Name: Klasse: Datum:

IPv6
Workbook
Grundlagen und Adressierung

Name: Klasse: Datum:

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: Kurz und knapp….

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].

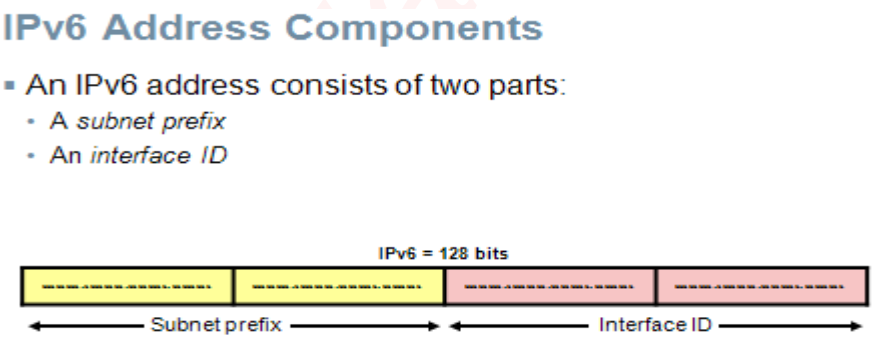
Heute übliche Verfahren wie Network Address Translation (NAT), welche derzeit die IPv4-Adressknappheit umgehen, verletzen das Ende-zu-Ende-Prinzip[13]. Sie ermöglichen den so angebundenen Rechnern nur ausgehende Verbindungen aufzubauen. Aus dem Internet können diese hingegen nicht ohne weiteres kontaktiert 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 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,

[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.

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.
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

[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

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: Kurz und knapp….

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

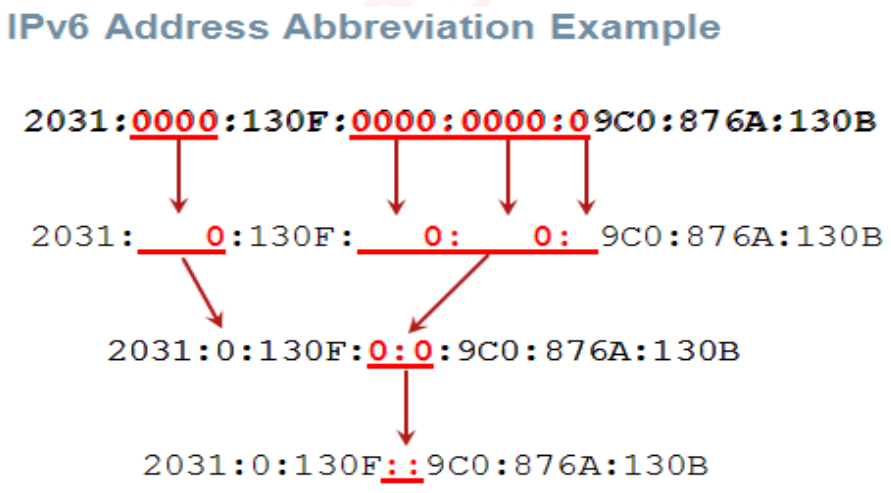
Name: Klasse: Datum:

Adressnotation

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

1. IPv6-Adressen werden gewöhnlich 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 entfallen: 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

Name: Klasse: Datum:

Aufgabe 3: Kurz und knapp….

Welches sind gültige IPv6-Adressen für einen Netzknoten?

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

Aufgabe 4: Kurz und knapp….

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 der kürzesten Schreibweise an:

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

Aufgabe 5: Kurz und knapp….

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: Kurz und knapp….

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

Name: Klasse: Datum:

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,
der Netzpräfix	2001:0db8:85a3:08d3:0000:0000:0000:0000/64
der Geräteteil oder Interface Identifier	1319:8a2e:0370:7347.

Aufgabe 7: Kurz und knapp….

Geben Sie den Netz-/Subnetzpräfix an in dem sich der Host mit der IPv6-Adresse 2001:0db8:85a3:08d3:1319:8a2e:0370:7344/64 befindet?

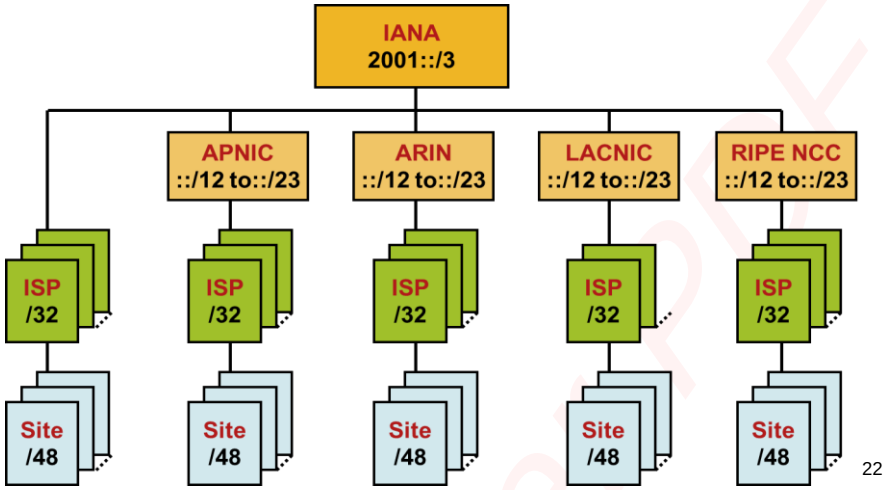
Aufgabe 8: Kurz und knapp….

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

Name: Klasse: Datum:

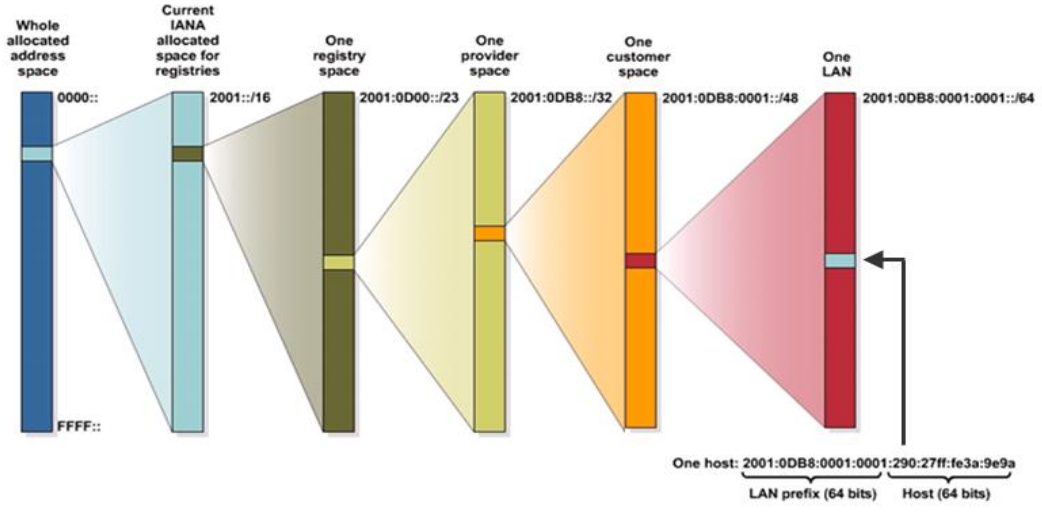
Adresszuweisung

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 in weitere Teilnetze unterteilt.



22

Die Länge der Zuteilung an Endkunden wird dabei dem ISP überlassen; vorgeschrieben ist die maximale 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].

