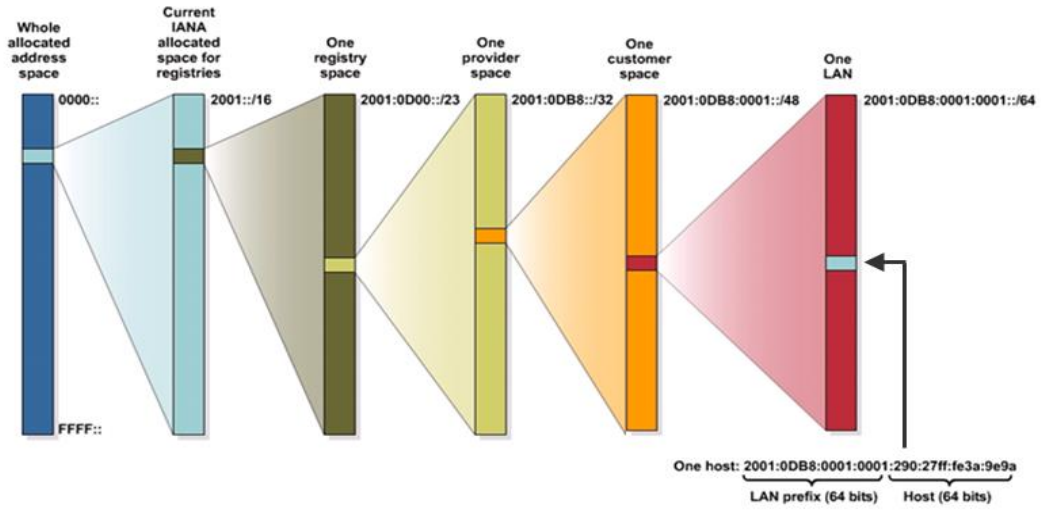
Adresszuweisung

Typischerweise bekommt ein Internetprovider (ISP) die ersten 32 Bit (oder weniger) als Netz von einer Regional Internet Registry (RIR) zugewiesen[21]. Dieser Bereich wird vom Provider weiter in Subnetze aufgeteilt.



22

Die Länge der Zuteilung an Endkunden wird dabei dem ISP überlassen; vorgeschrieben ist die minimale Zuteilung eines /64-Netzes[23] Ältere Dokumente (z. B. RFC 3177) schlagen eine Zuteilung von /48-Netzen an Endkunden vor; in Ausnahmefällen ist die Zuteilung größerer Netze als /48 oder mehrerer /48-Netze an einen Endkunden möglich[24].



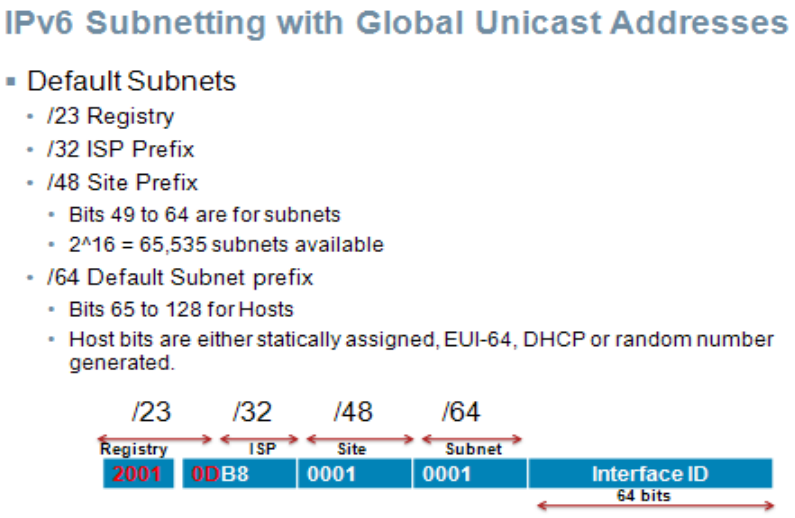
25

Informationen über die Vergabe von IPv6-Netzen können über die Whois-Dienste der jeweiligen RIRs abgefragt werden.

---

[21] IPv6 Address Allocation and Assignment Policy von APNIC, ARIN, RIPE NCC, Abschnitt 4.3
[22] IPv6-Part21-Addr-Types, 2006, Cisco Systems
[23] IPv6 Address Allocation and Assignment Policy, Abschnitt 5.4.1
[24] IPv6 Address Allocation and Assignment Policy, Abschnitt 5.4.2
[25] IPv6-Part21-Addr-Types, 2006, Cisco Systems

Einem einzelnen Netzsegment wird in der Regel ein 64 Bit langes Präfix zugewiesen, das dann zusammen mit einem 64 Bit langen Interface Identifier die Adresse bildet[26]. Der Interface Identifier kann entweder aus der MAC-Adresse der Netzwerkkarte erstellt oder anders eindeutig zugewiesen werden; das genaue Verfahren ist in RFC 4291, Anhang A beschrieben.



[27]

In diesem Beispiel hat der ISP eine Netzmaske von /32 von der regionalen Registrierungsbehörde erhalten. Dadurch stehen dem ISP 16 SLA Bits mit insg. 65535 /48er Netzwerken für die Adressierung von Kundennetzwerken zur Verfügung.

Aufgabe 9:

Der ISP hat der Service AG einen IPv6 Adressbereich mit der Netzmaske /56 zugewiesen. Erläutern Sie unter Angabe des Rechenwegs, wie viele Subnetze gebildet werden können, wenn der Hostanteil 64 Bit beträgt!

Lösung:

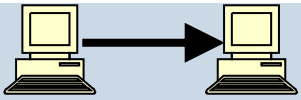
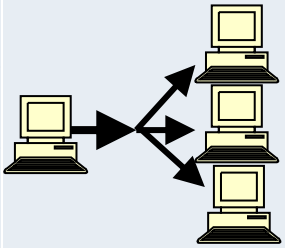
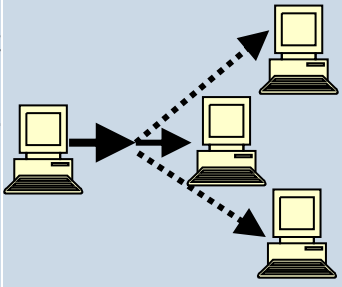
[26] RFC 4291, Abschnitt 2.5.4
[27] IPv6-Part21-Addr-Types, 2006, Cisco Systems

Aufgabe 10: Netzwerkplanung

Der in Aufgabe 9 genannte ISP hat von der Registrierungsbehörde einen Adressbereich mit einer Netzmaske /29 zugewiesen bekommen. Erläutern Sie unter Angabe des Rechenwegs, wie viele IPv6-Netzadressen (in Millionen) der ISP an seine Kunden vergeben kann.

