Datenkommunikation

Franz Kohnle

13. März 2014

Inhaltsverzeichnis

1. Grundlagen

1.1. Zahlensysteme

Dezimal	Hexadezimal	Dual / Binär
0	00	0000 0000
1	01	0000 0001
2	02	0000 0010
3	03	0000 0011
4	04	0000 0100
...	...	...
254	FE	1111 1110
255	FF	1111 1111

Übung

http://kohnlehome.de/netz/Uebung_Zahlensysteme.ods

1.2. Datenmengen und Datenübertragungsraten

http://kohnlehome.de/netz/Datenmengen.pdf

Einheiten von Datenmengen

Mit Binärpräfixen: b (bit), B (Byte), KiB (Kibibyte), MiB (Mebibyte), GiB (Gibibyte), TiB (Tebibyte)

Einheiten von Datenübertragungsraten

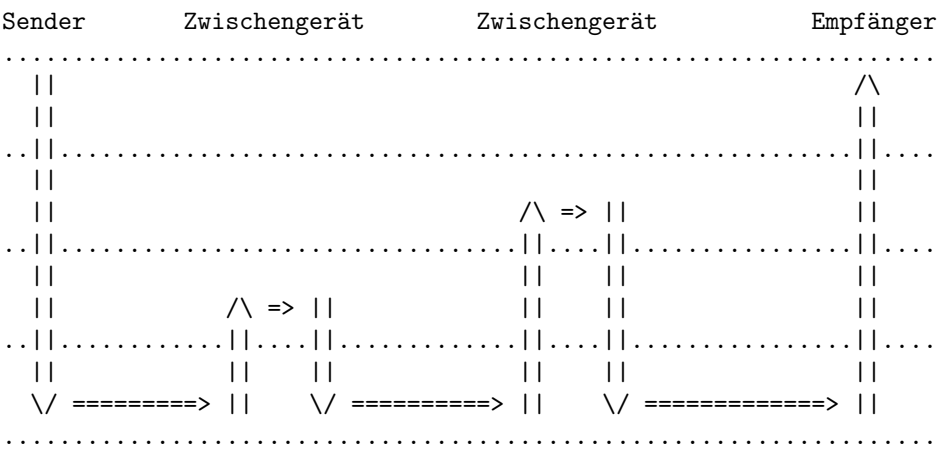
Mit SI-Präfixen: bps, bit/s, kbit/s, Mbit/s, Gbit/s, Tbit/s

Übung

http://kohnlehome.de/netz/uebung-datenmengen.pdf

2. Schichtenmodelle der Datenkommunikation

2.1. Kommunikation zwischen Sender und Empfänger



- **von oben nach unten:** einpacken, verpacken, encapsulation
- **von unten nach oben:** auspacken, entpacken, decapsulation

2.2. Netzwerkgeräte

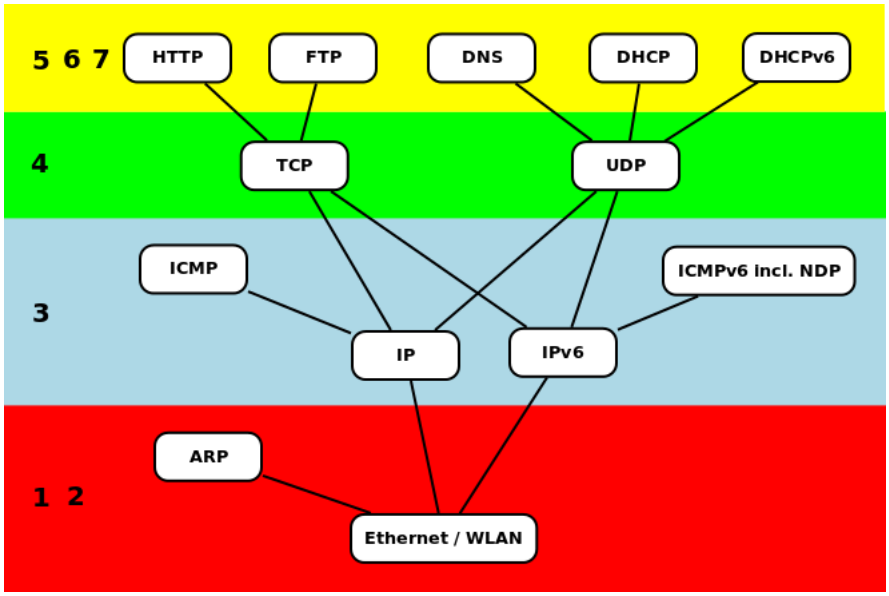
- **Endgeräte:** PC, Server, Tablet, Smartphone, Drucker, ...
- **Zwischengeräte:** Switch, Router, Modem, ...

2.3. OSI-Modell und TCP/IP-Referenzmodell

OSI-Modell		Aufgabe, *Adressen*, **Hardware**	**P**rotocol **D**ata **U**nit	**TCP/IP-Referenzmodell**
7	Application	Benutzerschnittstelle	Daten	Application
6	Presentation	Dateiformate, Verschlüsselung, Komprimierung		
5	Session	Auf- und Abbau einer Sitzung, Login, Passwörter		
4	Transport	Zuweisung zu Anwendung (*Portnummer*), Segmentierung, Zuverlässigkeit, Flusskontrolle	Segment	Transport
3	Network	logische Adressierung (*IP*), Routing, **Router**	Paket	Internet
2	Data Link	physikalische Adressierung (*MAC*), **NIC**, **Switch**	Frame	Network Access
1	Physical	physikalische Übertragung von Bits, **Kabel**, **Stecker**, **Hub**	Bits	

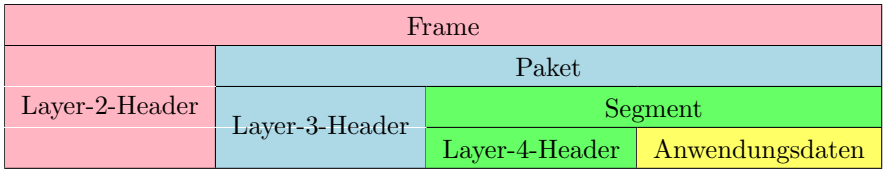
Merksatz **P**lease **D**o **N**ot **T**hrow **S**alami **P**izza **A**way

2.4. Protokolle im TCP/IP-Referenzmodell

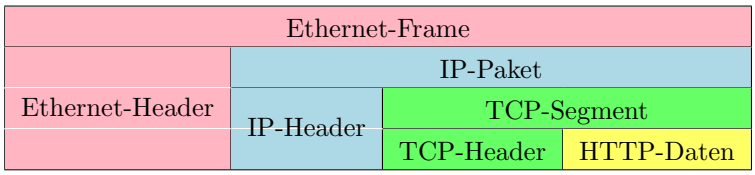


2.5. Kapselung: Daten - Segment - Paket - Frame

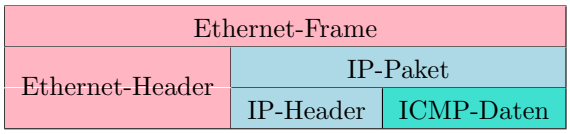
Allgemein



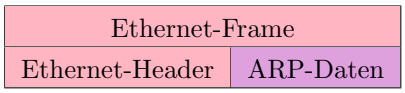
HTTP



ICMP



ARP



2.6. Netzneutralität

Jedes IP-Paket wird mit gleicher Priorität weitergeleitet, unabhängig davon, welche Quelle, welches Ziel und welchen Inhalt das Paket hat. Kein Paket wird bevorzugt. Der Inhalt eines Pakets wird nicht verändert.