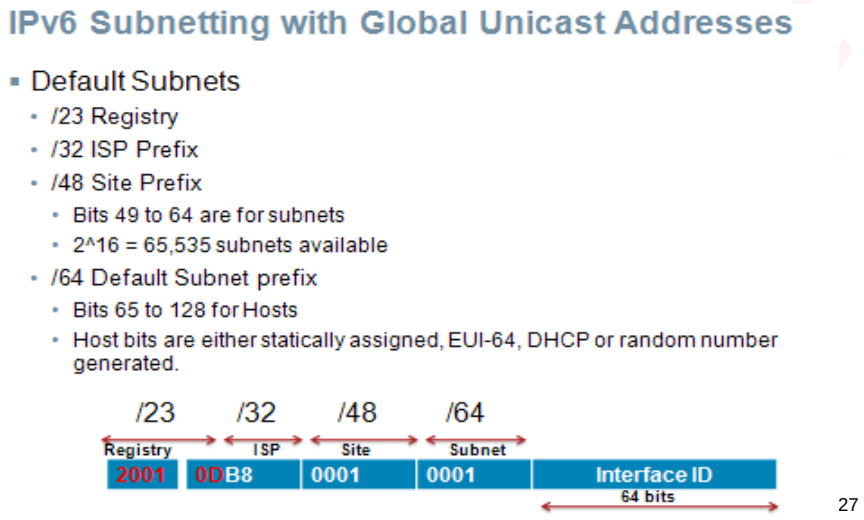


25

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.

[26] RFC 4291, Abschnitt 2.5.4

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

Name: Klasse: Datum:

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:

Aufgabe 10:

Der in Aufgabe 9 benannte 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:

Name: Klasse: Datum:

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. Unicastadressen 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.	**Erforderliche Parameter fehlen oder sind falsch.**
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.	**Erforderliche Parameter fehlen oder sind falsch.**
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.	**Erforderliche Parameter fehlen oder sind falsch.**

IPv6-Adressen mit besonderer Funktion

- ::/128 (128 0-Bits) ist die nichtspezifizierte 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.

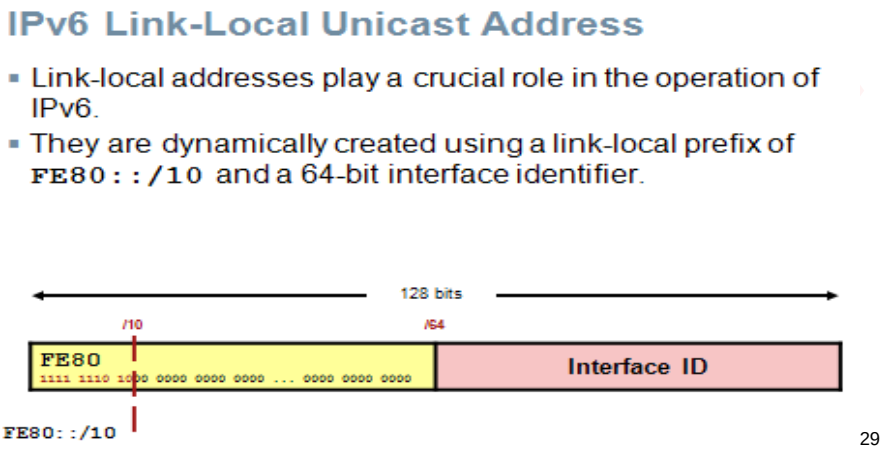
- ::1/128 (127 0-Bits, ein 1-Bit) ist die Adresse des eigenen Standortes (Loopback-Adresse, die in der Regel mit localhost verknüpft ist).

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

Name: Klasse: Datum:

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 von Adressen oder für das Neighbour-Discovery Protocol (NDP). 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.

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

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.

Unique Local Unicast

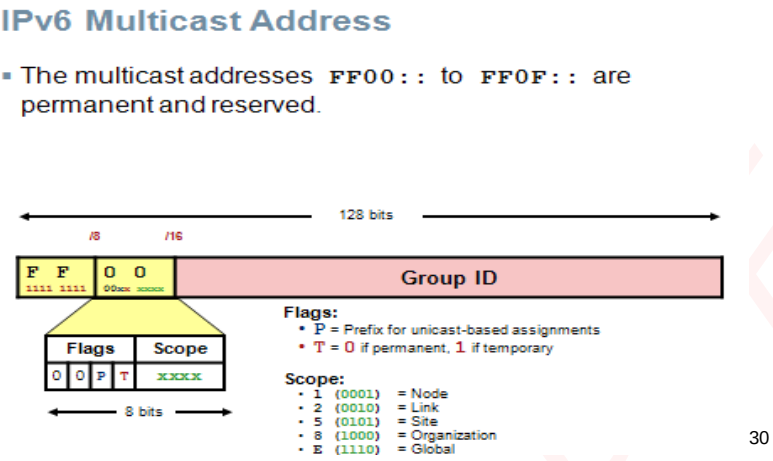
- fc00::/7 (fc… und fd…). Für private Adressen gibt es die Unique Local Addresses (ULA), beschrieben in RFC 4193. Derzeit ist nur das Präfix fd für lokal generierte ULA vorgesehen, mit dem Präfix fc werden in Zukunft wahrscheinlich global zugewiesene eindeutige ULA gekennzeichnet. Auf dieses Präfix folgen 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.

Name: Klasse: Datum:

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]
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

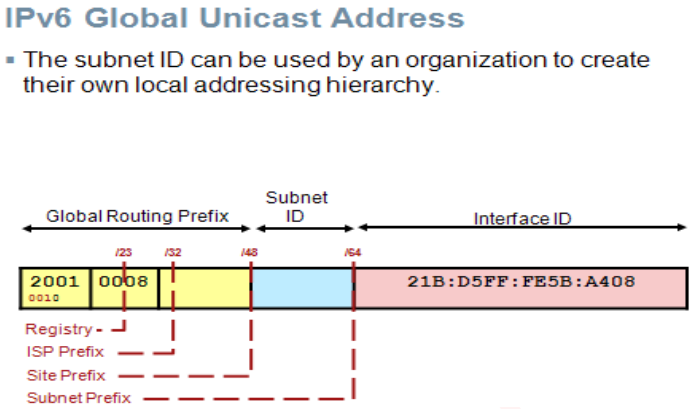
Die restlichen Bereiche sind nicht zugewiesen und dürfen von Administratoren benutzt werden, um weitere Multicast-Regionen zu definieren[34].

[30] IPv6-Part2-Addr-Types, 2006, Cisco Systems
[31] RFC 2373, Abschnitt 2.7
[32] RFC 3307, Abschnitt 4.1
[33] RFC 2373, Abschnitt 2.7
[34] RFC 4291, Abschnitt 2.7

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-Adressen



[36]

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

- ::/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 eindeutige 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.

[35] IANA: Internet Protocol Version 6 Multicast Addresses
[36] IPv6-Part2-Addr-Types, 2006, Cisco Systems
[37] IANA: IPv6 Unicast Address Assignments

Name: Klasse: Datum:

Aufgabe 11:

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

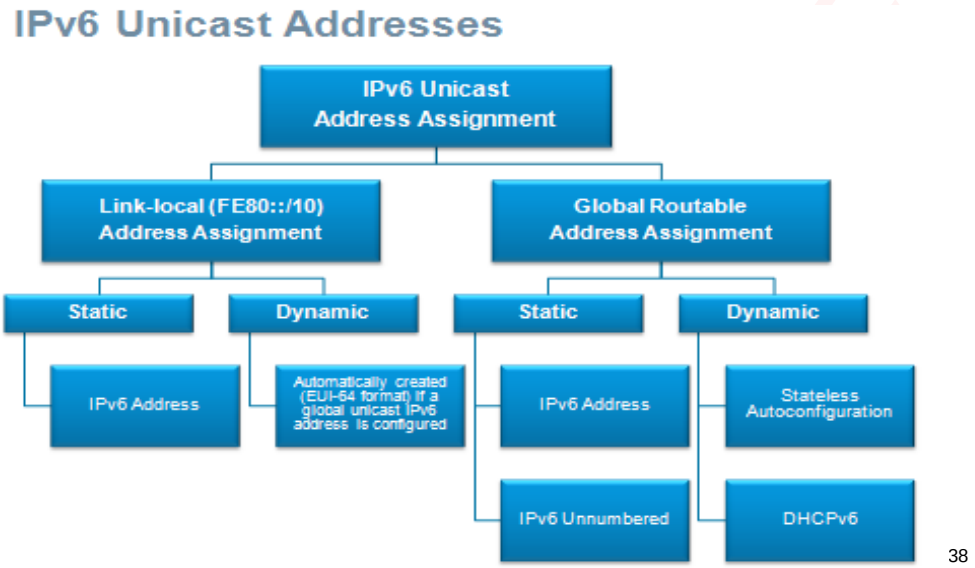
Beschreibung	IPv4	IPv6	Bemerkung
Loopback Adresse			
Default Route, nichtspezifizierte Adresse			
Private Adressen			
Multicast Adressen			

