

Netztechnik Teil-9

Inhalt

- Protokollfunktionen
- IPv4 (Protokoll / ARP / RARP / NAT / DHCP / ICMP / DNS)
- IPv6 (Protokoll / Unterschiede zu v4 / Übergänge von v4 zu v6 / ICMPv6 / DHCPv6)

Protokollfunktionen

- Vermittlung

- ◆ Leitungsvermittlung
- ◆ Speichervermittlung
- ◆ Paketvermittlung

- Signalisierung

- ◆ In-Band-Signalisierung
- ◆ Out-of-Band-Signalisierung

- Multiplexing

- ◆ Raummultiplex
- ◆ Zeitmultiplex
- ◆ Frequenzmultiplex
- ◆ Wellenlängenmultiplex
- ◆ Code-Multiplex

- Flusskontrolle

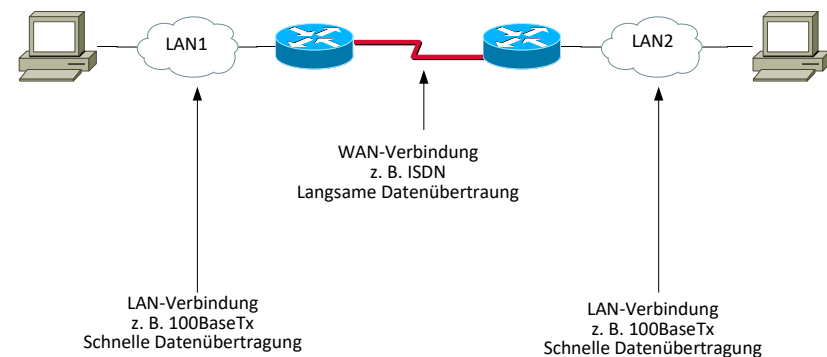
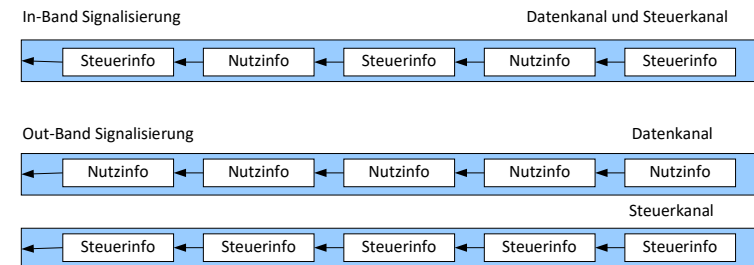
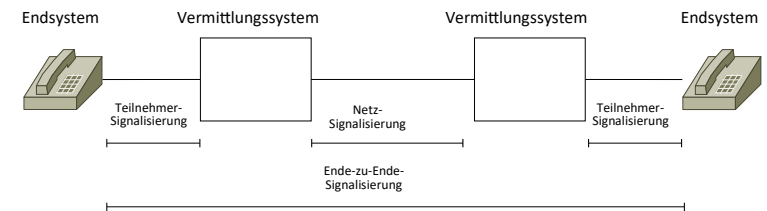
- Fehlerkorrekturverfahren (ECC = Error Correction Code)

- ◆ Vorwärtsfehlerkorrektur (FEC = forward Error Correction)

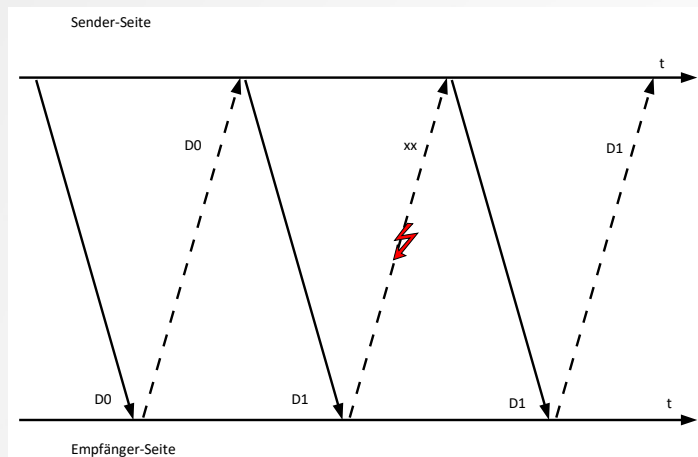
Daten werden mit zusätzlichen Bits versorgt um nach der Übertragung Fehler erkennen und beheben zu können.

- ◆ Rückwärtsfehlerkorrektur (BEC Backward Error Correction)

Z. B. durch Prüfsummen können nur Fehler erkannt, jedoch nicht korrigiert werden. Deshalb werden die Daten nochmals beim Sender angefordert.



Backward Error Correction (Quittungen)

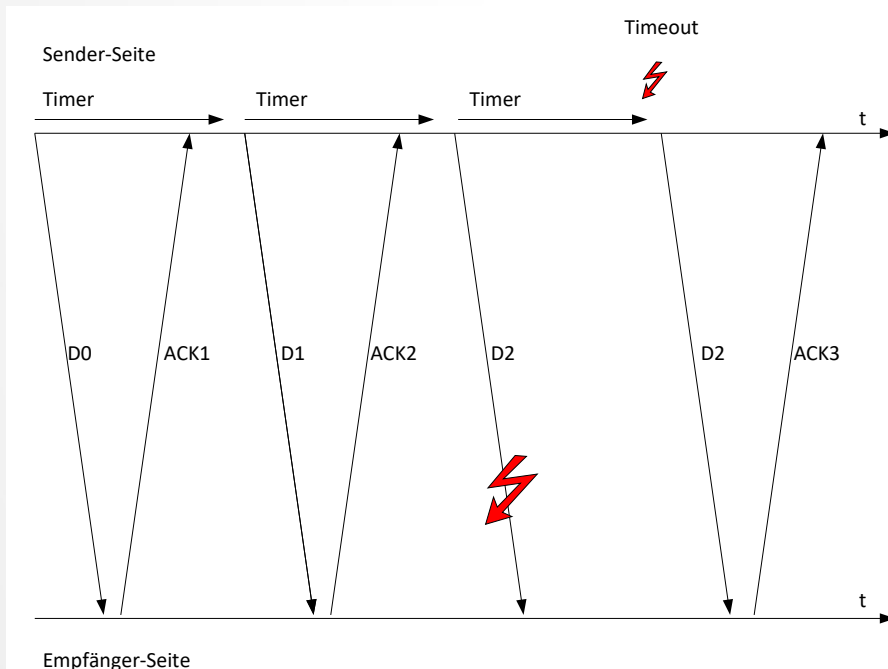


Ohne Quittungen müssten zur Sicherung der Übertragung die Daten wieder zurück übertragen werden.

Durch Einführung von Quittungen (ACK) kann die Datenmenge auf dem Rückweg verringert werden.

Wenn eine Rückmeldung fehlt, muss das bemerkt werden können.

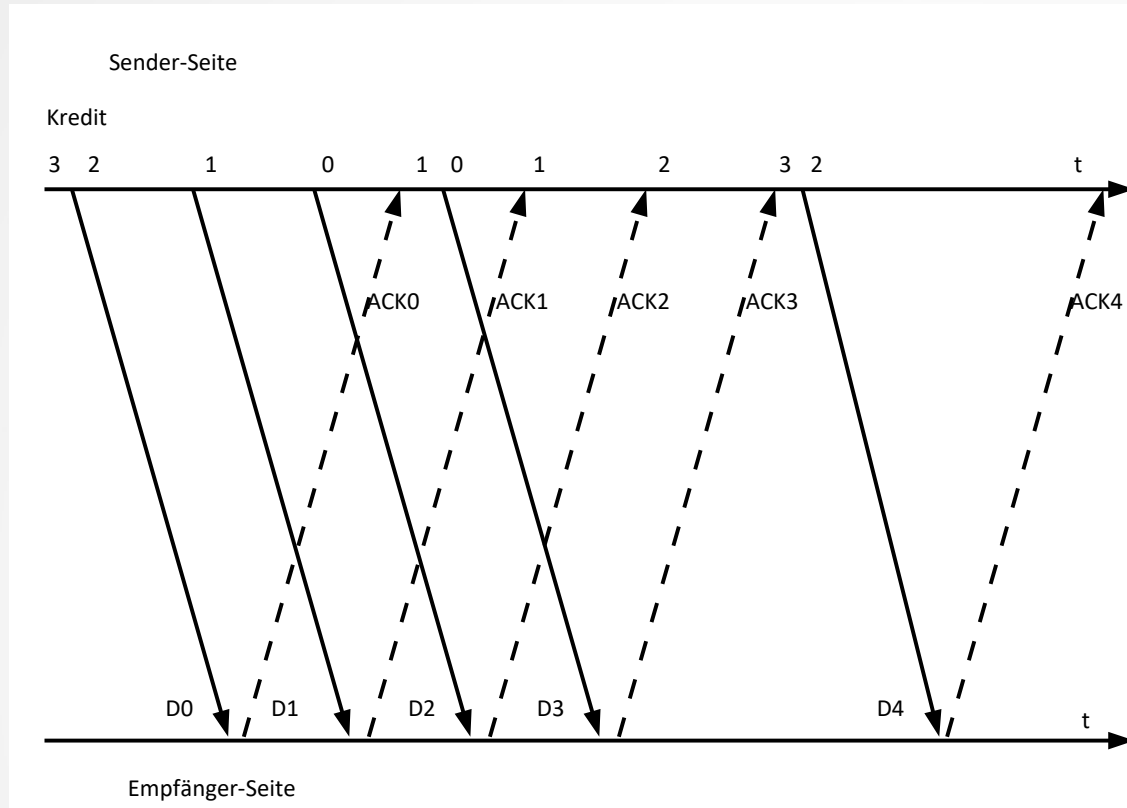
Einführung von Timern, damit die Kommunikation bei kollidierten Rahmen nicht einschläft.



Nach jeder Datenübertragung muss auf die **Quittung** oder einen **Timeout** gewartet werden.

Dieses Verfahren wird **Stop and Wait** genannt und bedeutet immer noch eine schlechte Kanalausnutzung, da nach jedem Datenpaket gewartet werden muss.

Backward Error Correction (Windowing)



Abhängig von mehreren Parametern (z. B. der Größe des Eingangspuffers des Empfängers), wird dem Sender zugestanden mehrere Rahmen zu senden, bevor er auf eine Quittung warten muss.

Die Anzahl der Rahmen, die hierbei gesendet werden dürfen, wird Kredit genannt.

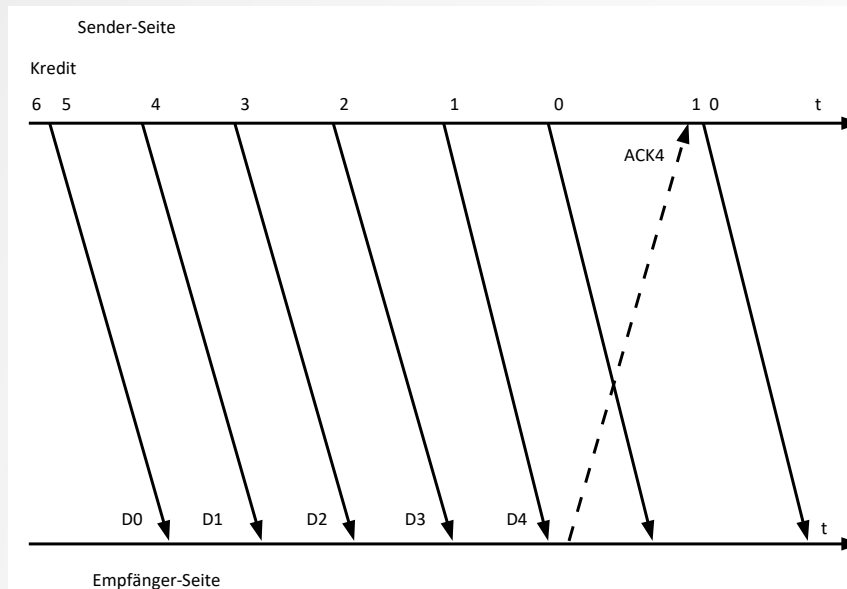
Bei jedem gesendeten Rahmen wird der Kredit dekrementiert.

So lange der Kredit > 0 ist darf gesendet werden.

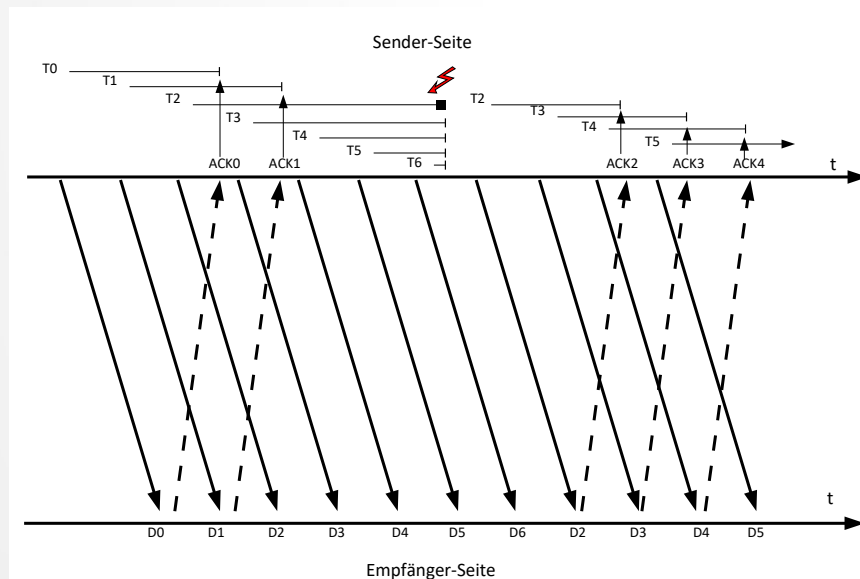
Ist der Kredit bei 0 angekommen, dürfen keine weiteren Rahmen mehr gesendet werden, und es muss gewartet werden.

Trifft dann wieder eine Quittung ein wird der Kredit inkrementiert und es darf wieder gesendet werden.

Backward Error Correction (Windowing)



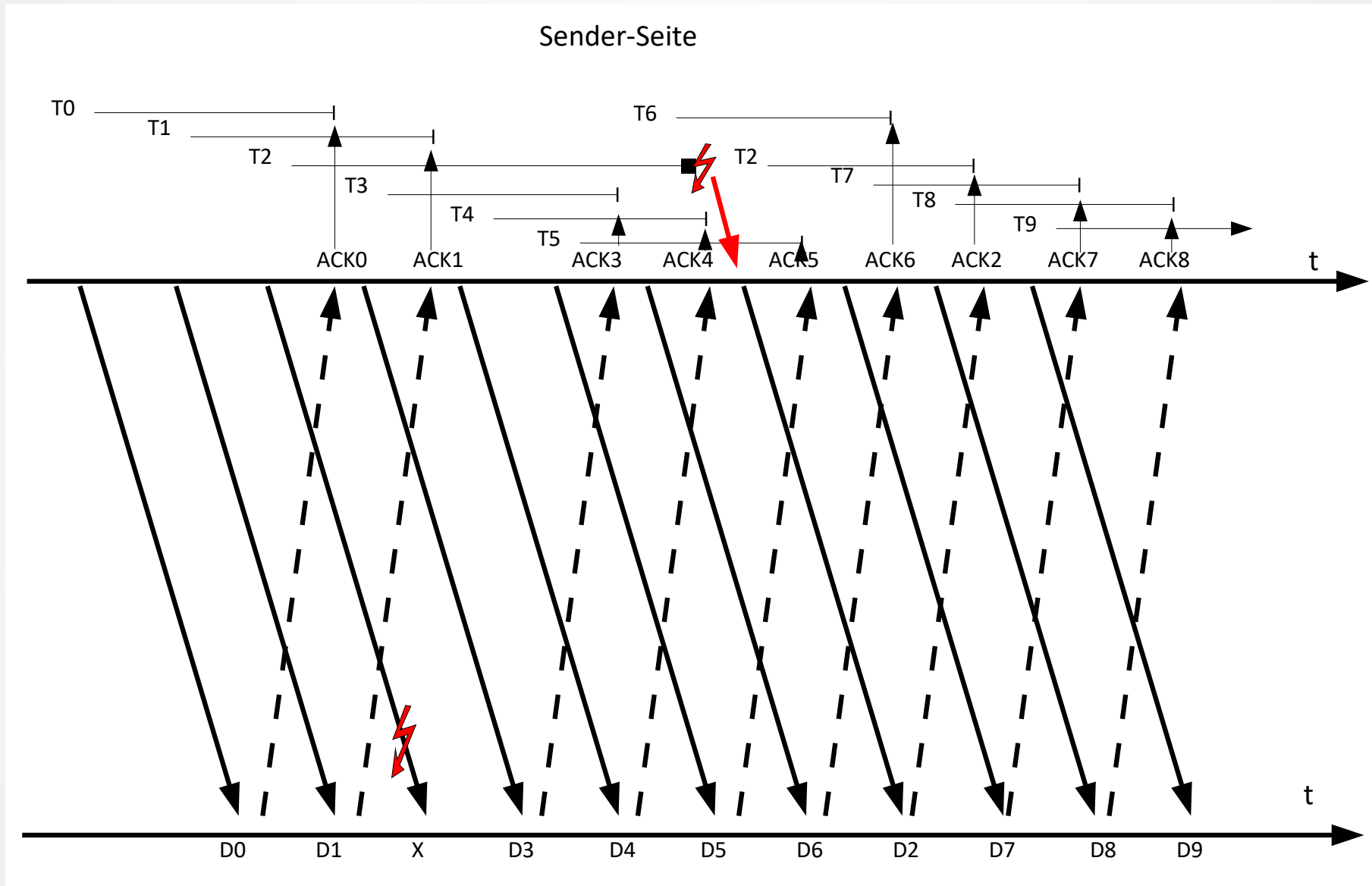
Eine Sammelquittung kann Einzelquittungen ersetzen.



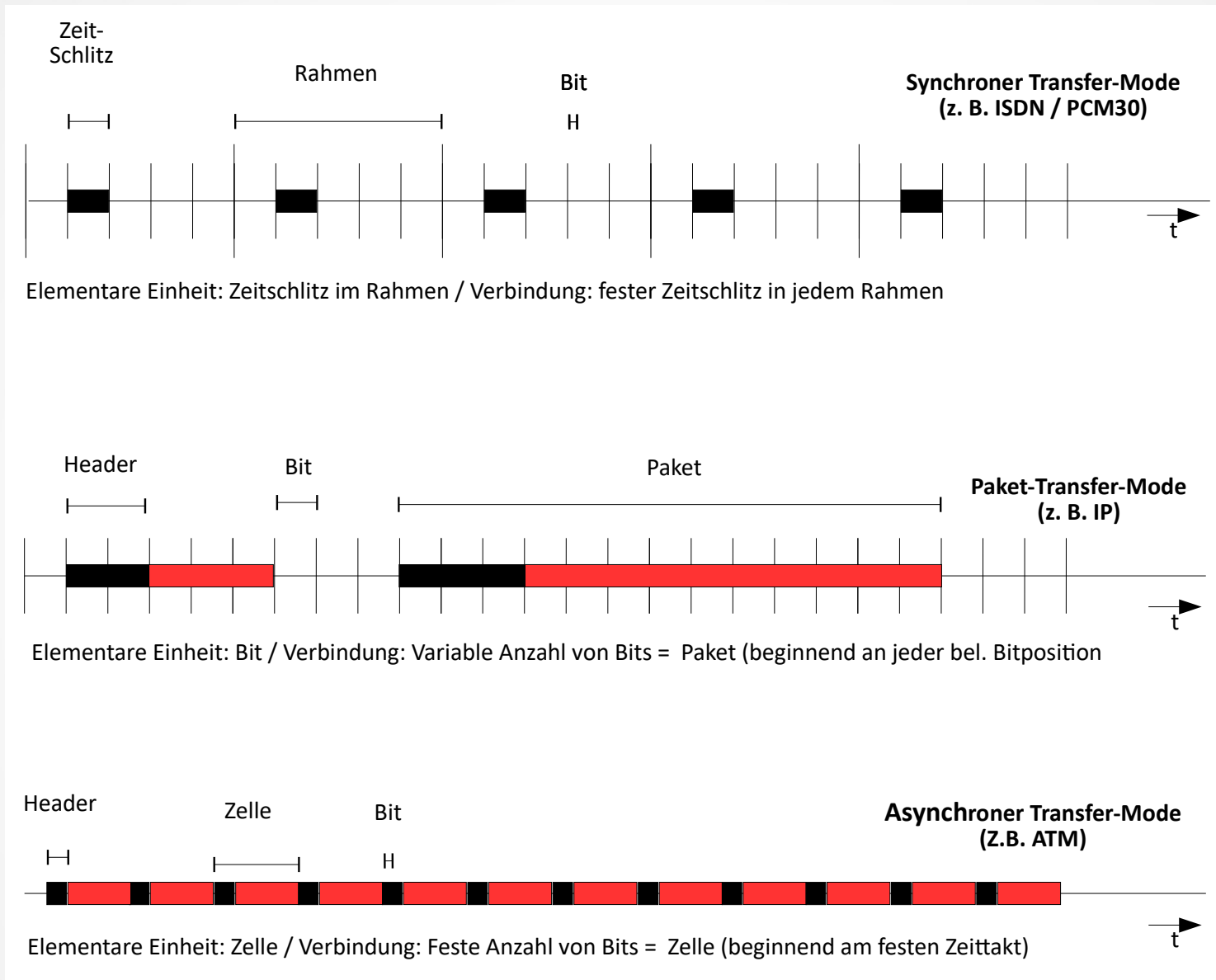
Falls eine Quittung verloren geht, könnte die Kommunikation einschlafen. Deshalb sind zusätzlich Timer erforderlich.

Damit kann bei der fehlenden Quittung mit der Datenübertragung nochmals aufgesetzt werden. (Go Back n)

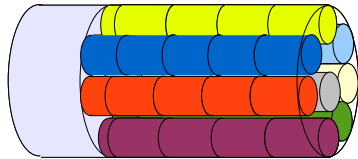
Selective Repeat



Zusammenfassung (Transfermodi Teil-1)

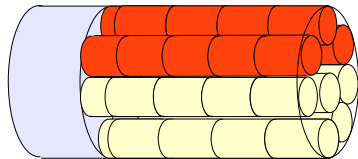


Zusammenfassung (Transfermodi Teil-2)



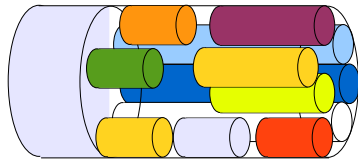
Synchroner Transfermodus (z. B. PCM30)

Leitungsvermittlung
Zeitschlitz



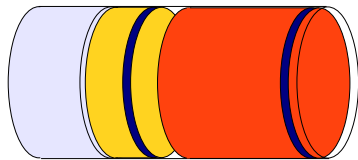
Multirate Circuit Switching (Z. B. ISDN)

Leitungsvermittlung
Zeitschlitz
Kanalbündelung



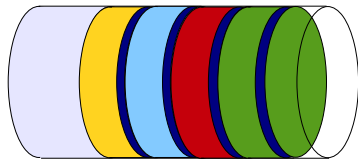
Fast Circuit Switching

Leitungsvermittlung
Freigabe nach Nutzung / Schneller Wiederaufbau



Packet-Transfer-Mode (Z. B. IP)

Paketvermittlung (Zielinformation im Header)
Unterschiedlich große Pakete



Asynchroner-Transfer-Mode (Z. B. ATM)

Zellvermittlung (Zielinformation im Header)
Alle Zellen haben die gleich Größe

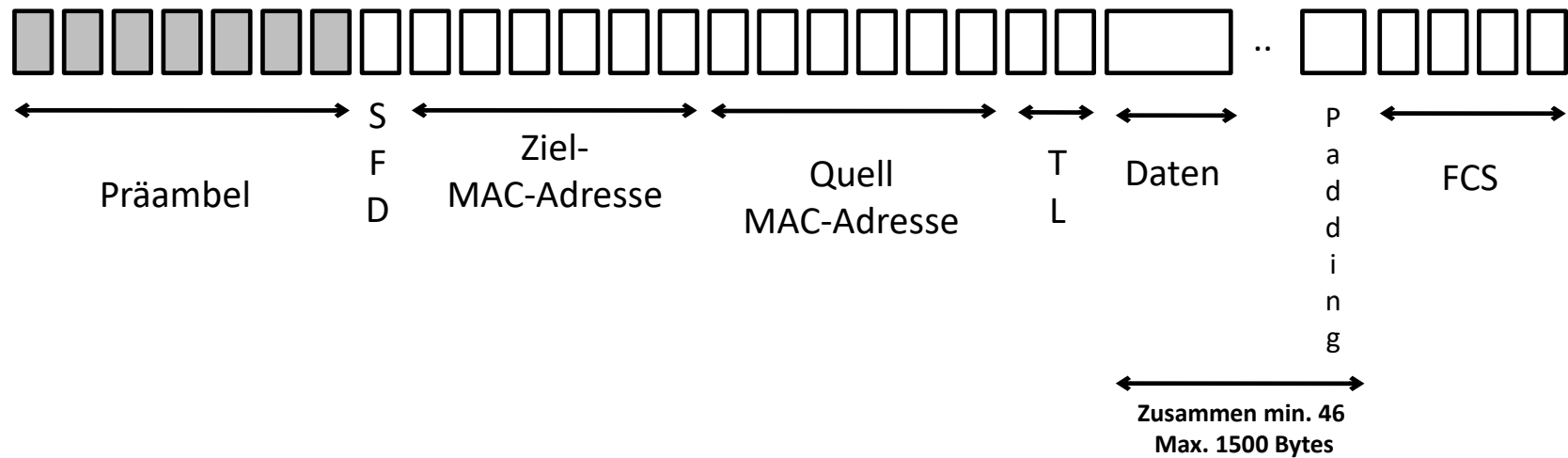
Protokollübersicht

DARPA-Layer

ISO/OSI-Layer

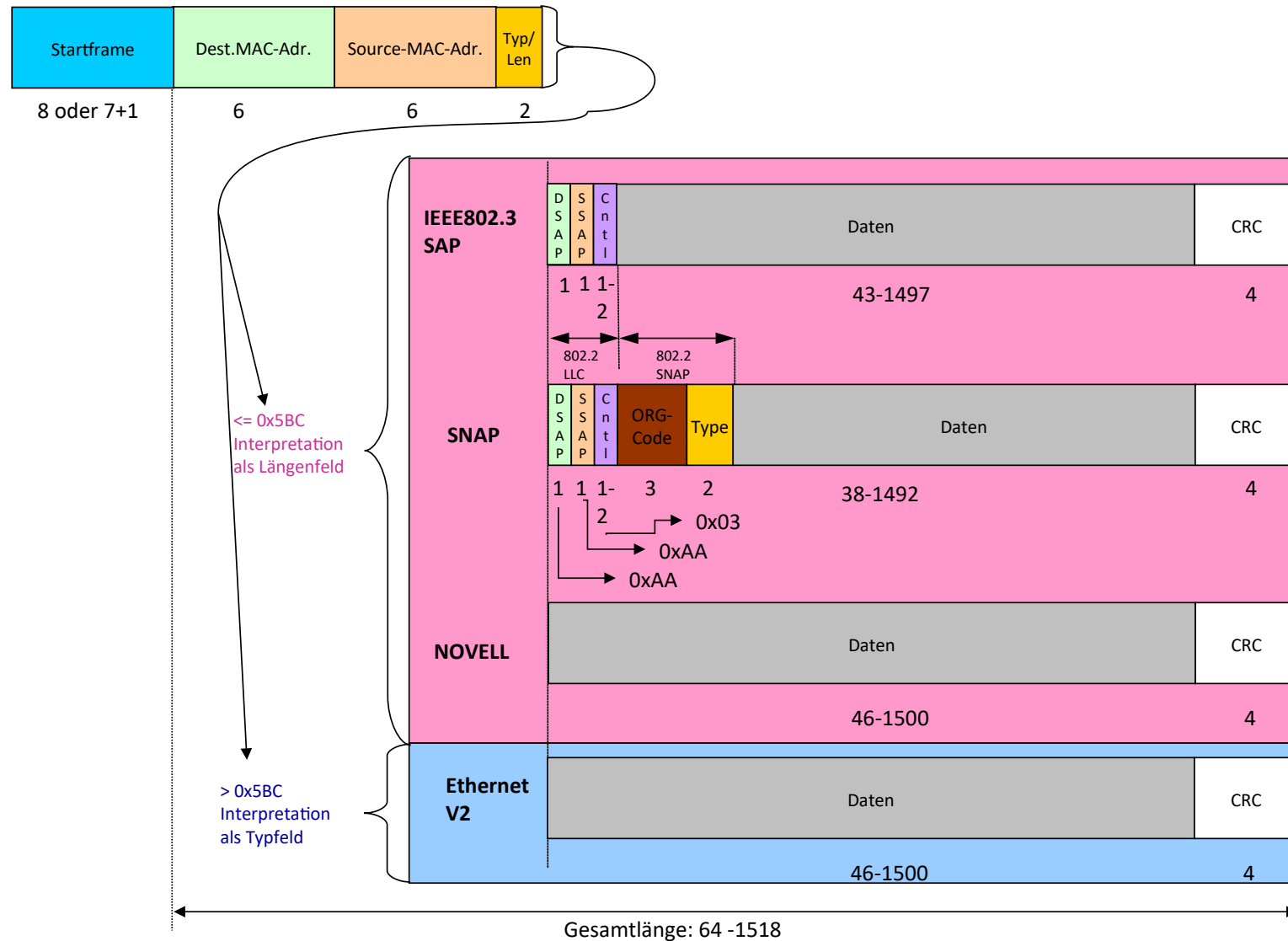
4 Prozess/An- wendung	Daten- Über-tragung	Electronic- Mail	Terminal- Emulation	Daten- Übertragung	Client- Server	Netzwerk- Verwaltung	7 Anwendung
	File-Transfer- Protocol (FTP) RFC 959	Simple-Mail- Transfer- Protocol (SMTP) RFC 821	TELNET RFC 854	Trivial-File- Transfer- Protocol (TFTP) RFC 783	SUN Network-File- Systems-Prot. (NFS) RFC 1014, 1057,1094	Simple-Network- Management- Protocol (SNMP) RFC 1157	6 Presentation
							5 Session
3 Host-to- Host	Transmission-Control-Protocol (TCP) RFC 793			User-Datagram-Protocol (UDP) RFC 768			4 Transport
2 Internet	Address-Resolution- Protokoll ARP RFC826 RARP RFC903		Internet-Protokoll (IP) RFC791		Internet-Control- Message-Protokoll (ICMP) RFC792		3 Network
1 Netzwerk- Schnittstelle	Netzwerkschnittstellenkarten Ethernet, StarLAN, Token-Ring, ARCNET RFC 894, 1042, 1201						2 Data-Link
	Übertragungsmedium Twisted Pair, Koax, Fiberglas, drahtlose Medien						1 Physical

Ethernet-Rahmen

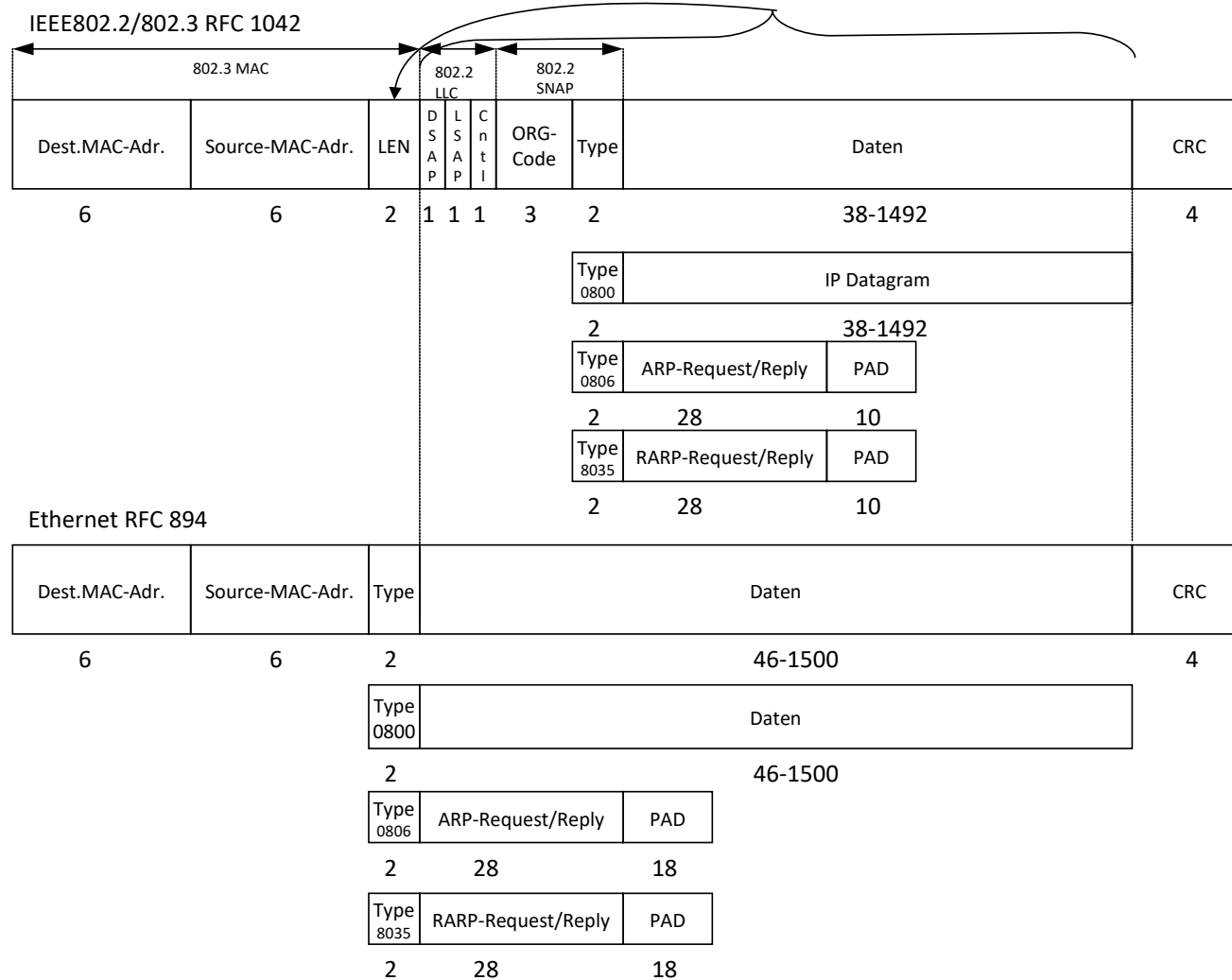


Bereich	Länge [Bytes]	Bedeutung	Wert
Präambel	7	Taktsynchronisation	Bitmuster 7 * 10101010
SFD	1	Start-Frame-Delimiter	Bitmuster 1 * 10101011
Ziel-MAC-Adr.	6	Ziel-Adresse fürMedia-Access-Control	
Quell-MAC-Adr.	6	Quell-Adresse fürMedia-Access-Control	
TL	2	Typ-Längen-Feld	
Padding	X	Füllzeichen damit der Datenteil mind. 46 Bytes enthält	<= 1500 = Framelänge > 1500 = Frametyp
FCS	4	Frame-Check-Sequence	Prüfsumme aus den Daten