Lösung:**Adressbereiche**

Es gibt verschiedene IPv6-Adressbereiche mit Sonderaufgaben und unterschiedlichen Eigenschaften. Diese werden meist schon durch die ersten Bits der Adresse signalisiert. Sofern nicht weiter angegeben, werden die Bereiche in RFC 4291 bzw. RFC 5156 definiert. Unicast-Adressen charakterisieren Kommunikation eines Netzknotens mit genau einem anderen Netzknoten; Einer-zu-vielen-Kommunikation wird durch Multicast-Adressen abgebildet.

Address Type[28]	Description	Topology
Unicast	"***One to One***" • An address destined for a single interface. • A packet sent to a unicast address is delivered to the interface identified by that address.	
Multicast	"***One to Many***" • An address for a set of interfaces (typically belonging to different nodes). • A packet sent to a multicast address will be delivered to all interfaces identified by that address.	
Anycast	"***One to Nearest***" (Allocated from Unicast) • An address for a set of interfaces. • In most cases these interfaces belong to different nodes. • created "automatically" when a single unicast address is assigned to more than one interface. • A packet sent to an anycast address is delivered to the closest interface as determined by the IGP.	

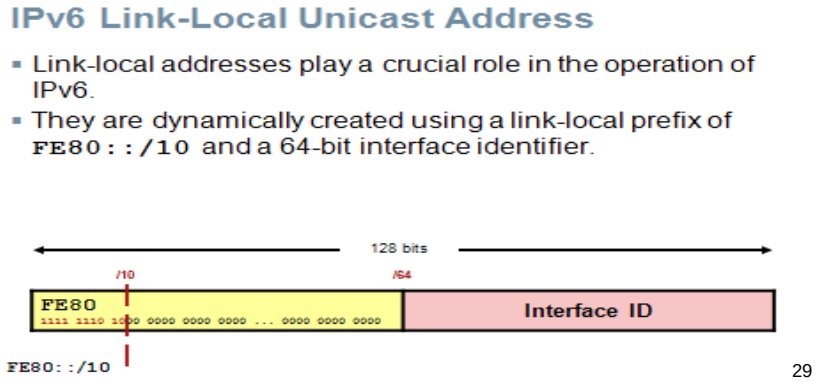
[28] IPv6-Part1-Addr-Types, 2006, Cisco Systems

Besondere Adressen

- ::/128 (128 0-Bits) ist die nicht spezifizierte Adresse. Sie darf keinem Host zugewiesen werden, sondern zeigt das Fehlen einer Adresse an. Sie wird beispielsweise von einem initialisierenden Host als Absenderadresse in IPv6-Paketen verwendet, solange er seine eigene Adresse noch nicht mitgeteilt bekommen hat. Jedoch können auch Serverprogramme durch Angabe dieser Adresse bewirken, dass sie auf allen Adressen des Hosts lauschen.
- ::1/128 (127 0-Bits, ein 1-Bit) ist die Adresse des eigenen Standortes (loopback-Adresse, die in der Regel mit localhost verknüpft ist).

Link-Local-Adressen

- Link-Local-Adressen werden innerhalb abgeschlossener Netzwerksegmente eingesetzt. Man identifiziert sie am Subnetz-Präfix (den ersten 10 Bits) mit dem Wert „fe80::/10“:



[29]

Link-Local-Adressen nutzt man zur Adressierung von Nodes in abgeschlossenen Netzwerksegmenten, sowie zur Autokonfiguration oder Neighbour-Discovery. Dadurch muss man in einem Netzwerksegment keinen DHCP-Server zur automatischen Adressvergabe konfigurieren. Link-Local-Adressen sind mit APIPA-Adressen im Netz 169.254.0.0/16 vergleichbar.

Soll ein Gerät mittels einer dieser Adressen kommunizieren, so muss die Zone ID mit angegeben werden (unter Windows ist das in der Regel die zugehörige Netzwerkschnittstelle), da eine Link-Lokale-Adresse auf einem Gerät mehrfach vorhanden sein kann. Bei einer einzigen Netzwerkschnittstelle würde eine Adresse etwa so aussehen: fe80::7645:6de2:ff:1%1.

Site Local Unicast (veraltet)

- fec0::/10 (fec0… bis feff…), auch standortlokale Adressen (site local addresses), waren die Nachfolger der privaten IP-Adressen (beispielsweise 192.168.x.x). Sie durften nur innerhalb der gleichen Organisation geroutet werden. Die Wahl des verwendeten Adressraums innerhalb von fec0::/10 war für eine Organisation beliebig. Site Local Addresses sind nach RFC 3879 inzwischen veraltet (engl. deprecated) und werden aus zukünftigen Standards verschwinden. Nachfolger der standortlokalen Adressen sind die Unique Local Addresses, die im nächsten Abschnitt beschrieben werden.

[29] IPv6-Part2-Addr-Types, 2006, Cisco Systems

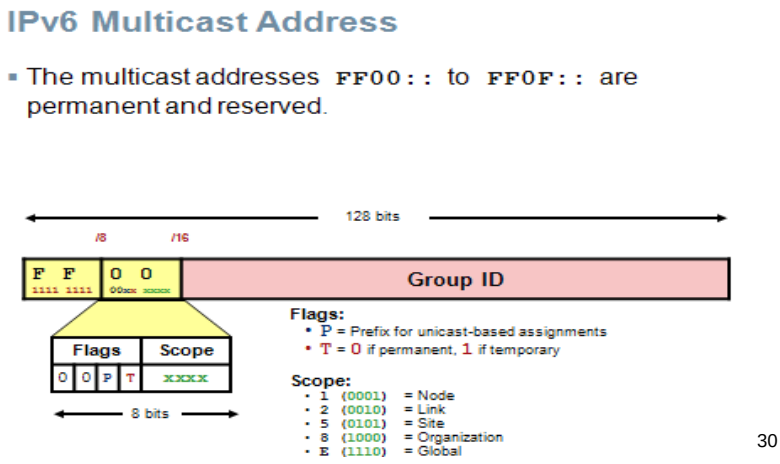
Unique Local Unicast

- fc00::/7 (fc… und fd…). Für private Adressen gibt es die Unique Local Addresses (ULA), beschrieben in RFC 4193. Derzeit ist nur das Präfix fd für lokal generierte ULA vorgesehen, mit dem Präfix fc werden in Zukunft wahrscheinlich global zugewiesene eindeutige ULA gekennzeichnet. Auf dieses Präfix folgen dann 40 Bits, die als eindeutige Site-ID fungieren. Diese Site-ID ist bei den ULA mit dem Präfix fd zufällig zu generieren und somit nur sehr wahrscheinlich eindeutig, bei den global vergebenen ULA jedoch auf jeden Fall eindeutig (RFC 4193 gibt jedoch keine konkrete Implementierung der Zuweisung von global eindeutigen Site-IDs an). Nach der Site-ID folgt eine 16-Bit-Subnet-ID, welche ein Netz innerhalb der Site angibt.