Name: Klasse: Datum:

Funktionalität

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

Wie bei IPv4, kann man IPv6 Adressen manuell (statisch) konfigurieren oder dynamischen generieren bzw. zugewiesen bekommen.



[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

Name: Klasse: Datum:

Dokumentieren Sie für die Fastethernet-Schnittstelle 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	

Name: Klasse: Datum:

Aufgabe 12

Das Firmennetzwerk besteht aus einer einzelnen Active Directory Domäne. Auf allen Servercomputern ist das Betriebssystem Microsoft Windows Server 2xxx installiert. Auf allen Clientcomputern wird Microsoft Windows Vista ausgeführt. Das Unternehmen umfasst aktuell drei Standorte. Ein vierter Standort befindet sich in der Planungsphase.
Ihr Vorgesetzter bittet Sie, dem neuen Standort ein Subnetz unter Verwendung des globalen Adresspräfixes 3FFA:FF2B:4D:A000::/51 zuzuweisen.

Gehen Sie wie folgt vor:

1. Lösen Sie den Netzpräfix der IPv6 Adresse binär auf. Da jedes Hex-Zeichen mit 4 Bit codiert wird, teilen Sie die 16-Bit-Blöcke in 4 mal 4 Bit und jedem Bit wird ein Wert 2^n zugewiesen
2. Da jetzt das existierende Netz /51 in 4 weitere Subnetze aufgeteilt werden soll, müssen 2 weitere Bits für das Subnetting zum Netzpräfix hinzugefügt werden. Der neue Netzpräfix ist dann /53.

Zu1)

1. Block

3				F				F				A			
2^3	2^2	2^1	2^0	2^3	2^2	2^1	2^0	2^3	2^2	2^1	2^0	2^3	2^2	2^1	2^0
0	0	1	1												
Netz															

2. Block

F				F				2				B			
2^3	2^2	2^1	2^0	2^3	2^2	2^1	2^0	2^3	2^2	2^1	2^0	2^3	2^2	2^1	2^0
Netz															

3. Block

0				0				4				D			
2^3	2^2	2^1	2^0	2^3	2^2	2^1	2^0	2^3	2^2	2^1	2^0	2^3	2^2	2^1	2^0
Netz															

4. Block

A				0				0				0			
2^3	2^2	2^1	2^0	2^3	2^2	2^1	2^0	2^3	2^2	2^1	2^0	2^3	2^2	2^1	2^0
Netz															

Name: Klasse: Datum:

Zu 2)

1. Block															
3				F				F				A			
2^3	2^2	2^1	2^0	2^3	2^2	2^1	2^0	2^3	2^2	2^1	2^0	2^3	2^2	2^1	2^0
0	0	1	1												
Netz															

2. Block															
F				F				2				B			
2^3	2^2	2^1	2^0	2^3	2^2	2^1	2^0	2^3	2^2	2^1	2^0	2^3	2^2	2^1	2^0
Netz															

1. Block															
0				0				4				D			
2^3	2^2	2^1	2^0	2^3	2^2	2^1	2^0	2^3	2^2	2^1	2^0	2^3	2^2	2^1	2^0
Netz															

4. Block															
A				0				0				0			
2^3	2^2	2^1	2^0	2^3	2^2	2^1	2^0	2^3	2^2	2^1	2^0	2^3	2^2	2^1	2^0
Netz															

Ergänzen Sie die Werte für die neuen Subnet-ID für die neuen Teilnetze:

Standort 1: 3FFA:FF2B:4D:A000:: /53

Standort 2: 3FFA:FF2B:4D:A800:: /53

Standort 3: 3FFA:FF2B:4D:B000:: /53

Standort 4: 3FFA:FF2B:4D:B800:: /53

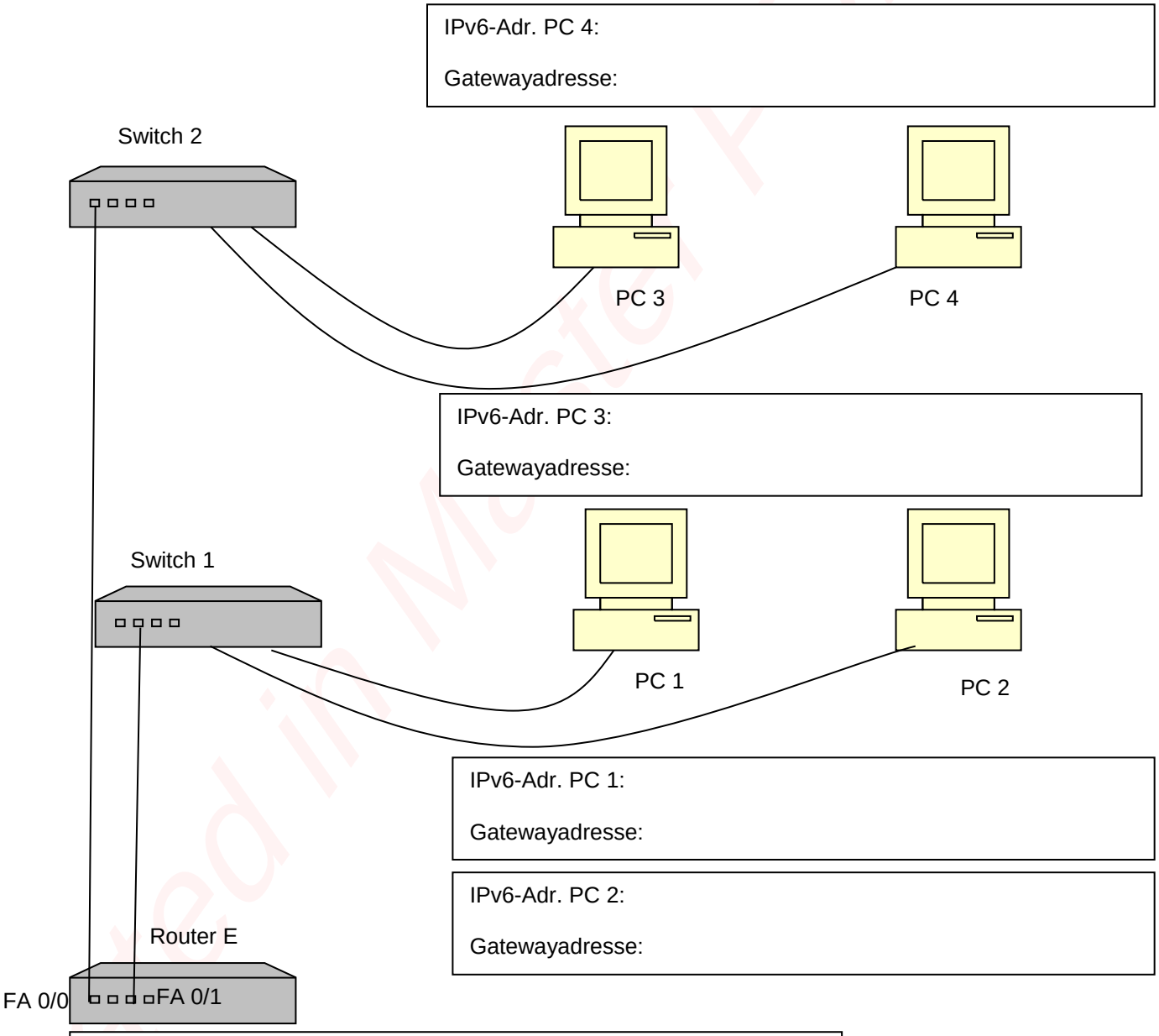
Name: Klasse: Datum:

Aufgabe 12A:

Erstellen Sie für den unten abgebildeten Ausschnitt aus dem Netzwerk einen Netzplan mit IPv6-Adressen. Beachten Sie dabei, dass PC 1 / PC 2 in einem anderen Subnetz liegen müssen als PC 3 / PC 4. Nutzen Sie zur Subnetzbildung die IPv6 Adresse: 2001:db8:ae45:2000::/52.