Unterschiedliche Ethernet-Varianten

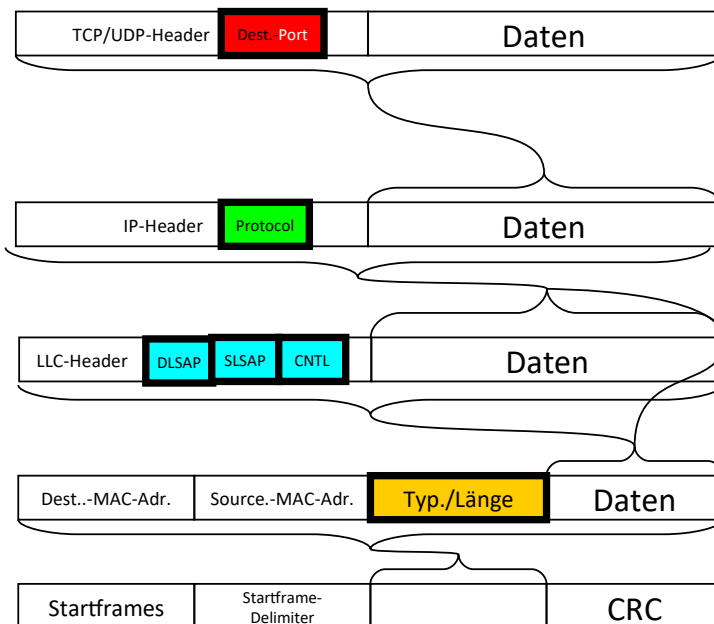


Auswirkungen der unterschiedlichen Ethernet-Varianten



Protokolle über ISO-7-Schichten Modell hinweg

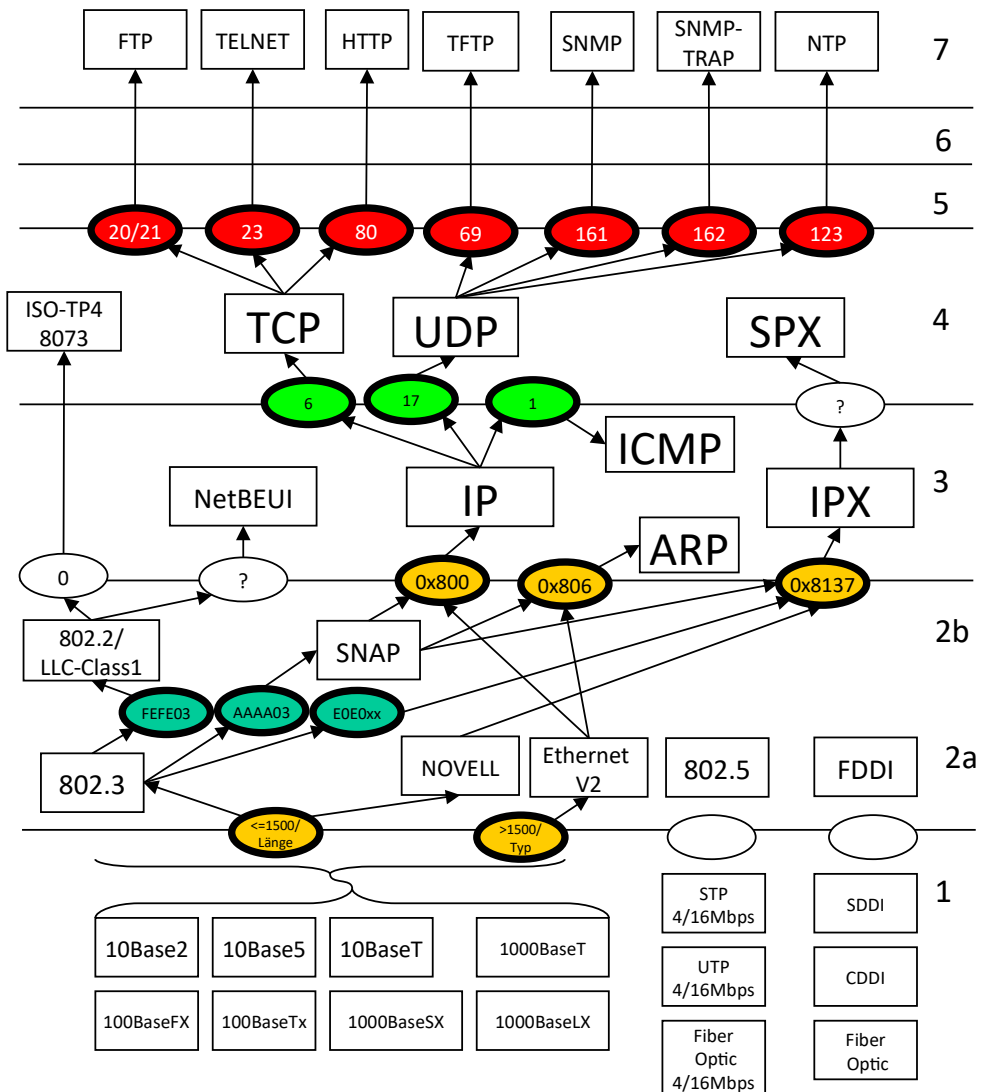
Relevanter Teil in der Datenübertragung



Protokollübersicht

Protokolle

ISO-7-Schicht-Ebene



IPv4-Funktionsübersicht

- IP ist im RFC791 beschrieben
- IP wurde zur ungesicherten Datenübertragung zwischen paketerorientierten Rechnernetzen entwickelt.
- Im IP werden zwei wichtige Funktionen des Internets abgewickelt.
 - ◆ Adressierung / Wegefindung
 - ◆ Fragmentierung (Zerlegung der Datagramme in transportierbare Größen) und
 - ◆ Reassemblierung (Zusammenbau der zerlegten Datagramme auf dem Zielsystem)

Der Dienst den die IP-Schicht liefert, wird mit 4 verschiedenen Parametern festgelegt

- TOS
- TTL
- Optionen
- Header Checksum

IP macht/regelt

- keine Flusskontrolle
- keine Wiederholungen
- keine Quittungen

Erkannte Fehler (Z. B. ein nicht erreichbarer Host) werden über das Internet Control Message Protocol (ICMP) gemeldet/abgehandelt.



IPv4-Adressen (classful)

Eine IP-Adresse besteht bei IPv4 aus 4 Bytes (=32Bits).

Die Darstellung besteht aus vier Integer-Zahlen im Bereich 0 bis 255, die mit Punkten getrennt werden. (dotted decimal)

Beispiel: 165.33.12.44

Klasse	1. Byte		2. Byte	3. Byte	4. Byte	Anzahl Netze	Anzahl Hosts
A	0	7 Bit Netz-Adr.	24 Bit Host-Adr.			127	16777213
B	10	14 Bit Netz-Adr	16 Bit Host-Adr.			16383	65533
C	110	21 Bit Netz-Adr.			8 Bit Host-Adr.	2097151	253

Netzwerk-Adressteil

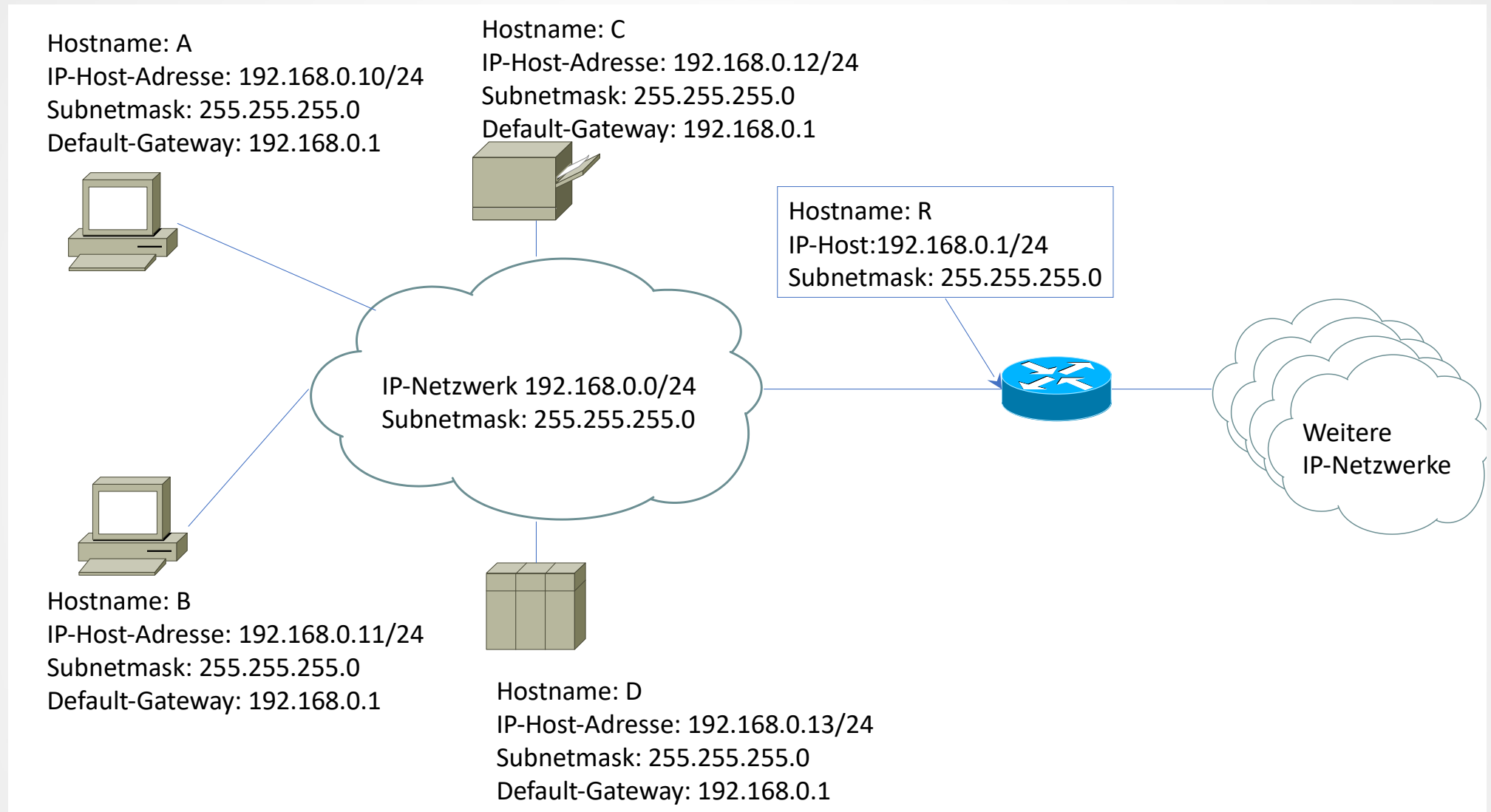
Host-Adressteil

IPv4-Adressklassen

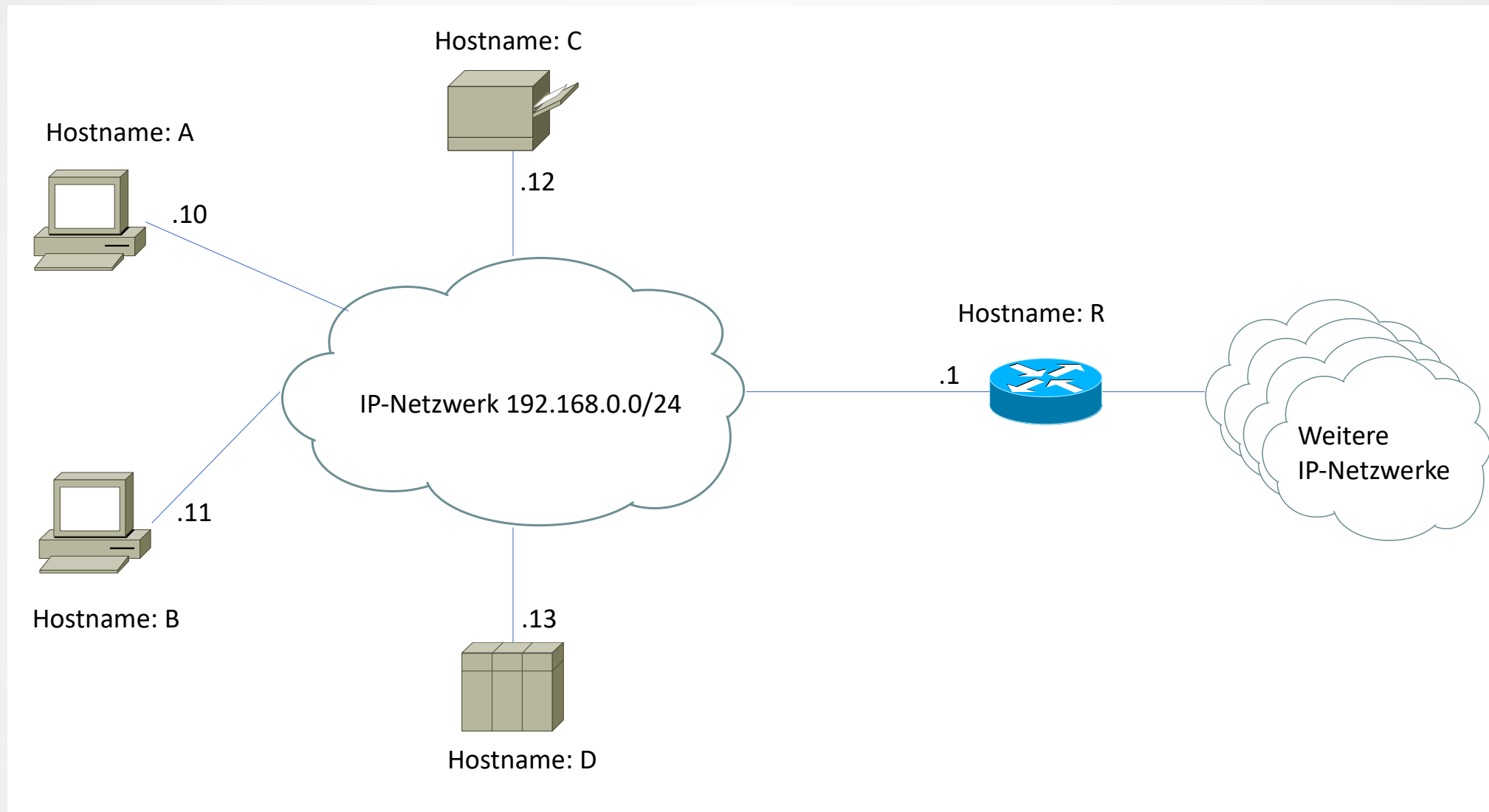
Klasse	Bereich	Subnet-Mask (classful)
A	0.0.0.0 - 127.255.255.255	255.0.0.0
B	128.0.0.0 - 191.255.255.255	255.255.0.0
C	192.0.0.0 - 223.255.255.255	255.255.255.0
D	224.0.0.0 - 239.255.255.255	Multicasts
E	240.0.0.0 - 255.255.255.255	Experimentelle Adressen / Broadcasts

Adress-Bereich	Bezeichnung	
224.x.x.x – 239.255.255.255	Multicasts	224.0.0.0 – 224.0.0.255 Link-Local Scope 224.0.1.0 – 238.255.255.255 Global Scope 239.0.0.0 – 239.255.255.255 Administrative Scope
240.x.x.x – 254.255.255.255	Experimentelle Adressen	
255.x.x.x	Broadcasts	

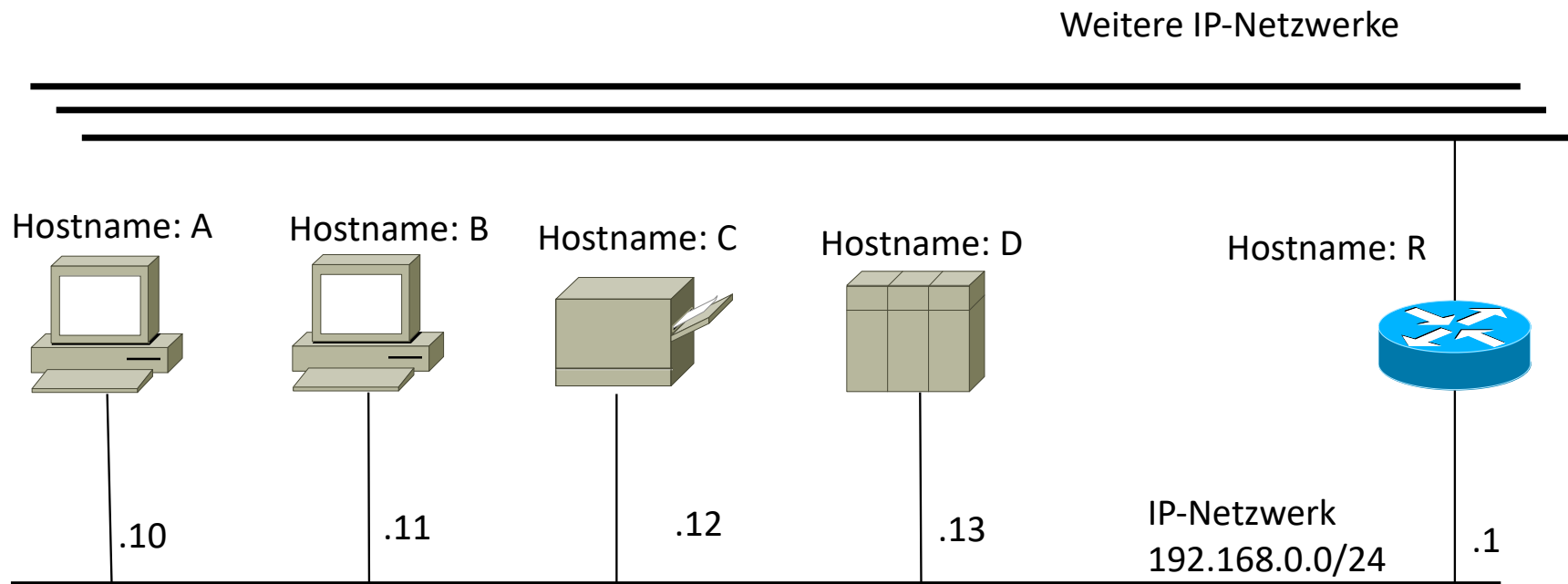
IPv4-Adressbeispiel



IPv4-Adressbeispiel (Vereinfachte Darstellung-1)



IPv4-Adressbeispiel (Vereinfachte Darstellung-2)

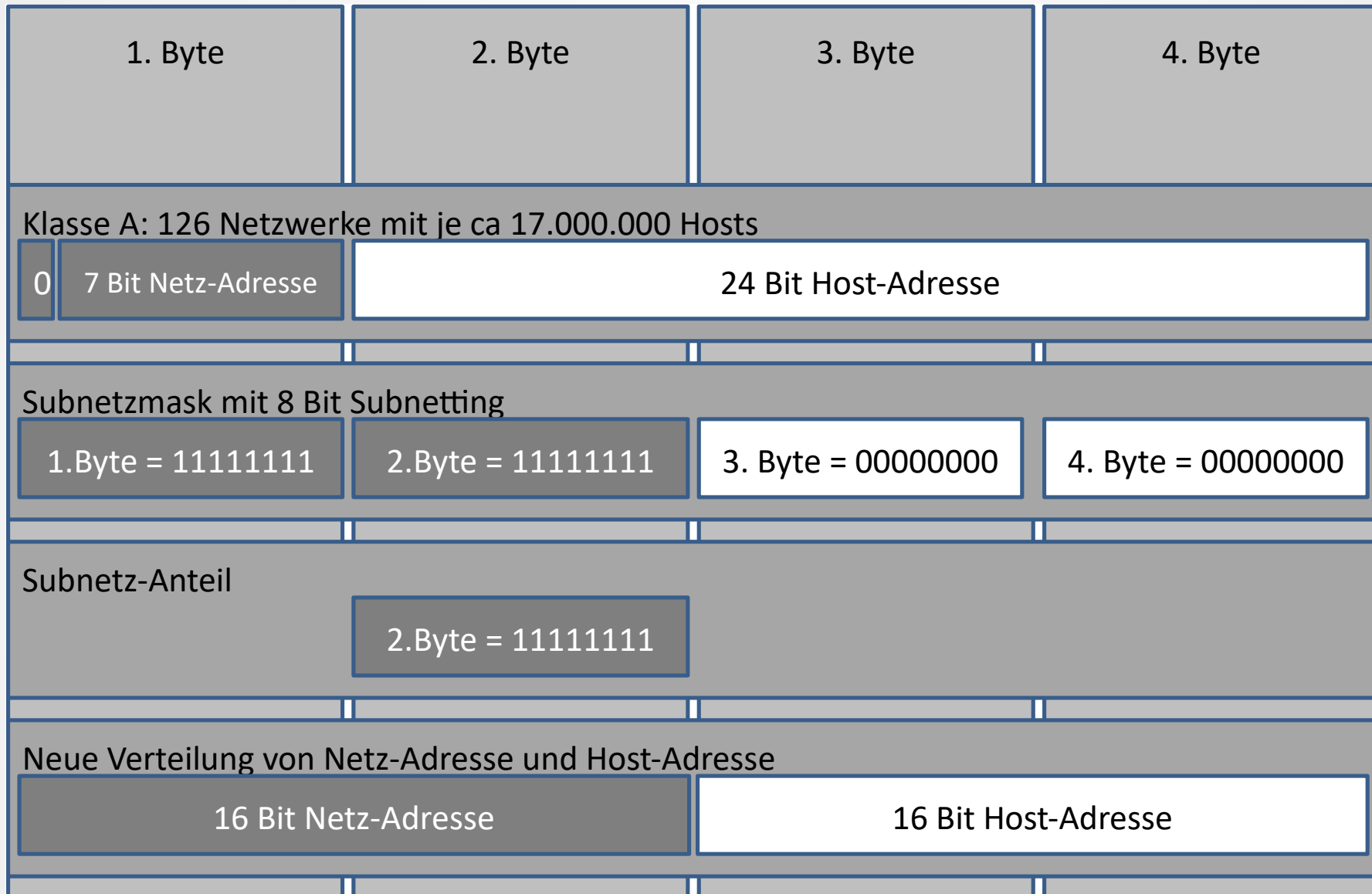


Ipv4 (Classful Subnetmask)

Klasse	Subnetzmaske (in dotted decimal Schreibweise)	Subnetzmaske (in binärer Schreibweise)	Subnetzmaske (in hexadezimaler Schreibweise)	Subnetzmaske (CIDR Schreibweise)
A	255.0.0.0	11111111 00000000 00000000 00000000	FF000000	/8
B	255.255.0.0	11111111 11111111 00000000 00000000	FFFF0000	/16
C	255.255.255.0	11111111 11111111 11111111 00000000	FFFFFF00	/24

A-Klasse 255.v.v.v Hierbei steht v.v.v, v.v oder v für den variablen Teil der Subnetz-Maske.
B-Klasse 255.255.v.v Links stehen immer die Einsen für den erweiterten Netzwerk-Teil und
C-Klasse 255.255.255.v rechts die Nullen für den restlichen Host-Teil.

IPv4-Subnetting



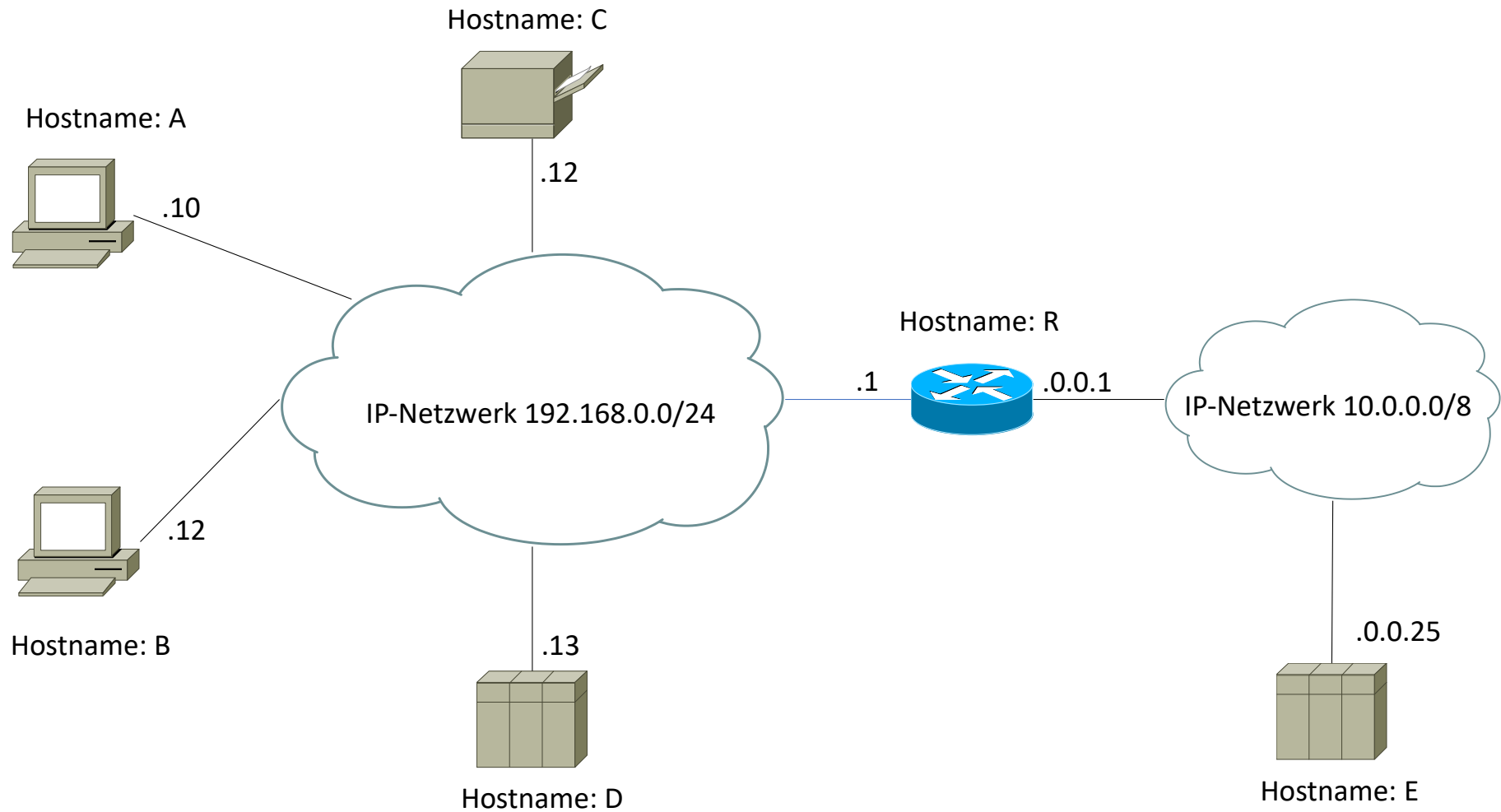
IPv4

Bitweise Änderung der Subnetmask

Dual-Darstellung	Dezimal-Darstellung	Hexadezimal-Darstellung
00000000	000	00
10000000	128	80
11000000	192	C0
11100000	224	E0
11110000	240	F0
11111000	248	F8
11111100	252	FC
11111110	254	FE
11111111	255	FF

IPv4

Anwendung der Subnetmask (Teil-1)



IPv4

Anwendung der Subnetmask (Teil-2)

Quelle

Host: A

IP-Adresse-A (192.168.0.10): 11000000.10101000.00000000.00001010
Subnet-Mask-A: 11111111.11111111.11111111.00000000
UND-Verknüpfung (1): 11000000.10101000.00000000.00000000 = Isolierter Netzwerkanteil (1)

Ziel im eigenen Netzwerk

Host D

IP-Adresse-B (192.168.0.13): 11000000.10101000.00000000.00001110
Subnet-Mask-A: 11111111.11111111.11111111.00000000
UND-Verknüpfung (2): 11000000.10101000.00000000.00000000 = Isolierter Netzwerkanteil (2)

Die UND-Verknüpfung (1) und die UND-Verknüpfung (2) liefern **das selbe Ergebnis**
→ Beide Kommunikationspartner liegen **im gleichen Netzwerk**

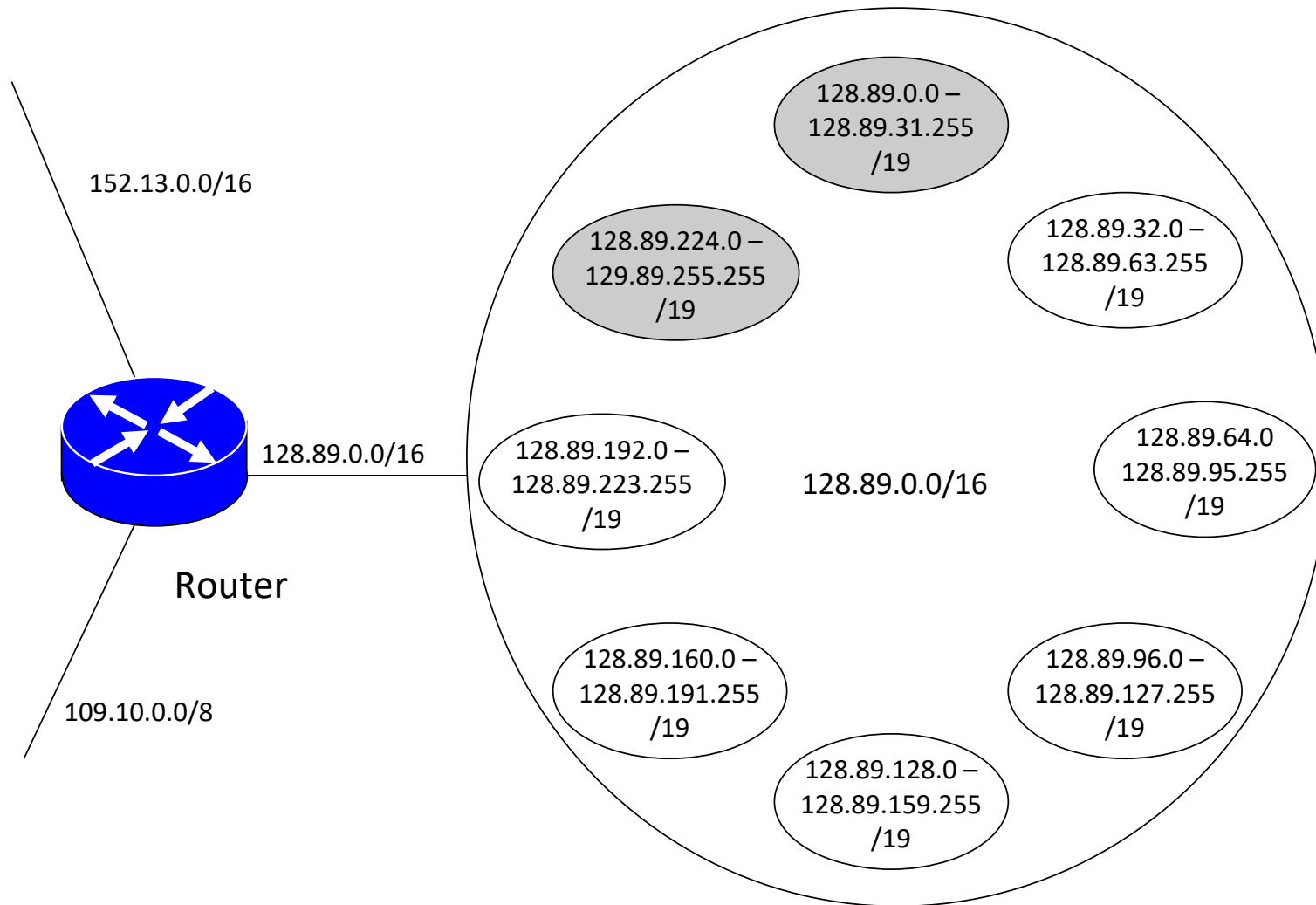
Ziel in anderem Netzwerk

Host E

IP-Adresse-E (10.0.0.25): 00001010.00000000.00000000.00011001
Subnet-Mask-A: 11111111.11111111.11111111.00000000
UND-Verknüpfung (3): 00001010.00000000.00000000.00000000 = Isolierter Netzwerkanteil (3)

Die UND-Verknüpfung (1) und die UND-Verknüpfung (3) liefern **nicht das selbe Ergebnis**
→ Beide Kommunikationspartner liegen **in unterschiedlichen Netzwerken**.

IPv4-Subnetting Beispiel



IPv4-Subnetting

Art des Subnetz	Dezimaler Wert	Binärer Wert	Anzahl der Subnetze	Anzahl der Hosts
2 Bit	192	11000000	$2^2 = 4$ Zustände -> 2 Subnetze	$2^6 = 64$ Zustände -> 62 Hosts
3 Bit	224	11100000	$2^3 = 8$ Zustände -> 6 Subnetze	$2^5 = 32$ Zustände -> 30 Hosts
4 Bit	240	11110000	$2^4 = 16$ Zustände -> 14 Subnetze	$2^4 = 16$ Zustände -> 14 Hosts
5 Bit	248	11111000	$2^5 = 32$ Zustände -> 30 Subnetze	$2^3 = 8$ Zustände -> 6 Hosts
6 Bit	252	11111100	$2^6 = 64$ Zustände -> 62 Subnetze	$2^2 = 4$ Zustände -> 2 Hosts

Ein-Bit-Subnetting sowie 7-Bit-Subnetting sind **bei C-Klasse-Netzwerken** zwecklos.