2.7. Tools

- Sniffer: Wireshark - http://www.wireshark.org
- Simulation: Cisco Packet-Tracer (nur für Cisco Networking Academy Students)
- Simulation: GNS3 - http://www.gns3.net
- Simulation: Filius - http://www.lernsoftware-filius.de

3. Anwendungsprotokolle (Layer 5,6,7)

3.1. Übersicht

Protokoll		Clientanwendung	Serveranwendung	Serverport
Hilfsprotokolle				
DHCP	Dynamic Host Configuration Protocol		dhcpd	UDP 67
DNS	Domain Name System		bind	TCP/UDP 53
Web				
HTTP	Hypertext Transfer Protocol	Firefox, IE, Opera	Apache, IIS	TCP 80
HTTPS	Hypertext Transfer Protocol Secure			TCP 443
Dateiübertragung				
FTP	File Transfer Protocol	ftp, IE	ProFTPd, Filezilla	TCP 20,21
SMB	Server Message Block	Windows-Explorer	Windows-Freigabe, Samba	TCP/UDP 139, 445
Remote Access				
Telnet		telnet		TCP 23
SSH	Secure Shell	PuTTY	sshd	TCP 22
E-Mail				
SMTP	Simple Mail Transfer Protocol	Thunderbird	postfix, qmail	TCP 25
POP	Post Office Protocol			TCP 110
IMAP	Internet Message Access Protocol			TCP 143

3.2. DHCP (Dynamic Host Configuration Protocol)

Funktionsweise

Der DHCP-Server teilt dem DHCP-Client seine Konfigurationsdaten mit: IP-Adresse, Subnetmaske, Default-Gateway, Adresse des DNS-Servers

```
Client               Server
   |                    |
   |-- DHCP-Discover -->|
   |                    |
   |<--- DHCP-Offer ----|
   |                    |
   |--- DHCP-Request -->|
   |                    |
   |<---- DHCP-Ack -----|
```

Windows-Befehle

`ipconfig`	Netzwerkkonfiguration anzeigen
`ipconfig /all`	Netzwerkkonfiguration ausführlich anzeigen
`ipconfig /release`	Daten vom DHCP-Server freigeben
`ipconfig /renew`	neue Daten vom DHCP-Server anfordern

Übung

DHCP-Vorgang mitsniffern

3.3. DNS (Domain Name System)

http://kohnlehome.de/netz/DNS.pdf

Windows-Befehle

`nslookup`	IP-Adresse eines Domänennamens ermitteln
`ipconfig /displaydns`	DNS-Cache anzeigen
`ipconfig /flushdns`	DNS-Cache leeren

Übung

DNS-Vorgang mitsniffern

3.4. HTTP (Hypertext Transfer Protocol)

Kommunikation zwischen Browser und Webserver

```
Client                Server
   |                     |
   |--- HTTP-REQUEST --->|
   |                     |
   |<-- HTTP-RESPONSE ---|
```

Datenformat

	HTTP-Request	HTTP-Response
Line	`POST /datei.php HTTP/1.1` `Methode URI HTTP-Version`	`HTTP/1.1 200 OK` `Version Statuscode`

Header	`Host: kohnlehome.de`
	`User-Agent: Mozilla...`
	`...`
		`Date: ...`
		`Server: Apache`
		`Content-Type: text/html`
		`...`

Body	`var1=wert1&var2=wert2`	`<html>`
		`...`
		`</html>`

	`Request-Methoden:`
	`GET (kein Body)`
	`POST`
	`PUT`
	`...`
		`Response-Statuscodes:`
		`200 OK`
		`403 Forbidden`
		`404 Not Found`
		`500 Internal Server Error`
		`...`

Übungen

- HTTP-Vorgang mitsniffern
- Mit Cisco-Packet-Tracer ein Netz mit PC, Laptop, Webserver, DNS-Server und DHCP-Server aufbauen.

4. Transportprotokolle (Layer 4)

4.1. Portnummern

Auf jedem Host können gleichzeitig mehrere Server- und Clientprozesse (Anwendungen) laufen. Anhand der Portnummer kann ein Netzwerkprozess innerhalb eines Hosts identifiziert werden. Eine Portnummer hat eine Länge von 16 Bit, d.h. es gibt $2^{16} = 65536$ verschiedene Portnummern.

Bereiche

0 - 1023	System Ports (Well Known Ports, registriert von IETF))	Server
1024 - 49151	User Ports (registriert von IANA)	Server + Clients
49152 - 65535	Dynamic / Private Ports (nicht registriert)	Clients

Offizielle Liste http://www.iana.org/assignments/port-numbers

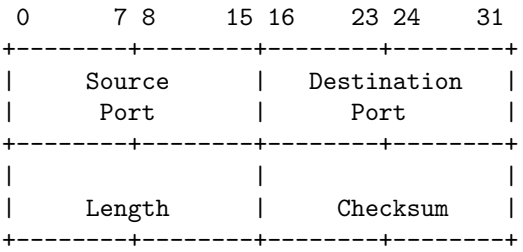
4.2. UDP (User Datagram Protocol)

Eigenschaften

- verbindungslos, kein Verbindungsaufbau
- wenig Overhead
- jedes Segment ist unabhängig

UDP-Header

RFC 768

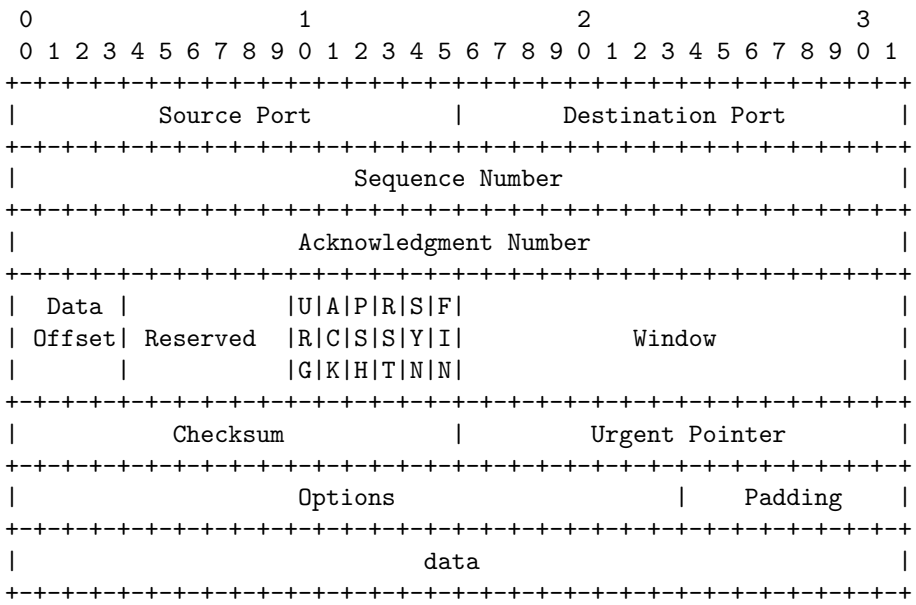


- Length: Länge in Byte von Header + Daten
- Checksum: Prüfsumme über Layer3-Adressen, Protocol, UDP-Length