Geben Sie die folgenden Präfixe an:

Site-Präfix:	2001:db8:ae45::/48
Subnet-Präfix	



Name: Klasse: Datum:

1. Stellen Sie den Netzpräfix der IPv6 Adresse binär dar. Da jedes Hex-Zeichen mit 4 Bit codiert wird, teilen Sie die 16-Bit-Blöcke in 4 mal 4 Bit und jedem Bit wird ein Wert 2^n zugewiesen
2. Da das existierende Netz eine Präfixlänge von /52 in _____weitere Teilnetze aufgeteilt werden soll, bedeutet dies, dass _____ weitere(s) Bit(s) aus dem Subnetzteil der Adresse verwendet werden soll. Der neue Netzpräfix hat nun eine Länge von /_____ .

1. Block

2				0				0				1			
2^3	2^2	2^1	2^0	2^3	2^2	2^1	2^0	2^3	2^2	2^1	2^0	2^3	2^2	2^1	2^0
Netz															

2.Block

0				D				B				8			
2^3	2^2	2^1	2^0	2^3	2^2	2^1	2^0	2^3	2^2	2^1	2^0	2^3	2^2	2^1	2^0
Netz															

3.Block

A				E				4				5			
2^3	2^2	2^1	2^0	2^3	2^2	2^1	2^0	2^3	2^2	2^1	2^0	2^3	2^2	2^1	2^0
Netz															

4. Block

2															
2^3	2^2	2^1	2^0	2^3	2^2	2^1	2^0	2^3	2^2	2^1	2^0	2^3	2^2	2^1	2^0
Netz															

3. Notieren Sie die IPv6 Netzpräfix für die entstandenen Netze und geben Sie den mögliche Wertebereich für die Adressen an.
4.

Subnetz 1: 2001:db8:ae45:2000::/53 /___

Hostbereich von: 2001:db8:ae45:2000::/53 /___ bis 2001:db8:ae45:24ff:ffff:ffff:ffff:ffff/53 /___

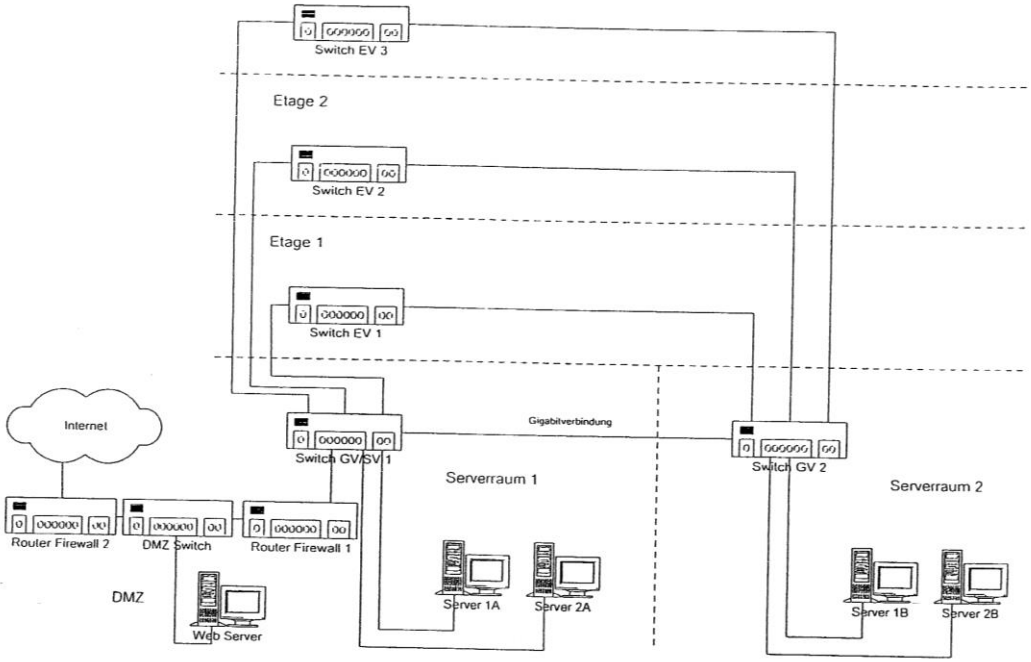
Subnetz 2: 2001:db8:ae45:2800::/53 /___

Hostbereich von: 2001:db8:ae45:2800::/53 /____ bis 2001:db8:ae45:2fff:ffff:ffff:ffff:ffff/53 /_

Name: Klasse: Datum:

Aufgabe 12B:

Die Weinstein AG in Stralsund ist eine Weinhandlung. Jährlich verkauft sie ca. 6 Mio. Flaschen Wein über verschiedene Vertriebswege. Sie betreibt einen Groß- und Versandhandel sowie eine Weinladenkette mit 60 Filialen. Sie sollen in einem Projektteam an der Umstellung auf ein neues DV System für eine neue Geschäftsstelle mitarbeiten.



Netzwerkplan der Geschäftsstelle:

Ebene 0: Technikbereich und Archiv
Etage 1: Eingangsbereich und Verkauf
Etage 2: Cafeteria und Verwaltung
Etage 3: Entwicklung

2001:b8:ae:00/00|0000|0000|0000|::/50
2001:b8:ae:00/00|0/000|0000|0000|::/53
2001:b8:ae:0::
2001:b8:ae:00/00|1/000|0000|0000|::/53
2001:b8:ae:800::/53
2001:b8:ae:00/01|0/000|0000|0000|::/53
2001:b8:ae:1000::/53
2001:b8:ae:00/01|1/000|0000|0000|::/53
2001:b8:ae:1800::/53
2001:b8:ae:2000::/53

a) Der Kunde wünscht für die neue Geschäftsstelle die Umsetzung von IPv6. Hierfür wurde Ihnen Sie der folgende IPv6-Netzpräfix zugewiesen:
2001: b8:ae::/50.
Jede Ebene des Gebäudes soll ein eigenes Teilnetz bilden. Die Teilnetze in den Ebenen sollen alle gleich groß sein und auf eine möglichst hohe Anzahl an Hosts pro Teilnetz optimiert werden. Geben Sie für jedes Teilnetz die Subnetzadresse an.