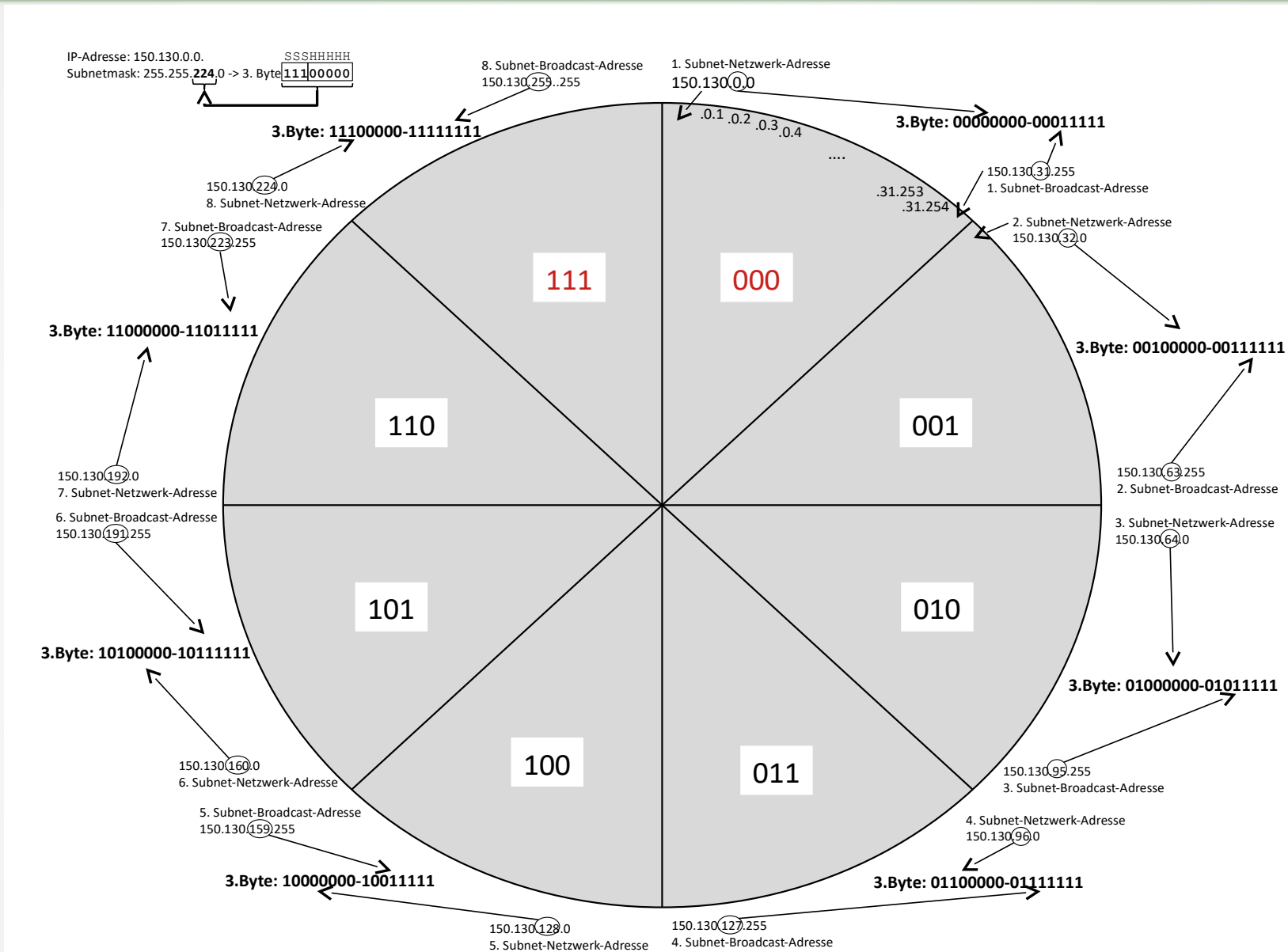
- Ein-Bit-Subnetting (10000000) lässt 0 Subnetze zu.
- 7-Bit-Subnetting (11111110) lässt **bei C-Klasse-Netzwerken** 0 Hosts zu.

Die Anzahl der Zustände bei den Subnetzen sowie bei den Hosts führt über die Formel:

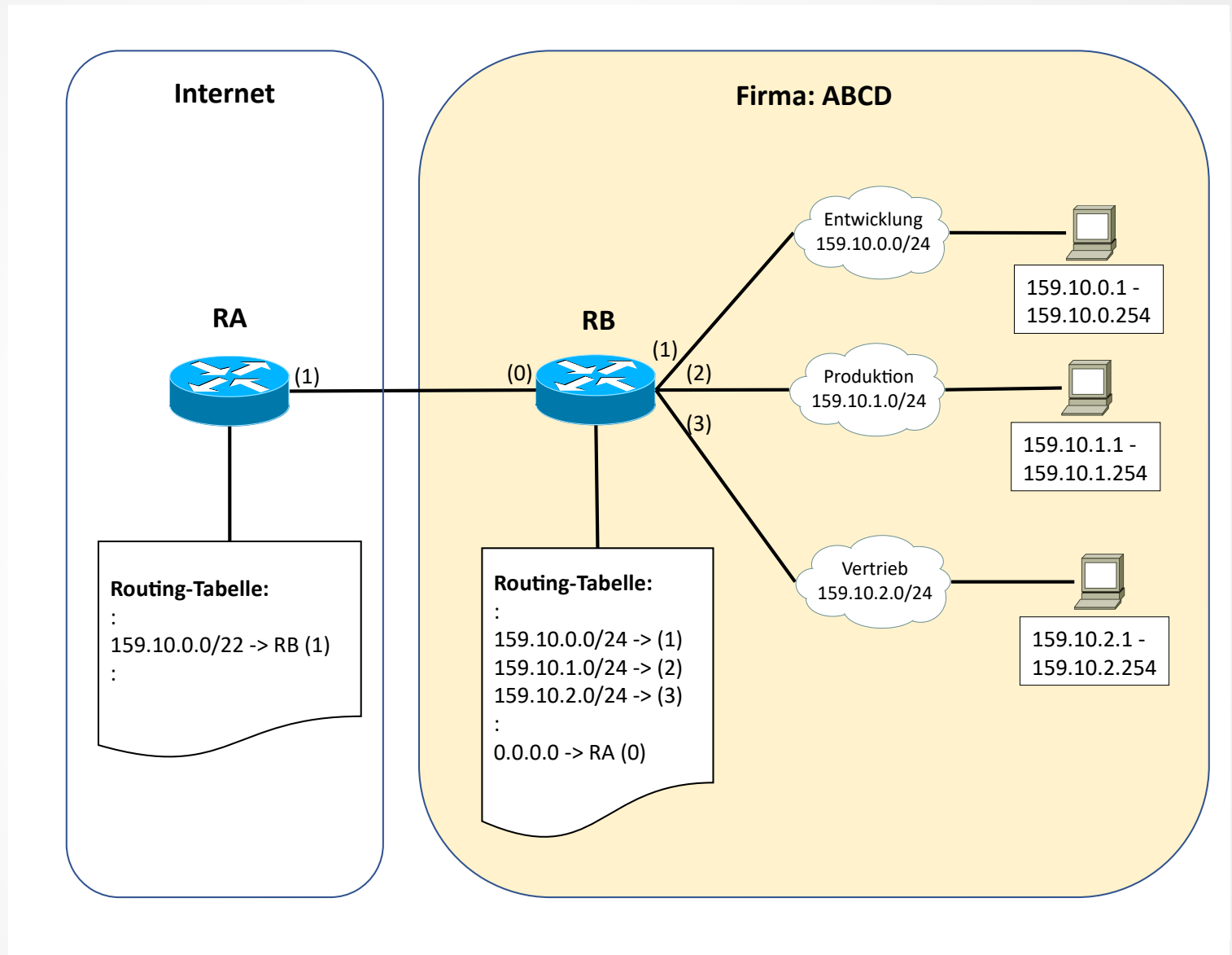
Anzahl = Anzahl der Zustände - 2

zu der möglichen Anzahl der Subnetze bzw. der Hosts.

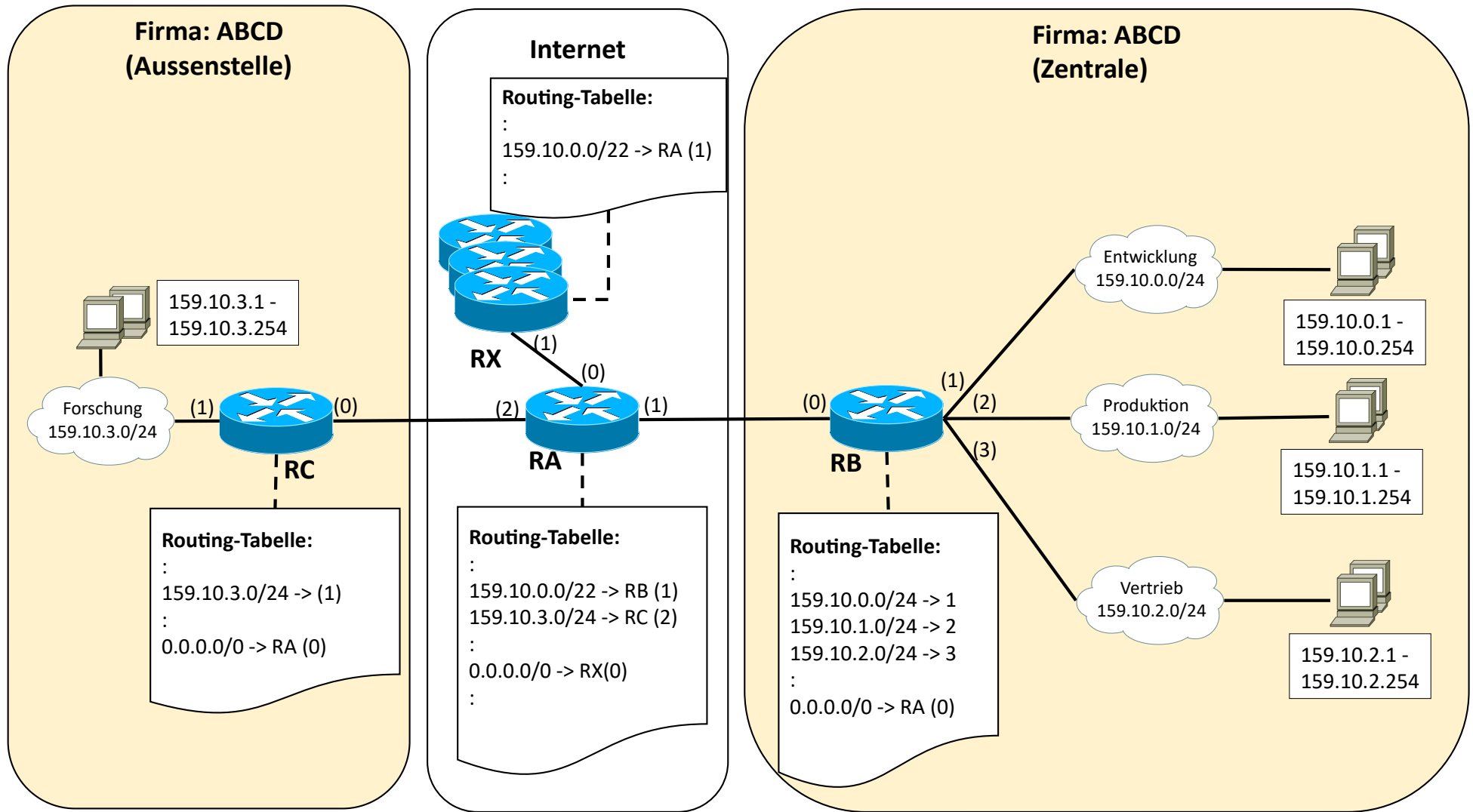
IPv4-Subnetting



IPv4-Supernetting (1)



IPv4-Supernetting (2)




IPv4-Unicasts / Multicasts / Broadcasts

Adressen	Bezeichnung	Verhalten
1.x.x.x : 223.x.x.x	Unicasts	Gehen von einem Sender an <u>einen</u> Empfänger
224.x.x.x	Multicasts	Gehen von einem Sender <u>an eine Gruppe</u> von Empfängern. So unterhalten sich z. B. Brücken miteinander
225.x.x.x : 255.x.x.x	Broadcasts	Gehen von einem Sender an alle Empfänger

IPv4-Multicasts

4 Bits	28Bits
1110	Multicast Group ID



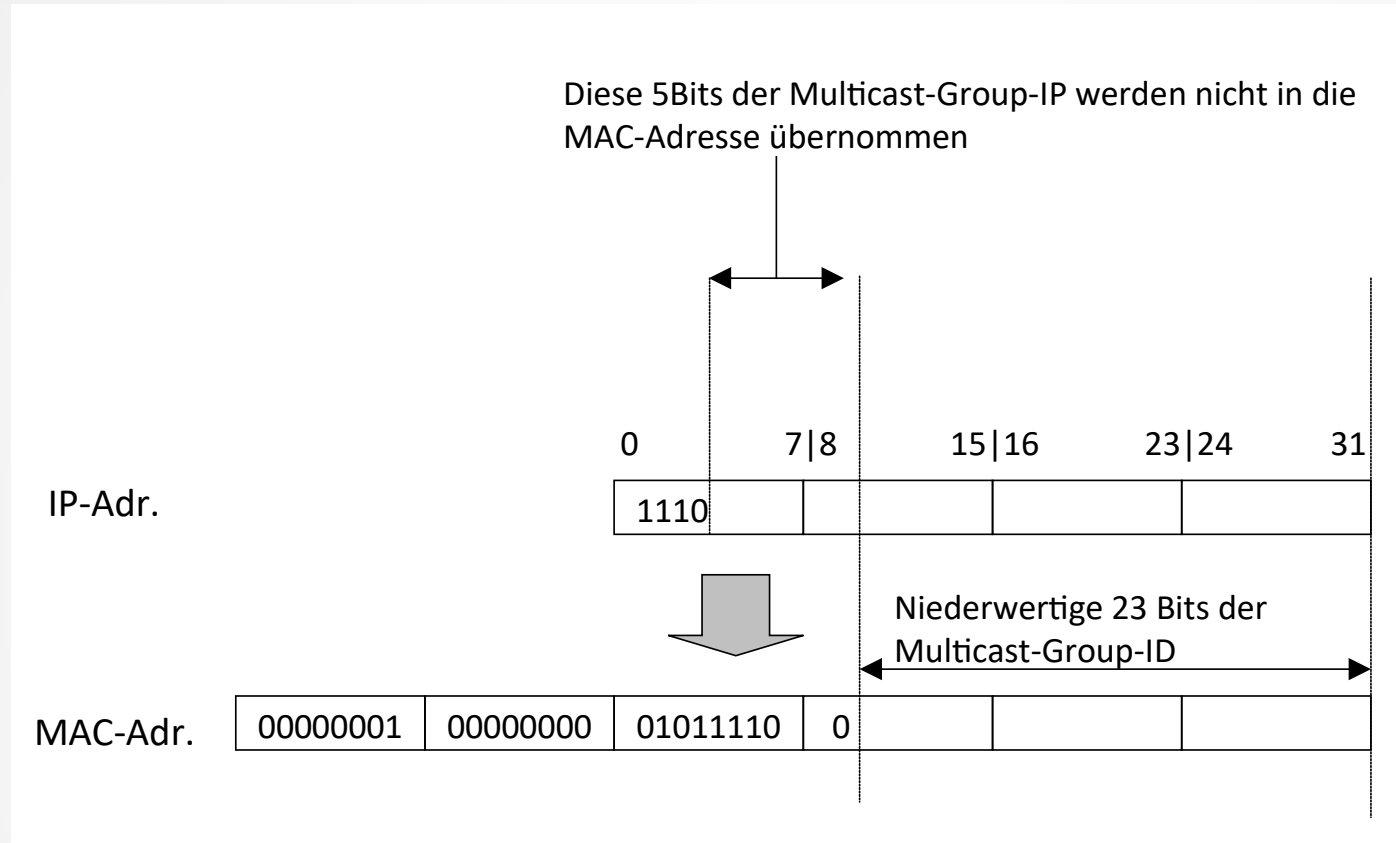
A horizontal line extends from the right side of the first table, and a vertical arrow points downwards from its end to the top of the second table.

Multicast-Group-ID	Bedeutung
224.0.0.1	Alle Systeme in diesem Subnetz
224.0.0.2	Alle Router in diesem Subnetz
224.0.0.9	RIP-2
224.0.1.1	NTP (Network Time Protocol)

IPv4

(Umsetzung der Multicast-IP-Adresse in eine MAC-Adresse)

Multicasts müssen, damit sie von der Netzwerk-Karte weiter geleitet werden, eine bestimmte MAC-Adresse haben



Dies bedeutet, dass bei Netzwerk-Teilnehmern, die Multicasts verarbeiten, die überlagerten Schichten die Multicasts filtern müssen!

Multicasts funktionieren auch mit mehreren Sendern (daher kommt auch der Name).

Rückmeldungen sind nicht möglich! Daher kann auch TCP nicht mit Multicasts verwendet werden.

Der Sender weiß nicht, wer ihm zuhört.

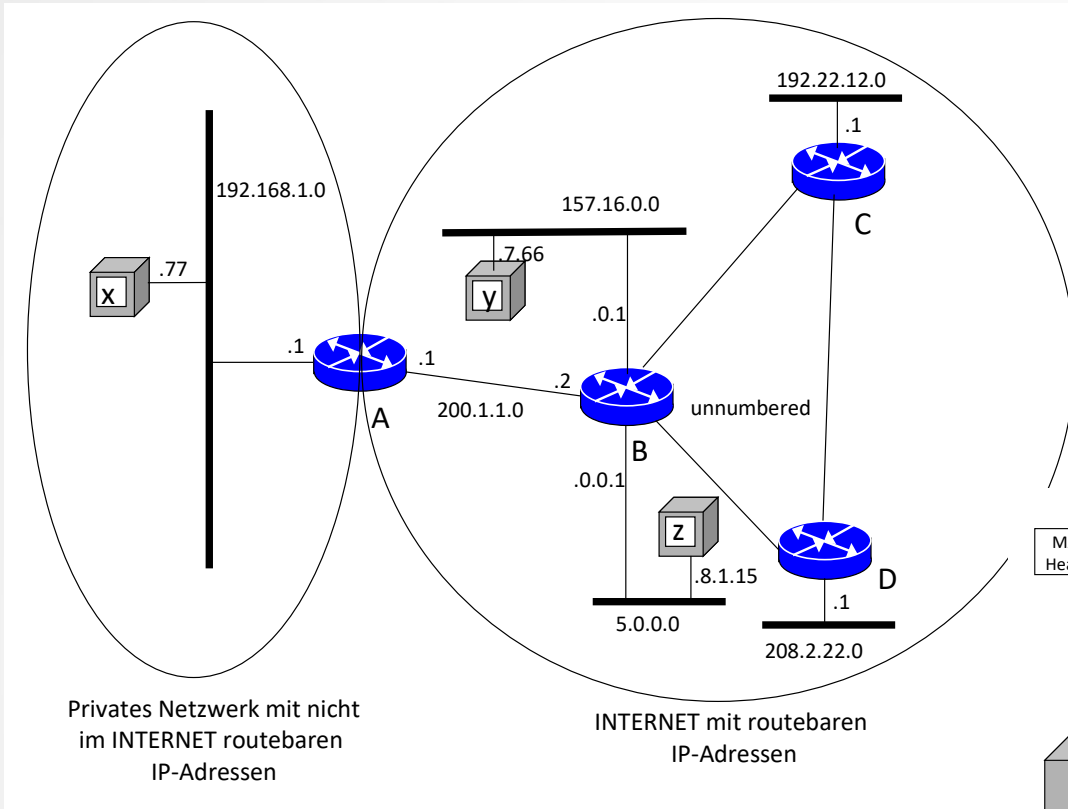
IPv4-Header

Version (4Bit)	IHL (4Bit)	TOS (8 Bit)	Length (16 Bit)	
ID (16 Bit)			Flags (3Bit)	Fragment Offset (13Bit)
TTL (8 Bit)		Protocol (8 Bit)	Checksum (16 Bit)	
Source Address (32Bit)				
Destination Address (32Bit)				
Options				Padding

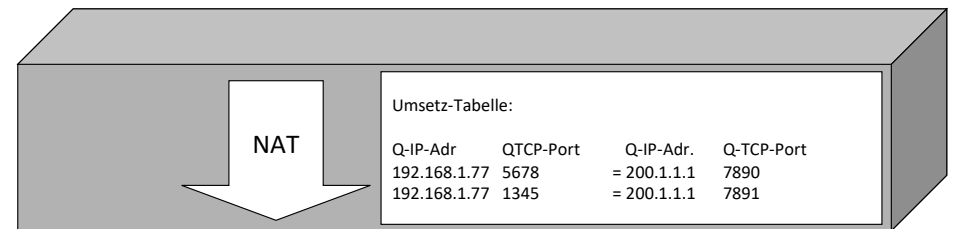
IPv4 (Referenznetzwerke)

Adressblock	Adressbereich	Beschreibung	Referenz
0.0.0.0/8	0.0.0.0 bis 0.255.255.255	aktuelles Netz (nur als Quelladresse gültig)	RFC 3232 (ersetzt RFC 1700)
10.0.0.0/8	10.0.0.0 bis 10.255.255.255	Netzwerk für den privaten Gebrauch	RFC 1918
127.0.0.0/8(1)	127.0.0.0 bis 127.255.255.255	Localnet	RFC 3330
169.254.0.0/16	169.254.0.0 bis 169.254.255.255	Zeroconf	RFC 3927
172.16.0.0/12	172.16.0.0 bis 172.31.255.255	Netzwerk für den privaten Gebrauch	RFC 1918
192.0.0.0/24	192.0.0.0 bis 192.0.0.255	reserviert, aber zur Vergabe vorgesehen	
192.0.2.0/24	192.0.2.0 bis 192.0.2.255	Dokumentation und Beispielcode (TEST-NET-1)	RFC 5737 (ersetzt RFC 3330)
192.88.99.0/24	192.88.99.0 bis 192.88.99.255	<u>6to4</u> -Anycast-Weiterleitungspräfix	RFC 3068
192.168.0.0/16	192.168.0.0 bis 192.168.255.255	Netzwerk für den privaten Gebrauch	RFC 1918
198.18.0.0/15	198.18.0.0 bis 198.19.255.255	Netz-Benchmark-Tests	RFC 2544
198.51.100.0/24	198.51.100.0 bis 198.51.100.255	Dokumentation und Beispielcode (TEST-NET-2)	RFC 5737
203.0.113.0/24	203.0.113.0 bis 203.0.113.255	Dokumentation und Beispielcode (TEST-NET-3)	RFC 5737
224.0.0.0/4	224.0.0.0 bis 239.255.255.255	Multicasts (früheres Klasse-D-Netz)	RFC 3171
240.0.0.0/4	240.0.0.0 bis 255.255.255.255	reserviert (früheres Klasse-E-Netz)	RFC 3232 (ersetzt RFC 1700)
255.255.255.255(2)	255.255.255.255	Broadcast	

IPv4 NAT / PAT



MAC-Header	Z-IP-Adr,:	Q-IP-Adr,:	IP-Prüf-Sum:	Z-TCP-Port:	Q-TCP-Port:	TCP-Prüf-Sum:	Daten
	157.16.7.66	192.168.1.77	uuu	1234	5678	vvv	

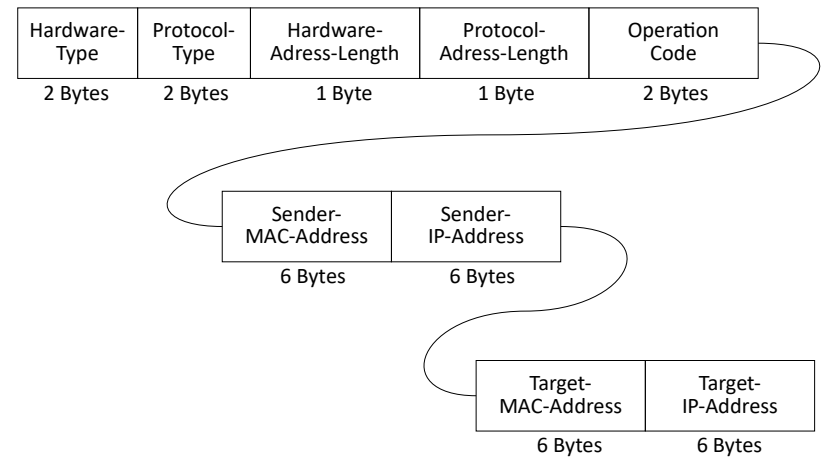
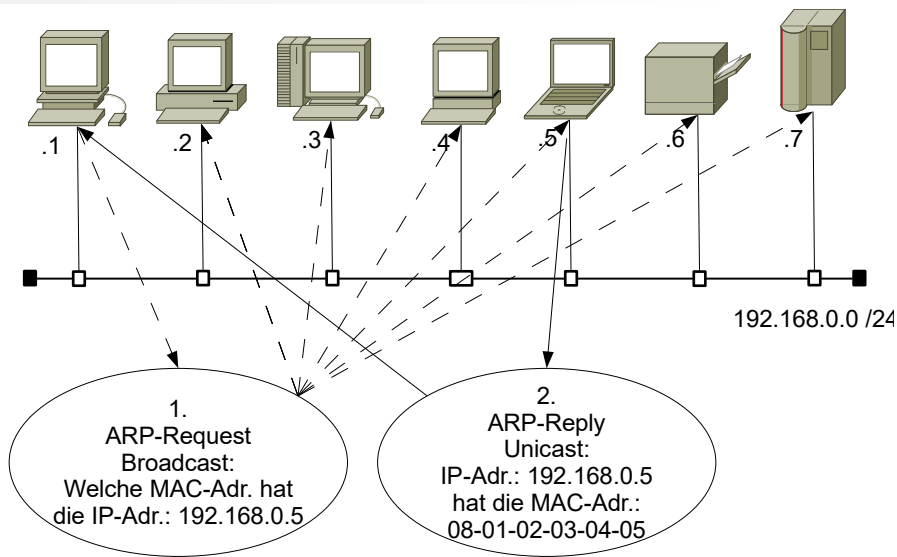
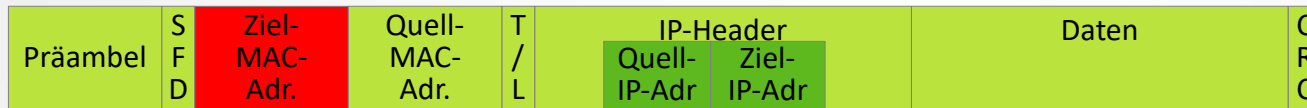


MAC-Header	Z-IP-Adr,:	Q-IP-Adr,:	IP-Prüf-Sum:	Z-TCP-Port:	Q-TCP-Port:	TCP-Prüf-Sum:	Daten
	157.16.7.66	200.1.1.1	yyy	1234	7890	zzz	

IPv4

ARP (Address Resolution Protocol)

Beim Aufbau eines Frames an ein neues Ziel ist bis auf die Ziel-MAC-Adresse alles bekannt. Die Ziel-MAC-Adresse wird mit dem ARP ermittelt.



Bearbeitung des ARP-Caches in der DOS-BOX

arp -a

arp -s <ip-adr> <mac-adr>

arp -d <ip-adr>

Ausgabe des ARP-Cache-Inhalts
ARP-Eintrag manuell vornehmen
ARP-Eintrag löschen

IPv4

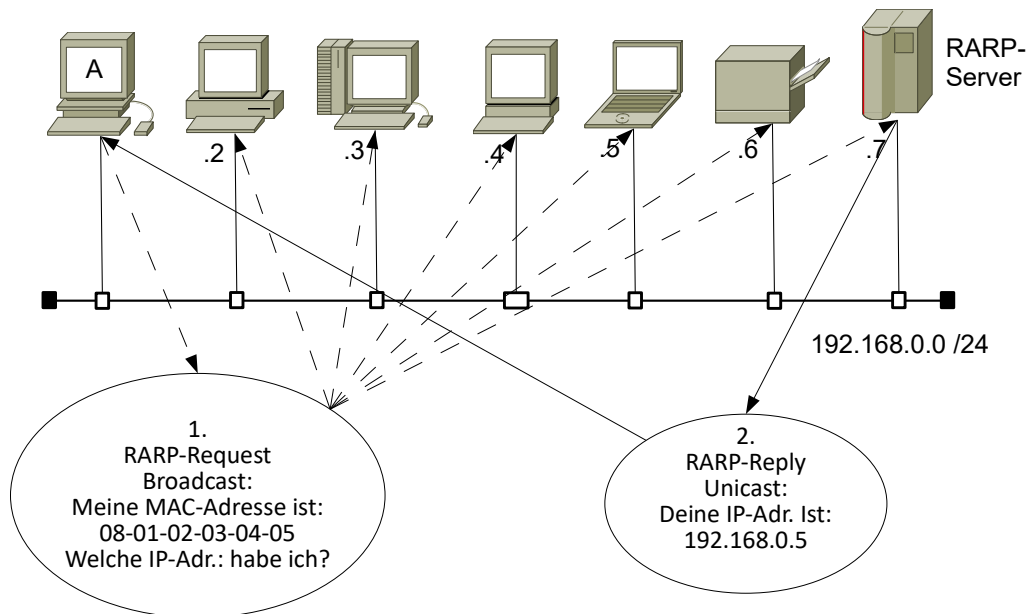
RARP (Reverse Address Resolution Protocol)

Will eine Station ihre IP-Adresse ermitteln, kann dies mit dem RARP erfolgen.

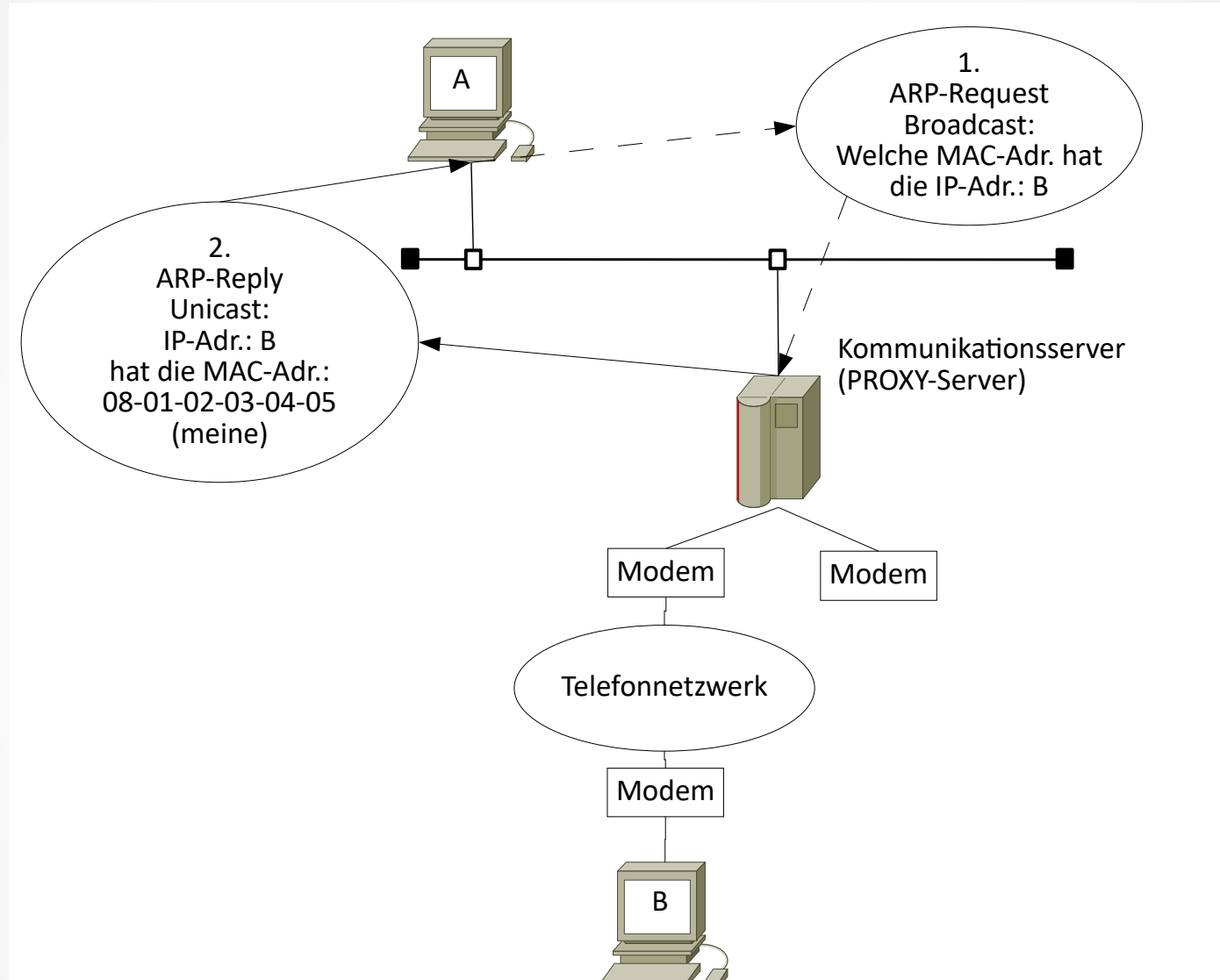
Präambel	S	Ziel-	Quell-	T	IP-Header		Daten	C
	F	MAC-	MAC-	/	Quell-	Ziel-		R
	D	Adr.	Adr.	L	IP-Adr	IP-Adr		C

Station A möchte seine eigene IP-Adresse erfahren.
Deshalb sendet Station A einen RARP-Request mit einem Broadcast an alle (Wer kennt mich?) (1.)