Eine Beispiel-ULA wäre fd9e:21a7:a92c:2323::1. Hierbei ist fd das Präfix für lokal generierte ULAs, 9e:21a7:a92c ein einmalig zufällig erzeugter 40-Bit-Wert und 2323 eine willkürlich gewählte Subnet-ID.

Die Verwendung von wahrscheinlich eindeutigen Site-IDs hat den Vorteil, dass zum Beispiel beim Einrichten eines Tunnels zwischen getrennt voneinander konfigurierten Netzwerken Adresskollisionen sehr unwahrscheinlich sind. Weiterhin wird erreicht, dass Pakete, welche an eine nicht erreichbare Site gesendet werden, mit großer Wahrscheinlichkeit ins Leere laufen, anstatt an einen lokalen Host gesendet zu werden, der zufällig die gleiche Adresse hat.

Multicast



30

- ff00::/8 (ff…) stehen für Multicast-Adressen.

Nach dem Multicast-Präfix folgen 4 Bits für Flags und 4 Bits für den Gültigkeitsbereich (Scope). Für die Flags sind zurzeit folgende Kombinationen gültig[31]:
0: Permanent definierte wohlbekannte Multicast-Adressen (von der IANA zugewiesen)[32]

[30] IPv6-Part2-Addr-Types, 2006, Cisco Systems
[31] RFC 2373, Abschnitt 2.7
[32] RFC 3307, Abschnitt 4.1

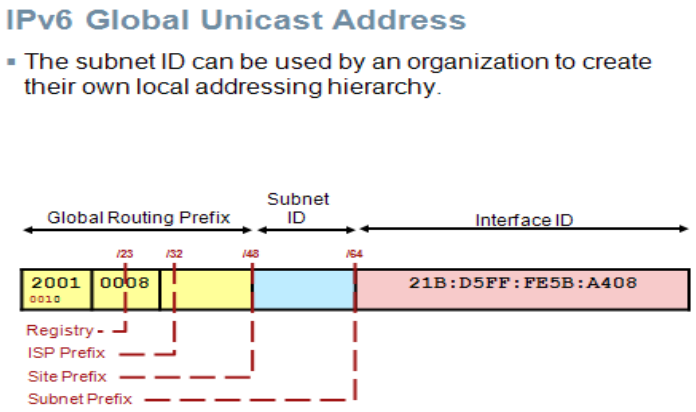
1: (T-Bit gesetzt) Transient (vorübergehend) oder dynamisch zugewiesene Multicast-Adressen
3: (P-Bit gesetzt, erzwingt das T-Bit) Unicast-Prefix-based Multicast-Adressen (RFC 3306)
7: (R-Bit gesetzt, erzwingt P- und T-Bit) Multicast-Adressen, welche die Adresse des Rendezvous Point enthalten (RFC 3956)

Die folgenden Gültigkeitsbereiche sind definiert[33]:
1: interfacelokal, diese Pakete verlassen die Schnittstelle nie. (Loopback)
2: link-lokal, werden von Routern grundsätzlich nie weitergeleitet und können deshalb das Teilnetz nicht verlassen.
4: adminlokal, der kleinste Bereich, dessen Abgrenzung in den Routern speziell administriert werden muss.
5: sitelokal, dürfen zwar geroutet werden, jedoch nicht von Border-Routern.
8: organisationslokal, die Pakete dürfen auch von Border-Routern weitergeleitet werden, bleiben jedoch „im Unternehmen“ (hierzu müssen seitens des Routing-Protokolls entsprechende Vorkehrungen getroffen werden).
e: globaler Multicast, der überallhin geroutet werden darf.
0, 3, f: reservierte Bereiche
Die restlichen Bereiche sind nicht zugewiesen und dürfen von Administratoren benutzt werden, um weitere Multicast-Regionen zu definieren[34].

Beispiele für wohlbekannte Multicast-Adressen[35]:

- ff01::1, ff02::1: All Nodes Adressen. Entspricht dem Broadcast.
- ff01::2, ff02::2, ff05::2: All Routers Adressen, adressiert alle Router in einem Bereich.

Global Unicast



36

Alle anderen Adressen gelten als Global-Unicast-Adressen. Von diesen sind jedoch bisher nur die folgenden Bereiche zugewiesen:

[33] RFC 2373, Abschnitt 2.7
[34] RFC 4291, Abschnitt 2.7
[35] IANA: Internet Protocol Version 6 Multicast Addresses
[36] IPv6-Part2-Addr-Types, 2006, Cisco Systems

- ::/96 (96 0-Bits) stand für IPv4-Kompatibilitätsadressen, welche in den letzten 32 Bits die IPv4-Adresse enthielten. Diese waren für den Übergang definiert, jedoch im RFC 4291 vom Februar 2006 für veraltet (engl. deprecated) erklärt.
- 0:0:0:0:0:ffff::/96 (80 0-Bits, gefolgt von 16 1-Bits) steht für IPv4 mapped (abgebildete) IPv6 Adressen. Die letzten 32 Bits enthalten die IPv4-Adresse. Ein geeigneter Router kann diese Pakete zwischen IPv4 und IPv6 konvertieren.
- 2000::/3 (was dem binären Präfix 001 entspricht) stehen für die von der IANA vergebenen globalen Unicast-Adressen, also routbare und weltweit einzigartige Adressen. 2001-Adressen werden an Provider vergeben, die diese an ihre Kunden weiterverteilen.
- Adressen aus 2001::/32 (also beginnend mit 2001:0:) werden für den Tunnelmechanismus Teredo benutzt.
- Adressen aus 2001:db8::/32 dienen Dokumentationszwecken, wie beispielsweise in diesem Artikel, und bezeichnen keine tatsächlichen Netzteilnehmer.
- 2002-Präfixe deuten auf Adressen des Tunnelmechanismus 6to4 hin.
- Auch mit 2003, 240, 260, 261, 262, 280, 2a0, 2b0 und 2c0 beginnende Adressen werden von Regional Internet Registries (RIRs) vergeben; diese Adressbereiche sind ihnen z. T. aber noch nicht zu dem Anteil zugeteilt, wie dies bei 2001::/16 der Fall ist[37].
- 64:ff9b::/96 kann für den Übersetzungsmechanismus NAT64 gemäß RFC 6146 verwendet werden.