4.3. TCP (Transmission Control Protocol)

TCP-Header

RFC 793

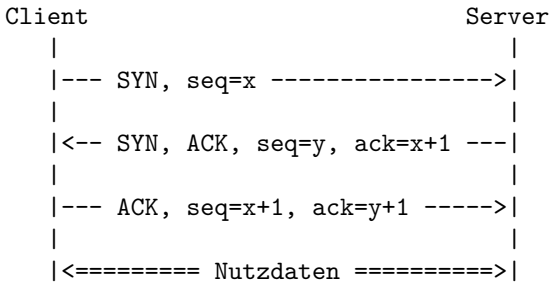


Eigenschaften

- Segmente sind mit fortlaufenden Sequenznummern durchnummeriert
- Zuverlässigkeit durch Acknowledgements vom Empfänger und evtl. Retransmission durch Sender
- Window (Fenstergröße): Anzahl der empfangenen Bytes, nach denen der Empfänger ACK sendet
- Flusskontrolle (Stauvermeidung) durch variable Fenstergröße

Verbindungsaufbau(3-way-handshake)

Client und Server übermitteln sich gegenseitig ihre Anfangssequenznummern, bevor die eigentlichen Nutzdaten in beide Richtungen gesendet werden können.



Übungen

- 3-way-handshake mitsniffern: http://kohnlehome.de/netz/Sniffer_tcp_3way_handshake.pdf
- 3-way-handshake im Packet-Tracer

5. IPv4 (Layer 3)

5.1. IP-Adressen, Subnetmasken, Netze

Definitionen

IP-Adresse Die Länge einer IP-Adresse ist 32 Bit, d.h. es gibt 2^{32} verschiedene IP-Adressen. Üblicherweise werden IP-Adressen in vier Oktette mit jeweils 8 Bit zerlegt, jedes Oktett als Dezimalzahl dargestellt und zwischen die einzelnen Oktette jeweils ein Punkt geschrieben. Die kleinste IP-Adresse lautet also 0.0.0.0, die größte 255.255.255.255.

Subnetmaske Eine Subnetmaske ist wie die IP-Adresse 32 Bit lang. Es gibt für Subnetmasken zwei Schreibweisen:

- Wie eine IP-Adresse, z.B. 255.255.128.0
- Kurzschreibweise, z.B. /17, d.h. die ersten 17 Bits haben den Wert 1, die restlichen Bits den Wert 0

Netzbits und Hostbits Die IP-Adresse besteht aus zwei Teilen. Die Bits des ersten (linken) Teils werden Netzbits genannt, die Bits des zweiten (rechten) Teils Hostbits. Wo genau die IP-Adresse geteilt wird, bestimmt die Subnetmaske. Diejenigen Bits der IP-Adresse, deren korrespondierende Bits der Subnetmaske den Wert 1 haben, sind Netzbits. Diejenigen Bits der IP-Adresse, deren korrespondierende Bits der Subnetmaske den Wert 0 haben, sind Hostbits.

Netz Alle IP-Adressen, die in den Netzbits übereinstimmen, bilden mit ihrer gemeinsamen Subnetmaske ein Netz.

Netzadresse Die Netzadresse bzw. Netz-ID ist diejenige IP-Adresse eines Netzes, deren Hostbits alle den Wert 0 haben. Kein Host darf eine Netzadresse als IP-Adresse verwenden.

Broadcastadresse Die Broadcastadresse ist diejenige IP-Adresse eines Netzes, deren Hostbits alle den Wert 1 haben. Kein Host darf eine Broadcastadresse als IP-Adresse verwenden.

Hostadressen Alle IP-Adressen eines Netzes, die nicht Netzadresse und nicht Broadcastadresse sind, werden Hostadressen genannt und können Hosts zugewiesen werden.

Beispiel

	Dual / Binär	Dezimal
	<----- Netzbits ------>|<- Hostbits ->|	
IP-Adresse	01010000.01010100.0110|1011.10110011	80. 84.107.179
Subnetmaske	11111111.11111111.1111|0000.00000000	255.255.240. 0
Netzadresse	01010000.01010100.0110|0000.00000000	80. 84. 96. 0
1. Hostadresse	|0000.00000001	80. 84. 96. 1
2. Hostadresse	|0000.00000010	80. 84. 96. 2
3. Hostadresse	|0000.00000011	80. 84. 96. 3
...	... ...	...
letzte Hostadresse	|1111.11111110	80. 84.111.254
Broadcastadresse	01010000.01010100.0110|1111.11111111	80. 84.111.255
	<----- Netzbits ------>|<- Hostbits ->|	

Subnetmasken und Netzgrößen

Die Subnetmaske bestimmt die Größe (Anzahl der IP-Adressen) eines Netzes.

kurz	dezimal	Netzgröße
/0	**0.0.0.0**	2^{32}
/1	128.0.0.0	2^{31}
/2	192.0.0.0	2^{30}
/3	224.0.0.0	2^{29}
/4	240.0.0.0	2^{28}
/5	248.0.0.0	2^{27}
/6	252.0.0.0	2^{26}
/7	254.0.0.0	2^{25}
/8	**255.0.0.0**	2^{24}
/9	255.128.0.0	2^{23}
/10	255.192.0.0	2^{22}
/11	255.224.0.0	2^{21}
/12	255.240.0.0	2^{20}
/13	255.248.0.0	2^{19}
/14	255.252.0.0	2^{18}
/15	255.254.0.0	2^{17}
/16	**255.255.0.0**	2^{16}
/17	255.255.128.0	2^{15}
/18	255.255.192.0	2^{14}
/19	255.255.224.0	2^{13}
/20	255.255.240.0	2^{12}
/21	255.255.248.0	2^{11}
/22	255.255.252.0	$2^{10} = 1024$
/23	255.255.254.0	$2^{9} = 512$
/24	**255.255.255.0**	$2^{8} = 256$
/25	255.255.255.128	$2^{7} = 128$
/26	255.255.255.192	$2^{6} = 64$
/27	255.255.255.224	$2^{5} = 32$
/28	255.255.255.240	$2^{4} = 16$
/29	255.255.255.248	$2^{3} = 8$
/30	255.255.255.252	$2^{2} = 4$
/31	255.255.255.254	$2^{1} = 2$
/32	255.255.255.255	$2^{0} = 1$

Liste mit Subnetzen eines /24-Netzes

http://kohnlehome.de/netz/subnetting.pdf

Übung

http://kohnlehome.de/netz/uebung-ip-adressen.pdf

IP-Rechner

http://kohnlehome.de/java/IPRechner.jar

5.2. VLSM (Variable Length Subnet Mask)

Teilen eines Netzes in unterschiedlich große Teilnetze.