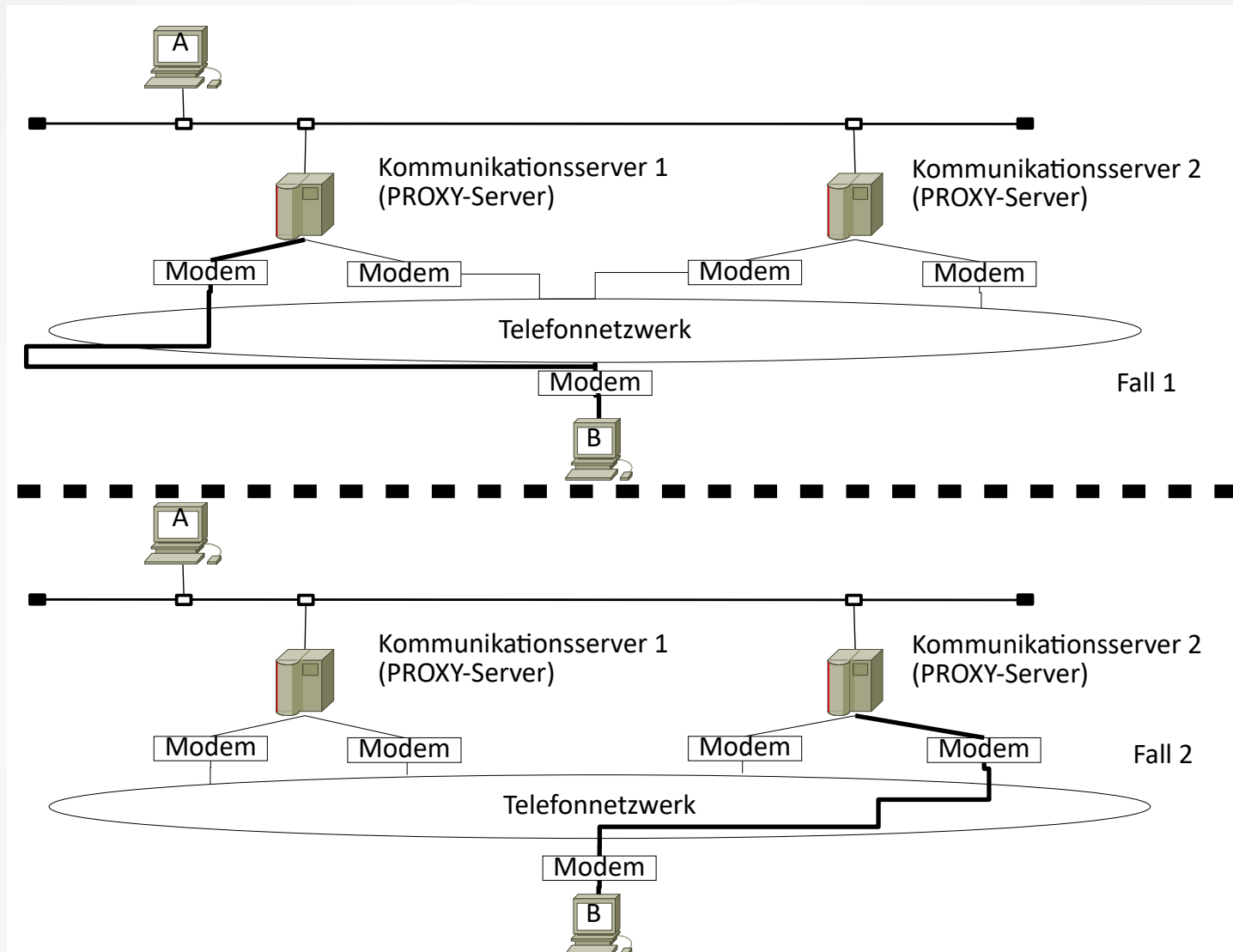
Der RARP-Server kennt die IP-Adresse und sendet sie an die Station A. (2.)



IPv4 PROXY ARP

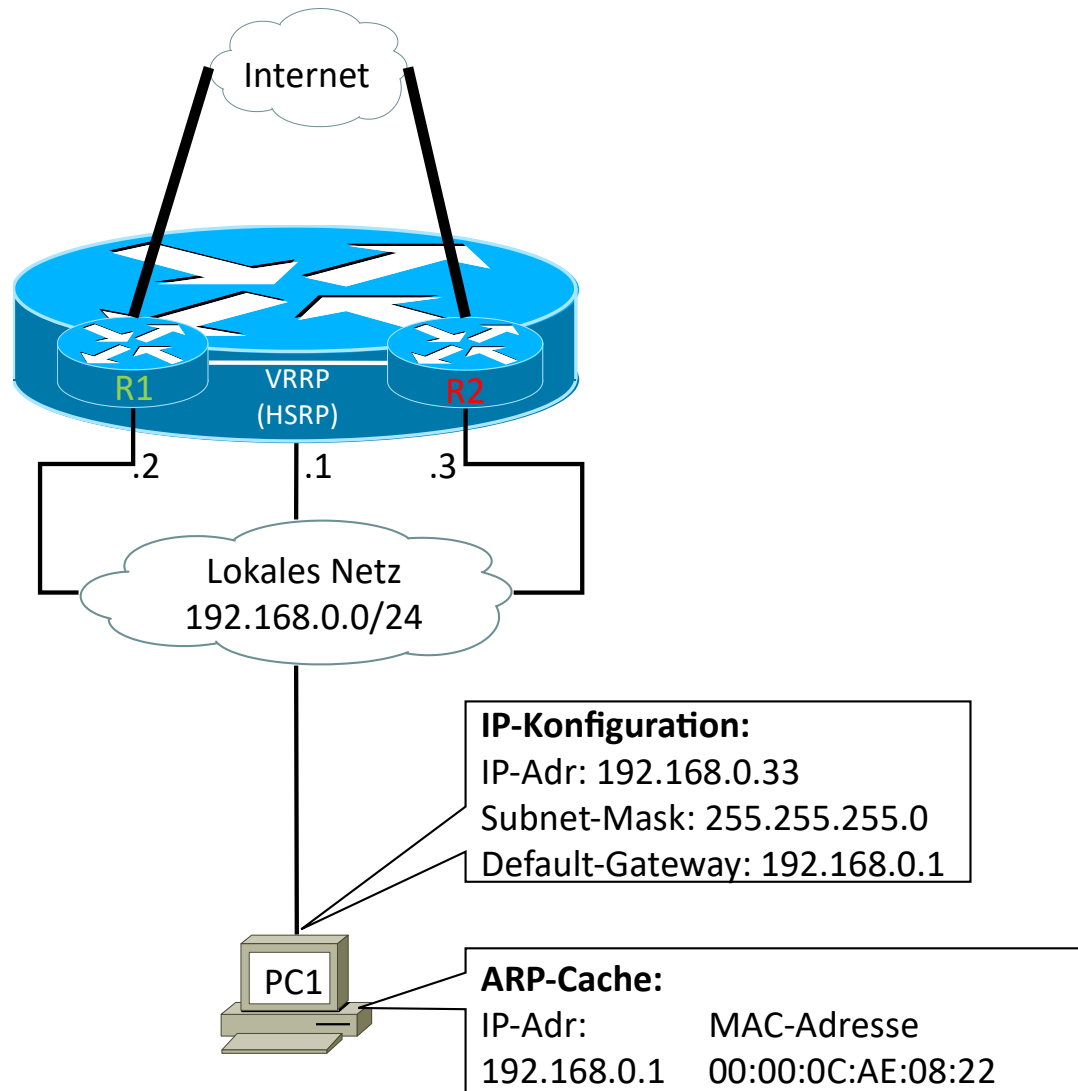


IPv4 UNARP

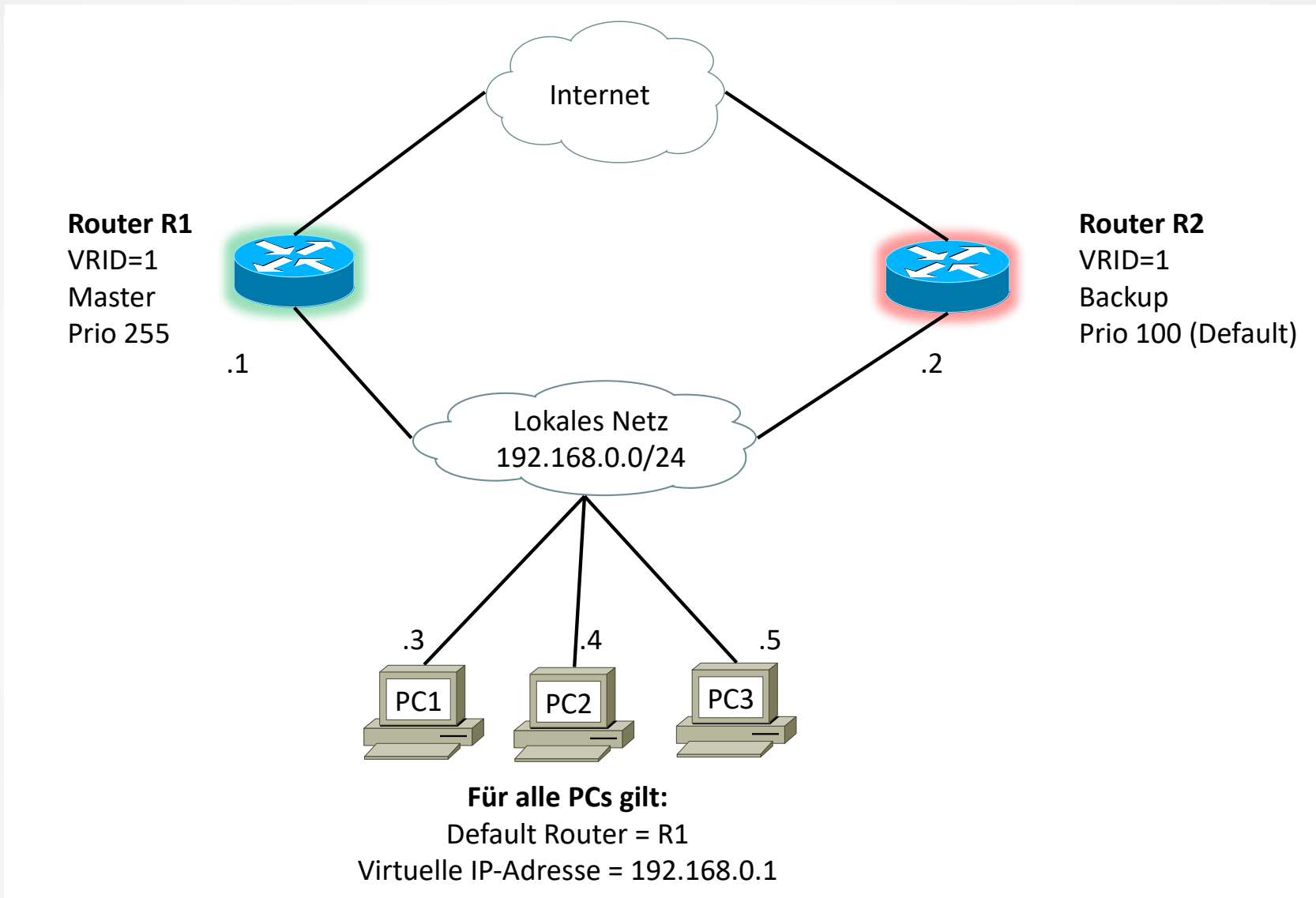


IPv4

GLBP / HSRP / VRRP

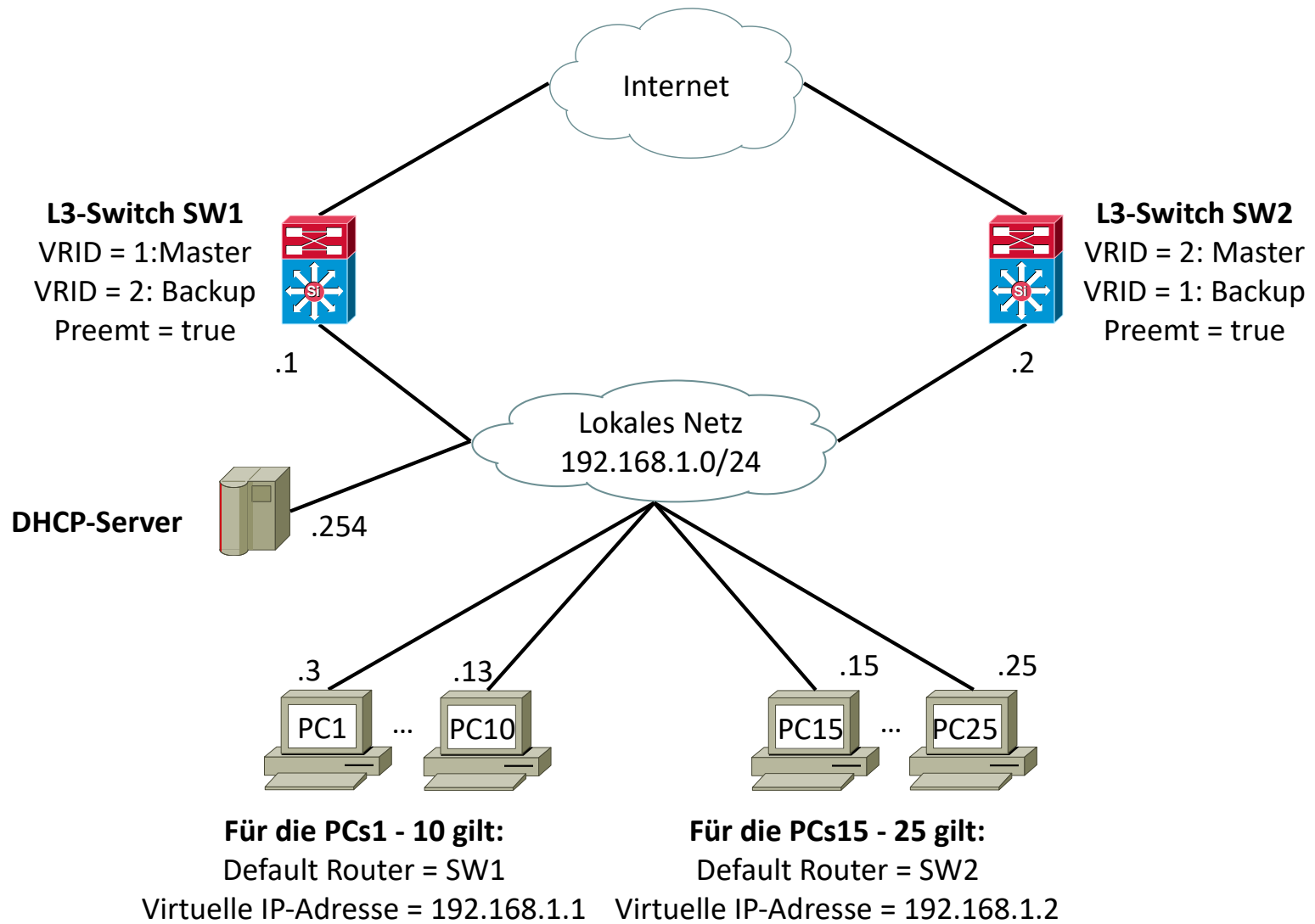


IPv4 VRRP-Beispiel-1



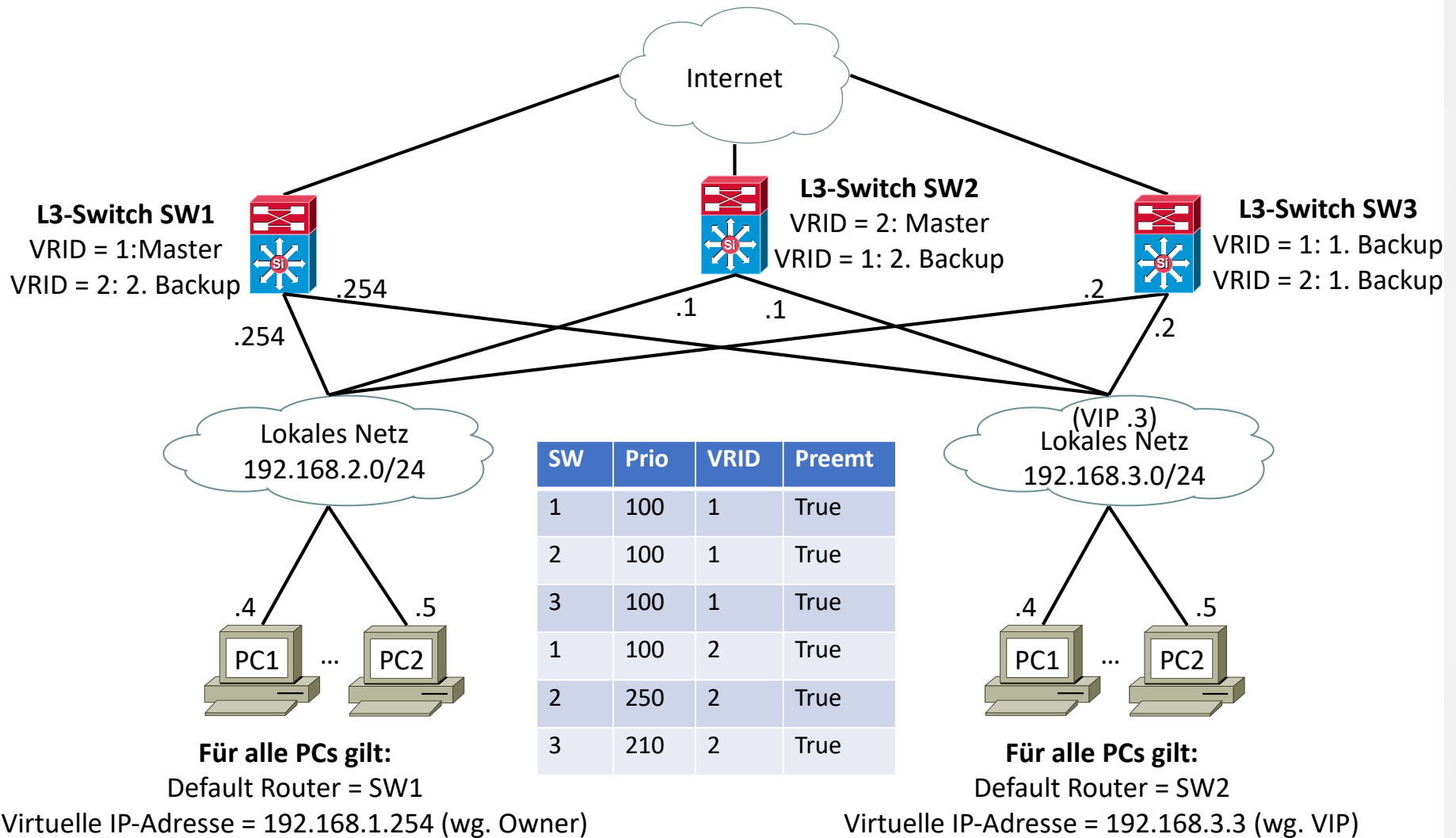
IPv4

VRRP-Beispiel-2

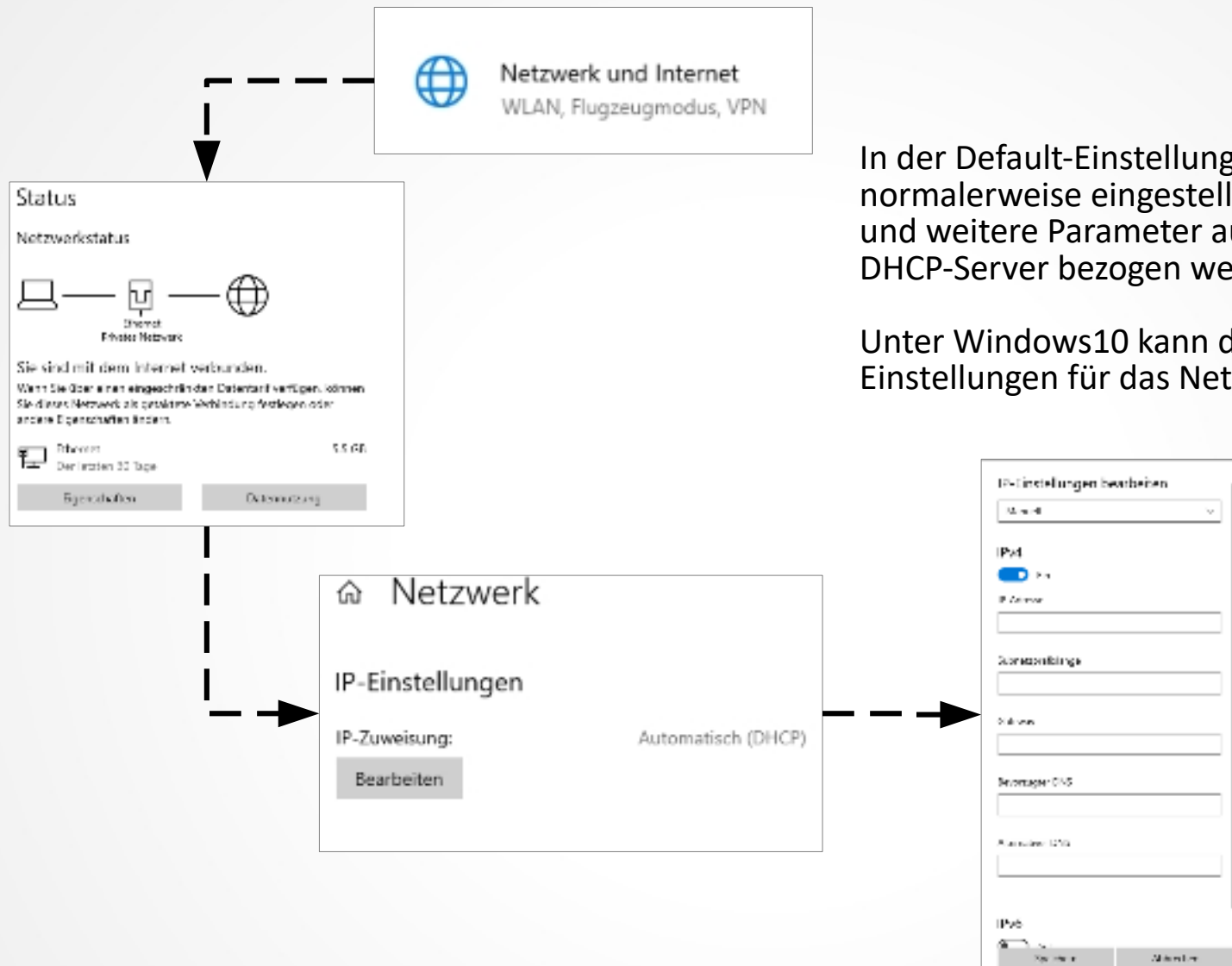


IPv4

VRRP-Beispiel-3



IPv4 DHCP

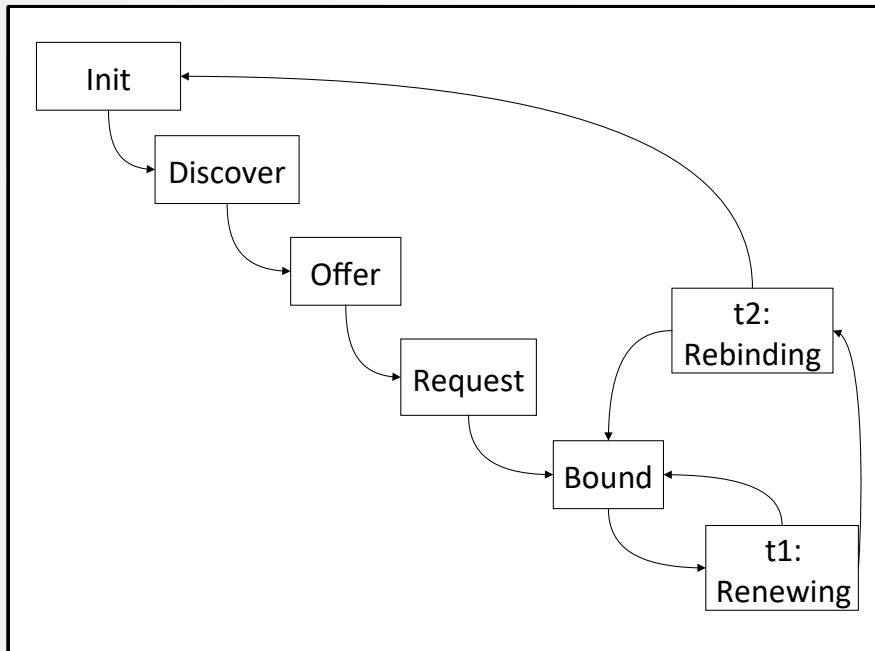


In der Default-Einstellung haben Clients normalerweise eingestellt, dass die IP-Adresse und weitere Parameter automatisch von einem DHCP-Server bezogen werden.

Unter Windows10 kann das unter den Einstellungen für das Netzwerk geändert werden.

IPv4 DHCP-Ablauf

Ablauf



DOS-Box-Kommandos

Informationsausgabe: `ipconfig /all`
Lease erneuern: `ipconfig /renew`
Lease freigeben: `ipconfig /release`

Lease-Erneuerung

Mit der Bestätigung des Lease wurde dem Client noch die Leasedauer mitgeteilt.

Aus der Leasedauer erzeugt der Client zwei Timer.

$t1 = 0,5 * \text{Leasedauer}$

Nach dieser Zeit muss der Client die Leaserime erneuern und sendet einen DHCP-Request aus.

Damit ist der Client im Zustand RENEWING. Empfängt der Client innerhalb einer Zeit $\leq t2$ einen DHCP-ACK, dann ist er wieder im Zustand BOUND.

$t2 = 0,875 * \text{Leasedauer}$

Empfängt der Client innerhalb der Zeit $t2$ keine Nachricht vom Server fällt er in den Zustand REBINDING.

Dann versucht er es über einen DHCP-Request als Broadcast an alle verfügbaren DHCP-Server.

Bekommt der Client eine Antwort fällt er in den Zustand BOUND. Kommt allerdings keine Antwort oder er erhält ein DHCP-NAK, fällt er in den Zustand INIT.

IPv4

Der DHCP-Server kann dem Client mit den Options eine Vielzahl von Parametern mitgeben.
Hier eine kleine Auswahl

Option Number	Name	Description
1	Subnet-Mask	Subnet-Mask
2	Time Offset	Time offset in seconds from UTC
3	Router	router addresses
4	Time-Server	time server addresses
5	Name-Server	IEN-116 server addresses
6	DNS-Server	DNS server adresse
7	LOG-Server	logging server adresse
8	Cookie-Server	quote server addresses
9	LPR Servers	printer server addresses
12	Host Name	Hostname string
15	Domain Name	The DNS domain name of the client
19	IP Layer Forwarding	Enable or disable IP forwarding
51	IP Address Lease Time	IP address lease time
58	Renew Time Value	DHCP renewal (T1) time
59	Rebinding Time Value	DHCP rebinding (T2) time

Eine detaillierte Liste gibt es z.B. bei:

<https://www.iana.org/assignments/bootp-dhcp-parameters/bootp-dhcp-parameters.xhtml#options>

IPv4

Zeroconf / APIPA

Ist entweder der DHCP-Server nicht vorhanden / erreichbar, oder ist der IP-Pool erschöpft, kann keine IP-Adresse zugewiesen werden.

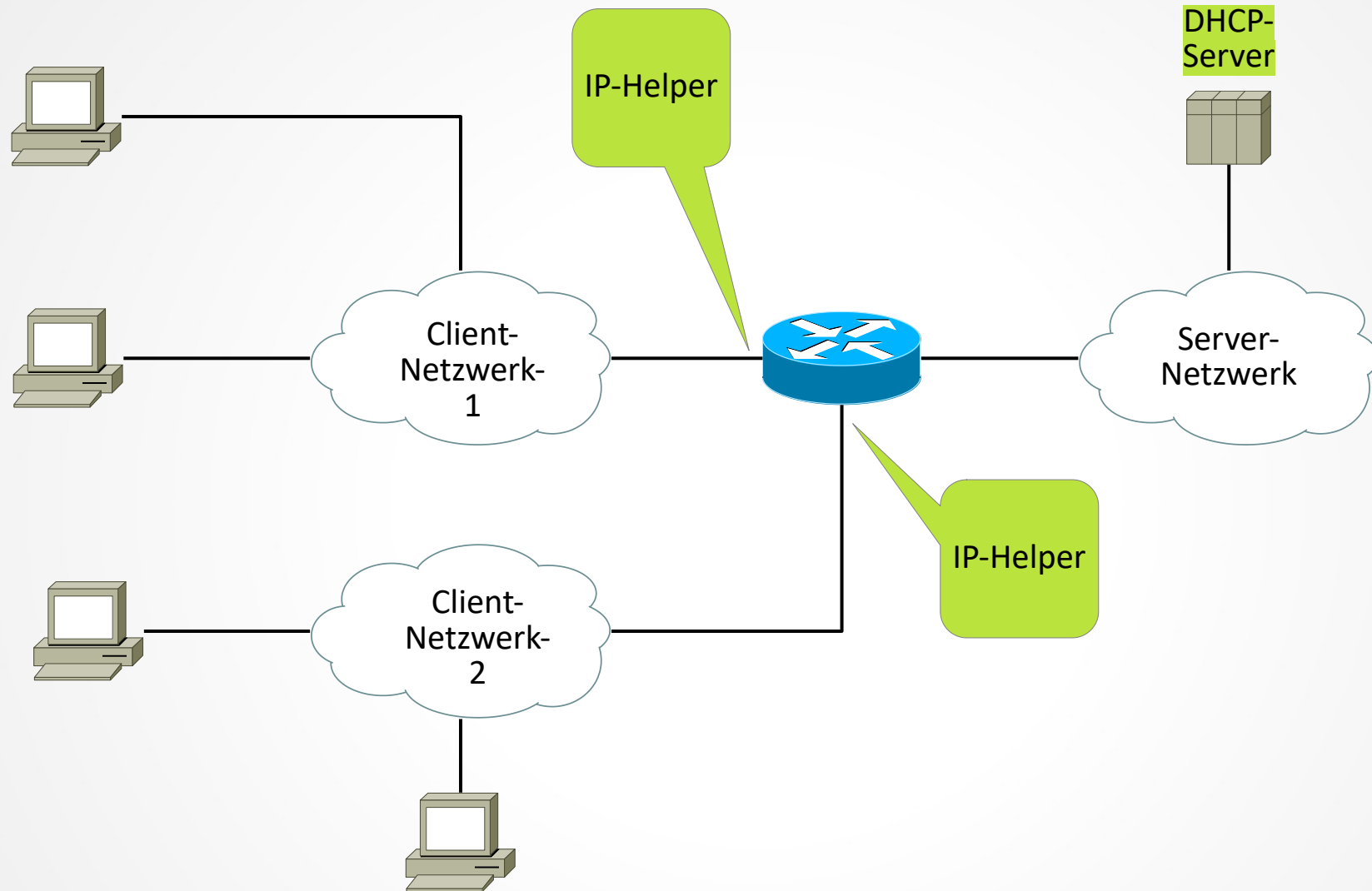
Damit ein Client dann trotzdem noch (wenigstens eingeschränkt) kommunizieren kann, gibt er sich über Zeroconf selbst eine IP-Adresse.

Dabei greift er auf einen hierfür reservierten IP-Adressbereich zurück 169.254.0.0/16

In diesem Netzwerk gibt er sich eine IP-Adresse. (z. B. 169.254.0.22/16)

Diese Adresse ist natürlich vor der Benutzung daraufhin zu testen ist, ob sie schon von einem anderen Client genutzt wird.

IPv4 Iphelper



IPv4 ICMP

ICMP-Aufbau

Datenbits			
01234567	01234567	01234567	01234567
Type	Code	Checksum	
Data			
...			

IP kann selbst keine Fehlermeldungen erzeugen.
Dazu verwenden die Geräte, die IP nutzen, **ICMP**

Feld	Beschreibung
Type	Typenfeld, abhängig von der Art der ICMP-Nachricht
Code	Zusatzinformation zur ICMP-Nachricht
Checksum	Prüfsumme des gesamten ICMP-Paketes
Data	Abhängig von der Art des ICMP-Paketes können hier mehrere 32-Bit-Worte übertragen werden

Typ	Bedeutung
0	Echo reply
3	Destination unreachable
4	Source quench
5	Redirect (route change)
8	Echo Request
11	Time exceeded for datagram
12	Parameterproblem on datagram
13	Time stamp request
14	Time stamp reply
15	Information request
16	Information reply
17	Address mask request
18	Address mask response

z. B. Typ = 3

Code	Data
0 = Net unreachable	Not used
1 = Host unreachable	Not used
2 = Protocol unreachable	Not used
3 = Port unreachable	Not used
4 = Fragmentation needed and df (don't fragment) set	Not used
5 = source route failed	Not used

IPv4

Namensauflösung

Anwender und auch Applikationen verwenden normalerweise zur Bezeichnung von Zielen sprechende Namen wie z. B. www.Amazon.com

Dahinter stehen IP-Adressen, die etwas umständlicher zu merken und zu schreiben sind.

Zur Auflösung der Namen in IP-Adressen werden Name-Services verwendet.

Historisches:

Als die Anzahl der verwendeten Geräte noch übersichtlich war wurden die Namen in Listen verwaltet.

Z. B. unter Unix: `/etc/hosts` und unter Windows `C:/Windows/System32/drivers/etc/hosts`

Da dies mit steigender Geräteanzahl nicht mehr vernünftig aktuell zu halten war wurden Server mit dem Verwalten der Namens-IP-Adress-Zuordnung entwickelt.

Internet-Name-Server

Die erste Lösung mit einer solchen Eigenschaft heißt Internet Name Service und ist unter der Internet Engineering Note 116 (IEN 116) veröffentlicht.

Im Name Server File können bis zu drei Name-Server hinterlegt werden.

Es gibt einen so genannten Primary Name Server, der immer als erster angesprochen wird.

Ist der Primary Name Server nicht erreichbar wird die Anfrage an den Secondary Name Server gesendet.

Primary Name Server 192.1.2.1

Secondary Name Server 192.1.2.5

Der Abfragende Rechner sendet einen Name-Request und erhält vom Name-Server einen Name-Reply zurück. Zur Sicherstellung, dass die Antwort auch zur Anfrage passt wird im Reply-Paket der angefragte Name nochmals zusammen mit der ermittelten IP-Adresse übertragen.

IPv4

DNS: Namensauflösung-1

DNS hat eine dezentrale Verwaltung mit einer Baumstruktur für den Namensraum. Weiterhin kann sichergestellt werden das Namen eindeutig sind und die Funktion erweitert werden kann. Bei der Baumstruktur haben die Blätter (Knoten) werden als Labels bezeichnet. Ein Label darf nur alphanumerische Zeichen und den Bindestrich (-) enthalten. Der Bindestrich darf nicht am Ende stehen. Ein kompletter Domainname besteht aus einer Verkettung aller Labels eines Pfades. Ein Label ist eine Zeichenkette mit mindestens einem Byte und maximal 64 Bytes (RFC 2181). Die Labels werden mit Punkten innerhalb eines Domainnamens miteinander verbunden/getrennt.

DNS nutzt UDP als Transportschicht und verwendet dort den Port 53. TCP ist ebenfalls möglich und wird auf jeden Fall für die Zonentransfers (Verteilung der Informationsdateien) genutzt.