[37] IANA: IPv6 Unicast Address Assignments

Aufgabe 11:Besondere IP Adressen

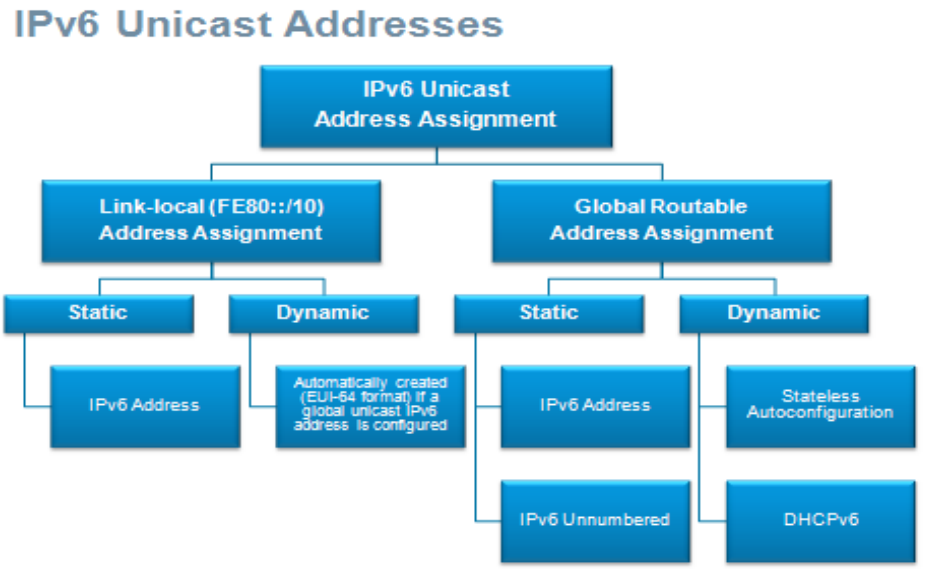
Es gibt verschiedene IPv6-Adressen mit Sonderaufgaben und unterschiedlichen Eigenschaften. Diese werden durch die ersten Bits der Adresse, das Präfix, signalisiert:
Vervollständigen Sie die folgende Tabelle

Beschreibung	IPv4	IPv6	Bemerkung
Loopback Adresse			
Default Route (undefinierte Adresse)			
Private Adressen			
Multicast Adressen			

Funktionalität

Die nachfolgende Grafik zeigt die verschiedenen Möglichkeiten, mit denen IPv6 Unicastadressen an Netzwerkschnittstellen vergeben werden können.

Wie bei IPv4 kann man IPv6 Adressen manuell (statisch) konfigurieren.



[38]

Übung 1: Bearbeiten Sie folgende Packet-Tracer-Activitiy zur manuellen Konfiguration von IPv6.

Sie finden die Activity in Ihrem Klassenorder im Unterordner *IPv6/PT_Uebungen*

a. *IPv6 Manual Addressing Initial.pka*

Dokumentieren Sie für die Fastethernetschnittstelle von Router 1:

Link-Local Adresse	
Global Unicast	

Dokumentieren Sie für die Fastethernetschnittstelle von PC1:

Link-Local Adresse	
Global Unicast	
Gateway	

[38] IPv6-Part2-Addr-Types, 2006, Cisco Systems

Dokumentieren Sie für die Fastethernetschnittstelle von Router 2:

Link-Local Adresse	
Global Unicast	

Dokumentieren Sie für die Fastethernetschnittstelle von PC2:

Link-Local Adresse	
Global Unicast	
Gateway	

Dokumentieren Sie für die Fastethernetschnittstelle von Router 3:

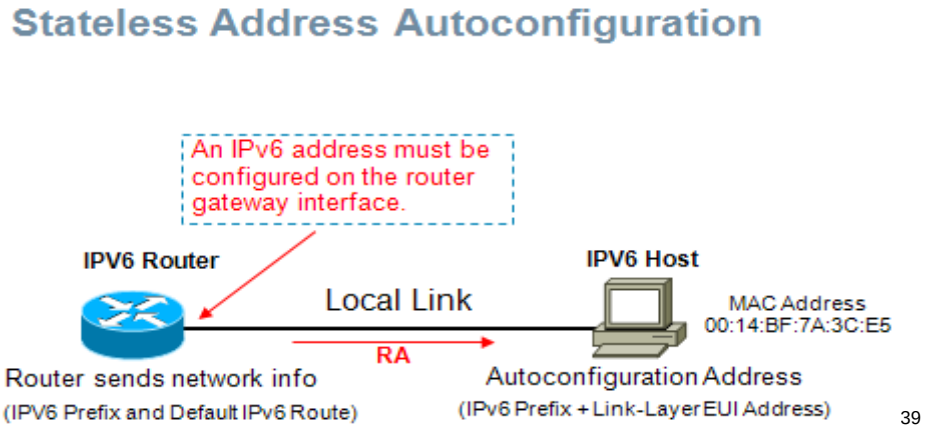
Link-Local Adresse	
Global Unicast	

Dokumentieren Sie für die Fastethernetschnittstelle von PC3:

Link-Local Adresse	
Global Unicast	
Gateway	

Autokonfiguration

Mittels Stateless Address Autoconfiguration (SLAAC, zustandslose Adressenautokonfiguration, spezifiziert in RFC 4862) kann ein Host vollautomatisch eine funktionsfähige Internetverbindung aufbauen. Dazu kommuniziert er mit den für sein Netzwerksegment zuständigen Routern, um die notwendige Konfiguration zu ermitteln.



[39]

Ablauf

Zur initialen Kommunikation mit dem Router weist sich der Host eine link-lokale Adresse zu, die im Falle einer Ethernet-Schnittstelle etwa aus deren Hardware-Adresse berechnet werden kann. Damit kann ein Gerät sich mittels des Neighbor Discovery Protocols (NDP) auf die Suche nach den Routern in seinem Netzwerksegment machen. Dies geschieht durch eine Anfrage an die Multicast-Adresse ff02::2, über die alle Router eines Segments erreichbar sind (Router Solicitation).

ICMPv6 Message[40]	Type	Description
Neighbor Solicitation (NS)	**135**	Sent by a host to determine the link-layer address of a neighbor. Used to verify that a neighbor is still reachable. An NS is also used for Duplicate Address Detection (DAD).
Neighbor Advertisement (NA)	**136**	A response to a NS message. A node may also send unsolicited NA to announce a link-layer address change.
Router Advertisement (RA)	**134**	RAs contain prefixes that are used for on-link determination or address configuration, a suggested hop limit value and MTU value. RAs are sent either periodically, or in response to a RS message.
Router Solicitation (RS)	**133**	When a host is booting it sends out an RS requesting routers to immediately generate an RA rather than wait for their next scheduled time.

Ein Router versendet auf eine solche Anfrage hin Router Advertisements. Sie besitzen Informationen über die Lifetime, die MTU und das Präfix des Netzwerks. An ein solches Präfix hängt der Host den auch für die link-lokale Adresse verwendeten Interface Identifier an.