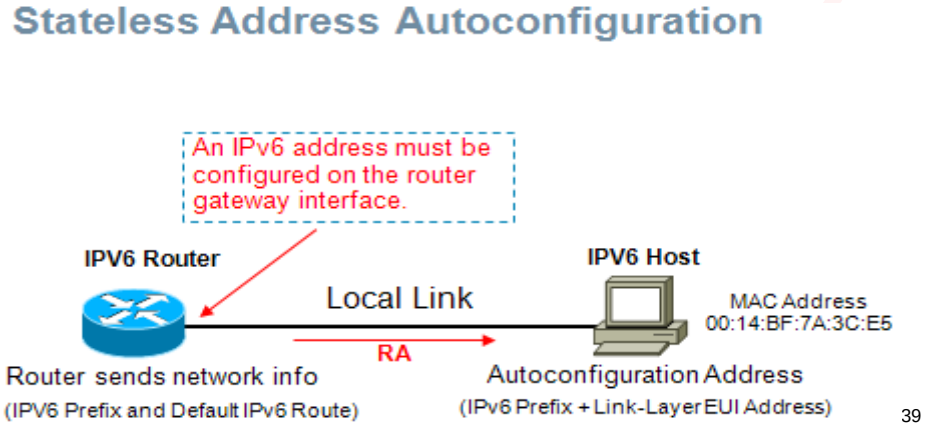
Name: Klasse: Datum:

Lösung:

Name: Klasse: Datum:

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:

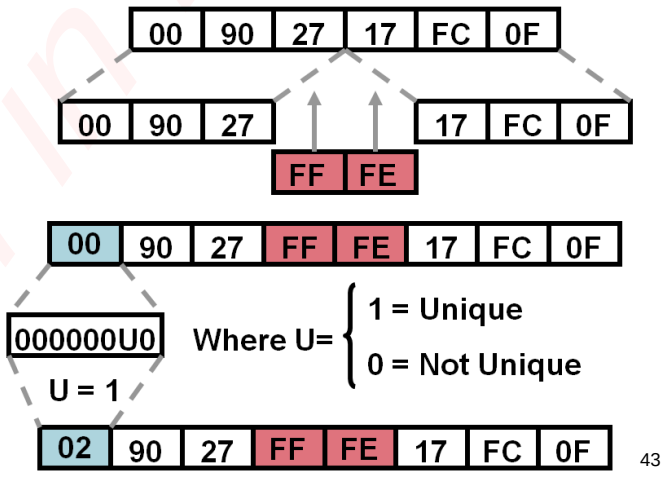
- Die ersten 24 Bit identifizieren den Hardwarehersteller (siehe OUI)
- Die restlichen 40 Bit dienen der Geräteidentifikation

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, invertiert 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

Name: Klasse: Datum:

Aufgabe 13: Kurz und knapp….

Mit IPv4 löst ein Host die MAC-Adresse mit Hilfe der IP-Adresse und dem Address Resolution Protocol (ARP) auf. Welches Protokoll wird hierfür bei IPv6 verwendet?

- ☐ 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	

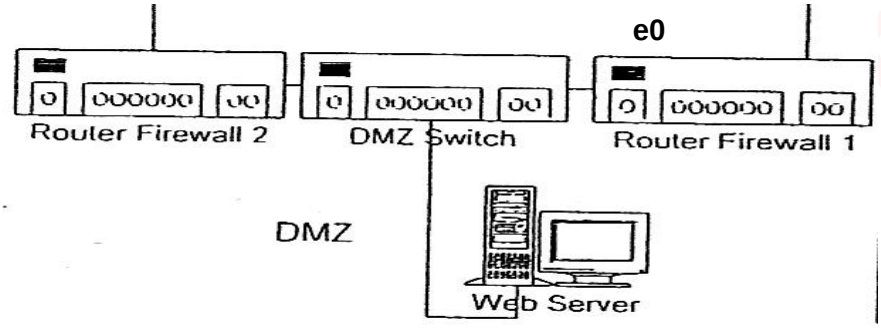
Dokumentieren Sie für die Fastethernetschnittstelle von PC3:

Link-Local Adresse	
EUI-64 Unicast	
Gateway	

Name: Klasse: Datum:

Aufgabe 14:

Netzwerkplan (Ausschnitt)



Sie verwenden Stateless Address Autoconfiguration mit EUI-64 (mod.) in der DMZ des Netzwerks. Die Routerfirewall 1 unterstützt auf seinem FastEthernet Interface e0 IPv6.

Ausschnitt aus der Konfiguration des Fastethernet Interface e0 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
Subnetzmaske  . . . . . . . . . : 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:

I. Die Link-Local Adresse des Webservers?

II. Die Global Unicast Adresse des Webservers, wenn in der DMZ ein Präfix von /64 verwendet wird?

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

Site-Präfix:	
Subnet-Präfix	
Interface Identifier	

IV. Das Standard Gateway des Webservers, das per Stateless Address Autoconfiguration auf dem Webserver eingetragen wird?

Name: Klasse: Datum:

Aufgabe 15:

Sie überprüfen die Konfiguration eines PC:

```
C:\>ipconfig /all

Windows-IP-Konfiguration

   Hostname . . . . . . . . . . . . : PC-20

Ethernet-Adapter LAN-Verbindung:

   Verbindungsspezifisches DNS-Suffix:
   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
   Subnetzmaske  . . . . . . . . . . : 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	
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 beschreiben Sie eine Lösungsmöglichkeit.

Name: Klasse: Datum:

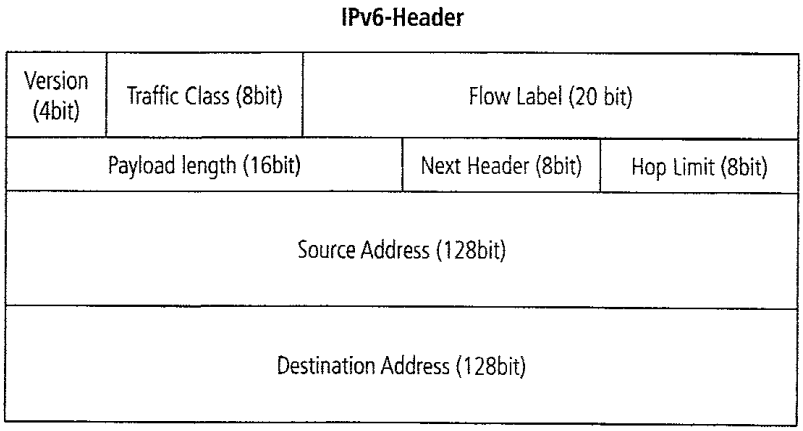
Der PC kann einen UNIX Server in der Firma nicht erreichen. Die Ausgabe der Schnittstelle eth0 des Servers zeigt folgende Konfiguration:

```
# ifconfig eth0
eth0: ether 00:90:dc:05:76:30
      inet 192.168.2.222 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 (1000base TX)
      status: active
```

Nennen Sie eine mögliche Fehlerursache und beschreiben Sie eine Lösung.

Name: Klasse: Datum:

Header-Format



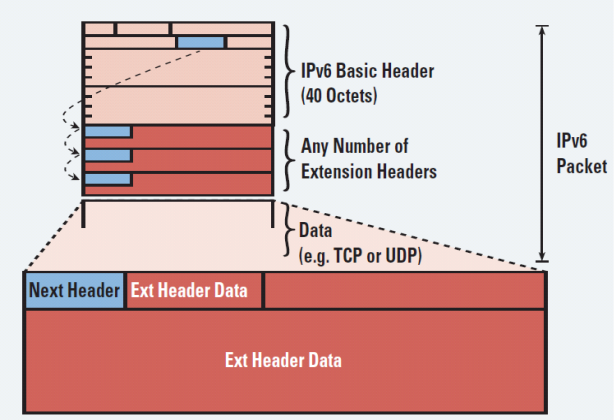
Im Gegensatz zu IPv4 hat der IP-Kopfdatenbereich (Header) bei IPv6 eine feste Länge von 40 Bytes (320 Bits).

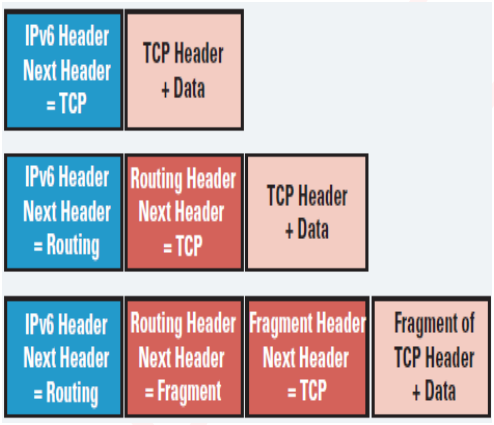
Optionale, seltener benutzte Informationen werden in so genannten Erweiterungs-Kopfdaten (engl.: *Extension Headers*) zwischen dem IPv6-Kopfdatenbereich und der eigentlichen Nutzlast (engl. *Payload*) eingebettet. Der Kopfdatenbereich eines IPv6-Paketes setzt sich laut RFC 2460 aus den folgenden Feldern 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 Lngth	16 Bit	Länge des IPv6-Paketinhaltes (ohne Kopfdatenbereich, aber inklusive der Erweiterungs-Kopfdaten) in Byte
Next Header	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

Name: Klasse: Datum:

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

Name: Klasse: Datum:

Aufgabe 16 :

Von einem Protokollanalyzer wurden die folgenden zwei IP-Pakete aufgezeichnet.

Trace 1