Der Service lässt sich in beiden Richtungen betreiben:

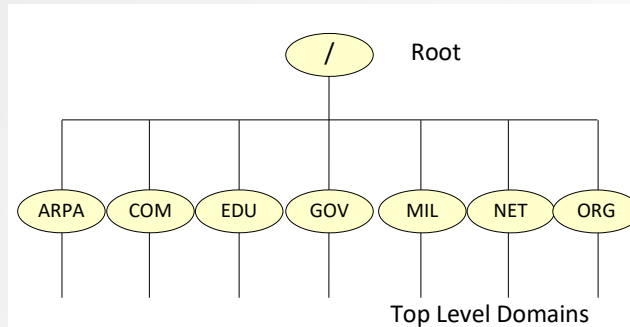
- Für einen Rechnernamen die zugehörige IP Adresse ermitteln (lookup)
- Für eine IP-Adresse den zugehörigen Namen ermitteln (reverse lookup)

Das DNS besteht aus den drei Hauptkomponenten:

- Domain-Namensraum
- Nameserver
- Resolver

IPv4

DNS: Namensauflösung-2



Neben den TLDs gibt es noch Country-TLDs. Z. B.:

.de	Deutschland
.au	Österreich
.li	Lichtenstein
.lu	Luxemburg
.us	USA

Der Domain-Namensraum hat eine baumförmige hierarchischen Aufbau. Von der Root ausgehend entwickelt sich der Baum. Bei der Baumstruktur werden die Blätter (Knoten) als Labels bezeichnet.

Jede Verzweigung entspricht einer Zone.

Die erste / oberste Ebene wird als Top-Level-Domains (TLD) bezeichnet.

TLDs wurden vom Network Information Center (NIC) definiert.

Ein kompletter Domainnamen (FQDN = Fully Qualified Domain Name) wird mit einem Punkt abgeschlossen und darf inklusive aller Punkte 255 Byte lang sein.

Je weiter ein Label im Domainnamen rechts steht, desto höher steht es im Baum.

Deshalb wird ein Domain-Name immer von links nach rechts delegiert und aufgelöst.

Ein vollständiger Domain-Name wird auch Fully Qualified Domain Name (FQDN) genannt.

Beispiel für ein FQDN: `www.amazon.com.`

Der letzte Punkt gehört zum DNS-Namen, kann jedoch weg gelassen werden.

IPv4

DNS: Namensauflösung-3

Die DNS-Objekte werden als Satz von Resource-Records in einer sogenannten Zonendatei (auch Zone genannt) gehalten und auf den autoritativen DNS-Servern über Zonentransfers abgeglichen.

Resource Records

Die von den DNS-Servern verwalteten Informationen sind in den so genannten Resource Records (RR) hinterlegt. Die RR werden als ASCII-Datei in den Zonendateien oder in den DNS-Transport-Paketen in komprimierter Form verarbeitet.

Resource Records Format

Im ASCII-Format haben die RRs den folgenden Aufbau im ASCII-Format:

<name> [<ttd>] [<class>] <type> <rdata> <length>

<name> Der Domänenname des Objekts, zu dem der Resource Record gehört (optional)

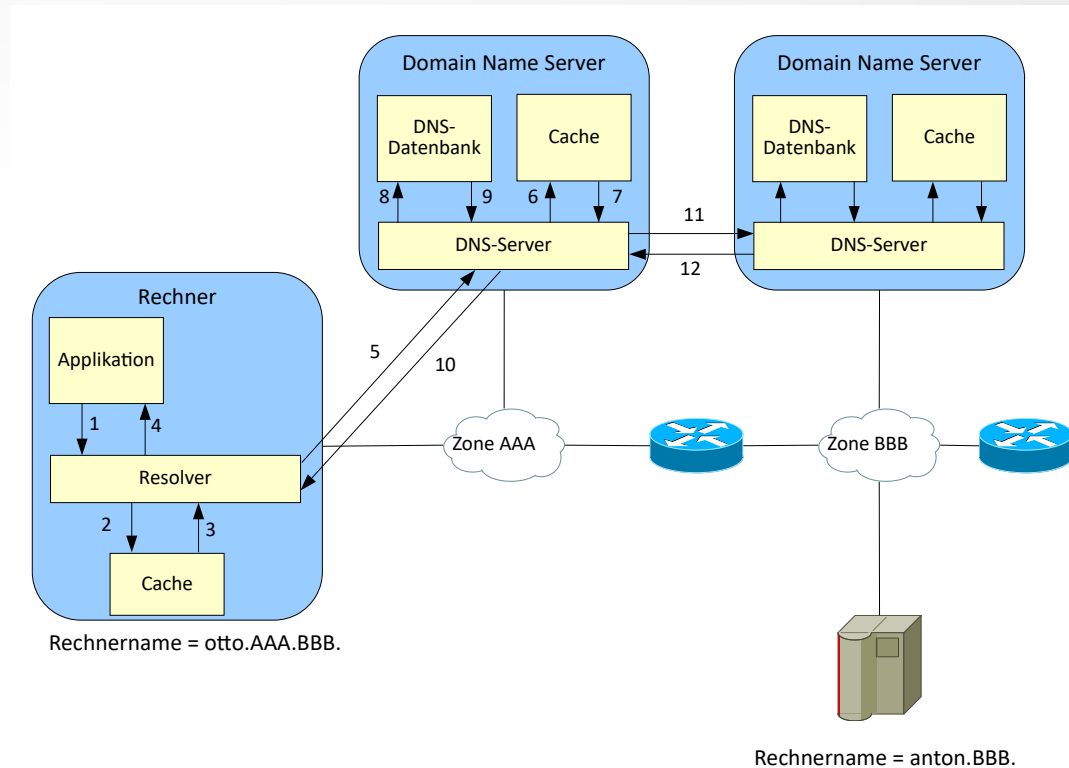
<ttd> **time to live** (in Sekunden). Gültigkeit des Resource Records (optional)

<class> Protokollgruppe, zu der der Resource Record gehört (optional)

<type> beschreibt den Typ des Resource Records

<rdata> (resource data) Daten, die den Resource Record näher beschreiben (zum Beispiel eine IP-Adresse für einen A-RR, oder einen Hostnamen für einen NS-RR)

<length> Länge der folgenden Daten



IPv4

DNS: Resource-Record

Die Typen der Resource-Record sind vielfältig. Hier eine kleine Auswahl.

Typ	Bedeutung
A	IPv4-Adresse eines Hosts
AAAA	IPv6-Adresse eines Hosts
CERT	Resource Record für das Speichern von Zertifikaten (siehe RFC 4398)
CNAME	Kanonischer Name für einen Host (die Domain mit diesem RR ist ein Alias)
DNAME	ähnlich CNAME, aber für komplette Domains, siehe RFC 2672
DNSKEY	enthält einen dem Namen zugeordneten Public-Key – löste bei DNSSEC ab 2004 den Typ KEY ab.
DS	dient der Verkettung DNSSEC-signierter Zonen
MX	Mail Exchange – der für diese Domain zuständige Mailserver
NAPTR	Naming Authority Pointer – Erweiterung des A Resource Record
NSAP	Network Service Access Point
NS	Hostname eines autoritativen Nameservers. Verknüpfungen (Delegationen) der Server untereinander
PTR	Domain Name Pointer (für das Reverse Mapping, um IP-Adressen Namen zuzuweisen)
RRSIG	enthält eine digitale Unterschrift (wird seit 2004 von DNSSEC (=DNS Security) verwendet und ersetzt SIG)
SOA	Start of Authority
SPF	Sender Policy Framework
SRV	angebotener Dienst (Service)
SSHFP	SSH Fingerprint, zum Veröffentlichen der Fingerprints von SSH-Schlüsseln, siehe RFC 4255
TXT	freidefinierbarer Text, wird u. a. auch für Sender Policy Framework (SPF) verwendet. Wird auch oft genutzt für Google-Site Verification

IPv4

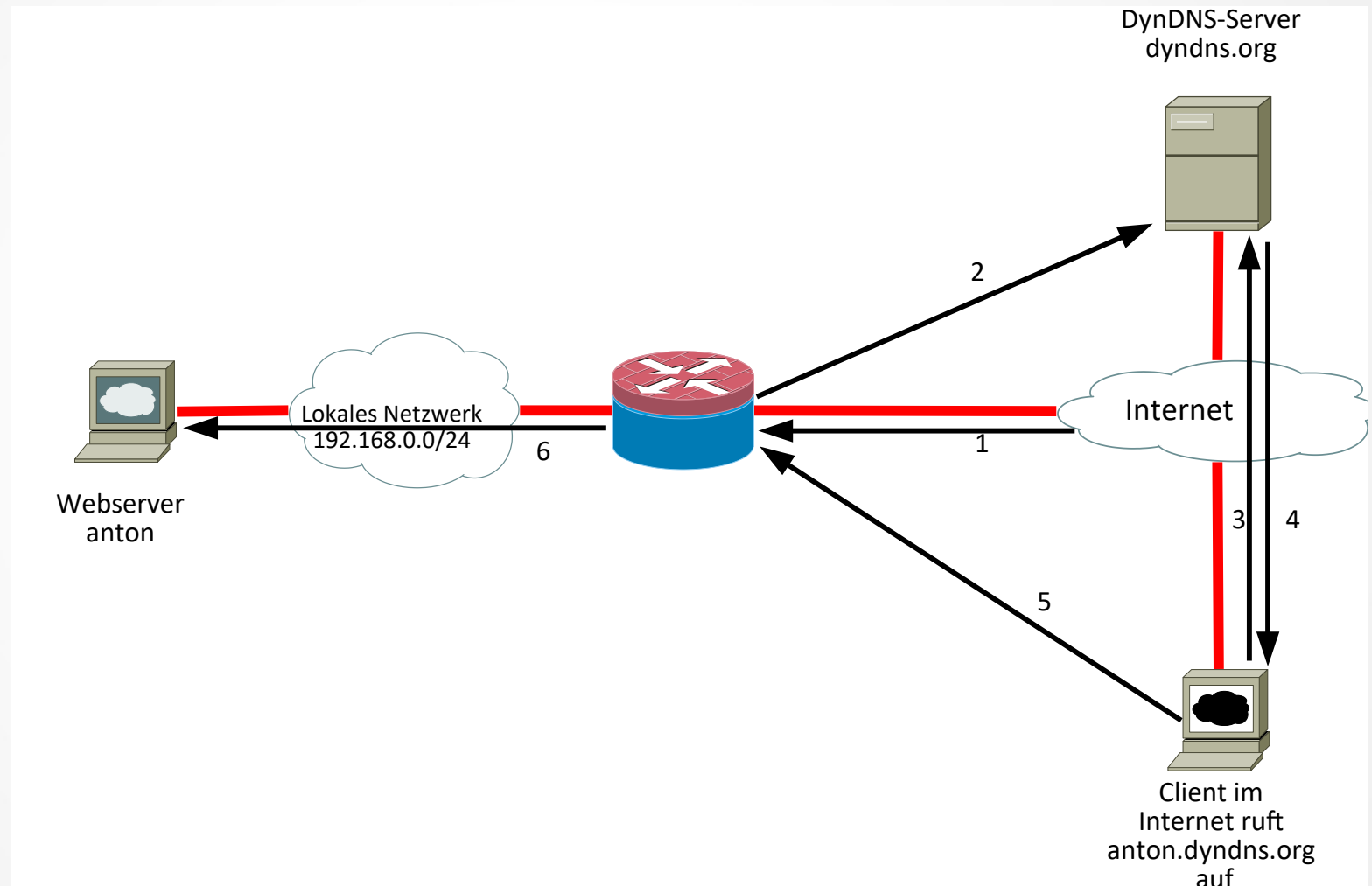
DNS: SOA-Record

Der Start of Authority (SOA) -Resource-Record ist ein wichtiger Bestandteil einer Zonendatei. Er enthält Angaben zur Verwaltung der Zone und zum Zonentransfer. Er ist spezifiziert im RFC1035.

Typ	Bedeutung
Name	Zonen-Name
IN	Zonenklasse Internet
Primary	Zonenmaster. Bestimmt an wen dynamische Updates gesendet werden.
Mail-Address	Mailadresse des Administrators. Datei wird das @-Zeichen durch „.“ ersetzt Punkte vor dem @-Zeichen werden durch „\.“ ersetzt. Damit wird aus otto.huber@abc.com otto\.huber.abc.com
Seriennummer	Wird bei jeder Änderung inkrementiert. Hat vorzugsweise das Format JJJJMMTTVV und ist ein Hinweis auf die letzte Änderungen
Refresh	Sekundenabstand in dem sekundäre Nameserver beim primären Nameserver die Seriennummer abfragen um Änderungen zu erkennen. RIPE-NCC-Empfehlung 86400 = 24 Stunden
Retry	Nach ausbleibender Antwort soll nach x Sekunden beim Primary Nameserver nachgefragt werden. Muss < als Refresh sein. RIPE-NCC-Empfehlung 7200 = 2 Stunden
Expire	Nach dieser Zeit in Sekunden soll bei ausbleibender Antwort vom Primary Nameserver nicht mehr auf Zonenabfragen geantwortet werden. Muss größer sein als Σ von Refresh + Retry
TTL	Time to Live für negatives Caching. RIPE-NCC-Empfehlung 172800 = 2 Tage

IPv4 DynDNS

Bei DDNS gibt es die Möglichkeit die Einträge des Name Servers dynamisch zu ändern oder zu ergänzen. Bei einer Serveranbindung über xDSL ergibt sich durch die dynamischen IP-Adresszuweisungen das Problem, dass alte DNS-Einträge auf dem Name Server ins Leere zeigen und bei der Namensauflösung die falschen Adressen zurück liefern.

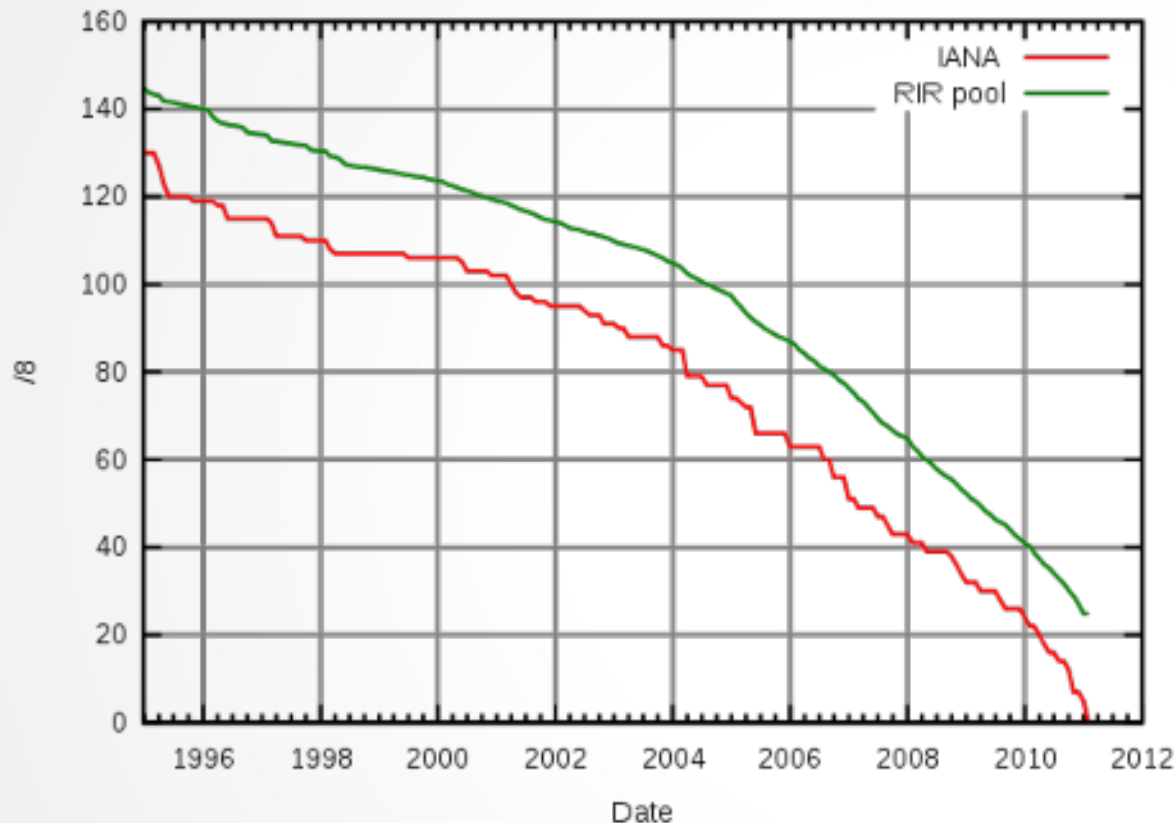


IPv6 Einführung

$2^{32} = 4.294.967.296$ IPv4-Adressen

$2^{128} = 340.282.366.920.948.463.374.607.431.768.21.456$ IPv6-Adressen

Free /8



Seit 2009 gibt es beim RIPE NCC unter dem Link <http://www.ripe.net/ripe/docs/ripe-373.html> die Möglichkeit providerunabhängige IPv6-Adressblöcke (IPv6 End User Site Assignment Request Form) zu beantragen.

IPv6 Terminologie

Das **Internet4** ist der über IPv4 erreichbare Teil des Internets und das **Internet6** ist der über IPv6 erreichbare Teil.

Ein **Node** ist ein Gerät, das über ein oder mehrere **Interfaces**, an einem oder mehreren Netzwerken angeschlossen ist.

Ein **Router** ist ein spezieller Node.

Er besitzt Routing-Eigenschaften und kann damit den Netzwerk-Verkehr über Netzwerk-Grenzen hinweg ermöglichen.

Ein **Host** ist ein Node ohne Routing-Eigenschaften.

Ein **Interface**, oder auch **Link**, ist die Verbindung zum Netzwerk.

Alle weiteren an diesen Link angeschlossenen Nodes sind **on-link** und damit Nachbarn (**Neighbours**).

Nodes, die nicht direkt erreicht werden können (etwa nur über eine Router), sind **off-link**.

IPv6 Header

Version (4Bit)	Traffic Class (8Bit)	Flow-Label (20Bit)		
Payload (16Bit)		Next Header (8Bit)	Hop Limit (8Bit)	
Source Address (128Bit)				
Destination Address (128Bit)				
Data				

Name	Länge in Bit	Bedeutung
Version	4	Versionskennung. Hat immer den Wert 6
Traffic Class	8	Die Traffic Class entspricht dem TOS (Type of Service unter IP-V4). Werte von 0 bis 7 werden für den lastgesteuerten Datenverkehr verwendet. Werte von 8 bis 15 sollen für Echtzeit Datenverkehr verwendet werden
Flow Label	20	Dient zur Kennzeichnung eines „Flows“
Payload Length	16	Gibt die Datenmenge in Bytes an, die den Header folgen. Hier ist eine Datenmenge bis 64 kByte möglich. Die Jumbo Payload-Option erlaubt Datagramme bis 4 GByte
Next Header	8	Hier wird die nächsthöhere Protokollschicht angegeben.
Hop Limit	8	Der Inhalt dieses Feldes wird bei jeder Übertragung durch Router um 1 decreментиert. Wird der Wert 0 erreicht, dann wird das Paket verworfen.
Source-Adresse	128	Quell-Adresse. Der Adress-Aufbau folgt.
Destination-Adresse	128	Ziel-Adresse. Der Adress-Aufbau folgt.
Data		Zu übertragene Daten, die dem Header folgen

IPv6

Unterschiede im Header im Vergleich zu IPv4

Fragmentation/Reassembly

Eine Fragmentierung gibt es bei IPv6 nicht.

Zu große Pakete werden von den Routern verworfen und müssen deshalb bereits beim Sender richtig dimensioniert werden.

Dazu sendet der Router ein ICMPv6-Paket an den Absender und teilt ihm mit, dass die Paketgröße kleiner zu wählen ist.

Die minimale MTU-Size wird von 576 Bytes bei IPv4 auf 1280 bei IPv6 angehoben.

Die Ermittlung der maximal möglichen MTU-Size, also der MTU-Size entlang des gesamten Weges vom Sender zum Ziel, dem so genannten MTU-Path, gewinnt hiermit an Bedeutung.

Checksumme

In der unterlagerten Schicht wurde bereits eine Checksumme bearbeitet.

Dies wäre eine redundante Bearbeitung. Die Checksummen-Bearbeitung müsste jedes mal, wenn der Next-Hop-Wert dekrementiert wird, ebenfalls durchlaufen werden.

Dies reduziert die Latenzzeiten (Durchlaufzeit vom Empfang bis zum weiter senden) in den Routern.

Optionen

Optionen werden durch einen Extension-Header möglich der im Next Header Feld eingetragen wird.

IPv6 Optionen

Optionen werden durch einen Extension-Header möglich, der im Next Header Feld eingetragen wird.

Name	Typ	Größe	Beschreibung	RFCs
Hop-By-Hop Option	0	variabel	Enthält Optionen, die von allen IPv6-Geräten, die das Paket durchläuft beachtet werden müssen. Wird für Jumbograms verwendet.	2460 2675
Routing	43	variabel	Durch diesen Header kann der Weg des Paketes durch das Netz beeinflusst werden. Anwendungsfall Mobile IPv6.	2460 3775 5095
Fragment	44	64 Bit	Parameter für eine Fragmentierung	2460
Authentication Header (AH)	51	variabel	Enthält Daten zur Sicherstellung der Vertraulichkeit des Paketes	4302
Encapsulation Security Payload (ESP)	50	variabel	Dient zur Verschlüsselung des Paketes	4302
Destination Options	60	variabel	Enthält Optionen die vom Zielrechner des Paketes beachtet werden müssen.	2460
No Next Header	59	leer	Platzhalter für den letzten Extension-Header	2460

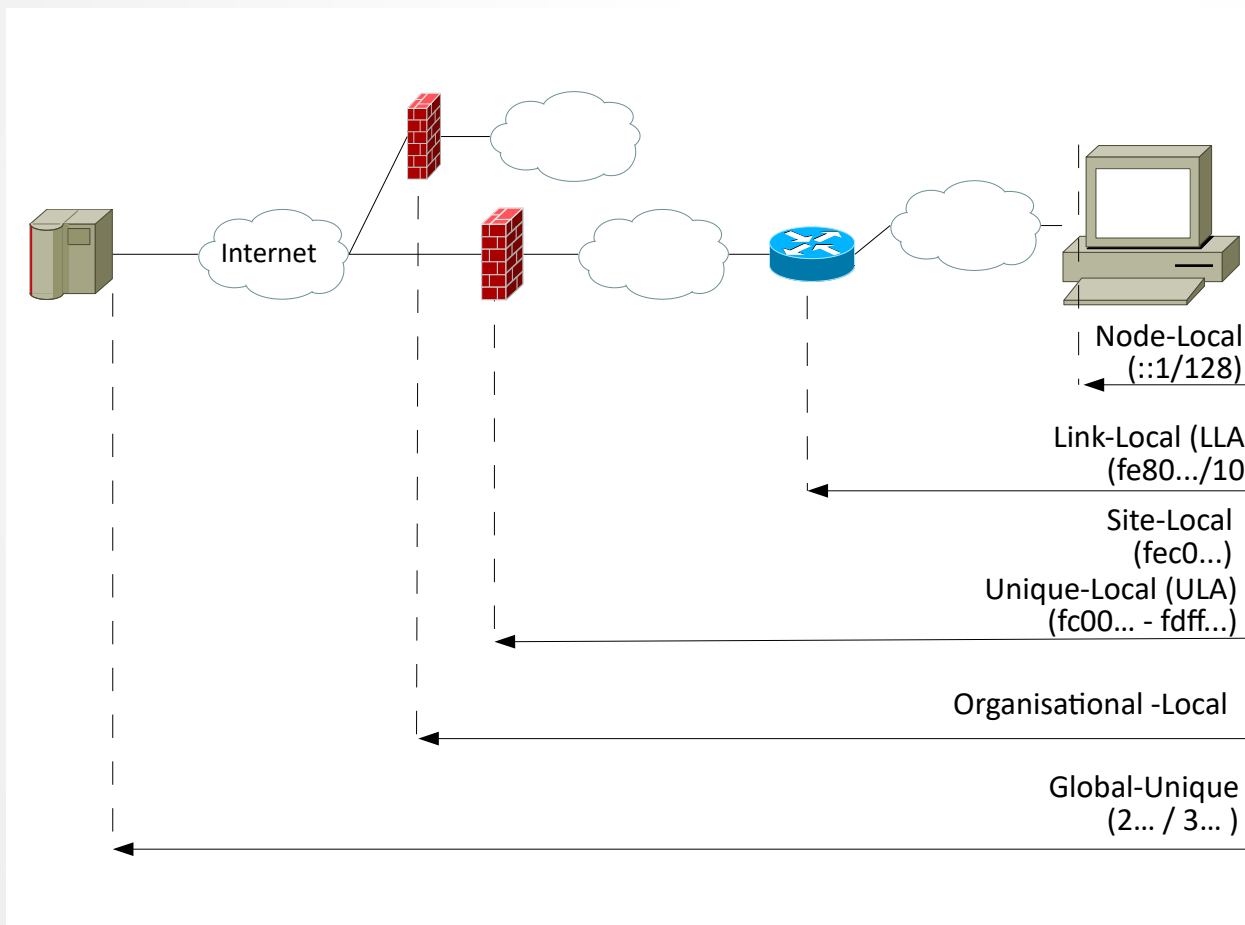
IPv6 Scope

Scope

Im Unterschied zu IPv4 haben IPv6-Nodes mehrere IP-Adressen.

Das sind sowohl Unicast als auch Multicast-Adressen.

Jede dieser Adressen hat einen Scope, um zu beschreiben, in welchen Teilnetzen oder Netzbereichen die Adresse ihren Gültigkeitsbereich und damit auch ihre Reichweite, hat. Dieser Scope kann die folgenden folgende Bereiche festlegen:



Der Scope kann die folgenden folgende Bereiche festlegen:

- Node Local Scope
- Link Local Scope
- Site Local Scope
- Unique Local Scope
- Unique Globally Scope

IPv6

Aufbau der Adresse

Der wichtigste und gebräuchlichste Adress-Aufbau ist der in RFC 3587 beschriebene globale Unicast-Adresse, der eine Adresse in einer allgemeinen Form beschreibt.

64 - n Bits	n Bits	64 Bits
Global Routing Präfix	Subnetz-ID	Interface ID

Der Global Routing Präfix entspricht dem Netzwerk-Teil einer IPv4-Adresse und legt ein international eindeutig gültiges, an ein weltweites Internet anschließbares Netzwerk fest.

Die Subnetz-ID bestimmt die Unterteilung in interne Sub-Netze, die für das öffentliche Internet ohne Belang sind.

In der Praxis hat sich die Real-World-Struktur durchgesetzt dabei ist der Global Routing Präfix auf 48 Bit festgelegt und die Subnetz-ID auf 16 Bit. Die Interface-ID hat 64 Bits.

48 Bits	16 Bits	64 Bits
Global Routing Präfix	Subnetz-ID	Interface ID

IPv6

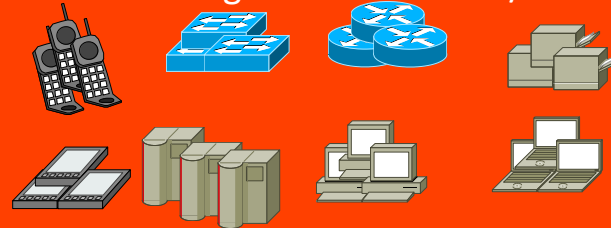
Aufteilung der Adressen

Gesamter IPv6-Adressraum 2^{128} Adressen

Einem Provider zugeteilter Adressraum /32 (oder /29)

Einer Site oder einer Firma zugeteilter Adressraum /48

Vom Admin zugeteiltes Subnetz /64



$2^{64} = 1,84467441\text{E}+19$ Interface-IDs

Einer Privatperson zugeteilter Adressraum /56

Von Priv. aufgeteiltes Subnetz /64



2^{64} Interface-IDs

Einer Privatperson zugeteilter Adressraum /64



2^{64} Interface-IDs

$2^{32} *$

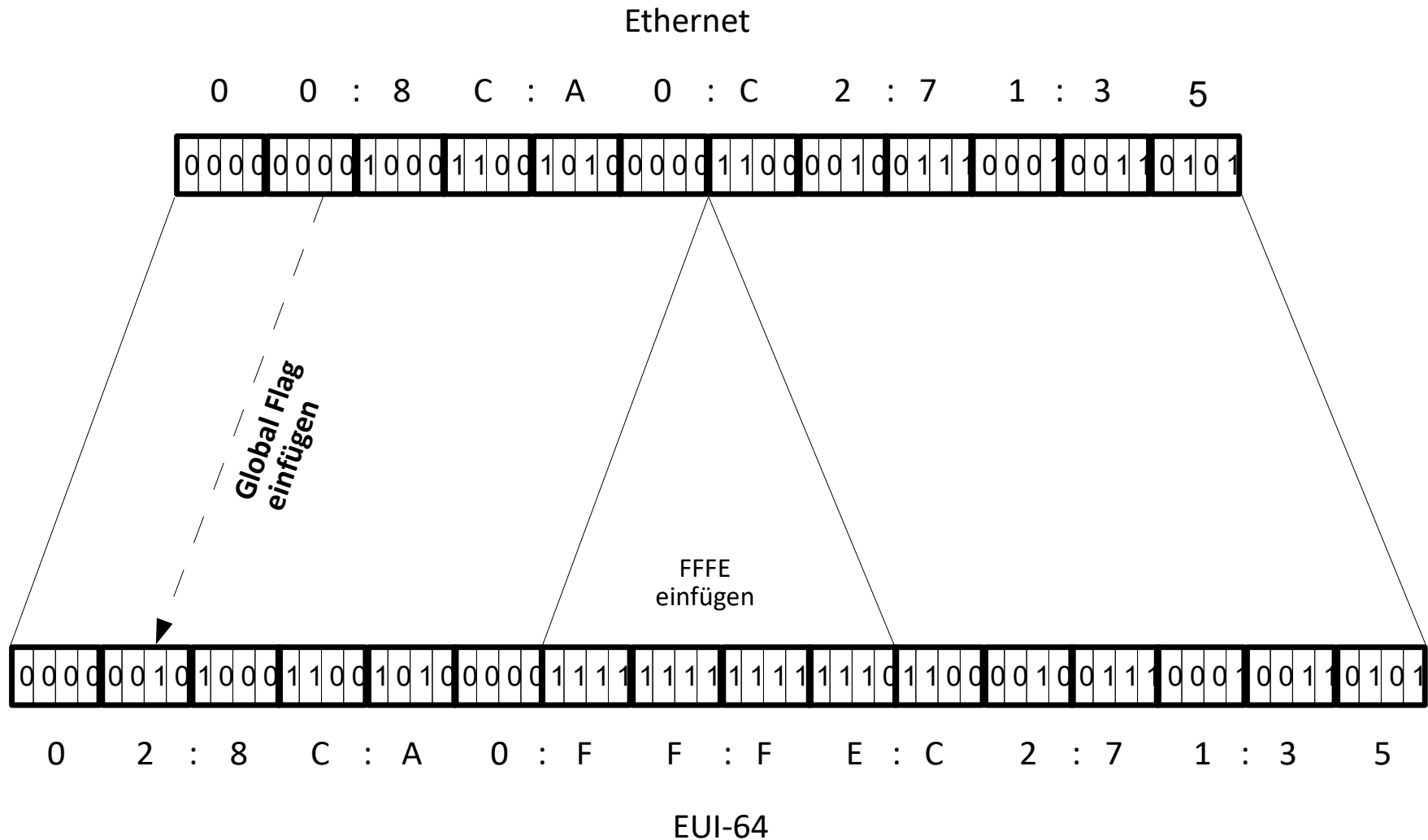
$2^{16} *$
oder
 $2^{19} *$

$2^{16} *$

$2^8 *$

IPv6

Aufbau der EUI-64-MAC-Adresse



IPv6

Unterschiede bei den IP-Adressen

Es gibt keine Broadcast-Adressen mehr!

Die Funktionalität der IPv6-Broadcast-Adressen wurden von der IPv6-Multicast-Adresse Link-Local-All-Nodes-Multicast-Address ff02::1 übernommen.

In IPv6 sind „All-0“ = „**All Zeros**“ und „All-1“ = „**All Ones**“ zunächst **zulässige Werte für Adressen**.
Die vollständige „All-0“ und „All-1“ über alle Felder sind nach wie vor ungültig!

Speziell Präfixe (also die vorderen Teile einer Adresse) können Felder mit Nullen enthalten.
Wichtig für den Beginn der Datenkommunikation ist die Interface ID innerhalb der IPv6-Adresse.
Sie wird aus der MAC-Adresse gebildet.
Alle anderen vorangestellten Teile lassen sich später ermitteln.

IPv6-Adressen werden den Schnittstellen (Interfaces) zugewiesen. Nicht den Knoten (Nodes)!

Da jede Schnittstelle zu einem Knoten gehört, kann jede Schnittstellen-Unicast-Adresse dazu verwendet werden den Knoten zu bezeichnen.

Alle Schnittstellen müssen mindestens eine „Link-Local-Unicast-Adresse“ haben.

Damit kann eine Schnittstelle mehrere Adressen von jedem Typ (Uni-, Any- oder Multicast) oder Scope haben.
Unicast Adressen mit mehr als der Link-Scope-Adresse werden als Ziel- oder Quell-Adresse nicht benötigt.
Damit kann innerhalb eines Netzwerks kommuniziert werden.
Dies ist vor allem für Punkt-zu-Punkt-Verbindungen angenehm.

Ausnahme:

Eine Unicast-Adresse oder reine Menge von Unicast-Adressen können zu mehreren Schnittstellen zugewiesen werden, wenn die Implementierung für alle darüber liegenden Schichten die Schnittstellen als eine einzige Schnittstelle behandelt.

Dies ist nützlich für Loadsharing (deutsch: Last-Teilung) über mehrere physikalische Schnittstellen.

IPv6

Aussehen einer Adresse

Die bevorzugte Form

x:x:x:x:x:x:x

wobei x eine 16Bit-Hexadezimalzahl ist. Buchstaben (a,b,c,d,e,f) werden immer klein geschrieben.

So sieht eine IPv6-Adresse beispielsweise so aus.

fedc:ba98:7654:3210:fedc:ba98:7654:3210

oder

1080:0:0:0:8:800:200c:417a

Führende Nullen innerhalb eines 16-Bit-Feldes können weggelassen werden.

Darstellung langer 0-Ketten

Bei langen 0-Ketten ist es möglich, eine beliebig lange Folge von Nullen mit „::“ zu beschreiben

Diese Möglichkeit besteht pro Adresse jedoch nur einmal!

Damit sind folgende Adress-Beispiele mit unterschiedlichen Schreibweisen möglich.