[39] IPv6-Part2-Addr-Types, 2006, Cisco Systems
[40] IPv6-Part2-Addr-Types, 2006, Cisco Systems

Um die doppelte Vergabe einer Adresse zu verhindern, ist der Mechanismus Duplicate Address Detection (DAD – Erkennung doppelt vergebener Adressen) vorgesehen[41]. Ein Gerät darf bei der Autokonfiguration nur unvergebene Adressen auswählen. Der DAD-Vorgang läuft ebenfalls ohne Benutzereingriff via NDP ab.

EUI-64[42]

Als EUI-64 (64-Bit Extended Unique Identifier) bezeichnet man ein vom IEEE standardisiertes IP-Adressformat zur Identifikation von Netzwerkgeräten. Eine EUI-64 Adresse ist 64 Bit lang und setzt sich aus zwei Teilen zusammen:

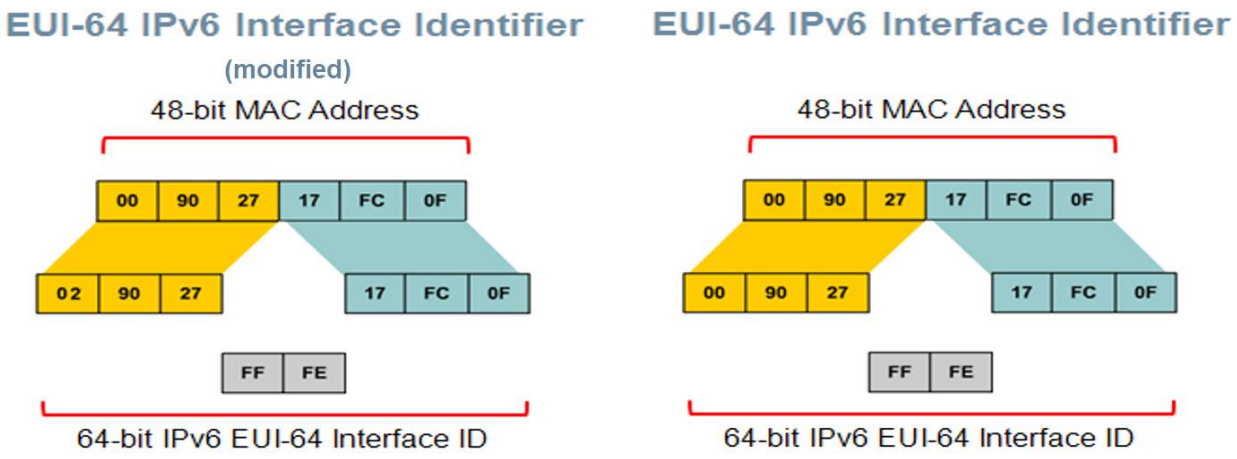
- Die ersten 24 Bit identifizieren den Hardwarehersteller (siehe OUI)
- Die restlichen 40 Bit dienen der Geräteidentifikation

Eine Variante davon ist das sogenannte modifizierte EUI-64 Adressformat, welches bei IPv6 zum Einsatz kommt. Dieses unterscheidet sich darin, dass der Wert des siebten Bits einer EUI-64 Adresse, auch Universal Bit genannt, von 0 auf 1 gesetzt wird.

Umrechnung

Eine 48 Bit lange MAC-Adresse lässt sich auch ohne Probleme in das modifizierte EUI-64 Adressformat umrechnen. Dazu geht man wie folgt vor:

1. Die MAC-Adresse wird in zwei 24 Bit lange Teile geteilt, wobei der erste Teil die ersten 24 Bit und der zweite Teil die letzten 24 Bit der modifizierten EUI-64 Adresse bilden
2. Die restlichen 16 Bits werden nach folgendem Bitmuster belegt: 1111 1111 1111 1110 (Hexadezimal: FFFE)
3. Nach Schritt zwei befindet sich die Adresse im EUI-64-Format. Wenn man nun wie oben erwähnt den Wert des **siebten** Bits invertiert, erhält man die **modifizierte** EUI-64-Adresse.



[43]

[41] RFC 2462, Abschnitt 5.4
[42] Meinel Christoph, Harald Sack: Internetworking: Technische Grundlagen und Anwendungen. Springer, Heidelberg 2012
[43] IPv6-Part2-Addr-Types, 2006, Cisco Systems

Aufgabe 12: ARP bei IPv6?

In IPv4 findet ein Host die Ethernet-Adresse zu einer IP-Adresse mit Hilfe des Address Resolution Protocol (ARP). Welches Protokoll dient dazu in IPv6?

- ☐ Ebenfalls ARP
- ☐ ARPv6
- ☐ Neighbor Discovery Protocol (NDP)
- ☐ Next Hop Recognition Protocol (NHRP)

Übung 2: Bearbeiten Sie folgende Packet-Tracer-Activitiy zur dynamischen Konfiguration von IPv6.

Sie finden die Activity in Ihrem Klassenorder im Unterordner *IPv6/PT_Uebungen*

a. *IPv6 Auto-Configuration Addressing Initial.pka*

Dokumentieren Sie für die Fastethernetschnittstelle von Router 1:

Link-Local Adresse	
EUI-64 Unicast	

Dokumentieren Sie für die Fastethernetschnittstelle von PC1:

Link-Local Adresse	
EUI-64 Unicast	
Gateway	

Dokumentieren Sie für die Fastethernetschnittstelle von Router 2:

Link-Local Adresse	
EUI-64 Unicast	

Dokumentieren Sie für die Fastethernetschnittstelle von PC2:

Link-Local Adresse	
EUI-64 Unicast	
Gateway	

Dokumentieren Sie für die Fastethernetschnittstelle von Router 3:

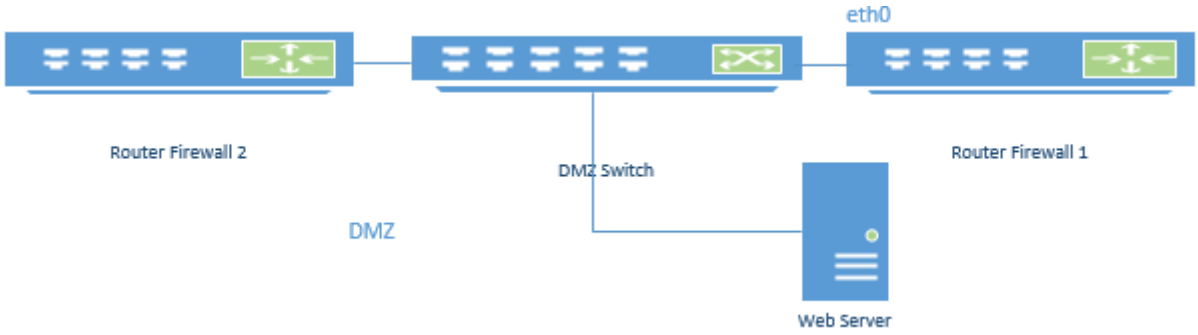
Link-Local Adresse	
EUI-64 Unicast	

Dokumentieren Sie für die Fastethernetschnittstelle von PC3:

Link-Local Adresse	
EUI-64 Unicast	
Gateway	

Aufgabe 13:

Netzwerkplan (Ausschnitt)



Sie verwenden stateless host autoconfiguration mit EUI-64 in der DMZ des Netzwerks. Die Routerfirewall 1 unterstützt auf seinem Fastethernet Interface eth0 IPv6.