Beispiel

Das Netz 21.22.32.0 /20 soll in folgende Subnetze geteilt werden:

- 5 Netze für je 20 Hosts
- 1 Netz für 200 Hosts
- 2 Netze für je 1000 Hosts
- 3 Netze für P2P-Verbindungen

benötigte Hosts	Netzgröße	Subnetmaske		Netzadresse
1000	1024	/22	255.255.252.0	21.22.32.0
1000	1024	/22	255.255.252.0	21.22.36.0
200	256	/24	255.255.255.0	21.22.40.0
20	32	/27	255.255.255.224	21.22.41.0
20	32	/27	255.255.255.224	21.22.41.32
20	32	/27	255.255.255.224	21.22.41.64
20	32	/27	255.255.255.224	21.22.41.96
20	32	/27	255.255.255.224	21.22.41.128
2	4	/30	255.255.255.252	21.22.41.160
2	4	/30	255.255.255.252	21.22.41.164
2	4	/30	255.255.255.252	21.22.41.168
				21.22.41.172

5.3. Klassifizierung von IP-Adressen

Private IP-Adressen

Werden im Internet nicht weitergeroutet. Können in Verbindung mit NAT in privaten Netzen verwendet werden.

- 10.0.0.0 /8
- 172.16.0.0 /12
- 192.168.0.0 /16

Sonstige besondere IP-Bereiche nach RFC6890

0.0.0.0/8	"This host on this network"
100.64.0.0/10	Shared Address Space
127.0.0.0/8	Loopback
169.254.0.0/16	Link Local
192.0.0.0/24	IETF Protocol Assignments
192.0.2.0/24	TEST-NET-1
192.88.99.0/24	6to4 Relay Anycast
198.18.0.0/15	Benchmarking
198.51.100.0/24	TEST-NET-2
203.0.113.0/24	TEST-NET-3
224.0.0.0/4	Multicast
240.0.0.0/4	Reserved
255.255.255.255/32	Limited Broadcast

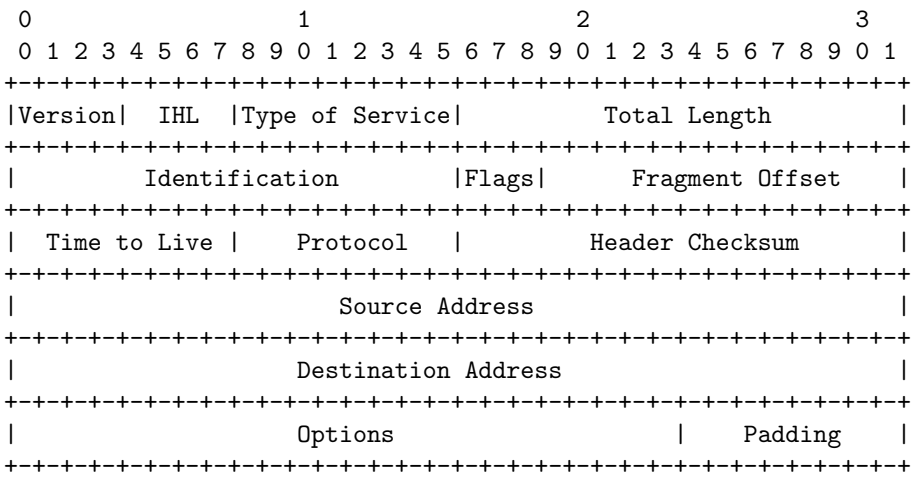
IP-Klassen

(obsolet, nur noch in wenigen Anwendungen relevant)

Klasse	binär	Bereich	Standardsubnetmaske
A	0...	0.0.0.0 - 127.255.255.255	/8
B	10...	128.0.0.0 - 191.255.255.255	/16
C	110...	192.0.0.0 - 223.255.255.255	/24
D	1110...	224.0.0.0 - 239.255.255.255	- (Multicast)
E	1111...	240.0.0.0 - 255.255.255.255	- (Reserved for Future Use)

5.4. IPv4-Header

RFC791



- TTL (Time to Live): Jeder Router vermindert diesen Wert um eins. Ist TTL=0, wird das Paket verworfen und der Absender per ICMP darüber informiert.
- Protocol: Next Level Protocol (ICMP=1, TCP=6, UDP=17, ...)

Übung

Verifizieren Sie durch Sniffern die Protocol-Werte im IP-Header für ICMP, TCP und UDP.

6. Routing (Layer 3)

6.1. Grundlagen

Begriff

Jedes einzelne IP-Paket wird anhand seiner Ziel-IP-Adresse vom Sendergerät bis zum Empfängergerät weitergeleitet (geroutet).

Routing eines sendenden Endgeräts

Der Sender versucht, ein IP-Paket mit Hilfe der OSI-Schicht 2 direkt zum Empfängergerät zu schicken, falls sich die Ziel-IP-Adresse im eigenen Netz befindet. Befindet sich die Ziel-IP-Adresse nicht im eigenen Netz, schickt der Sender das IP-Paket mit Hilfe der OSI-Schicht 2 zum Gateway.

Routing eines Routers

Ein Router leitet Pakete, deren Ziel-IP-Adresse nicht mit der eigenen IP-Adresse übereinstimmen, weiter, d.h. er routet sie. Dazu sucht er in seiner Routingtabelle einen Eintrag (Route) zu einem Netz, in dem die Ziel-IP-Adresse enthalten ist und schickt das IP-Paket an der entsprechenden Schnittstelle raus.

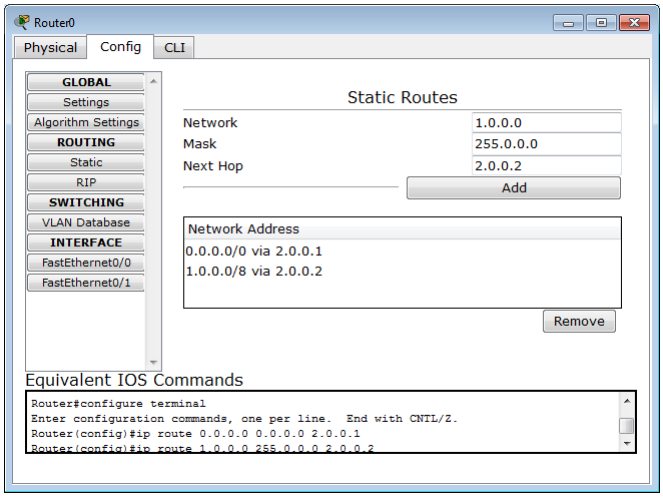
Routingtabellen

Eine Routingtabelle enthält im Allgemeinen mehrere Zeilen (Routen). Jede Zeile enthält folgende Informationen: Netzadresse, Subnetmaske und Name der Ausgangsschnittstelle oder Next-Hop-IP-Adresse.

6.2. statische Routen

Statische Routen werden vom Administrator konfiguriert. Eine spezielle statische Route ist die Default-Route. Sie gibt an, wo Pakete hingeschickt werden sollen, wenn kein zur Ziel-IP-Adresse des Pakets passender Eintrag in der Routingtabelle existiert.