Ausgeschriebene Form	Komprimierte Form	Bedeutung
1080:0:0:0:8:800:200C:417a	1080::8:800:200C:417a	Unicast-Adresse
ff01:0:0:0:0:0:0:101	ff01::101	Multicast-Adresse
0:0:0:0:0:0:0:1	::1	Loopback-Adresse
0:0:0:0:0:0:0:0	::	Unspezifizierte Adresse

IPv6

Aussehen einer IPv4-Adresse

Unter IPv6 genutzte IPv4 -Adressen

x:x:x:x:x.d.d.d.d

x entspricht einem 16-Bit-Hexadezimalwert (0 – FFFF) auf der höherwertigen Seite der Adresse.

d entspricht einem 8-Bit-Dezimalwert (0 – 255) auf der niederwertigen Seite der Adresse.

Diese Schreibweise dient nur der internen Darstellung und wird nie als Quell- oder Zieladresse versendet!

0:0:0:0:0:0:d.d.d.d

Beispiel:

::abba:815 = 0:0:0:0:0:0:171.186.8.21 = ::171.186.8.21

IPv4-mapped IPv6-Adresse

Hierbei sind die ersten 80 Bits auf 0 gesetzt.

Danach werden die nächsten 16 Bits auf 1 gesetzt.

Beispiel:

Ausgeschriebene Form

0:0:0:0:0:ffff.129.144.52.38

Komprimierte Form

::ffff.129.144.52.38

IPv6

Adress-Präfix

Bedeutung

Mit einem Präfix oder Format-Präfix werden Adressen näher spezifiziert.
So können Klassen oder Typen näher beschrieben werden.

Adress-Präfix-Schreibweise

Die Schreibweise entspricht der aus IPv4 bekannten CIDR-Schreibweise mit dem Schrägstrich.
Dargestellt wird die Adresse sowie eine Längenangabe getrennt mit dem Schrägstrich:

<IPv6-Adresse> / <Präfixlänge in Bits>

IPv6

Adress-Präfix

Bedeutung	Präfix in Binärschreibweise	Präfix in Hexadezimal
Unspezifizierte Adresse (RFC4291)	0000 0000	::/128
Loopback-Adresse (Entspricht 127.0.0.1 in IPv4) (RFC4291)	0000 0001	::1/128
Reserviert oder spezifisch	0000 0000	0000::/8
Reserviert für NASP Belegung	0000 0010	0200::/8
Nicht zugewiesen (ehemals für IPX reserviert)	0000 0100	0400::/8
Aggregierbare globale Unicast-Adresse	0010	2000::/3
Teredo (RFC 4380)	0010 0000 0000 0001 0000 0000 0000 0000	2001::/32
Benchmarking	0010 0000 0000 0001 0000 0000 0000 0010 0000 0000 0000 0000	2001:2::/48
ORCHID (RFC4843)	0010 0000 0000 0001 0000 0000 0001 0000	2001:10::/28
Documentation (RFC 3849)	0010 0000 0000 0001 1101 1011 0001 0000	2001:db8/32
6to4-Adresse	0010 0000 0000 0010	2002::/16
Unique Local (Entspricht den RFC 1918-Adressen in IPv4) (RFC 4193)	1111 1100	fc00::/7
Link-Local Unicast-Adresse entspricht 169.254.0.0 unter IPv4 (APIPA) (RFC4291)	1111 1110 1000 0000	fe80::/10
Site-Local Unicast-Adresse	1111 1110 1100 0000	fec0::/10
Multicast-Adresse entspricht 224.0.0.0/4 bei IPv4 (RFC4291)	1111 1111 0000 0000	ff00::/8
IPv4-Mapped-Adresse (RFC4038)	0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 1111 1111 1111 1111 0000 0000	::ffff:0:0/96
IPv4 compatible Adresse (RFC 4291)	0000 000	:/96

IPv6

Multicast-Adressen

Aufbau von Multicast-Adressen

Laut RFC4291 bauen sich Multicast-Adressen unter IPv6 folgendermaßen auf:

ff0s:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX

Dabei steht s für den Scope:

Wert (s)	Scope	Bedeutung
1	Node Local	Multicast Loopback
2	Link Local	Nicht routebar. Nur am betreffenden Link gültig
4	Administration Local	Administrativ zusammenhängende Netzwerke innerhalb einer Site
5	Site Local	Alle Netzwerke eine Site
8	Organisational Local	Alle Netzwerke einer Organisation
e	Global	Global Routing fähig

Ausschnitt:

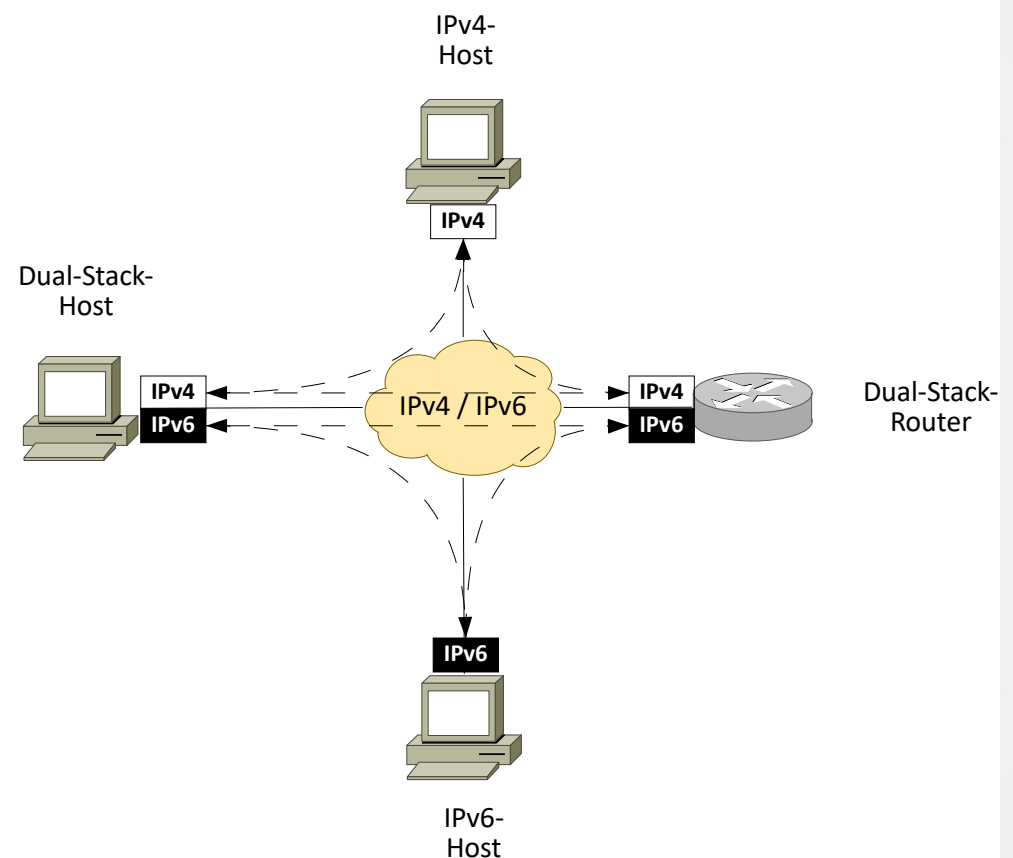
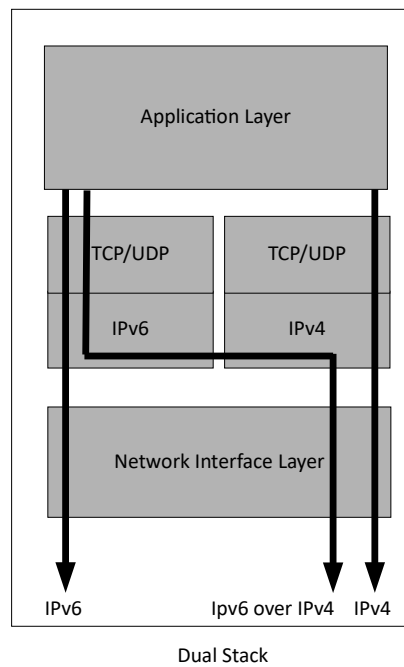
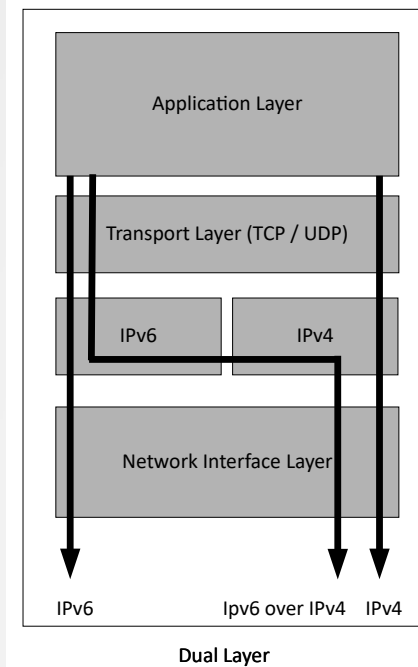
Wert (X)	Bedeutung	Gültig in Scope			
		1 (Node Local)	2(Link Local)	5(Site Local)	X(All Scopes)
::1	All Nodes	X	X		
::2	All Routers	X	X	X	
::4	DVMRP-Routers		X		
::5	OSPFGRP		X		
::6	OSPFGRP Designated Routers		X		
::7	ST Routers		X		
::8	ST Hosts		X		
::9	RIP Routers		X		
::A	EIGRP Routers		X		

IPv6

Weitere Protokolle im Umfeld von IPv6

Protokoll	Beschreibung
ICMPv6	Internet Control Message Protocol RFC2463. Diesem Protokoll kommt eine zentrale Bedeutung zu. Es darf von Firewalls nicht mehr geblockt werden wie bei IPv4.
DNSv6	Domain Name Service RFC3596
NDP	Neighbour Discovery Protocol. Damit wird das ARP-Protokoll abgelöst.
DHCPv6	Dynamic Host Configuration Protocol RFC3315
RIPng for IPv6	Routing Information Protocol RFC2080
OSPF for IPv6	Open Shortest Path First RFC2740

Übergang von IPv4 zu IPv6



ICMPv6

ICMPv6 wurde als Ergänzung für IPv6 entwickelt.
Ihm kommt mehr Bedeutung und Funktionalität als bei der IPv4-Version zu.
So wurden die Protokolle ARP und RARP in ICMPv6 integriert.
Deshalb dürfen ICMPv6-Pakete nicht mehr grundsätzlich
von Firewalls geblockt werden.

Folgende Funktionen werden behandelt:

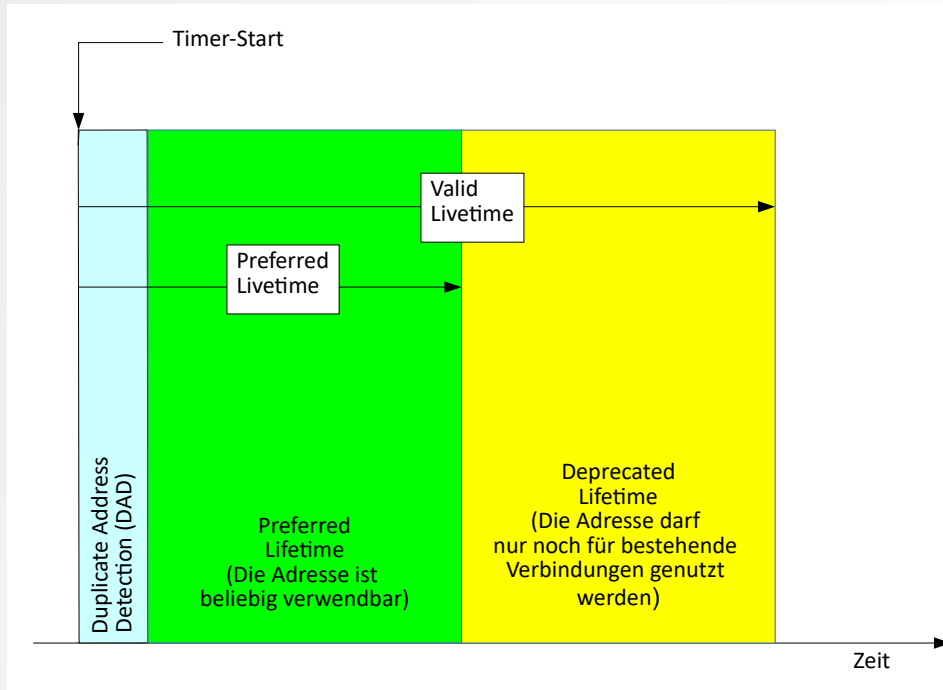
- Fehlermeldungen
- Informationsmeldungen

Typ-Feld-Wert	Fehlermeldung	Code-Feld-Wert
1	Destination unreachable	0 = No Route to Destination 1 = Communication administratively prohibited 2 = Not Assigned 3 = Address unreachable 4 = Port unreachable
2	Packet too big	0
3	Time Exceeded	0 = Hop-Limit exceeds 1 = Fragment-Reassembly-Time exceeded
4	Parameter-Problem	0 = Fehlerhaftes-Header-Feld 1 = Unbekannter Next-Header 2 = Unbekannte IPv6-Option

Typ-Feld-Wert	Information
128	Echo Request
129	Echo Reply
130	Multicast Listener Query
131	Version 1 Multicast Listener Report
132	Multicast Listener done
133	Router Solicitation Message
134	Router Advertisement Message
135	Neighbour Solicitation Message
136	Neighbour Advertisement Message
137	Redirect Message
138	Router Renumbering
139	ICMP Node Information Query
140	ICMP Node Information Response
141	Inverse Neighbour Discovery Solicitation Message
142	Inverse Neighbour Discovery Advertisement Message
143	Version 2 Multicast Listener Report
144	Home Agent Address Discovery Request Message

.....

DHCPv6



Über RAs erzeugte IP-Adressen haben einen Valid-Lifetime. Das entspricht der Lease-Time von mit DHCP erzeugten IP-Adressen.

Die Valid-Lifetime ist die gesamte Gültigkeitsdauer von der Erzeugung bis zum Löschen.

Innerhalb dieses Zeitraums ist eine Adresse zuerst preferred danach deprecated.

Während der Preferred-Lifetime verwendet der Rechner diese IP-Adresse. Danach (während der Deprecated-Lifetime) wird die IP-Adresse nur noch für bestehende Verbindungen genutzt.

Nach Ablauf der Valid-Lifetime wird die IP-Adresse gelöscht.

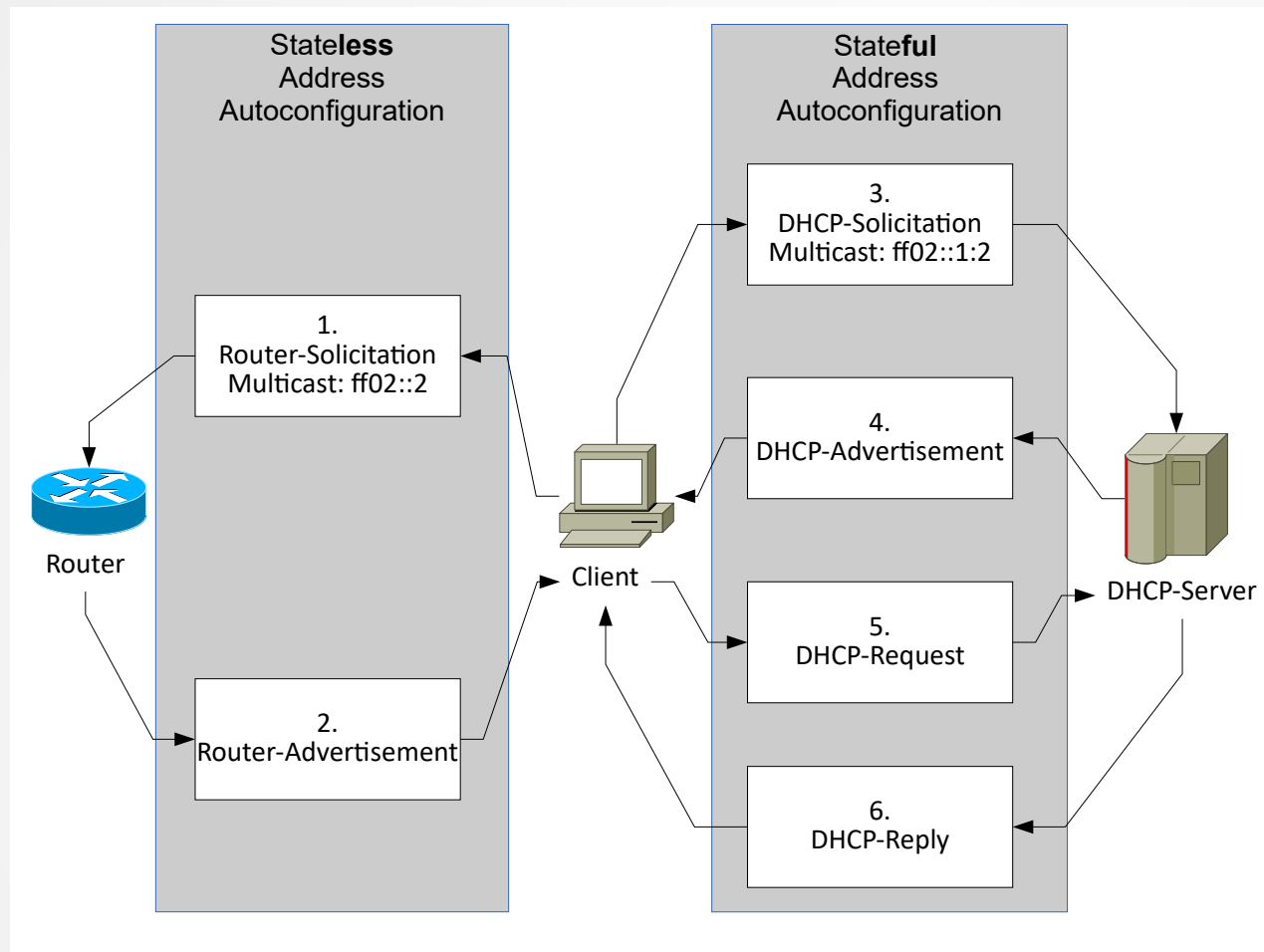
Mit der Absender-Adresse des Routers wird gleichzeitig auch das Default Gateway festgelegt.

Unterstützen Router und Client die RDNSS-Option (Recursive DNS Server) wie im RFC 6106 beschrieben, kann die Adresse des DNS-Servers auch über die RAs mitgeteilt werden.

Damit ist die Autokonfiguration mittels der Router-Advertisements (RA) abgeschlossen. Da die IP-Adressen der Clients nirgendwo gespeichert / verwaltet werden, heißt dieses Verfahren Stateless Address Autoconfiguration (SLAAC).

Die Router senden in regelmäßigen Zeitabständen die RAs an die Link-Local-All-Nodes-Multicast-Adresse (ff02::1), damit die Clients die Konfiguration auf dem neuesten Stand halten können.

DHCPv6



Behandelte Themen

- Protokollfunktionen
- IPv4 (Protokoll / ARP / RARP / NAT / DHCP / ICMP / DNS)
- IPv6 (Protokoll / Unterschiede zu v4 / Übergänge von v4 zu v6 / ICMPv6 / DHCPv6)

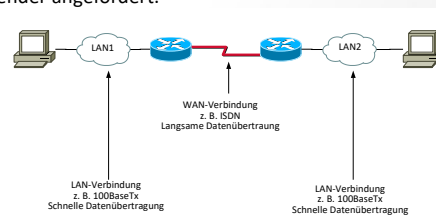
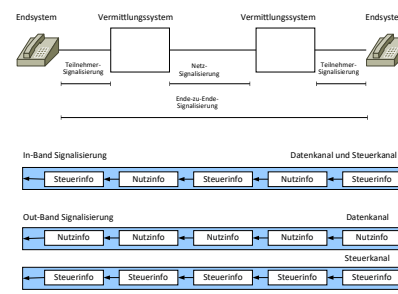
Netztechnik Teil-9

Inhalt

- Protokollfunktionen
- IPv4 (Protokoll / ARP / RARP / NAT / DHCP / ICMP / DNS)
- IPv6 (Protokoll / Unterschiede zu v4 / Übergänge von v4 zu v6 / ICMPv6 / DHCPv6)

Protokollfunktionen

- Vermittlung
 - ⚡ Leitungsvermittlung
 - ⚡ Speichervermittlung
 - ⚡ Paketvermittlung
- Signalisierung
 - ⚡ In-Band-Signalisierung
 - ⚡ Out-of-Band-Signalisierung
- Multiplexing
 - ⚡ Raummultiplex
 - ⚡ Zeitmultiplex
 - ⚡ Frequenzmultiplex
 - ⚡ Wellenlängenmultiplex
 - ⚡ Code-Multiplex
- Flusskontrolle
- Fehlerkorrekturverfahren (ECC = Error Correction Code)
 - ⚡ Vorwärtsfehlerkorrektur (FEC = forward Error Correction)
Daten werden mit zusätzlichen Bits versorgt um nach der Übertragung Fehler erkennen und beheben zu können.
 - ⚡ Rückwärtsfehlerkorrektur (BEC Backward Error Correction)
Z. B. durch Prüfsummen können nur Fehler erkannt, jedoch nicht korrigiert werden. Deshalb werden die Daten nochmals beim Sender angefordert.



Stand: 27.11.2022

Netztechnik

Seite 3/8

Die **Vermittlung** dient der Wegefindung.
Je nach Vorgehensweise ist der Aufwand unterschiedlich.

Die **Signalisierung** dient dem Verbindungs-Aufbau sowie dem -Abbau
Und kann im Datenkanal, oder in einem getrennten Signalisierungs-Kanal
Erfolgen.

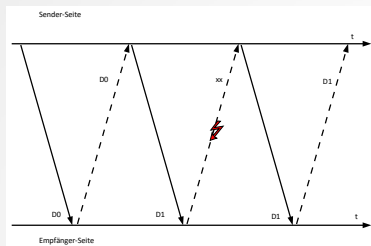
Da selten nur ein Kommunikationspartner einen Kanal nutzt sind
Multiplexing-Verfahren erforderlich.
Ablauf: Multiplexing → Datenübertragung → Demultiplexing

Flusskontrolle ist da erforderlich wo Stausituationen auftreten können.
Z. B. beim Übergang von unterschiedlichen Medien.
Dabei kann dem Sender signalisiert werden die Datenmenge zu drosseln
oder ganz zu warten, bis sich die Situation wieder entspannt hat.

FEC ist da anzuwenden, wo ein Rückwärtskanal fehlt, oder die Kosten zu
groß sind. Das gilt für einige Unicasts jedoch besonders für Multicasts
und Broadcasts.

BEC unterbricht den Datenfluss und ist beim Auftreten von wenigen
Fehlern sinnvoll.

Backward Error Correction (Quittungen)

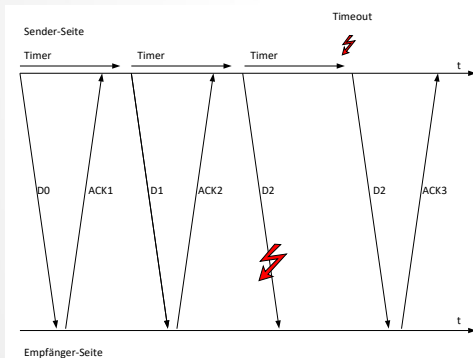


Ohne Quittungen müssten zur Sicherung der Übertragung die Daten wieder zurück übertragen werden.

Durch Einführung von Quittungen (ACK) kann die Datenmenge auf dem Rückweg verringert werden.

Wenn eine Rückmeldung fehlt, muss das bemerkt werden können.

Einführung von Timern, damit die Kommunikation bei kollidierten Rahmen nicht einschläft.



Nach jeder Datenübertragung muss auf die **Quittung** oder einen **Timeout** gewartet werden.

Dieses Verfahren wird **Stop and Wait** genannt und bedeutet immer noch eine schlechte Kanalausnutzung, da nach jedem Datenpaket gewartet werden muss.

Die BER wird mit Quittungen abgehandelt.

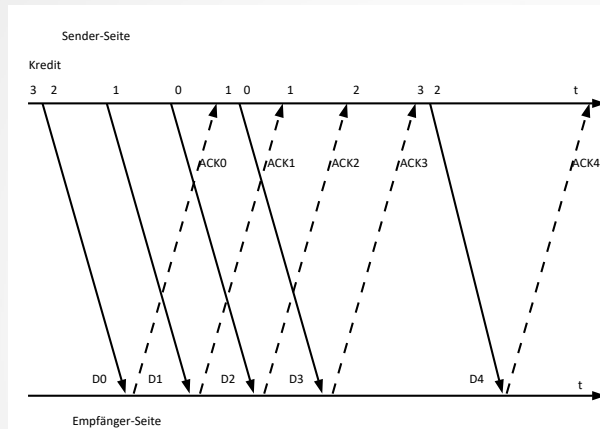
Nach jedem Daten-Frame muss auf eine Quittung gewartet werden. Diese Vorgehensweise wird „**Stop And Wait**“ genannt

Fallen Quittungen oder Daten-Frames aus, kann die Bearbeitung hängen bleiben.

Damit das nicht passiert, ist für jeden Daten-Frame ein Timer zu starten. Läuft der Timer ab bevor die Quittung eintrifft, muss der Daten-Frame wiederholt werden.

Wie in der Folie zu sehen ist, wird durch die Wartezeiten der Kanal nicht gut ausgenutzt.

Backward Error Correction (Windowing)



Abhängig von mehreren Parametern (z. B. der Größe des Eingangspuffers des Empfängers), wird dem Sender zugestanden mehrere Rahmen zu senden, bevor er auf eine Quittung warten muss.

Die Anzahl der Rahmen, die hierbei gesendet werden dürfen, wird Kredit genannt.

Bei jedem gesendeten Rahmen wird der Kredit dekrementiert.

So lange der Kredit > 0 ist darf gesendet werden.

Ist der Kredit bei 0 angekommen, dürfen keine weiteren Rahmen mehr gesendet werden, und es muss gewartet werden.

Trifft dann wieder eine Quittung ein wird der Kredit inkrementiert und es darf wieder gesendet werden.

Um den Kanal besser auszulasten gibt es die Möglichkeit mehrere Datenframes auszusenden, bevor auf eine Quittung gewartet werden muss.

Allerdings geht das nur bei verbindungsorientierten Protokollen, denn es muss beim Verbindungsaufbau erst ausgehandelt werden wie viele Daten-Frames gesendet werden dürfen, bevor auf eine Quittung gewartet werden muss.

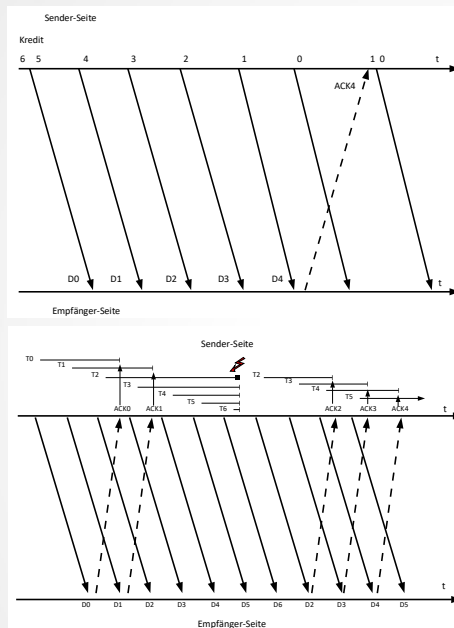
Abhängig von der maximalen Segmentgröße und der Puffergröße des Empfängers kann der Sender einen Kredit-Wert setzen. Je größer der Empfangspuffer des Empfängers ist, desto größer kann der Kredit-Wert auf der Senderseite gesetzt werden.

Bei jedem Senden eines Daten-Frames dekrementiert der Sender seinen Kredit. Ist der Kredit bei 0 angekommen, muss mit dem Senden so lange gewartet werden, bis der Kredit wieder durch eine Quittung inkrementiert wurde.

Schiebepfensterprotokolle gibt es nur bei Full-Duplex-Verbindungen.

Es kann nicht beliebig lange auf Quittungen gewartet werden. Deshalb sind auch hier Timer für jeden Frame erforderlich.

Backward Error Correction (Windowing)



Eine Sammelquittung kann Einzelquittungen ersetzen.

Falls eine Quittung verloren geht, könnte die Kommunikation einschlafen. Deshalb sind zusätzlich Timer erforderlich.

Damit kann bei der fehlenden Quittung mit der Datenübertragung nochmals aufgesetzt werden. (Go Back n)

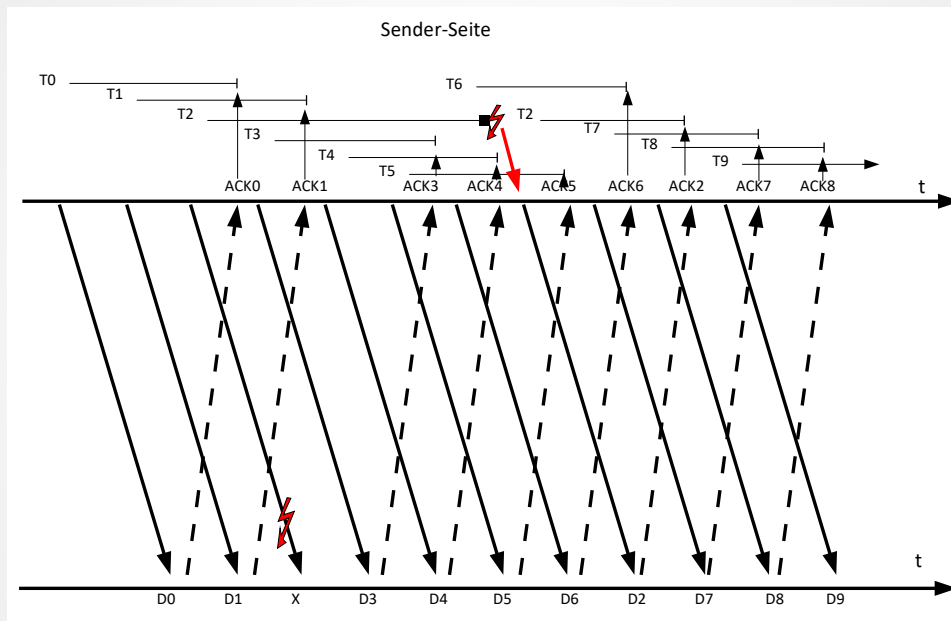
Es ist auch denkbar Sammelquittungen zu verwenden um die Netzlast weiter zu senken.

Da auch hier Daten-Frames oder Quittungen verloren gehen können, sind auch hier Timer zu setzen.

Bei einem Timeout wird ab dem entsprechenden Daten-Frame nochmals mit dem Senden der Daten-Frames aufgesetzt.
Dies wird „**Go Back n**“ genannt.

Diese Vorgehensweise wird bei TCP verwendet. Dabei wird in der Quittung eine Sequenznummer mitgegeben, auf die der Sender seinen Pointer für die Übertragung des nächsten Segments positioniert.

Selective Repeat



Stand: 27.11.2022

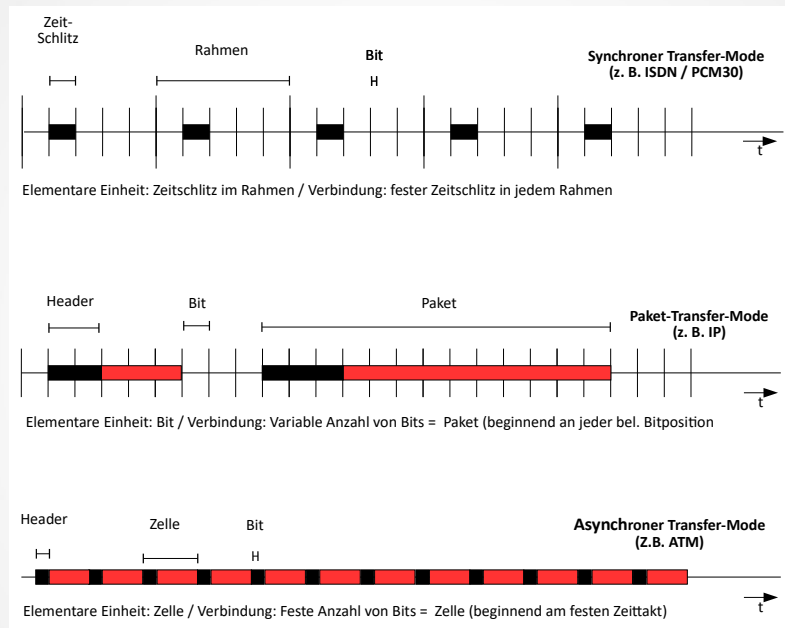
Netztechnik Teil-9

Folie: 7:78

Soll nur der nicht quitierte Daten-Frame wiederholt werden könnte dies mit einem „**Selective Repeat**“ erfolgen.

Das hat allerdings zur Folge, dass der Empfänger eine Verwaltung der Daten-Frame-Reihenfolge hat, um das einzeln wiederholte Daten-Frame richtig in die empfangenen Daten einzusortieren.

Zusammenfassung (Transfermodi Teil-1)



Stand: 27.11.2022

Netztechnik Teil-9

Folie: 8:78

Synchroner Transfermode:

Voraussetzung ist ein TDM (Time Division Multiplex) bei der ein Teilnehmer einen Zeitschlitz zugeordnet bekommt. Die Datenmenge pro Zeitschlitz ist immer gleich.

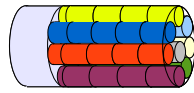
Asynchroner Transfermode:

Hier gibt es keine zeitliche Koordinierung. Es werden Zellen mit immer gleicher Header- und Daten-Größe verwendet. Die Zellgröße ist ein Kompromiss zwischen kleinen Datenmengen für Sprache und großen Datenmengen für Filetransfer.

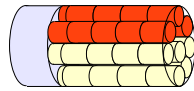
Paket Transfermode:

Je nach Anwendungsfall können unterschiedliche Frame-Größen verwendet werden.

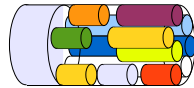
Zusammenfassung (Transfermodi Teil-2)



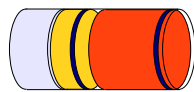
Synchroner Transfermodus (z. B. PCM30)
Leitungsvermittlung
Zeitschlitz



Multirate Circuit Switching (Z. B. ISDN)
Leitungsvermittlung
Zeitschlitz
Kanalbündelung



Fast Circuit Switching
Leitungsvermittlung
Freigabe nach Nutzung / Schneller Wiederaufbau



Packet-Transfer-Mode (Z. B. IP)
Paketvermittlung (Zielinformation im Header)
Unterschiedlich große Pakete



Asynchroner-Transfer-Mode (Z. B. ATM)
Zellvermittlung (Zielinformation im Header)
Alle Zellen haben die gleich Größe

Ein Beispiel für den **synchronen Transfermodus** ist ISDN. Ein Teilnehmer bekommt einen Kanal zugeordnet.
Hier können auch Kanäle wie beim **Multirate Circuit Switching** gebündelt werden.