Ausschnitt aus der Konfiguration des Fastethernet Interface eth0 der Router Firewall 1:

```
Physikalische Adresse . . . . : 00-E0-81-55-32-A7
DHCP aktiviert .. . . . . : Nein
IP-Adresse . . . . . : 2001:db8:ae45:232::c7b:303a
IP-Adresse . . . . . : fe80::2e0:81ff:fe55:32a7%5
IP-Adresse . . . . . : 192.168.2.20
Subnetz-Maske . . . . . : 255.255.255.0
```

Die IPv6-Adressvergabe- Einstellungen des Webservers stehen auf „Auto“. Die physikalische Adresse des Webservers lautet: 0A-E0-FF-02-AB-CD. Wie lautet:

a) Die Link Local IPv6 Adresse des Webservers?

b) Die Global Unicast Adresse des Webservers, wenn im in der DMZ ein Präfix von /64 verwendet wird?

Geben Sie für die Global Unicast Adresse des Webservers folgendes an:

Site-Präfix:	
Subnet-Präfix	
Das Netz	
Interface Identifier	

c) Das Standard Gateway des Webservers, das per stateless host autoconfiguration auf dem Webserver eingetragen wird?

Aufgabe 14:

Sie überprüfen die Konfiguration eines PC:

```
C:\> ipconfig /all
Windows-IP-Konfiguration
        Hostname.. : PC-20
Ethernet-Adapter LAN-Verbindung:
Beschreibung . . . . . : IntelPro100/1000
Physikalische Adresse . . . . : 00-E0-81-55-32-A7
DHCP aktiviert .. . . . . : Nein
IP-Adresse . . . . . : 2001:db8:ae45:232::c7b:303a
IP-Adresse . . . . . : fe80::2e0:81ff:fe55:32a7%5
IP-Adresse . . . . . : 192.168.2.20
Subnetz-Maske . . . . . : 255.255.255.0
Standardgateway . . . . . . 192.168.2.254
DNS-Server . . . . . : 192.168.2.254
                                    2001:db8:ae45:232::45b:1
```

Nennen Sie die Link-Local-Adresse des PC:

Nennen Sie die IPv6-Unicast-Adresse des PC.

Geben Sie für die IPv6-Unicast-Adresse des PC folgendes an:

Site-Präfix:	
Subnet-Präfix	
Das Netz	
Interface Identifier	

Bei einem Ping-Test vom PC zum aktiven Server „2001:db8:1234:45::a66:b7“ wird dieser nicht erreicht. Nennen Sie einen möglichen Grund und eine beschreiben Sie eine Lösungsmöglichkeit.

Der PC kann einen UNIX Server in der Firma nicht erreichen. Ausgabe der Schnittstelle eth0 des Servers zeigt folgende Konfiguration:

```
# ifconfig eth0
eth0: ether 00-90-dc-05-76-30
      inet 192.168.2.22 netmask 255.255.255.0 broadcast 192.168.2.255
      inet6 fe80::290:dcff:fe05:7630%eth0 prefixlen 64
      inet6  2001:db8:ae45:232::c7b:303a prefixlen 64 duplicated
      media: Ethernet autoselect (100base TX)
      status: active
```

Nennen Sie eine mögliche Fehlerursache und beschreiben Sie eine Lösung.

***Header-Format* : IPv6-Header**

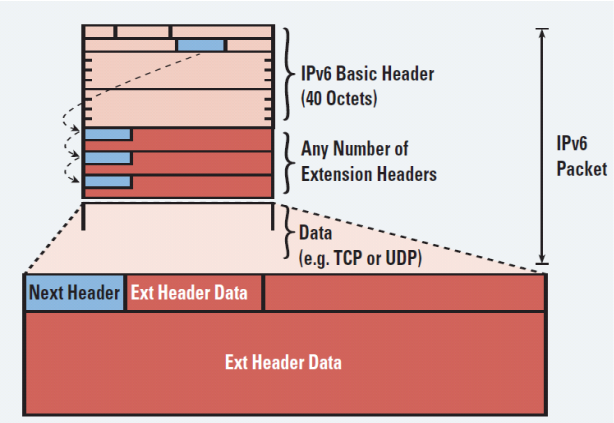
Version (4 bit)	Traffic Class (8bit)	Flow Label (20bit)	
Payload lenght (16bit)		Next Header (8bit)	Hop Limit (8bit)
Source Address (128bit)			
Destination Address (128bit)			
Payload (up to 1024 bytes)			

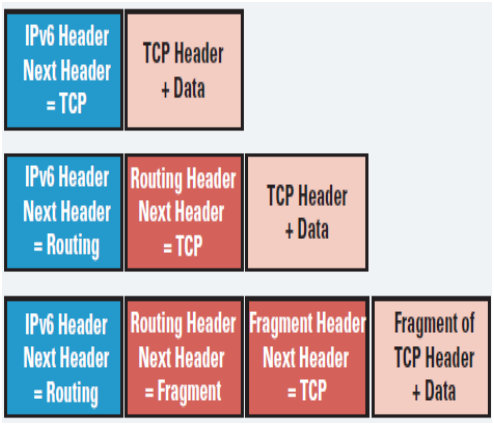
Im Gegensatz zu IPv4 hat der IP-Kopfdatenbereich (Header) bei IPv6 eine feste Länge von 40 Bytes (320 Bits).