```
60 00 00 00 00 40 3A 40 FE C0 00 01 00 00 00 00
00 00 AF C1 00 B4 00 01 FE C0 00 01 00 00 00 00
00 00 00 BE FE 30 01 F0 81 00 A4 6B 0C 1C 00 41
52 0F 36 47 9F 89 0C 00 08 09 0A 0B 0E 0F 10 11
...
```

Trace 2

```
45 00 00 54 A1 1B 00 00 41 01 55 52 C0 A8 01 02
C0 A8 01 E9 00 00 9B E3 3F 1C 00 09 24 13 36 47
D5 98 0D 00 08 09 0A 0B 0C 0D 0E 0F 10 11 12 13
14 15 16 17 18 19 1A 1B 1C 1F 20 21 22 23 24 25
...
```

Für IPv6 sind die Adressen zusätzlich in verkürzter Schreibweise an.

Nennen Sie für Trace 1

a) die Protokollversion

b) die Senderadresse

c) die Empfängeradresse

Geben Sie für die IPv6 Senderadresse an:

Das Netz	
Interface Identifier	

Geben Sie für die IPv6 Empfängeradresse an:

Das Netz	
Interface Identifier	

Nennen Sie für Trace 2

d) die Protokollversion

e) die Senderadresse

f) die Empfängeradresse

Name: Klasse: Datum:

Aufgabe 17:

In einem vorhandenen Netzwerk befinden sich zwei IPv6-konfigurierte Endgeräte. Von einem Protokollanalyzer wurden die folgenden zwei IP-Pakete aufgezeichnet.

Trace 1

```
60 00 00 00 00 40 3A 40 FE C0 01 01 00 00 00 00
00 00 AF C1 00 B8 00 51 FE C0 00 03 00 00 00 00
00 00 00 BE FE 30 01 F0 81 00 A4 6B 0C 1C 00 41
52 0F 36 47 9F 89 0C 00 08 09 0A 0B 0E 0F 10 11
...
```

Trace 2