Für das **Fast Circuit Switching** gibt es keine technische Realisierung

Der **Packet Transfer Mode** wird bei Ethernet verwendet.

Der **Asynchrone Transfer Mode** wird bei ATM verwendet (wie der Name schon sagt)

Protokollübersicht

DARPA-Layer						ISO/OSI-Layer	
4 Prozess/Anwendung	Daten-Übertragung	Electronic-Mail	Terminal-Emulation	Daten-Übertragung	Client-Server	Netzwerk-Verwaltung	7 Anwendung
	File-Transfer-Protocol (FTP) RFC 959	Simple-Mail-Transfer-Protocol (SMTP) RFC 821	TELNET RFC 854	Trivial-File-Transfer-Protocol (TFTP) RFC 783	SUN Network-File-Systems-Prot. (NFS) RFC 1014, 1057, 1094	Simple-Network-Management-Protocol (SNMP) RFC 1157	6 Presentation
							5 Session
3 Host-to-Host	Transmission-Control-Protocol (TCP) RFC 793			User-Datagram-Protocol (UDP) RFC 768			4 Transport
2 Internet	Address-Resolution-Protokoll ARP RFC826 RARP RFC903		Internet-Protokoll (IP) RFC791		Internet-Control-Message-Protokoll (ICMP) RFC792		3 Network
1 Netzwerk-Schnittstelle	Netzwerkschnittstellenkarten Ethernet, StarLAN, Token-Ring, ARCNET RFC 894, 1042, 1201						2 Data-Link
	Übertragungsmedium Twisted Pair, Koax, Fiberglas, drahtlose Medien						1 Physical

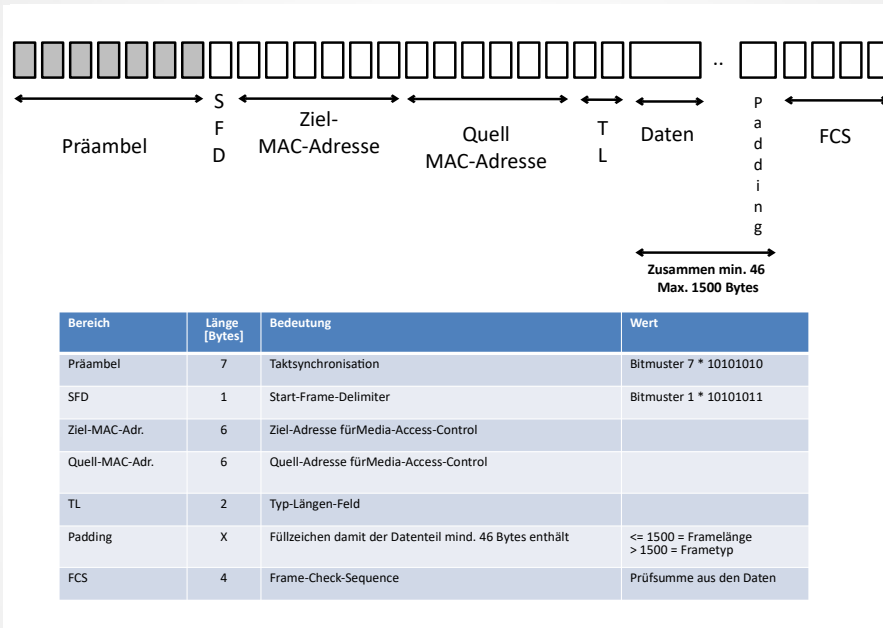
Stand: 27.11.2022

Netztechnik Teil-9

Folie: 10:78

Auf der Folie sind die Ebenen des DARPA-RM und des ISO OSI-RM den einzelnen Protokollen zugeordnet die im Folgenden abgehandelt werden.

Ethernet-Rahmen



Stand: 27.11.2022

Netztechnik Teil-9

Folie: 11:78

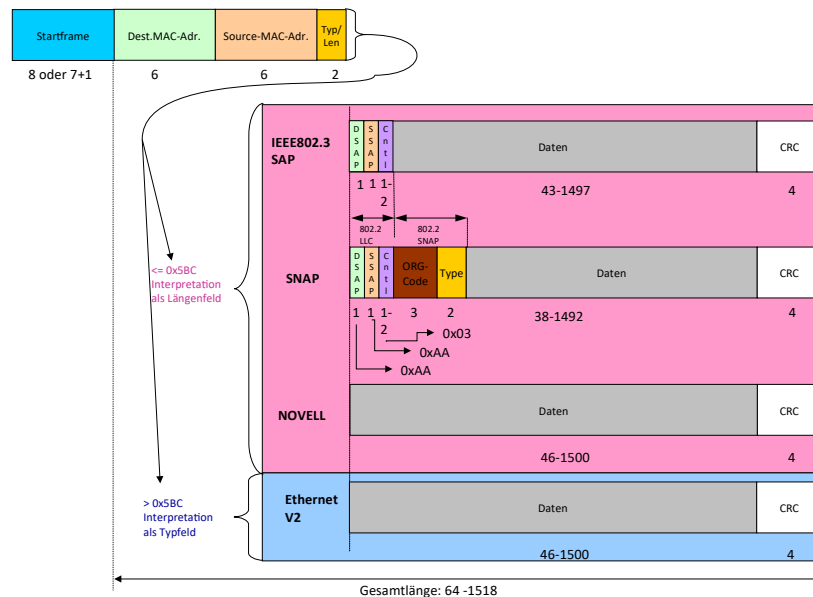
In der Folie sind die Bestandteile der

Ebene 1 (Präambel und Start Frame Delimiter (SFD))
und der

Ebene 2 (MAC-Adressen, Typ-Längen-Feld und Frame Check Sequence(FCS))
dargestellt

Falls durch die Daten die minimale Framegröße nicht erreicht werden kann,
muss der Datenteil mit Nullen im Padding-Teil aufgefüllt werden.

Unterschiedliche Ethernet-Varianten



Stand: 27.11.2022

Netztechnik Teil-9

Folie: 12:78

Nach der Präambel und den MAC-Adressen wird in einem Typ-Längen-Feld unterschieden welcher Fall gilt.

Abhängig von Wert des Typ-Längen-Feldes erfolgt eine Interpretation (Verwendung) als Typ oder als Länge.

Wert ≤ 1500 (Interpretation als Länge)

Novell hat die erste Version eines Ethernet-Frame veröffentlicht. Es sind maximal 1500 Bytes möglich.

IEEE802.3 hat in seiner ersten Version einen weiteren Header nach dem Längelfeld.

Darin gibt es einen Destination Service Access Point (DSAP) und einen Source Service Access Point (SSAP) gefolgt von einem Control-Feld.

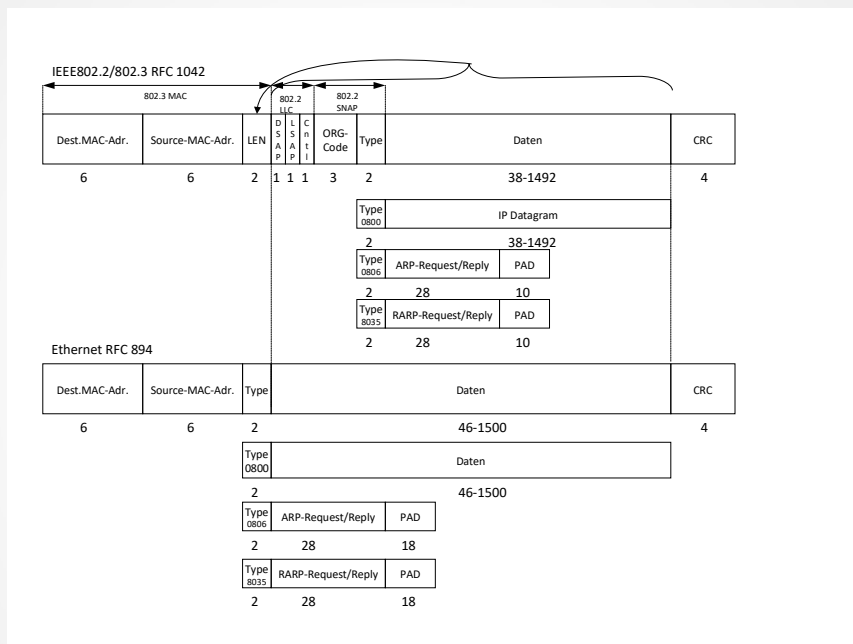
Da diese Definition nicht für alle denkbaren Fälle ausreichte wurde der Header in der **SNAP** Version noch durch einen ORG-Code und ein Typ-Feld erweitert. Das DSAP-, SSAP- und das Control-Feld haben festgelegte Werte.

Wert > 1500 (Interpretation als Typ)

In der zweiten Ethernet-Version (**Ethernet II**) besteht der Datenteil aus maximal 1500 Bytes und das Typ-Längelfeld wird als Typ interpretiert.

Ethernet-II wird mittlerweile überall verwendet.

Auswirkungen der unterschiedlichen Ethernet-Varianten



Stand: 27.11.2022

Netztechnik Teil-9

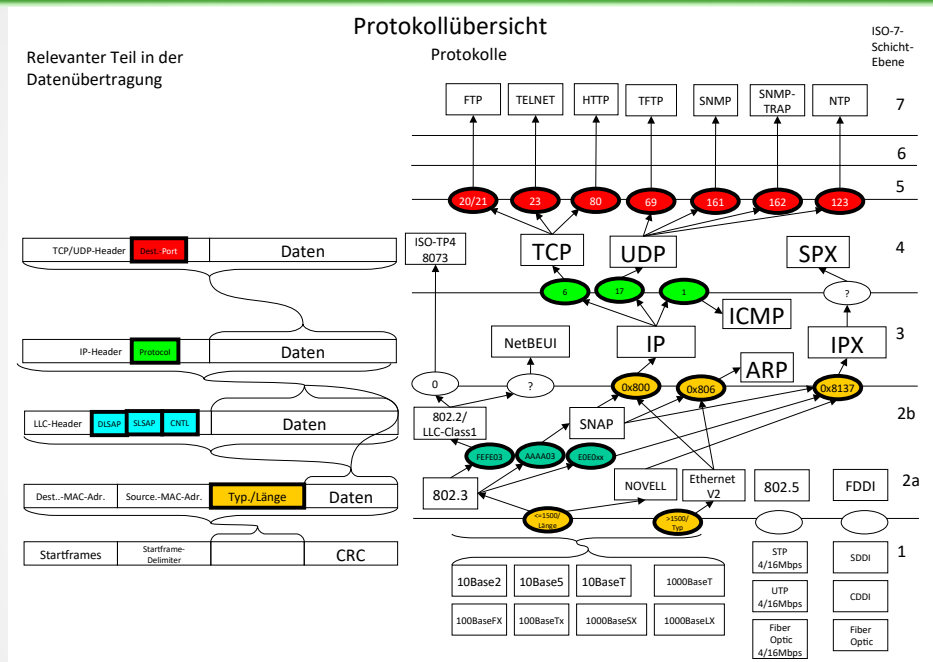
Folie: 13:78

In der Folie sind die Auswirkungen durch die unterschiedlich großen Datenteile dargestellt.

Bei kleinen Framegrößen ist das nicht relevant.

Bei einem Filetransfer können allerdings bei jedem Frame weniger Daten übertragen werden, was zu mehr Frames führt.

Protokolle über ISO-7-Schichten Modell hinweg



Ab der Ebene 2 gibt es Felder, in denen auf das Protokoll der nächsten Ebene verwiesen wird.

So verweist z. B. auf Ebene 3 das Protocol-Feld auf die auf IP aufsetzende Protokolle:

- 1 = ICMP
- 6 = TCP
- 17 = UDP

IPv4-Funktionsübersicht

- IP ist im RFC791 beschrieben
- IP wurde zur ungesicherten Datenübertragung zwischen paketorientierten Rechnernetzen entwickelt.
- Im IP werden zwei wichtige Funktionen des Internets abgewickelt.
 - ⚡ Adressierung / Wegefindung
 - ⚡ Fragmentierung (Zerlegung der Datagramme in transportierbare Größen) und
 - ⚡ Reassemblierung (Zusammenbau der zerlegten Datagramme auf dem Zielsystem)

Der Dienst den die IP-Schicht liefert, wird mit 4 verschiedenen Parametern festgelegt

- TOS
- TTL
- Optionen
- Header Checksum

IP macht/regelt

- keine Flusskontrolle
- keine Wiederholungen
- keine Quittungen

Erkannte Fehler (Z. B. ein nicht erreichbarer Host) werden über das Internet Control Message Protocol (ICMP) gemeldet/abgehandelt.



TOS (Type Of Service, deutsch: Art des Dienstes) wird benutzt, um die Qualität des gewünschten Dienstes zu parametrieren.

TTL (Time To Live, deutsch: Lebensdauer) Der TTL-Wert wird beim Senden vom IP-Stack der Datenquelle vergeben (z. B. 32).

Jeder Netzknoten (Router), über den ein Datagramm hinweg transportiert wird, reduziert den TTL-Wert um 1.

Erreicht der TTL-Wert den Wert 0, ohne sein Ziel erreicht zu haben, wird das zugehörige Datagramm zerstört und der Sender mit einer ICMP-Meldung darüber unterrichtet.

Somit ist ein TTL letztendlich ein hopgesteuerter Selbstvernichtungsauslöser.

Die **Optionen** dienen zur Steuerung von Funktionen, die in bestimmten Situationen nützlich sind. Hier werden Zeitstempel, Sicherheitsmechanismen und spezielles Routing ermöglicht.

Die **Header Checksum** dient zur Ermittlung, ob der Header richtig übertragen wurde. Diese Checksumme ist nur in der IP-Version 4 realisiert. In der Version 6 ist die Checksumme für den Header entfallen, da er zum CRC redundant ist.

IPv4-Adressen (classful)

Eine IP-Adresse besteht bei IPv4 aus 4 Bytes (=32Bits).
Die Darstellung besteht aus vier Integer-Zahlen im Bereich 0 bis 255, die mit Punkten getrennt werden. (dotted decimal)
Beispiel: 165.33.12.44

Klasse	1. Byte	2. Byte	3. Byte	4. Byte	Anzahl Netze	Anzahl Hosts
A	0	7 Bit Netz-Adr.	24 Bit Host-Adr.		127	16777213
B	10	14 Bit Netz-Adr.	16 Bit Host-Adr.		16383	65533
C	110	21 Bit Netz-Adr.		8 Bit Host-Adr.	2097151	253

Netzwerk-Adressteil Host-Adressteil

Stand: 27.11.2022

Netztechnik Teil-9

Folie: 16:78

Jede IPv4-Adresse hat einen Netzwerk-Teil und einen Host-Teil.

Handelt es sich bei einer IPv4-Adresse um einen Netzwerk-Adresse ist der Hostteil = 0

Je nachdem, wie groß der Anteil des Netzwerk-Teils an der IP-Adresse ist, kann die IP-Adresse einer Klasse zugeordnet werden.

1 Byte → Klasse A

2 Byte → Klasse B

3 Byte → Klasse C

Die Klasse kann auch am ersten Byte erkannt werden:

0 – 127 (erstes Bit = 0) → Klasse A

128 - 191 (erste zwei Bits = 10) → Klasse B

192 – 223 (erste 3 Bits = 110) → Klasse C

224 – 239 (erste 4 Bits = 1110) → Klasse D

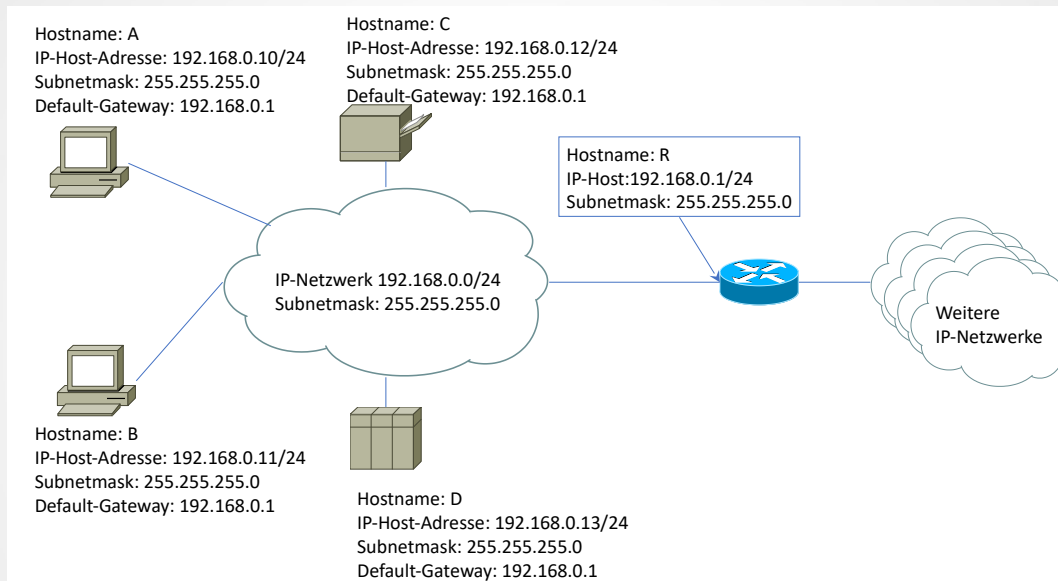
240 - 255 (erste 4 Bits = 1111) → Klasse E

IPv4-Adressklassen

Klasse	Bereich	Subnet-Mask (classful)
A	0.0.0.0 - 127.255.255.255	255.0.0.0
B	128.0.0.0 - 191.255.255.255	255.255.0.0
C	192.0.0.0 - 223.255.255.255	255.255.255.0
D	224.0.0.0 - 239.255.255.255	Multicasts
E	240.0.0.0 - 255.255.255.255	Experimentelle Adressen / Broadcasts

Adress-Bereich	Bezeichnung	
224.x.x.x – 239.255.255.255	Multicasts	224.0.0.0 – 224.0.0.255 Link-Local Scope 224.0.1.0 – 238.255.255.255 Global Scope 239.0.0.0 – 239.255.255.255 Administrative Scope
240.x.x.x – 254.255.255.255	Experimentelle Adressen	
255.x.x.x	Broadcasts	

IPv4-Adressbeispiel



Stand: 27.11.2022

Netztechnik Teil-9

Folie: 18:78

- Bei der Konfiguration eines Gerätes für IPv4 sind die folgenden Angaben zu machen:
- **IP-Adresse** des Hosts. Diese Adresse identifiziert den Host eindeutig innerhalb des Netzwerks.
- **Subnetmask** des Netzes, dessen Mitglied die Station werden soll. Damit wird der Netzwerkteil einer IP-Adresse definiert. Somit wird eingestellt, wie die eigene Adresse zu interpretieren ist. Die IP-Adresse wird erst im Zusammenhang mit der Subnetmask interpretierbar!

Default Gateway-IP-Adresse.

An diese IP-Adresse werden alle Pakete gesendet, deren Empfänger nicht im gleichen Netz liegen.

Evtl. Broadcast-Adresse

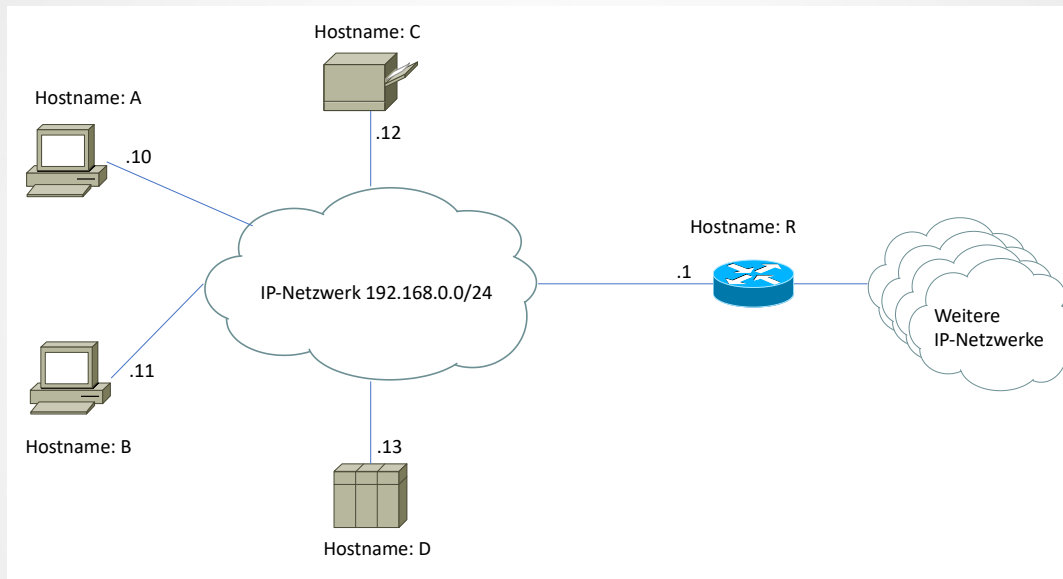
Wird Subnetting eingesetzt, kann die Broadcast-Adresse von der Broadcast Adresse der IP-Netzklasse abweichen. Eine Erklärung erfolgt weiter unten. Siehe auch Broadcasts.

IP-Netzwerke können wie im obigen Beispiel als **Wolke** oder mit einem **Bus-System** dargestellt werden. Dabei kann die **Subnetmask** voll ausgeschrieben werden (255.255.255.0) oder in der **CIDR-Schreibweise** (CIDR = Classless-Inter-Domain-Routing) mit /24 abgekürzt werden. Damit ist die **Klasse des IP-Netzwerks** durch das erste Byte der Netzwerk-Adresse festgelegt (192 = C-Klasse). Ist die Adressierung **classful**, so richtet sie sich auf Bytegrenzen aus. Da die Subnetmask 24 Bit entspricht ist das in diesem Beispiel gegeben.

Die Kommunikationsteilnehmer an einem Netzwerk werden bei IPv4 als **Hosts** bezeichnet. Durch die Festlegung auf ein **C-Klasse-Netzwerk** ist es möglich **253 Hosts** in diesem Netzwerk zu adressieren. Die **erste Adresse des Netzwerks** kann nicht für Hosts verwendet werden, da sie das Netzwerk selbst beschreibt. Die **letzte Adresse** kann nicht verwendet werden, da sie für die **Broadcast-Adresse** (also zur Sendung eines Paketes an alle Hosts im Netzwerk des Senders) reserviert ist.

Sind mehr als die 253 Host zu adressieren, muss auf eine andere Netzwerk-Klasse (mit kleinerem Netzwerk-Anteil) ausgewichen werden (z. Klasse A oder Klasse B) Damit ändert sich dann mindestens die Subnetmask.

IPv4-Adressbeispiel (Vereinfachte Darstellung-1)



Stand: 27.11.2022

Netztechnik Teil-9

Folie: 19:78

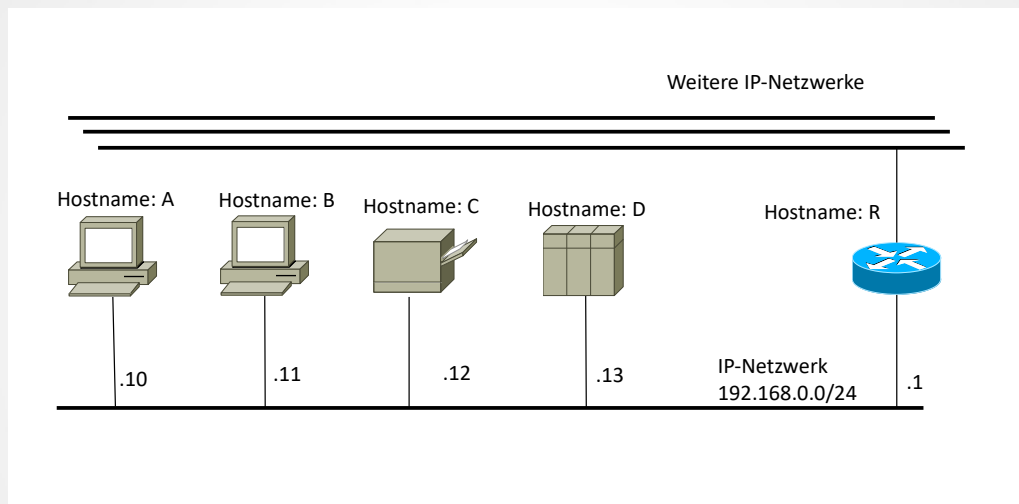
Diese Informationen sind für die meisten IPv4-Netzwerke ausreichend.

Da es pro Netzwerk meist auch noch weitere wichtige Zulieferer (z. B. DNS-Server, DHCP-Server, Zeit-Server,...) gibt, können diese bei der Beschreibung des Netzwerks in der Wolke mit hinterlegt werden.

In Sonderfällen kann es gewünscht sein, dass ein Teil der Hosts nur über einen bestimmten Weg (Router) in andere Netzwerke gehen soll, der andere Teil soll nur über einen anderen Weg gehen.

Dafür müssen dann unterschiedliche Router (also Default-Gateways) zur Verfügung gestellt werden, die dann bei der Beschreibung der Hosts wieder anzugeben sind.

IPv4-Adressbeispiel (Vereinfachte Darstellung-2)



Darstellung der gleichen Abbildung mit Bus-System

Ipv4 (Classful Subnetmask)

Klasse	Subnetzmaske (in dotted decimal Schreibweise)	Subnetzmaske (in binärer Schreibweise)	Subnetzmaske (in hexadezimaler Schreibweise)	Subnetzmaske (CIDR Schreibweise)
A	255.0.0.0	11111111 00000000 00000000 00000000	FF000000	/8
B	255.255.0.0	11111111 11111111 00000000 00000000	FFFF0000	/16
C	255.255.255.0	11111111 11111111 11111111 00000000	FFFFFF00	/24

A-Klasse 255.v.v.v Hierbei steht v.v.v, v.v oder v für den variablen Teil der Subnetz-Maske.
 B-Klasse 255.255.v.v Links stehen immer die Einsen für den erweiterten Netzwerk-Teil und
 C-Klasse 255.255.255.v rechts die Nullen für den restlichen Host-Teil.

Stand: 27.11.2022

Netztechnik Teil-9

Folie: 21:78

Eine Subnetz-Maske von 255.255.0.255 ist denkbar, führt allerdings nicht zu übersichtlichen Netzwerken und wird von modernen Betriebssystemen unterbunden.

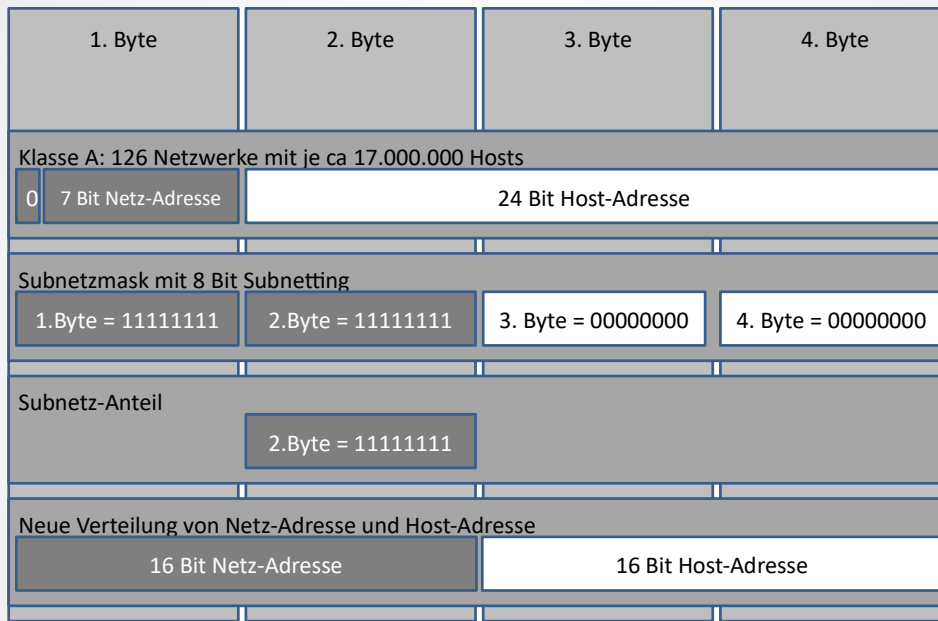
Liegt der Übergang von Einsen zu Nullen auf Bytegrenze spricht man von einem Klassen-basierten Netzwerk. Hier sind aber die Portionsgrößen nicht immer praktikabel. Das lässt sich ändern führt jedoch zu classless Netzwerken. Sobald das erfolgt werden Subnetzmasken benötigt.

Hat man nun zum Beispiel ein A-Klasse-Netz und möchte die möglichen 126 Netzwerke unterteilen, kann dies durch Subnetting erfolgen.

So kann zum Beispiel die Adresse 56.15.12.33 mit der Subnetmask 255.255.0.0 in ein funktionales Klasse-B-Netz überführt werden. Hier kann man sehen, dass, obwohl das erste Byte auf ein Klasse-A-Netz hinweist, das Netz funktional ein Klasse-B-Netz geworden ist.

Als Erkenntnis ist daraus zu ziehen, dass eine IP-Adresse immer erst zusammen mit ihrer Subnetmask richtig in Netzwerk- und Host-Teil zu unterteilen ist. Die ausschließliche Betrachtung des Wertes des ersten Bytes ist nicht ausreichend!

IPv4-Subnetting



Stand: 27.11.2022

Netztechnik Teil-9

Folie: 22:78

Bei einem A-Klasse Netzwerk gibt es 126 Netzwerke mit jeweils 16.777.214 Hosts.

Eine solche Anzahl von Host lässt sich in einem Netzwerk nicht vernünftig verwalten.

Deshalb gibt es die Möglichkeit den Netzwerk-Teil zu vergrößern. Dadurch wird jedoch der Host-Adressen-Teil verkleinert.

Im obigen Beispiel gibt es als Ergebnis ca. 65000 Netze mit jeweils 65000 Hosts in einem A-Klasse-Netz das zu einem B-Klasse-Netz gemacht wurde.

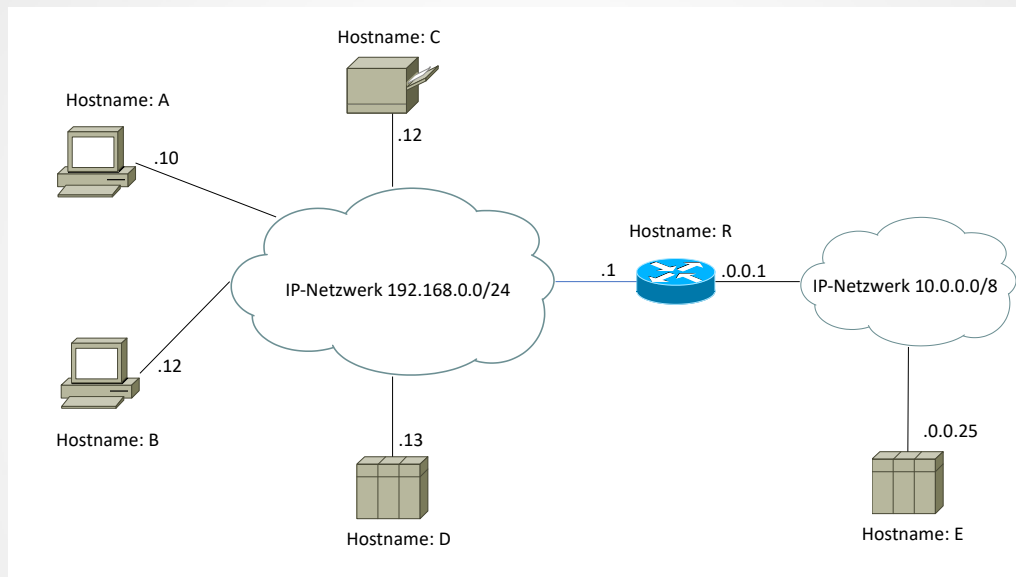
IPv4 Bitweise Änderung der Subnetmask

Dual-Darstellung	Dezimal-Darstellung	Hexadezimal-Darstellung
00000000	000	00
10000000	128	80
11000000	192	C0
11100000	224	E0
11110000	240	F0
11111000	248	F8
11111100	252	FC
11111110	254	FE
11111111	255	FF

Im 2., 3. und 4. Byte der Subnetzmaske kann die Grenze Bitweise verschoben werden.

Wie schon beschrieben darf der 1-0-Übergang nur einmal stattfinden, da es nur einen Übergang vom Netzwerk-Teil zum Host-Teil gibt!

IPv4 Anwendung der Subnetmask (Teil-1)



Stand: 27.11.2022

Netztechnik Teil-9

Folie: 24:78

Solange es nur ein Netzwerk mit einer Netzwerkadresse gibt, wissen alle Hosts, dass ihre Kommunikationspartner im gleichen Netzwerk liegen.

Dies bedeutet, dass ein Kommunikationspartner direkt angesprochen werden kann. Dazu muss ein Sender nur noch die MAC-Adresse des Empfängers kennen. Kennt er sie nicht, kann er sie mit einem ARP-Request ermitteln. Dabei fragt der Sender alle Netzteilnehmer, ob sie die zugehörige MAC-Adresse der Empfänger-IP-Adresse kennen. Ist der Empfänger im Netz vorhanden, wird er auf den ARP-Request mit einem ARP-Response antworten und seine MAC-Adresse dem Sender mitteilen. Die zurückgemeldete Zuordnung IP-Adresse zu MAC-Adresse merkt sich der Sender in einem so genannten ARP-Cache.