Optionale, seltener benutzte Informationen werden in so genannten Erweiterungs-Kopfdaten (engl.: *Extension Headers*) zwischen dem IPv6-Kopfdatenbereich und der eigentlichen Nutzlast (engl. *Payload*) eingebettet. Der Kopfdatenbereich eines IPv6-Paketes setzt sich laut RFC 2460 aus den folgenden Feldern zusammen:

Feld	Länge	Inhalt
Version	4 Bit	IP-Versionsnummer (6)
Traffic Class	8 Bit	Für Quality of Service (QoS) verwendeter Wert. Eine Art Prioritätsvergabe.
Flow Label	20 Bit	Ebenfalls für *QoS* oder Echtzeitanwendungen verwendeter Wert. Pakete, die dasselbe Flow Label tragen, werden gleich behandelt.
Payload Length	16 Bit	Länge des IPv6-Paketinhaltes (ohne Kopfdatenbereich, aber inklusive der Erweiterungs-Kopfdaten) in Byte
Next Hader	8 Bit	Identifiziert den Typ des nächsten Kopfdatenbereiches, dieser kann entweder einen Erweiterungs-Kopfdatenbereich (siehe nächste Tabelle) oder ein Protokoll höherer Schicht (engl.: *Upper Layer Protocol*) bezeichnen, wie z.B. TCP (Typ 6) oder UDP (Typ 17).
Hop Limit	8 Bit	Maximale Anzahl an Zwischenschritten über Router, die ein Paket zurücklegen darf; wird beim Durchlaufen eines Routers („Hops“) um eins verringert. Pakete mit null als *Hop Limit* werden verworfen. Es entspricht dem Feld Time to Live (TTL) bei IPv4.
Source Address	128 Bit	Adresse des Senders
Destination Address	128 Bit	Adresse des Empfängers

Wie im *Next Header* Feld verwiesen sind einige *Extension Headers* und ein Platzhalter definiert:





[44]

Name	Typ	Größe	Beschreibung	RFCs
Hop-By-Hop Options	0	variabel	Enthält Optionen, die von allen IPv6-Geräten, die das Paket durchläuft, beachtet werden müssen. Wird z. B. für Jumbograms benutzt.	RFC 2460, RFC 2675
Routing	43	variabel	Durch diesen Header kann der Weg des Paketes durch das Netzwerk beeinflusst werden, er wird unter anderem für Mobile IPv6 verwendet.	RFC 2460, RFC 6275, RFC 5095
Fragment	44	64 Bit	In diesem Header können die Parameter einer Fragmentierung festgelegt werden.	RFC 2460
Authentication Header (AH)	51	variabel	Enthält Daten, welche die Vertraulichkeit des Paketes sicherstellen können (siehe IPsec).	RFC 4302
Encapsulating Security Payload (ESP)	50	variabel	Enthält Daten zur Verschlüsselung des Paketes (siehe IPsec).	RFC 4303
Destination Options	60	variabel	Enthält Optionen, die nur vom Zielrechner des Paketes beachtet werden müssen.	RFC 2460
Mobility	135	variabel	Enthält Daten für *Mobile IPv6*.	RFC 6275
No Next Header	59	leer	Dieser Typ ist nur ein Platzhalter, um das Ende eines Header-Stapels anzuzeigen.	RFC 2460

Die meisten IPv6-Pakete sollten ohne *Extension Headers* auskommen, diese können bis auf den *Destination Options Header* nur einmal in jedem Paket vorkommen. Befindet sich ein *Routing Extension Header* im Paket, so darf davor ein weiterer *Destination Options Header* stehen. Die Reihenfolge bei einer Verkettung ist bis auf die genannte Ausnahme die der Tabelle. Alle *Extension Headers* enthalten ein *Next-Header*-Feld, in dem der nächste *Extension Header* oder das *Upper Layer Protocol* genannt wird.
Des Weiteren werden (im Gegensatz zu IPv4) keine Prüfsummen mehr über die IP-Kopfdaten berechnet, es wird nur noch die Fehlerkorrektur in den Schichten 2 und 4 genutzt.

[44] IPv6-Part1-Addr-Types, 2006, Cisco Systems

Aufgabe 15:

p	t	k	n	u	p	l	e	p	p	o	d
o	s	z	f	o	g	u	f	i	e	k	n
m	m	e	d	e	j	n	t	p	o	m	ä
u	e	e	c	n	a	i	s	m	s	a	c
l	l	i	a	v	y	c	p	e	g	x	h
t	c	a	n	y	c	a	s	t	b	i	s
l	u	f	m	s	t	s	l	r	a	m	t
c	r	o	p	i	g	t	t	l	o	a	e
a	r	h	b	b	f	s	l	a	k	l	n
s	h	e	x	a	d	e	z	i	m	a	l
t	l	a	e	a	n	r	p	a	k	e	t
t	t	d	s	a	e	s	s	e	r	d	a
e	h	e	c	z	w	i	s	c	h	e	n
u	c	r	e	o	n	e	t	z	t	e	l
w	a	b	w	ä	r	t	s	o	n	f	c
m	z	i	e	l	r	e	c	h	n	e	r

IPv6 WORDSEARCH EXERCISE

Work on your own and fill in the blanks with the correct terms.
Then find them in the wordsearch grid.

1. Die IPv6 Adresse wird _____ beschrieben
2. Die Adresse wird in _____ Blöcke geteilt
3. Die Blöcke werden durch einen _____ getrennt
4. Die 32-Bit der IPv4-Adresse werden in die _____ Stellen der 128-Bit Struktur des IPv6 übernommen
5. IPv6 ermöglicht drei Verfahren für das Versenden der Daten: _____ , _____ und _____
6. Ein Datenpaket, das zu einer Unicast-Schnittstelle gesendet wird, wird an der durch die _____ bestimmten Schnittstelle abgeliefert.
7. Ein Datenpaket, das zu einer Multicast-Schnittstelle gesendet wird, wird bei _____ durch das Set definierten Schnittstellen abgeliefert.
8. In IPv6 werden Erweiterungs- _____ zum Transport zusätzlicher Informationen verwendet.
9. Sie werden _____ dem Basis Header und den Nutzdaten (upper layer header) platziert.
10. Options-Header werden verwendet, um Optionen zu transportieren, welche bei _____ Transportschritt ausgewertet werden müssen.
11. Jeder Header (außer dem Destination Options Header) darf nur _____ -mal verwendet werden.

Routing

Während statisches Routing für IPv6 analog zu IPv4 eingerichtet werden kann, ergeben sich für die dynamischen Routingprotokolle einige Änderungen. Zwischen Autonomen Systemen wird das Border Gateway Protocol mit den Multiprotocol Extensions (definiert in RFC 4760) eingesetzt. Als Interior Gateway Protocol stehen OSPF in der Version 3, IS-IS mit Unterstützung von IPv6-TLVs und RIPng als offene Standards zur Verfügung. Die meisten Hersteller unterstützen für IS-IS Multi-Topology Routing, also gleichzeitiges Routing für beide Adressfamilien auch dann, wenn IPv4- und IPv6-Netz sich nicht genau überdecken.

An Endsysteme können eine oder mehrere Default-Routen per Autokonfiguration oder DHCPv6 übergeben werden. Mit DHCPv6-PD (Prefix Delegation) können auch Präfixe zwecks weiteren Routings zum Beispiel an Kundenrouter verteilt werden[45].