```
45 00 00 54 A1 1B 00 00 41 01 55 52 C0 A8 01 02
C0 A8 01 E9 00 00 9B E3 3F 1C 00 09 24 13 36 47
D5 98 0D 00 08 09 0A 0B 0C 0D 0E 0F 10 11 12 13
14 15 16 17 18 19 1A 1B 1C 1F 20 21 22 23 24 25
...
```

Bestimmen Sie den Trace mit dem IPv6 Paket

Nennen Sie IPv6 Senderadresse

Nennen Sie die IPv6 Empfängeradresse

Geben Sie für die IPv6 Senderadresse an:

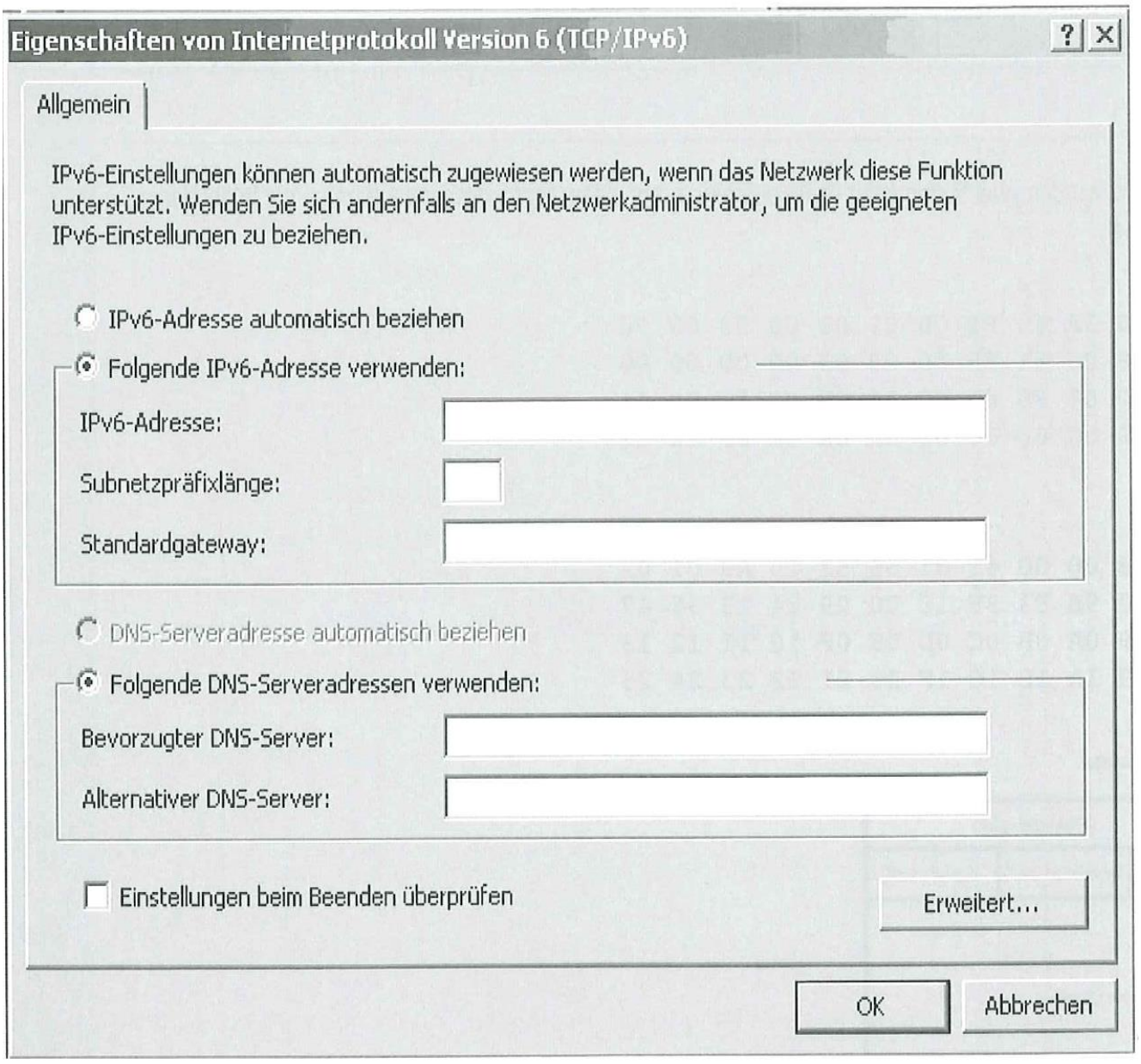
Das Netz	
Interface Identifier	

Geben Sie für die IPv6 Empfängeradresse an:

Das Netz	
Interface Identifier	

Name: Klasse: Datum:

Sie sollen an einem weiteren PC die IPv6-Konfiguration manuell eingeben. Dieser soll mit den beiden konfigurierten Geräten kommunizieren können. Ein IPv6 DNS-Server ist unter FEC0::16/10 erreichbar. Das Standardgateway hat die erste mögliche Adresse im Netz.



Name: Klasse: Datum:

Aufgabe 18:

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.

Time: 30 minutes

1. Die IPv6 Adresse wird _____ dargestellt.
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 MyDrive 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 MyDrive 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 19: Kurz und knapp…

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

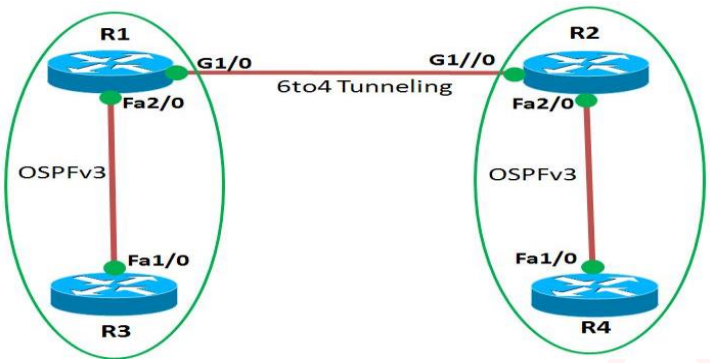
IPv6 6to4 Tunneling Configuration Example[47]

This document provides sample configuration of IPv6 6to4 tunneling in Cisco IOS routers. 6to4 Tunneling is one of the IPv6 translation mechanism which encapsulates the IPv6 packets into IPv4 which allows remote IPv6 networks to communicate across the IPv4 infrastructure(core network or Internet). The main difference between the manual tunnels and automatic 6to4 tunnels is that the tunnel is not point-to-point but it is point-to-multipoint.

In this example, router R1 and R2 are connected via Gigabit Ethernet G1/0. The routers R1 and R2 runs OSPFv3 in their internal network with routers R3 and R4 respectively. Note that internal routing protocols such as EIGRPv6 OSPFv3 cannot be used across the 6to4 tunnels since they use Link-Local address to form adjacencies. You can either use BGP which forms adjacencies using Global Unicast Address or Static routes as we use in this example.

[47] https://supportforums.cisco.com/docs/DOC-28959#Requirements

Name: Klasse: Datum:



Configuration

Router R1	Router R2	Router R3 & R4
! version 15.2 ! **hostname R1** ! ipv6 unicast-routing ipv6 cef ! **interface Tunnel0** **no ip address** **no ip redirects** **ipv6 address** **2002:C0A8:1E01::/48** **tunnel source 192.168.30.1** **tunnel mode ipv6ip 6to4** ! interface GigabitEthernet1/0 ip address 192.168.30.1 255.255.255.0 negotiation auto ! interface FastEthernet2/0 no ip address speed auto duplex auto ipv6 address 1000::2/64 ipv6 ospf 1 area 0 ! **ipv6 route** **2002:C0A8:1E02::/48 Tunnel0** **ipv6 route 1010::/64** **2002:C0A8:1E02::** !	! version 15.2 ! **hostname R2** ! ipv6 unicast-routing ipv6 cef ! **interface Tunnel0** **no ip address** **no ip redirects** **ipv6 address** **2002:C0A8:1E02::/48** **tunnel source 192.168.30.2** **tunnel mode ipv6ip 6to4** ! interface GigabitEthernet1/0 ip address 192.168.30.2 255.255.255.0 negotiation auto ! interface FastEthernet2/0 no ip address speed auto duplex auto ipv6 address 1010::1/64 ipv6 ospf 1 area 0 ! **ipv6 route** **2002:C0A8:1E01::/48 Tunnel0** **ipv6 route 1000::/64** **2002:C0A8:1E01::** ipv6 router ospf 1 router-id 2.2.2.2 redistribute static	! version 15.2 ! **hostname R3** ! ipv6 unicast-routing ipv6 cef !interface FastEthernet1/0 no ip address speed auto duplex auto ipv6 address 1000::1/64 ipv6 ospf 1 area 0 ! ipv6 router ospf 1 router-id 3.3.3.3 ! ! end ! version 15.2 ! **hostname R4** ! ipv6 unicast-routing ipv6 cef ! interface FastEthernet1/0 no ip address speed auto duplex auto ipv6 address 1010::2/64 ipv6 ospf 1 area 0 !

ipv6 router ospf 1 router-id 1.1.1.1 redistribute static ! end	! ! end	ipv6 router ospf 1 router-id 4.4.4.4 ! end

Note: Necessary Static routes are configured to achieve connectivity across 6to4 tunnel. First a static route is created for 2002:C0A8:1E02::/48 to be reachable via Tunnel Interface and then another static route for the internal /64 route which is to be routed via 6to4 tunnel interface.

Übung 5: Bearbeiten Sie folgende Packet-Tracer-Übung zur 6to4 Tunneling mit IPv6.

Sie finden die Übung und die Konfigurationen in Ihrem MyDrive Klassenorder im Unterordner *IPv6/PT_Uebungen*

a. *6to4Tunnel.pkt*

Verify Commands

Ping

To verify the connectivity across the 6to4 tunnels, you can ping the internal networks of router R1 and R2. i.e. The routers R4 and R3 should be able to ping each other.

In router R3

Try ping router R4 (1010::2) from router R3.

R3#ping 1010::2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 1010::2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 88/156/240 ms

Similarly from Router R4, ping router R3 (1000::1)

R4#ping 1000::1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 1000::1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 64/212/548 ms

Show ipv6 route to display routing table information

R1#show ipv6 route
IPv6 Routing Table - default - 7 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
B - BGP, HA - Home Agent, MR - Mobile Router, R - RIP
I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
D - EIGRP, EX - EIGRP external, ND - Neighbor Discovery
O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
O 1000::1/128 [110/1]
via FE80::C807:8EFF:FEB4:1C, FastEthernet2/0
LC 1000::2/128 [0/0]
via FastEthernet2/0, receive
S 1010::/64 [1/0]
via 2002:C0A8:1E02::
C 2002:C0A8:1E01::/48 [0/0]
via Tunnel0, directly connected
L 2002:C0A8:1E01::/128 [0/0]
via Tunnel0, receive
S 2002:C0A8:1E02::/48 [1/0]
via Tunnel0, directly connected
L FF00::/8 [0/0]
via Null0, receive

R2#show ipv6 route
IPv6 Routing Table - default - 7 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
B - BGP, HA - Home Agent, MR - Mobile Router, R - RIP
I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
D - EIGRP, EX - EIGRP external, ND - Neighbor Discovery
O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
S 1000::/64 [1/0]
via 2002:C0A8:1E01::
O 1010::1/128 [110/1]
via FE80::C808:8EFF:FEB4:1C, FastEthernet2/0
LC 1010::2/128 [0/0]
via FastEthernet2/0, receive
S 2002:C0A8:1E01::/48 [1/0]
via Tunnel0, directly connected
C 2002:C0A8:1E02::/48 [0/0]
via Tunnel0, directly connected
L 2002:C0A8:1E02::/128 [0/0]
via Tunnel0, receive
L FF00::/8 [0/0]
via Null0, receive

You can see that the static routes are shown in the routing table and is received via Tunnel 0.

Show ipv6 interface tunnel 0

To display the detailed information of the interface, use this command

```
R1#show ipv6 interface tunnel 0
Tunnel0 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80::C0A8:1E01
  No Virtual link-local address(es):
  Global unicast address(es):
    2002:C0A8:1E01::, subnet is 2002:C0A8:1E01::/48
  Joined group address(es):
    FF02::1
    FF02::2
    FF02::1:FF00:0
    FF02::1:FFA8:1E01
  MTU is 1480 bytes
  ICMP error messages limited to one every 100 milliseconds
  ICMP redirects are enabled
  ICMP unreachables are sent
  ND DAD is not supported
  ND reachable time is 30000 milliseconds (using 30000)
  Hosts use stateless autoconfig for addresses.
```

Traceroute

To trace the path of the packet for reaching the destination use this command.