Konfiguration statischer Routen im Packet-Tracer



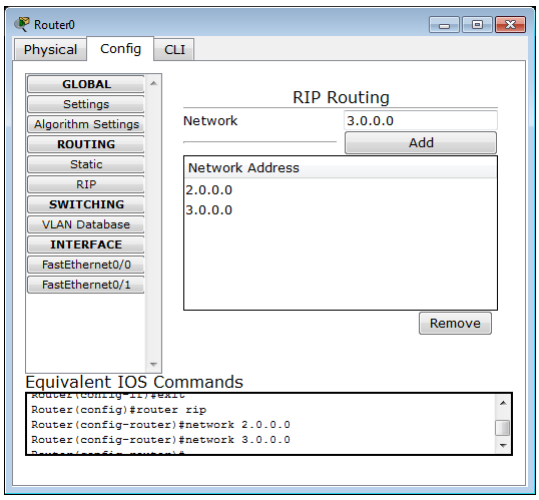
Übungen mit Packet-Tracer

- Netz mit einem Router aufbauen und Routingtabellen anschauen.
- Netz mit zwei Routern aufbauen und statische Routen konfigurieren.
- Netz mit zwei Routern aufbauen und Default-Routen konfigurieren.
- Netz mit mehreren Routern aufbauen und mit statischen Routen incl. Default-Routen unterschiedliche Hin- und Rückwege konfigurieren.

6.3. dynamische Routen

Dynamische Routen werden durch Routingprotokolle (z.B. RIP, OSPF, EIGRP) automatisch in die Routingtabellen eingetragen. Über Routingprotokolle tauschen Router untereinander Informationen über ihnen bekannte Netze aus.

Konfiguration von RIP im Packet-Tracer



Bedeutung des network-Befehls bei RIP

- Alle Schnittstellen des Routers, deren IP-Adressen im angegebenenen Netz liegen, senden RIP-Updates
- Alle Schnittstellen des Routers, deren IP-Adressen im angegebenenen Netz liegen, empfangen RIP-Updates
- Alle anliegenden Netze des Routers, die vollständig im angegebenenen Netz liegen, werden in RIP-Updates integriert

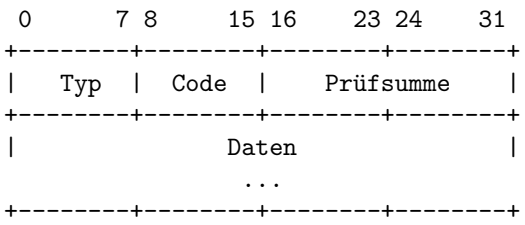
Übungen mit Packet-Tracer

- Netz mit zwei Routern aufbauen und mit RIP konfigurieren.
- Netz mit mehreren Routern aufbauen und mit RIP konfigurieren.

7. ICMP - Internet Control Message Protocol (Layer 3)

Hilfsprotokoll für das IP-Protokoll, mit dem Router Fehlermeldungen versenden können.

Aufbau eines ICMP-Pakets



Verschiedene Arten von ICMP-Meldungen

Art	Typ
Echo	8
Echo Reply	0
Time Exceeded	11
Destination Unreachable	3

Windows-Befehle

`ping`	Verbindung auf Layer 3 prüfen
`tracert`	Alle Router aud dem Weg zum Ziel anzeigen
`pathping`	Alle Router aud dem Weg zum Ziel anzeigen

Übungen

- ping mitsniffern: http://kohnlehome.de/netz/Sniffer_ping.pdf
- tracert und pathping mitsniffern
- ping und tracert im Packet-Tracer

8. NAT und Portforwarding (Layer 3,4)

8.1. NAT (Network Address Translation)

IP-Pakete mit privaten Ziel-IP-Adressen werden im Internet nicht weitergeroutet. Damit Clientgeräte mit privaten IP-Adressen trotzdem mit öffentlichen Servern im Internet kommunizieren können, ersetzt ein NAT-Router (z.B. ein "DSL-Router") die private Quell-IP-Adresse im vom Clientgerät gesendeten Paket durch die öffentliche IP-Adresse seiner WAN-Schnittstelle. Außerdem ersetzt er eventuell den Quellport und merkt sich die Kombination aus Quell-IP-Adresse, originalem Quell-Port und neuem Quellport, damit er im IP-Paket, das der Server als Antwort schickt, die Ersetzungen wieder in der anderen Richtung durchführen kann. Die NAT-Funktionalität sorgt dafür, dass sich viele Rechner im LAN eine einzige öffentliche IP-Adresse teilen können und ist der Grund dafür, dass es weltweit immer noch (aber nicht mehr lang!) genug IPv4-Adressen gibt.

Flash-Animation

http://kohnlehome.de/netz/Masquerading.swf

Übung mit Packet-Tracer

- NAT-Vorgang mit linksys-Router simulieren

8.2. Portforwarding

Clientanwendungen in privaten Netzen hinter einem NAT-Router können auf Serveranwendungen im Internet zugreifen. Aber Server, die sich hinter einem NAT-Router im LAN befinden, sind von Clients aus dem Internet nur erreichbar, wenn auf dem NAT-Router Portforwarding konfiguriert ist.

Flash-Animation

http://kohnlehome.de/netz/PortForwarding.swf

Übungen mit Packet-Tracer

- Portforwarding mit linksys-Router konfigurieren
- Umfangreiches Beispiel mit mehreren Routern, Routing, NAT, Portforwarding

9. Ethernet - IEEE 802.3 (Layer 1,2)

9.1. Ethernet-Verkabelung (Layer 1)

Verschiedene Technologien

	Twisted-Pair-Kupferkabel mit RJ-45 bzw. 8P8C Steckverbindern max. 100m	Lichtwellenleiter aus Glasfaser mit diversen Steckverbindern Single-Mode / Multi-Mode bis zu 40km
10 Mbit/s Ethernet	10BASE-T, 4 Adern TIA-568 A/B	
100 Mbit/s FastEthernet	100BASE-TX, 4 Adern TIA-568 A/B	100BASE-FX
1 Gbit/s GigabitEthernet	1000BASE-T, 8 Adern	1000BASE-SX 1000BASE-LX
10 Gbit/s 10 GbE	10GBASE-T	10GBASE-LX4

Strukturierte Verkabelung

- Primärverkabelung: Gebäude - Gebäude
- Sekundärverkabelung (vertikale Verkabelung): Hauptverteiler - Etagenverteiler
- Tertiärverkabelung (horizontale Verkabelung): Patchfeld im Etagenverteiler - Wandanschlussdose
- Arbeitsplatzverkabelung: Wandanschlussdose - PC

Straight-Through vs. Crossover

Gleichartige Geräte werden mit einem Crossover-Kabel (X) verbunden, verschiedenartige Geräte mit einem Straight-Trough-Kabel (||). Moderne Geräte schalten automatisch um.