Übung 3: Bearbeiten Sie folgende Packet-Tracer-Activitiy zur statischen Routing mit IPv6.
Sie finden die Activity in Ihrem Klassenorder im Unterordner *IPv6/PT_Uebungen*

a. *IPv6 Static Routes Initial.pka*

Übung 4: Bearbeiten Sie folgende Packet-Tracer-Activitiy zur dynamischen Routing mit IPv6.
Sie finden die Activity in Ihrem Klassenorder im Unterordner *IPv6/PT_Uebungen*

a. *IPv6 RIP Initial.pka*

IPv6-Übergangsmechanismen

IPv4 und IPv6 lassen sich auf derselben Infrastruktur, insbesondere im Internet, parallel betreiben. Für den Übergang werden also in der Regel keine neuen Leitungen, Netzwerkkarten oder Geräte benötigt, sofern dafür geeignete Betriebssysteme zur Verfügung stehen. Es gibt zurzeit kaum Geräte, welche IPv6, aber nicht gleichzeitig auch IPv4 beherrschen. Damit jedoch Geräte, die ausschließlich über IPv4 angebunden sind, auch mit Geräten kommunizieren können, die ausschließlich über IPv6 angebunden sind, benötigen sie Übersetzungsverfahren.
Um einen einfachen Übergang von IPv4- zu IPv6-Kommunikation im Internet zu ermöglichen, wurden verschiedene Mechanismen entwickelt. IPv6 wird dabei in der Regel hinzugeschaltet, ohne IPv4 abzuschalten. Grundlegend werden folgende drei Mechanismen unterschieden:

- **Parallelbetrieb (Dual-Stack)**
- **Tunnelmechanismen**
- **Übersetzungsverfahren**

Parallelbetrieb und Tunnelmechanismen setzten voraus, dass die Betriebssysteme der angebundenen Rechner beide Protokolle beherrschen.

[45] Vishwas Manral: RSVP-TE IPv6
Vishwas Manral: Updates to LDP for IPv6

Es gibt bereits heute Bereiche des Internet, die ausschließlich mittels IPv6 erreichbar sind, andere Teile, die über beide Protokolle angebunden sind und große Teile, die sich ausschließlich auf IPv4 verlassen

Dual-Stack
Bei diesem Verfahren werden allen beteiligten Schnittstellen neben der IPv4-Adresse zusätzlich mindestens eine IPv6-Adresse und den Rechnern die notwendigen Routinginformationen zugewiesen. Die Rechner können dann über beide Protokolle unabhängig kommunizieren. Dieses Verfahren sollte der Regelfall sein, es scheitert derzeit oft daran, dass einige Router (meistens die Zugangsserver des Internetproviders oder die Heimrouter bei den Kunden) auf dem Weg zum IPv6-Internet noch keine IPv6-Weiterleitung eingeschaltet haben oder unterstützen.

Dual-Stack Lite (DS-Lite)
Aufgrund der knappen IPv4-Adressen hat die IETF den Mechanismus "Dual-Stack Lite" (RFC 6333) entwickelt. Hierbei werden dem Kunden nur via IPv6 global routbare IP-Adressen bereitgestellt.
Im LAN des Kunden werden private IPv4-Adressen benutzt (analog zum Vorgehen bei einem NAT). Statt einer NAT-Übersetzung werden die IPv4-Pakete dann durch das Customer Premises Equipment (CPE) in IPv6-Pakete gekapselt. Das CPE benutzt seine globale IPv6-Verbindung, um die Pakete in das Carrier-grade NAT des Internet Service Providers zu transportieren, welches über globale IPv4-Adressen verfügt. Hier wird das IPv6-Paket entpackt und das originale IPv4-Paket wieder hergestellt, danach wird das IPv4-Paket mit NAT auf eine öffentliche IP-Adresse umgesetzt und ins öffentliche IPv4-Internet geroutet.

Tunnelmechanismen
Um Router, die IPv6 nicht weiterleiten, auf dem Weg zum IPv6-Internet zu überbrücken, gibt es eine Vielzahl von Tunnelmechanismen. Dabei werden IPv6-Pakete in den Nutzdaten anderer Protokolle, meist IPv4, zu einer Tunnelgegenstelle übertragen, die sich im IPv6-Internet befindet. Dort werden die IPv6-Pakete herausgelöst und zum Ziel via IPv6-Routing übertragen. Der Rückweg funktioniert analog.
6in4 benutzt zum Beispiel den Protokolltyp 41, um IPv6 direkt in IPv4 zu kapseln.

Der Mechanismus 6to4 benötigt keine Absprache mit einer Gegenstelle, denn diese benutzt wohlbekannte, mehrfach im Internet vergebene IPv6-Adressen (Anycast), und die getunnelten Pakete werden zur nächstgelegenen Gegenstelle zugestellt und dort verarbeitet. Dem angebundenen Rechner steht dann ein IPv6-Adressbereich zur Verfügung, der sich aus dessen öffentlicher IPv4-Adresse errechnet. Auch ein solcher Tunnel kann auf aktuellen Linux-Rechnern mit öffentlicher IPv4-Adresse durch wenige Handgriffe eingerichtet werden[46].

Befindet sich ein Rechner in einem privaten IPv4-Adressbereich und findet beim Verbinden mit dem Internet NAT statt, so können Mechanismen wie AYIYA oder Teredo helfen. Diese Protokolle kapseln IPv6-Pakete als Nutzdaten meist in UDP-Paketen.

[46] Peter Bieringer: Linux IPv6 Howto, Abschnitt 9.4

Natürlich ist es auch möglich, IPv6 über allgemeinere Tunnelverfahren wie GRE, L2TP oder MPLS zu transportieren, insbesondere, wenn noch Routingprotokolle wie IS-IS parallel übertragen werden müssen.

Übersicht über gängige Übergangsmechanismen:

4in6	Tunneling von IPv4 in IPv6
6in4	Tunneling von IPv6 in IPv4
6over4	Transport von IPv6-Datenpaketen zwischen Dual-Stack Knoten über ein IPv4-Netzwerk
6to4	Transport von IPv6-Datenpaketen über ein IPv4-Netzwerk
AYIYA	Anything In Anything
Dual-Stack	Netzknoten mit IPv4 und IPv6 im Parallelbetrieb
Dual-Stack Lite	Wie Dual-Stack, jedoch mit globaler IPv6 und Carrier-NAT IPv4
6rd	IPv6 rapid deployment
ISATAP	Intra-Site Automatic Tunnel Addressing Protocol
NAT64	Übersetzung von IPv4-Adressen in IPv6-Adressen
Teredo	Kapselung von IPv6-Datenpaketen in IPv4-UDP-Datenpaketen
SIIT	Stateless IP/ICMP Translation

Aufgabe 16: Dual-Stack-Systeme

Welche IP-Version sollten Dual-Stack-Systeme bevorzugen?

- ☐ grundsätzlich IPv6
- ☐ grundsätzlich IPv4
- ☐ Natives IPv6, dann IPv4, dann IPv6 per Teredo oder 6to4
- ☐ IPv6 per Teredo oder 6to4, dann IPv4, dann natives IPv6