```
R3#traceroute 1010::2

Type escape sequence to abort.
Tracing the route to 1010::2

  1 1000::2 144 msec 156 msec 28 msec
  2 2002:C0A8:1E02:: 184 msec 112 msec 120 msec
```

You can see that the router R3 reaches the network 1010:: via Tunnel interface

Name: Klasse: Datum:

Aufgabe 19: Zur Wiederholung…

Ordnen Sie die Aussagen den richtigen Erläuterungen zu:

Nr.	Aussage
1	Two rules for shortening IPv6 addresses
2	Rules for writing IPv6 prefixes?
3	What IPv6 prefix defines the addresses used as global unicast addresses
4	Registry prefix is assigned by / to
5	ISP prefix is assigned by / to
6	Site prefix is assigned by / to
7	Subnet prefix is assigned by / to
8	How long is the site prefix
9	How long is the Interface ID
10	How does the MAC address turn into the Interface ID
11	What prefix do IPv6 multicasts have?|
12	If you use the eui-64 keyword with the ipv6 address command, how long of a prefix should you provide?
13	NDP
14	NDP is part of what larger protocol?
15	What part of IPv6 performs the function that ARP performed for IPv4
16	Two main NDP messages
17	What does the multicast FF02::2 mean
18	What does the multicast FF02::1 mean
19	NDP is {enabled | disabled} by default
20	Class A range of private IPv4 addresses
21	Class B range of private IPv4 addresses
22	Class C range of private IPv4 addresses
23	stateless autoconfiguration allows you to learn what
24	T/F: Stateless autoconfiguration uses NDP RS/RA messages
25	Unique local addresses have what prefix
26	Three categories of IPv6 unicast addresses
27	T/F: Packets from link local addresses are never forwarded to other subnets
28	Link local addresses have what prefix

Aussage Nr.	Erläuterung
	48 bits
	It is broken in half and FFFE is inserted in the middle The 7th bit (from l to right) of the 1st half, is inverted
	FF00::/8
	Neighbor Discovery Protocol
	2000::/3
	IPv6
	enterprise engineer to a particular link
	RA (router advertisement) RS (router solicitation)
	All routers on this link
	All IPv6 nodes on this link
	omit the leading 0s in any given quartet represent 1 or more consecutive quartets of all hex 0s with a double colon, but only once in an address
	172.16.0.0 to 172.31.255.255
	192.168.0.0 to 192.168.255.255
	RIR to an ISP
	127.0.0.1
	10.0.0.0 to 10.255.255.255
	ICANN to an RIR
	anycast
	Write up to the last quartet that isn`t all 0s. Finish the entire quartet, even if the last digits are 0s. Show a double colon and then the slash and the number
	ISP to a customer (site)
	TRUE
	global unicast, unique local, link local
	TRUE
	FE80::/10
	First ten bits of FE80, 54 zeros, and the EUI-64 formatted interface ID
	/16
	NDP
	64-bit

Name: Klasse: Datum:

29	What is the format of the link local address			64 bits
30	All multicast addresses that should stay on a local link have what prefix length?			FD00::/8
31	IPv6 replaces the broadcast with the _____|			IPv6 address, prefix, default router IP address
32	What is the IPv4 loopback address			FALSE, IPv6 does not use the network command
33	What is the unknown address and what is it for			ipv6 rip name enable
34	T/F: To enable IPv6 routing on an interface, use the network command with the IPv6 connected network			Allows two dual-stack hosts to create a tunnel to each other using a tunnel through the IPv4 network/internet
35	Global configuration command to enable IPv6 routing			Manually Configured Tunnel
36	how to enable an RIPng on an interface			show ipv6 route
37	command to show the IPv6 routing table			It´s ::, meaning all 0s, and it can be used when hosts send packets in an effort to discover their IP addresses
38	T/F: the name given in the ipv6 router rip name command must be the same on all routers in an AS			ipv6 unicast-routing
39	MCT			Intra-site Automatic Tunnel Addressing Protocol
40	ISATAP			Allows two dual-stack hosts to create a tunnel to each other using a tunnel through the IPv4 network/internet
41	How does Teredo tunnelling work			FALSE
42	Difference between ISATAP and 6to4 tunneling			FF02::2
43	What address are RS messages sent and what set of hosts do they identify?|			ISATAP does not support IPv4 NAT

Anhang:

IPv6 Subnet Tabelle

Die Subnet Tabelle verschafft einen schnellen Überblick über Netzwerk- und Hostnanteil einer IPv6-Adresse.

Für jede Präfix-Länge (Netzwerkanteil der IP-Adresse) sind rechts die Anzahl der IP-Adressen im Subnetz angegeben.

Provider bekommen in der Regel ein /32 Netz zugewiesen, Endkunden für gewöhnlich ein /48 oder /56 Netz. Für die Autokonfiguration benötigt man zumindest ein /64 Netz

```
2001:0db8:0126:0000:0000:0000:0000:0000                    Anzahl der IP-Adressen
     |||| |||| |||| |||| |||| |||| ||||
     |||| |||| |||| |||| |||| |||| |||128 ------------------------------------ 1
     |||| |||| |||| |||| |||| |||| ||124 ------------------------------------ 16
     |||| |||| |||| |||| |||| |||| |120 ------------------------------------ 256
     |||| |||| |||| |||| |||| |||| 116 ------------------------------------ 4 096
     |||| |||| |||| |||| |||| |||112 ------------------------------------ 65 536
     |||| |||| |||| |||| |||| ||108 ------------------------------------ 1 048 576
     |||| |||| |||| |||| |||| |104 ------------------------------------ 16 777 216
     |||| |||| |||| |||| |||| 100 ------------------------------------ 268 435 456
     |||| |||| |||| |||| |||96 ------------------------------------ 4 294 967 296
     |||| |||| |||| |||| ||92 ------------------------------------ 68 719 476 736
     |||| |||| |||| |||| |88 ------------------------------------ 1 099 511 627 776
     |||| |||| |||| |||| 84 ------------------------------------ 17 592 186 044 416
     |||| |||| |||| |||80 ------------------------------------  281 474 976 710 656
     |||| |||| |||| ||76 ------------------------------------ 4 503 599 627 370 500
     |||| |||| |||| |72 ------------------------------------ 72 057 594 037 927 900
     |||| |||| |||| 68 ------------------------------------ 1 152 921 504 606 850 000
     |||| |||| |||64 ------------------------------------ 18 446 744 073 709 600 000
     |||| |||| ||60 ------------------------------------ 295 147 905 179 353 000 000
     |||| |||| |56 ------------------------------------ 4 722 366 482 869 650 000 000
     |||| |||| 52 ------------------------------------ 75 557 863 725 914 300 000 000
     |||| |||48 ------------------------------------ 1 208 925 819 614 630 000 000 000
     |||| ||44 ------------------------------------ 19 342 813 113 834 100 000 000 000
     |||| |40 ------------------------------------ 309 485 009 821 345 000 000 000 000
     |||| 36 ------------------------------------ 4 951 760 157 141 520 000 000 000 000
     |||32 ------------------------------------ 79 228 162 514 264 300 000 000 000 000
     ||28 ------------------------------------ 1 267 650 600 228 230 000 000 000 000 000
     |24 ------------------------------------ 20 282 409 603 651 700 000 000 000 000 000
     20 ------------------------------------ 324 518 553 658 427 000 000 000 000 000 000
```