- Geräte mit Netzwerkkarte: PC, Server, Router
- Geräte ohne Netzwerkkarte: Switch, Hub

	PC	Router	Hub	Switch
PC	X	X	||	||
Router	X	X	||	||
Hub	||	||	X	X
Switch	||	||	X	X

Pinbelegung der RJ45-Stecker

TIA-568-A

Pin 1	Grün-Weiß
Pin 2	Grün
Pin 3	Orange-Weiß
Pin 4	Blau
Pin 5	Blau-Weiß
Pin 6	Orange
Pin 7	Braun-Weiß
Pin 8	Braun

TIA-568-B

Pin 1	Orange-Weiß
Pin 2	Orange
Pin 3	Grün-Weiß
Pin 4	Blau
Pin 5	Blau-Weiß
Pin 6	Grün
Pin 7	Braun-Weiß
Pin 8	Braun

X-Over-Kabel

Ein Stecker mit	TIA-568-A,
der andere mit	TIA-568-B

Videos

- RJ45 plug on UTP cable - Installing: http://www.youtube.com/watch?v=v7H8OoKA4F8
- How to punch wires into patch panels: http://www.youtube.com/watch?v=D8PnNuDbkAw
- Netzwerkdose selbst aufklemmen - Hausbau: http://www.youtube.com/watch?v=6_zYIHcQeEs

9.2. CSMA/CD (Carrier Sense Multiple Access / Collision Detection - Layer 1)

- Carrier Sense: Sender sendet erst, wenn die Leitung frei ist.
- Multiple Access: Mehrere Geräte teilen sich das selbe Medium.
- Collision Detection: Wenn eine Kollision auftritt, d.h. wenn die Frames mehrerer Sender "zusammenstoßen", und der Sender diese Kollison erkennt, sendet er ein "Jam-Signal", damit alle anderen Geräte auch erkennen, dass eine Kollision aufgetreten ist und wartet eine zufällige Zeitspanne, bis er wieder versucht, das Frame zu senden. Gibt es im Netz keine Hubs mehr, sondern nur noch Switches im Vollduplexbetrieb, so treten keine Kollisionen auf.

9.3. Ethernet-Switching (Layer 2)

MAC-Adressen

Jede Ethernet-NIC (Network Interface Card) hat eine weltweit einmalige 48 Bit lange MAC-Adresse. Die ersten 24 Bit der MAC-Adresse kennzeichnen den Hersteller (OUI – Organizationally Unique Identifier), die restlichen 24 Bit bilden die individuelle Kennung der NIC. MAC-Adressen werden üblicherweise mit Hexadezimalziffern dargestellt. Dabei sind verschiedene Schreibweisen geläufig:

- `00:1e:8c:86:4e:d3`
- `00-1e-8c-86-4e-d3`
- `001e.8c86.4ed3`

Windows-Kommando zum Ermitteln der MAC-Adresse

```
ipconfig /all
```

spezielle MAC-Adressen

`ff:ff:ff:ff:ff:ff`	Broadcast
`01:00:5e:00:00:00`	IPv4-Multicast
-	die letzten 23 Bit entsprechen den letzen 23 Bit der IP-Adresse
`01:00:5e:7f:ff:ff`	Bsp: RIPv2-IPv4: 224.0.0.9 ⇒ RIPv2-MAC: 01:00:5e:00:00:09
`33:33:00:00:00:00`	IPv6-Multicast
-	die letzten 32 Bit entsprechen den letzen 32 Bit der IP-Adresse
`33:33:ff:ff:ff:ff`	Bsp: RIPng-IPv6: ff02::9 ⇒ RIPng-MAC: 33:33:00:00:00:09

Ethernet II - Frame

<table>
<tr><td colspan="3">Ethernet-Header</td><td rowspan="2">Daten</td><td>Ethernet-Trailer</td></tr>
<tr><td>Ziel-MAC</td><td>Quell-MAC</td><td>Typ</td><td>FCS</td></tr>
</table>

- Typ: Kennzeichnung des Inhalts des Frames (Daten), z.B. 0x0800 - IPv4, 0x0806 - ARP, 0x86DD - IPv6, 0x8100 - mit VLAN-Tag
- FCS (Frame Check Sequence): Der Sender berechnet die FCS, der Empfänger vergleicht die FCS mit seiner eigenen Berechnung. Falls die einen anderen Wert ergibt, wird das Frame verworfen.

Switching-Vorgang

Jeder Switch hat eine MAC-Address-Table, in der die zu den Switchports zugehörigen MAC-Adressen gespeichert sind. Empfängt ein Switch ein Frame, speichert er dessen Quell-MAC zusammen mit dem Eingangsport in der MAC-Address-Table. Findet er die Ziel-MAC in der Tabelle, so sendet er das Frame nur am entsprechenden Port raus. Findet er die Ziel-MAC nicht in seiner Tabelle, so sendet er das Frame an allen Ports ausser dem Eingangsport raus.

Übungen

- Simulation mit zwei Switches an der Tafel
- MAC-Address-Tables im Packet-Tracer

Switching-Modi

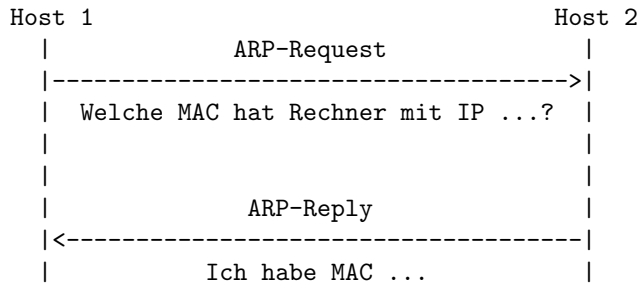
- Cut-Through / Fast-Forward: Frame wird nach dem Lesen der Ziel-MAC weitergeleitet
- Cut-Through / Fragment-Free: Frame wird nach dem Lesen der ersten 64 Byte weitergeleitet
- Store and Forward: Frame wird nach Berechnung der FCS weitergeleitet

9.4. Kollisions- und Broadcastdomänen

- Kollisionsdomäne: begrenzt durch Switch und Router
- Broadcastdomäne: begrenzt durch Router

10. ARP - Address Resolution Protocol (Layer 2)

Zu jeder Ethernet-NIC gehört eine arp-Tabelle, in der Paare aus MAC- und IP-Adressen anderer Hosts gespeichert sind. Möchte ein Gerät ein Paket an eine bestimmte IP-Adresse senden, so muss es dieses Paket in ein Frame verpacken. Dazu benötigt es die MAC-Adresse des Empfängergeräts bzw. des Routers. Diese MAC-Adresse wird als Ziel-MAC in den Ethernet-Header eingetragen. Fehlt der entsprechende Eintrag in der arp-Tabelle, wird ein arp-Request als Broadcast gesendet ("Wer hat die IP ..."). Der Host mit der entsprechenden IP-Adresse antwortet mit einem arp-Reply.



Windows-Befehle

`arp -a`	zeigt arp-Tabelle an
`arp -d`	löscht arp-Tabelle

Übungen

- ARP-Vorgang im Packet-Tracer
- ARP-Vorgang mitsniffern

11. STP - Spanning Tree Protocol - IEEE 802.1D (Layer 2)

Durch redundante Pfade (loops) erzeugte Probleme

- Broadcast Storm
- Mehrfache Übertragung von Frames
- inkorrekte Einträge in MAC-Address-Tables

Lösung

Aufbruch von Loops durch Blockieren einzelner Switchports mittels STP.

Vorgehensweise

Alle Switches senden alle zwei Sekunden BPDUs (Bridge Protocol Data Units) und werten die empfangenen BPDUs aus:

1. eine **Root-Bridge** wählen (Switch mit kleinster Bridge-ID)
2. pro Switch einen **Root-Port** wählen (Port am nächsten zur Root-Bridge)
3. pro Segment (Leitung) einen **Designated-Port** wählen (Port am nächsten zur Root-Bridge)
4. alle restliche Ports **blockieren**

Übungen

- Simulation mit mehreren Switches an der Tafel
- Spanning-Tree-Protocol im Packet-Tracer

12. VLANS (Layer 2)

Durch "virtuelles Zersägen"von Switches wird ein physikalisches Netz in mehrere virtuelle Teilnetze geteilt, zwischen denen die Switches keine Frames austauschen. Jedes VLAN hat eine eigene MAC-Address-Table. Üblicherweise erhalten unterschiedliche VLANs unterschiedliche IP-Netze zugewiesen, sodass zwischen den VLANs mit einem Router geroutet werden muss.

12.1. Konfiguration von VLANS an Switches

- VLANs erstellen
- Switchports den VLANs zuweisen (Access-Ports)

Beispiele

- mehrere VLANs an einem Switch
- mehrere VLANs an zwei Switches
- mehrere VLANs an zwei Switches mit Router

12.2. Trunking - IEEE 802.1q

Verbindungsleitungen zwischen zwei Switches können als Trunk-Leitungen konfiguriert werden. Über Trunk-Leitungen werden Frames aus verschiedenen VLANs transportiert. Damit der empfangende Switch ein Frame wieder zum richtigen VLAN zuordnen kann, werden Frames auf Trunk-Leitungen "getaggt", d.h. ihre VLAN-ID wird in den Frame-Header geschrieben. Der empfangende Switch entfernt das Tag wieder.

Auch eine Leitung zwischen einem Switch und einem Router kann als Trunk-Leitung konfiguriert werden. Dazu muss auf der physikalischen Schnittstelle des Routers für jedes VLAN eine eigene Subschnittstelle konfiguriert werden. Jede Subschnittstelle wird einem speziellen VLAN zugewiesen und erhält eine eigene IP-Adresse.

Format eines getaggten Frames

<table>
<tr><td colspan="5">Ethernet-Header</td><td rowspan="2">Daten</td><td>Ethernet-Trailer</td></tr>
<tr><td>Ziel-MAC</td><td>Quell-MAC</td><td>Typ1</td><td>TCI</td><td>Typ2</td><td>FCS</td></tr>
</table>

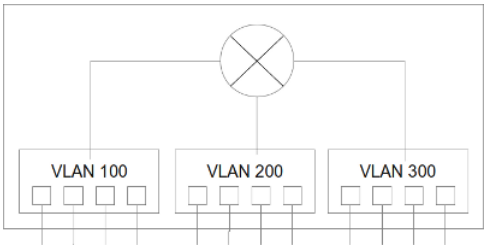
- Typ1: 0x8100 (Kennzeichnung als getaggt)
- TCI: 3 Bit Priority Code Point, 1 Bit Drop Eligible Indicator, 12 Bit VLAN-ID
- Typ2: Kennzeichnung des Inhalts (Daten)

Beispiele

- Trunk-Leitung zwischen zwei Switches
- Trunk-Leitung zwischen Switch und Router

12.3. Layer-3-Switch

Ein Layer-3-Switch ist ein Switch mit Routingfunktionalität. Der interne Router kann zwischen den einzelnen VLANs des Switches routen. Dazu wird jedem VLAN eine IP-Adresse zugewiesen. Das ist die IP-Adresse der entsprechenden internen Routerschnittstelle.



13. WLAN - IEEE 802.11 (Layer 1,2)

13.1. Standards

Standard	Bandbreite	Frequenzband
IEEE 802.11a	54 Mbit/s	5 GHz
IEEE 802.11b	11 Mbit/s	2,4 GHz
IEEE 802.11g	54 Mbit/s	2,4 GHz
IEEE 802.11n	600 Mbit/s	2,4 GHz / 5 GHz
IEEE 802.11ac	1,3 Gbit/s	5 GHz
IEEE 802.11ad	7 Gbit/s	60 GHz

13.2. Authentication + Encryption

- Authentication: Beweisen, dass man derjenige ist, der man behauptet zu sein.
- Encryption: Sender verschlüsselt Daten, damit sie auf dem Übertragungsweg nicht von Dritten gelesen werden können. Der Empfänger entschlüsselt die Daten wieder.

Authentication	Encryption	Sicherheit
keine	keine	I
WEP	keine / WEP	I
WPA	TKIP	I
WPA2	AES	V

13.3. WLAN-Geräte

- NIC (PCI, PCMCIA, USB)
- Access-Point: Schnittstelle zwischen 802.11 WLAN und 802.3 kabelgebundenem Ethernet
- WLAN-Router: Kombinationsgerät enthält Access-Point, Switch, Router, DSL-Modem, ...

13.4. WLAN-Topologien

- Ad-hoc-Modus IBSS (Independent Basic Service Set): ohne Access-Point
- Infrastrukturmodus BSS (Basic Service Set): mit zentralem Acces-Point
- Infrastrukturmodus ESS (Extended Service Set): mehrere über ein DS (Distribution System) zusammenhängende BSS
- WDS-Bridge (Point-to-Point): P2P-Verbindung zweier als "Bridge"fungierender Access-Points
- WDS-Repeater (Point-to-Point): Erweiterung eines BSS durch einen als Repeater fungierenden Access-Point

13.5. Übungen

- Infrastrukturmodus im Packet-Tracer

14. IPv6 (Layer 3)

14.1. Anzahl

Es gibt 2^{128} verschiedene Adressen. Das entspricht 10^{17} Adressen pro mm^2 Erdoberfläche.

14.2. Adressnotation

- hexadezimal, 8 Blöcke: `0011:2233:4455:6677:8899:AABB:CCDD:EEFF /64`
- führende Nullen innerhalb eines Blocks können weggelassen werden
- zusammenhängende Blöcke aus Nullen (0000) können durch :: ersetzt werden
- URL-Notation: `http://[1234::5]:80`
- Subnetmasken: nur Slash-Schreibweise, meist `/64`

14.3. Adressbereiche

IPv6-Bereich		vergleichbarer IPv4-Bereich
unknown	`::`	`0.0.0.0`
localhost	`::1 /128`	`127.0.0.1`
link-local	`FE80:: /10`	`169.254.0.0 /16`
Verbindungslokale IPv6-Adresse		APIPA

unique local	`FD00:: /8`	`10.0.0.0 /8`
		`172.16.0.0 /12`
		`192.168.0.0 /16`
		private IP-Adressen

global unicast	`2000:: /3`	öffentliche IP-Adressen
multicast	`FF00:: /8`	`224.0.0.0 /4`
subnet broadcast	`FF02::1`	`255.255.255.255`
all routers	`FF02::2`	`255.255.255.255`
ospf	`FF02::5`	`224.0.0.5`
	`FF02::6`	`224.0.0.6`
ripv2	`FF02::9`	`224.0.0.9`
eigrp	`FF02::A`	`224.0.0.10`

14.4. ICMPv6

ICMPv6 Error Messages

- Destination Unreachable
- Packet Too Big
- Time Exceeded
- Parameter Problem

ICMPv6 Informational Messages

- Echo Request
- Echo Reply

ICMPv6 Informational Messages NDP (Neighbor Discovery Protocol)

- Router Solicitation
- Router Advertisement
- Neighbor Solicitation (vgl. IPv4 ARP-Request)
- Neighbor Advertisement (vgl. IPv4 ARP-Reply)
- Redirect Message

14.5. SLAAC (Stateless Address Autoconfiguration)

1. Client weist sich selbst link-local-Adresse zu (FE80:: /10)
2. Client schickt Router Solicitation an FF02::2 (alle Router)
3. Router schickt Router Advertisement incl. Präfix zurück an FF02::1 (Subnet Broadcast)
4. Client verwendet Präfix + Interface-ID nach EUI-64

EUI-64 Bsp. MAC 0123.4567.89AB
linke Hälfte der MAC + FFFE + rechte Hälfte der MAC = 0123:46FF:FE67:89AB
7.Bit invertieren = 0323:46FF:FE67:89AB

14.6. DHCPv6

M- und O-Flags stehen im Router-Advertisement
M = Managed Address Configuration
O = Other Configuration

M-Flag	O-Flag		Vom Router	Vom DHCP-Server
1	1	Stateful DHCPv6	-	Netz, IP, ... mit DHCP-DISCOVER
0	1	Stateless DHCPv6	Netzpräfix, Gateway	DNS, ...
0	0	Autoconfiguration	Netzpräfix, Gateway	-

14.7. Übungen mit Cisco-Packet-Tracer

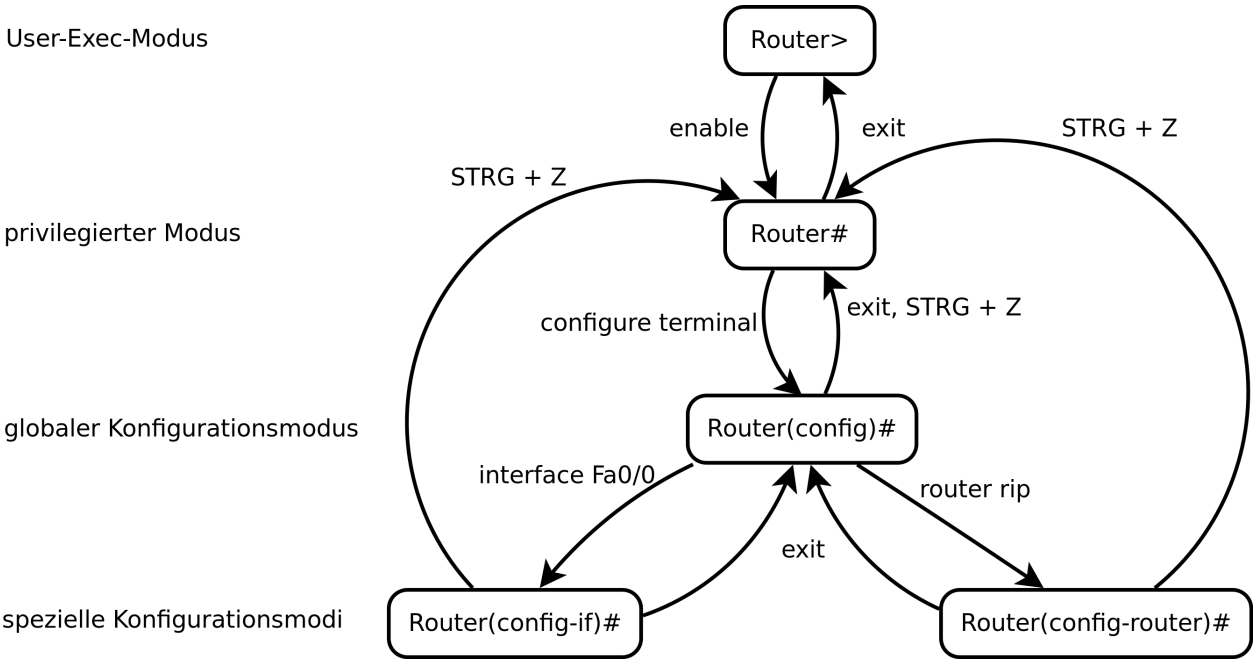
- PC: Auto-Config ⇒ link-local Adresse nach EUI-64
- PC - Switch - PC: Auto-Config ⇒ ping
- Router: ipv6 enable ⇒ link-local Adresse nach EUI-64
- Router: ipv6 unicast-routing ⇒ joined groups: FF02::2 (all routers)
- Router mit global-unicast-Adresse ⇒ PCs machen SLAAC
- Routing mit statischen IPv6-Routen
- Routing mit RIPng

A. Konfiguration von Cisco-Geräten

A.1. Speicherelemente eines Cisco-Gerätes

- ROM: Boot-Programm
- RAM: IOS, running-config, Routingtabellen, Zwischenspeicher für Pakete, ...
- Flash: IOS-Image
- NVRAM: startup-config

A.2. Konfigurationsmodi



A.3. Befehle

Konfiguration speichern

```
ROUTER# write
```

Konfiguration anzeigen

```
ROUTER# show running-config
```

Hostname

```
ROUTER(config)# hostname NAME
```

Schnittstelle

```
ROUTER(config)# interface Fa0/0
ROUTER(config-if)# ip address 1.2.3.4 255.0.0.0
ROUTER(config-if)# no shutdown
```

Clockrate bei serieller DCE-Schnittstelle

```
ROUTER(config-if)# clock rate 56000
```

Schnittstelle eines Layer-3-Switches

```
SWITCH(config)# interface vlan 100
SWITCH(config-if)# ip address 1.2.3.4 255.0.0.0
```

Layer-3-Switch

`SWITCH(config)# ip routing` (Routing aktivieren)

Subschnittstelle bei VLANs

```
ROUTER(config)# interface Fa0/0
ROUTER(config-if)# no shutdown
ROUTER(config-if)# interface Fa0/0.100
ROUTER(config-subif)# encapsulation dot1q 100
ROUTER(config-subif)# ip address 1.0.0.1 255.0.0.0
ROUTER(config-subif)# interface Fa0/0.200
ROUTER(config-subif)# encapsulation dot1q 200
ROUTER(config-subif)# ip address 2.0.0.1 255.0.0.0
```

Statische Route

`ROUTER(config)# ip route 1.0.0.0 255.0.0.0 2.3.4.5` (mit Next-Hop-Adresse)
`ROUTER(config)# ip route 1.0.0.0 255.0.0.0 S2/0` (mit Exit-Interface)

RIP

`ROUTER(config)# router rip`
`ROUTER(config-router)# network 1.0.0.0` (alle angeschlossenen Netze)

IPv6: link-local-Adresse

`ROUTER(config-if)# ipv6 enable` (erstellt link-local-Adresse nach EUI-64)
`ROUTER(config-if)# ipv6 address fe80::1 link-local` (link-local-Adresse manuell)

IPv6: statische global-unicast-Adresse

`ROUTER(config-if)# ipv6 address 2000::1/64`

IPv6: Routing einschalten

`ROUTER(config)# ipv6 unicast-routing`

IPv6: statische Route

`ROUTER(config)# ipv6 route 3000::/64 2000::1` (Zielnetz, Next-Hop)

RIPng

`ROUTER(config)# ipv6 router rip PROZESSNAME` (RIPng-Prozess erstellen)
`ROUTER(config-if)# ipv6 rip PROZESSNAME enable` (RIPng auf Schnittstelle aktivieren)

Diagnose

`ROUTER# show running-config` (aktuelle Konfiguration)
`ROUTER# show ip interface brief` (IP-Adressen und Status aller Netzwerkschnittstellen)
`ROUTER# show ipv6 interface brief`
`ROUTER# show ip route` (Routingtabelle)
`ROUTER# show ipv6 route`
`ROUTER# show ip protocol` (Routingprotokolle)
`ROUTER# show ipv6 protocol`