Damit braucht er beim nächsten Mal keinen ARP-Request zu senden, sondern er kann direkt die MAC-Adresse aus dem ARP-Cache verwenden. Damit bei einem Rechner-Umzug nicht alte IP-MAC-Adress-Zuordnungen in den ARP-Caches herumdümpeln, unterliegen sie einem Ageing-Mechanismus (deutsch: Alterungs-Mechanismus). Der sorgt dafür, dass die ARP-Cache-Einträge nach einer bestimmten Zeit gelöscht werden (ca. 20 –30 Minuten). Manche Hersteller tun dies aufgrund ihrer Voreinstellungen erst einmal nicht z. B. Nortel-Networks (Bay)

IPv4 Anwendung der Subnetmask (Teil-2)

Quelle

Host: A

IP-Adresse-A (192.168.0.10): 11000000.10101000.00000000.00001010

Subnet-Mask-A: 11111111.11111111.11111111.00000000

UND-Verknüpfung (1): 11000000.10101000.00000000.00000000 = Isolierter Netzwerkanteil (1)

Ziel im eigenen Netzwerk

Host D

IP-Adresse-B (192.168.0.13): 11000000.10101000.00000000.00001110

Subnet-Mask-A: 11111111.11111111.11111111.00000000

UND-Verknüpfung (2): 11000000.10101000.00000000.00000000 = Isolierter Netzwerkanteil (2)

Die UND-Verknüpfung (1) und die UND-Verknüpfung (2) liefern **das selbe Ergebnis**

→ Beide Kommunikationspartner liegen **im gleichen Netzwerk**

Ziel in anderem Netzwerk

Host E

IP-Adresse-E (10.0.0.25): 00001010.00000000.00000000.00011001

Subnet-Mask-A: 11111111.11111111.11111111.00000000

UND-Verknüpfung (3): 00001010.00000000.00000000.00000000 = Isolierter Netzwerkanteil (3)

Die UND-Verknüpfung (1) und die UND-Verknüpfung (3) liefern **nicht das selbe Ergebnis**

→ Beide Kommunikationspartner liegen **in unterschiedlichen Netzwerken**

Sobald jedoch mehrere Netzwerke über Router miteinander verbunden sind, geht das nicht mehr so einfach.

Nun kann unter Umständen ein Host nicht mehr sein Paket dem Kommunikations-Partner direkt senden. Er muss sein Paket einem Router senden, der für den Weitertransport der Daten in andere Netzwerke zuständig ist.

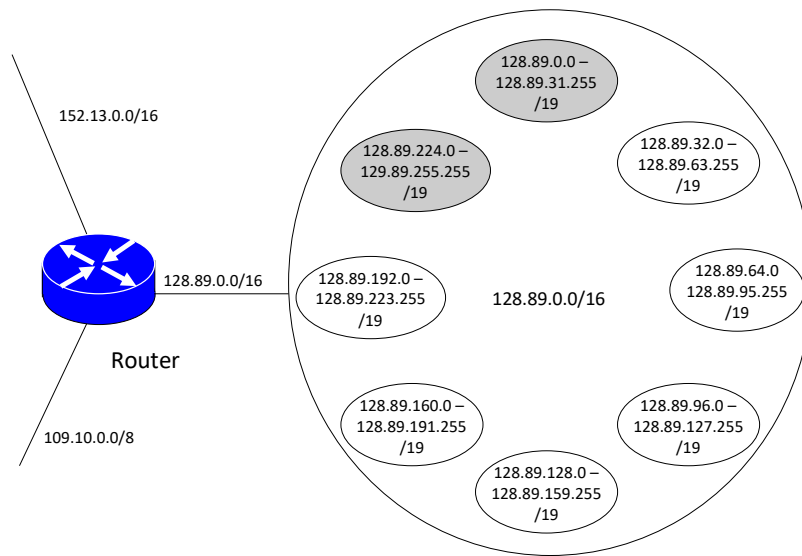
Damit nun ein Host mit einem zweiten Host in einem anderen Netzwerk kommunizieren kann, muss er erkennen können, ob der zweite Host im gleichen Netzwerk oder in einem anderen Netzwerk liegt. Um zu erkennen, ob beide Kommunikationspartner im gleichen Netzwerk liegen, müssen die Netzwerk-Teile der IP-Adressen isoliert werden.

Dazu verwendet der Sender seine eigene IP-Adresse, die IP-Adresse des Partners und seine eigene Subnetmask. Die IP-Adresse des Partners sowie die eigene IP-Adresse wird mit der eigenen Subnetmask UND-verknüpft. Das Ergebnis der beiden UND-Verknüpfungen wird miteinander verglichen. Sind beide Ergebnisse gleich, liegt der Partner im gleichen Netz. Dies bedeutet, dass der Partner direkt mit einem IP-Paket angesprochen werden kann.

Sind beide Ergebnisse ungleich, liegt der Partner in einem anderen Netz. Dies bedeutet, dass der Partner nicht direkt mit einem IP-Paket angesprochen werden kann. Das Paket muss zu einem Router (Default Gateway) gesendet werden.

Ein beliebter Fehler beim Umzug eines Rechners von einem Netzwerk in ein Netzwerk mit einer anderen Subnet-Mask ist zu vergessen die Subnet-Mask anzupassen.

IPv4-Subnetting Beispiel



Stand: 27.11.2022

Netztechnik Teil-9

Folie: 26:78

Die 3 Bit für die Unterteilung des Netzwerks ermöglichen 8 Subnetze.

Das erste und das letzte Subnetz ist nicht nutzbar.

Das erste Subnetz beschreibt das gesamte Netzwerk und das letzte Subnetz bildet die Broadcast Adresse für das Netzwerk.

Um das erste und das Subnetz trotzdem verfügbar zu machen muss die Verwendung des RFC1878 aktiviert werden.

IPv4-Subnetting

Art des Subnetz	Dezimaler Wert	Binärer Wert	Anzahl der Subnetze	Anzahl der Hosts
2 Bit	192	11000000	$2^2 = 4$ Zustände -> 2 Subnetze	$2^6 = 64$ Zustände -> 62 Hosts
3 Bit	224	11100000	$2^3 = 8$ Zustände -> 6 Subnetze	$2^5 = 32$ Zustände -> 30 Hosts
4 Bit	240	11110000	$2^4 = 16$ Zustände -> 14 Subnetze	$2^4 = 16$ Zustände -> 14 Hosts
5 Bit	248	11111000	$2^5 = 32$ Zustände -> 30 Subnetze	$2^3 = 8$ Zustände -> 6 Hosts
6 Bit	252	11111100	$2^6 = 64$ Zustände -> 62 Subnetze	$2^2 = 4$ Zustände -> 2 Hosts

Ein-Bit-Subnetting sowie 7-Bit-Subnetting sind **bei C-Klasse-Netzwerken** zwecklos.

- Ein-Bit-Subnetting (10000000) lässt 0 Subnetze zu.
- 7-Bit-Subnetting (11111110) lässt **bei C-Klasse-Netzwerken** 0 Hosts zu.

Die Anzahl der Zustände bei den Subnetzen sowie bei den Hosts führt über die Formel:

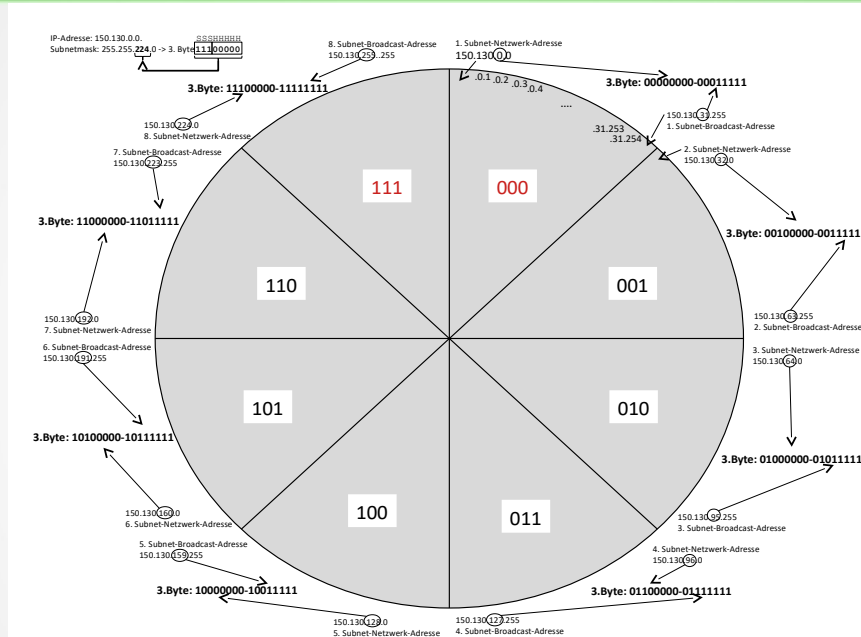
Anzahl = Anzahl der Zustände - 2

zu der möglichen Anzahl der Subnetze bzw. der Hosts.

Ein 1-Bit-Subnetting führt zu zwei Subnetzen. Damit ist ein erstes und ein letztes Netz entstanden. Beide Netzwerke sind nicht nutzbar.

Ein 7-Bit-Subnetting lässt 2 Adressen übrig, die für das Netzwerk selbst und für die Broadcast-Adresse reserviert und deshalb nicht für Hosts nutzbar sind.

IPv4-Subnetting



Stand: 27.11.2022

Netztechnik Teil-9

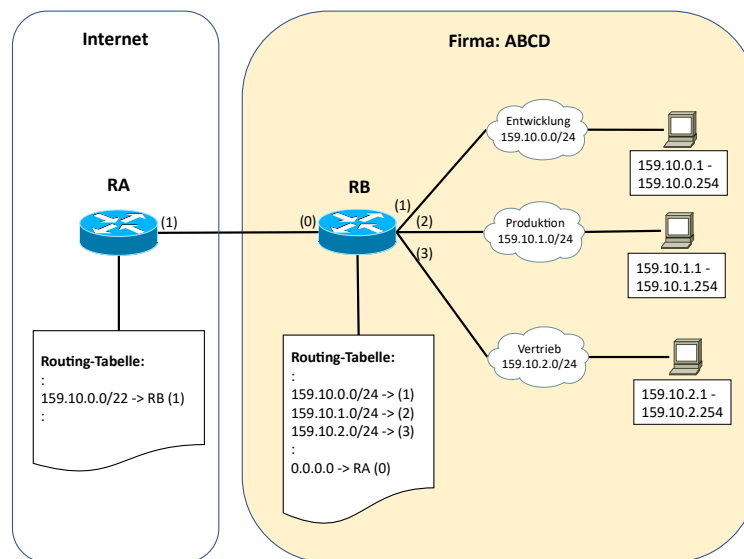
Folie: 28:78

Zu beachten ist, dass der Bereich mit den Subnetz-Werten **000** und **111** nicht für gültige Netze verwendet werden kann!

Der Ausschluss des ersten und des letzten IP-Subnetzes, wie im RFC 950 beschrieben, bedeutet eine unnötige Verschwendung von Adressbereichen.

Um den ersten und letzten Adressbereich trotzdem zu nutzen bieten diverse Hersteller die Möglichkeit der Verwendung der „**All-Ones**“ und „**All-Zeros**“-Subnetze einzuschalten. Diese Eigenschaft ist im **RFC 1878** beschrieben.

IPv4-Supernetting (1)



Stand: 27.11.2022

Netztechnik Teil-9

Folie: 29:78

Angenommen die Firma ABCD hat von ihrem Provider den IP-Adressraum 159.10.0.0 /22 bekommen. Damit steht ihr der Adressraum 159.10.0.0 bis 159.10.3.255 zur Verfügung.

Alle Geräte sollen eine im Internet gültige IP-Adresse bekommen. Der Router RB verwaltet 3 C-Klasse-Netzwerke. Je eines für Entwicklung, Produktion und Vertrieb. Die Netzwerke sind jeweils an ein physikalisches Interface (in Klammern) direkt angeschlossen. Zusätzlich hat der Router RB eine Verbindung in das Internet über die Default-Route (0.0.0.0) und dem Interface (0).

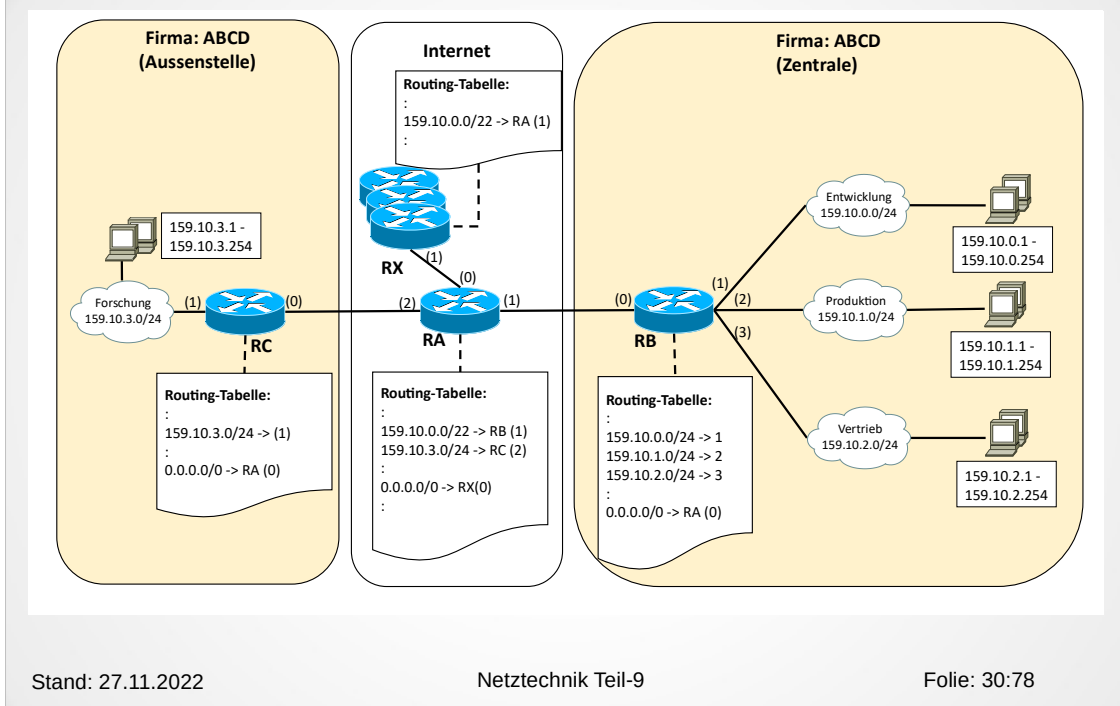
Unter anderem hat er für jedes Netzwerk in seiner Routing-Tabelle einen Eintrag.

159.10.0.0 /24 → (1)
159.10.1.0 /24 → (2)
159.10.2.0 /24 → (3)
0.0.0.0 → RA (0)

Die Clients in den einzelnen Netzwerken können das Internet über die Default-Route des Routers RB über das Interface (0) erreichen und die Clients können im Internet vom Router RA über das Interface (1) erreicht werden.

Eigentlich müsste der Router RA im Internet die gleiche Tabelleneinträge in seiner Routing Tabelle haben, doch Router RB propagiert nur ein Netzwerk (159.10.0.0), allerdings mit der Subnetmask /22. Damit ist der gesamte Netzwerk-Bereich von 159.10.0.0 bis 159.10.3.255 abgedeckt und der Router RA benötigt nur diesen einen Routing Tabelleneintrag. Dieses Zusammenfassen von Einträgen in der Routing-Tabelle reduziert sowohl beim Update der Routing-Tabelle als auch beim Lookup in der Routing-Tabelle den Bearbeitungsaufwand. Weiterhin wird weniger Speicherplatz für die Routing-Tabelle benötigt.

IPv4-Supernetting (2)



Das übrig gebliebene Netzwerk (159.10.3.0/24) soll nun für die Forschungsabteilung in einer Außenstelle genutzt werden. Die Außenstelle soll über das Internet erreicht werden. Dazu wird der Router RC einerseits mit den Interface (0) mit dem Internet verbunden und andererseits bekommt er am Interface (1) das Forschungs-Netzwerk konfiguriert. Damit wird der Router RC das Forschungsnetzwerk in das Internet propagieren.

Auf diese Weise entsteht beim Router RA ein Problem in der Routing-Tabelle. Das Forschungsnetzwerk kommt als zusätzlicher Eintrag in die Routing-Tabelle.
 159.10.0.0 /22 → RB (1)
 159.10.3.0 /24 → RC (2)

In der Routing-Tabelle des Routers RA gibt es nun zwei überschneidende Einträge, denn 159.10.3.0 /24 ist ein Teil von 159.10.0.0 /22.

Kommt nun ein Paket für das Ziel 159.10.3.65 beim Router RA an, findet er zwei passende Einträge in seiner Routing-Tabelle. Um nun den richtigen Eintrag auszuwählen, gilt es die Regel des „Longest-Match“ anzuwenden. Das bedeutet, der Eintrag mit dem längsten passenden Netzwerk-Teil, also dem längsten Präfix, wird für die Routing-Entscheidung herangezogen. Das Paket wird darauf hin über das Interface (2) an den Router RC weiter geleitet.

Kommt ein Paket für das Ziel 159.10.1.44 beim Router RA an, kann er dafür nur einen passenden Eintrag in seiner Routing-Tabelle finden (159.10.0.0 /22) und das Paket an den Router RB weiter leiten.

Da die Provider für ganze Regionen Adressbereiche zugewiesen bekommen, können diese für das Routing im Internet entsprechend zusammengefasst werden. Dies reduziert die Routing-Tabellen erheblich. So können die beiden Routing-Tabelleneinträge im Router RA bei Routern RX (und dahinter) in anderen Internet-Regionen wiederum zu einem Netzwerk (159.10.0.0 /22) zusammen gefasst werden.

IPv4-Unicasts / Multicasts / Broadcasts

Adressen	Bezeichnung	Verhalten
1.x.x.x : 223.x.x.x	Unicasts	Gehen von einem Sender an <u>einen</u> Empfänger
224.x.x.x	Multicasts	Gehen von einem Sender <u>an eine Gruppe</u> von Empfängern. So unterhalten sich z. B. Brücken miteinander
225.x.x.x : 255.x.x.x	Broadcasts	Gehen von einem Sender an alle Empfänger

Stand: 27.11.2022

Netztechnik Teil-9

Folie: 31:78

Broadcasts

Broadcasts werden, wie **Multicasts**, als **UDP-Datagramme** gesendet. Bei TCP sind nur Peer to Peer Verbindungen möglich! Es ist auch vor jedem TCP-Datenverkehr eine Verbindung aufzubauen und danach wieder abzubauen!

Um zu verstehen, was Broadcasts, Multicasts und Unicasts bedeuten, muss man sich vergegenwärtigen, dass jede Netzwerkkarte, die an ein Ethernet angeschlossen wird, ständig alle Frames auf dem Ethernet mit liest. (Zumindest der Ethernet Header wird mit gelesen)

Alle Broadcasts, Multicasts an die eigene Gruppe und Unicasts an die eigene MAC Adr. werden an die nächsthöhere Schicht weitergegeben. Alle anderen Frames werden von der Netzwerkkarte verworfen und nicht weiterbearbeitet.

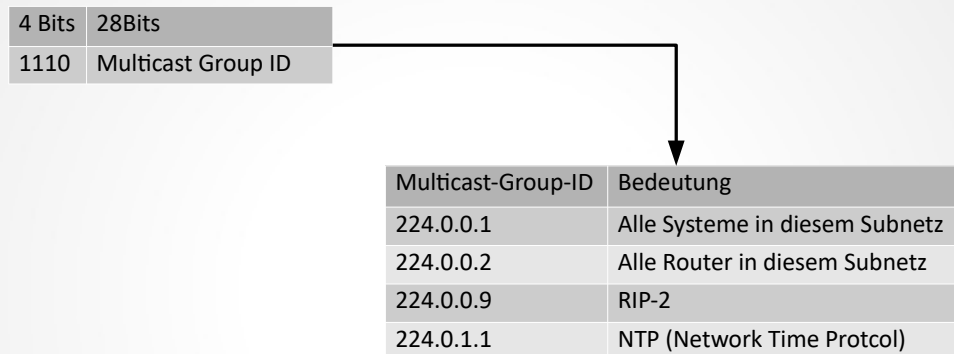
Davon gibt es eine **Ausnahme**:

Wird die Netzwerkkarte in den **Promiscuous Mode** gesetzt, leitet sie alle Frames an die nächsthöhere Schicht weiter. Dies wird von Netzwerk-Analysesoftware wie z. B. tcpdump ausgenutzt.

Broadcasts haben den Nachteil, dass sich je nach Interface-Karte auch die CPU mit dem Fame befassen muss, da ein Interrupt erzeugt wird. Dies ist vor allem dann schlecht, wenn der Rechner den empfangenen Broadcast nur verwirft, weil er nicht für ihn ist. Somit wird CPU-Leistung unnötig verschwendet! Ein erhöhtes Broadcast Aufkommen führt dann auch zu erhöhter CPU-Last. Dies kann im schlimmsten Fall dazu führen, dass der Rechner seiner eigentlichen Arbeit nicht mehr nachkommt, weil die CPU nur damit beschäftigt ist Broadcasts weg zu werfen. Dies entspricht einem Denial Of Service.

Das bedeutet, dass Broadcast-lastige Protokolle für alle am Netzwerk angeschlossenen Geräte eine CPU-Grundlast darstellt. Dies ist ein Grund warum IP Netzwerke möglichst klein sein sollten. Damit werden auch die Broadcast-Domänen begrenzt.

IPv4-Multicasts

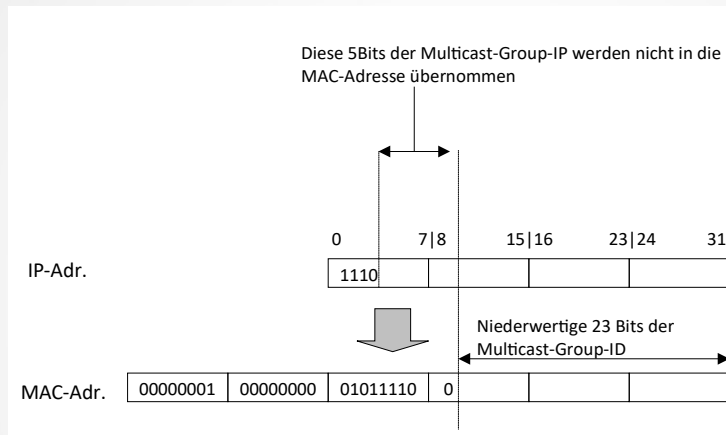


Die Multicast-IPv4-Adresse beginnt immer mit 224.x.x.x

Je nach Multicastgruppe werden die verbleibenden 3 Bytes befüllt.

IPv4 (Umsetzung der Multicast-IP-Adresse in eine MAC-Adresse)

Multicasts müssen, damit sie von der Netzwerk-Karte weiter geleitet werden, eine bestimmte MAC-Adresse haben



Dies bedeutet, dass bei Netzwerk-Teilnehmern, die Multicasts verarbeiten, die überlagerten Schichten die Multicasts filtern müssen!
Multicasts funktionieren auch mit mehreren Sendern (daher kommt auch der Name).
Rückmeldungen sind nicht möglich! Daher kann auch TCP nicht mit Multicasts verwendet werden.
Der Sender weiß nicht, wer ihm zuhört.

Beim Senden einer IPv4-Multicast-Adresse muss eine MAC-Multicast-Adresse zugeordnet werden.

Dafür gibt es den OUI-Bereich 01-00-5E

Der Rest wird über die oben dargestellte Vorgehensweise zugeordnet.
Dabei werden jedoch die höchstwertigen Bits der Multicast-Gruppe nicht in die MAC-Adresse überführt.

IPv4-Header

Version (4Bit)	IHL (4Bit)	TOS (8 Bit)	Length (16 Bit)	
ID (16 Bit)			Flags (3Bit)	Fragment Offset (13Bit)
TTL (8 Bit)		Protocol (8 Bit)	Checksum (16 Bit)	
Source Address (32Bit)				
Destination Address (32Bit)				
Options				Padding

Stand: 27.11.2022

Netztechnik Teil-9

Folie: 34:78

Version

Version des IP-Headers. Dieser Header-Aufbau bezieht sich auf die Version 4

IHL

Internet-Header-Length (wird in 32-Bit-Worten gerechnet)

Die minimale Headerlänge ist 5

TOS

Type Of Service

Length

Länge des gesamten Datagramms

ID

Identifikation des Datagramms für das Reassemblieren von fragmentierten Datagrammen

Flags

Steuerflags für das Fragmentieren

TTL

Time To Live

Maximale Lebensdauer des Datagramms. Bei jedem Weiterreichen eines Datagramms durch einen Router in ein weiteres Netzwerk wird der Wert um 1 reduziert. Sobald der TTL-Wert = 0 ist, wird das Datagramm verworfen und eine ICMP-Meldung erzeugt.

Protocol

Kennung des Protokolls der nächsthöheren Ebene (beschrieben in RFC790, siehe auch im Anhang)

Checksum

Checksumme des Headers

Source

Quell-IP-Adresse

Destination

Ziel-IP-Adresse

Options

Können, müssen aber nicht definiert sein

Padding

Füll-Bits

IPv4 (Referenznetzwerke)

Adressblock	Adressbereich	Beschreibung	Referenz
0.0.0.0/8	0.0.0.0 bis 0.255.255.255	aktuelles Netz (nur als Quelladresse gültig)	RFC 3232 (ersetzt RFC 1700)
10.0.0.0/8	10.0.0.0 bis 10.255.255.255	Netzwerk für den privaten Gebrauch	RFC 1918
127.0.0.0/8(1)	127.0.0.0 bis 127.255.255.255	Localnet	RFC 3330
169.254.0.0/16	169.254.0.0 bis 169.254.255.255	Zeroconf	RFC 3927
172.16.0.0/12	172.16.0.0 bis 172.31.255.255	Netzwerk für den privaten Gebrauch	RFC 1918
192.0.0.0/24	192.0.0.0 bis 192.0.0.255	reserviert, aber zur Vergabe vorgesehen	
192.0.2.0/24	192.0.2.0 bis 192.0.2.255	Dokumentation und Beispielcode (TEST-NET-1)	RFC 5737 (ersetzt RFC 3330)
192.88.99.0/24	192.88.99.0 bis 192.88.99.255	6to4-Anycast-Weiterleitungspräfix	RFC 3068
192.168.0.0/16	192.168.0.0 bis 192.168.255.255	Netzwerk für den privaten Gebrauch	RFC 1918
198.18.0.0/15	198.18.0.0 bis 198.19.255.255	Netz-Benchmark-Tests	RFC 2544
198.51.100.0/24	198.51.100.0 bis 198.51.100.255	Dokumentation und Beispielcode (TEST-NET-2)	RFC 5737
203.0.113.0/24	203.0.113.0 bis 203.0.113.255	Dokumentation und Beispielcode (TEST-NET-3)	RFC 5737
224.0.0.0/4	224.0.0.0 bis 239.255.255.255	Multicasts (früheres Klasse-D-Netz)	RFC 3171
240.0.0.0/4	240.0.0.0 bis 255.255.255.255	reserviert (früheres Klasse-E-Netz)	RFC 3232 (ersetzt RFC 1700)
255.255.255.252)	255.255.255.255	Broadcast	

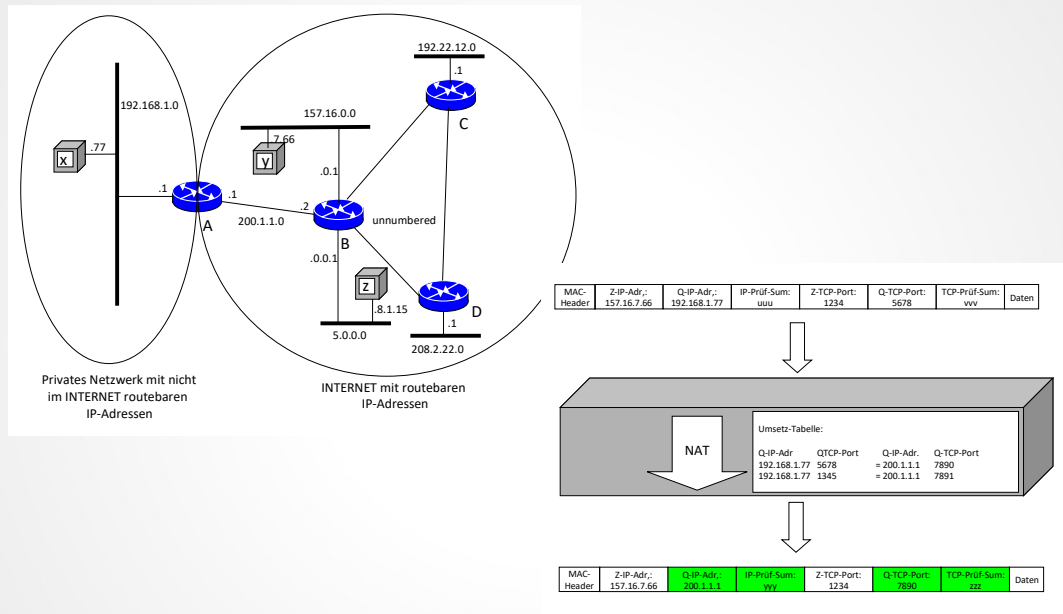
Stand: 27.11.2022

Netztechnik Teil-9

Folie: 35:78

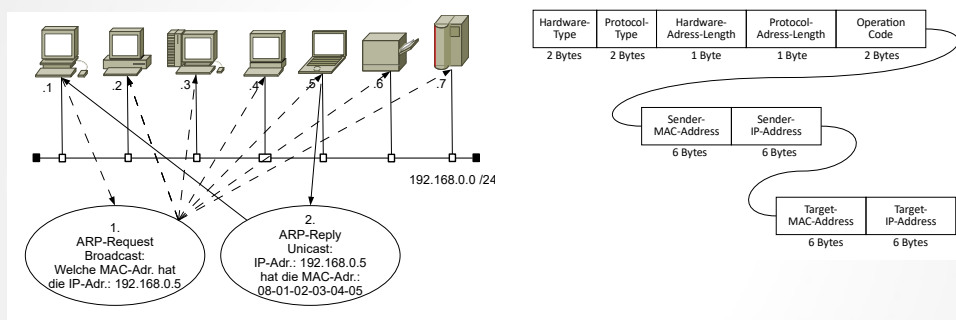
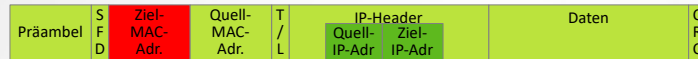
Für unterschiedliche Zwecke gibt es einige Bereiche mit besonderen Funktionen

IPv4 NAT / PAT



IPv4 ARP (Address Resolution Protocol)

Beim Aufbau eines Frames an ein neues Ziel ist bis auf die Ziel-MAC-Adresse alles bekannt.
Die Ziel-MAC-Adresse wird mit dem ARP ermittelt.



Bearbeitung des ARP-Caches in der DOS-BOX

arp -a Ausgabe des ARP-Cache-Inhalts
arp -s <ip-adr> <mac-adr> ARP-Eintrag manuell vornehmen
arp -d <ip-adr> ARP-Eintrag löschen

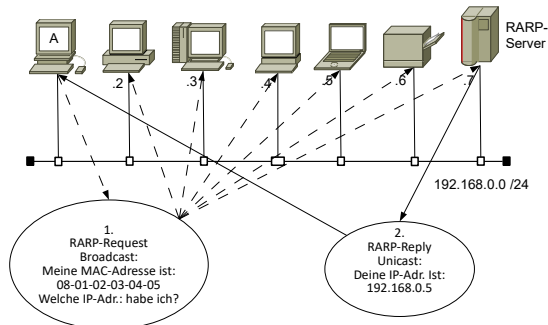
IPv4

RARP (Reverse Address Resolution Protocol)

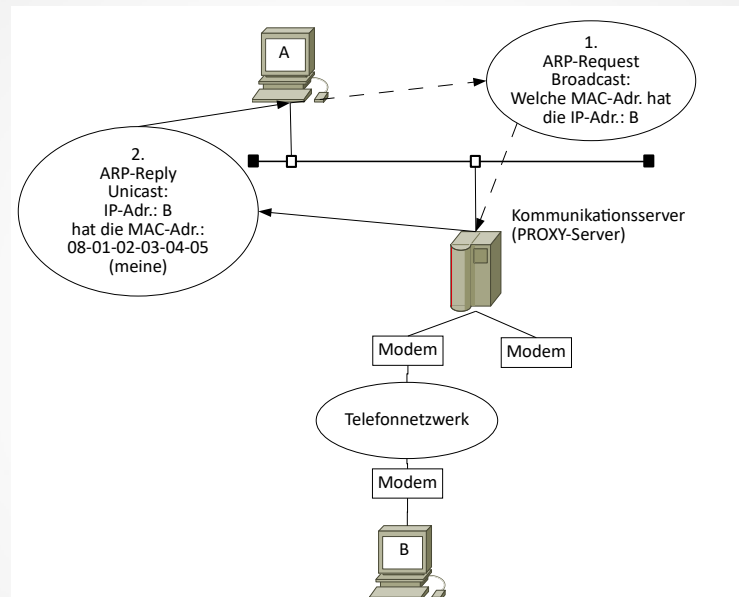
Will eine Station ihre IP-Adresse ermitteln, kann dies mit dem RARP erfolgen.

Präambel	S F D	Ziel- MAC- Adr.	Quell- MAC- Adr.	T / L	IP-Header		Daten	C R C
					Quell- IP-Adr.	Ziel- IP-Adr.		

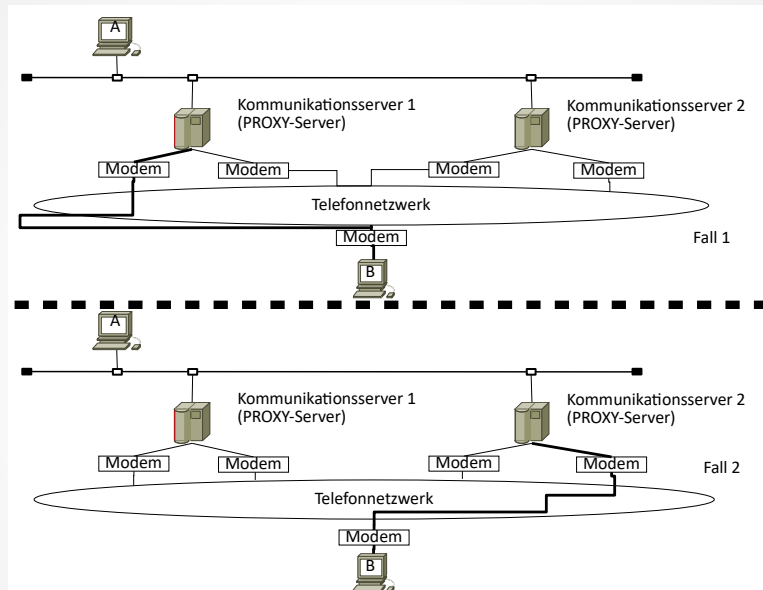
Station A möchte seine eigene IP-Adresse erfahren.
Deshalb sendet Station A einen RARP-Request mit einem Broadcast an alle (Wer kennt mich?) (1.)
Der RARP-Server kennt die IP-Adresse und sendet sie an die Station A. (2.)



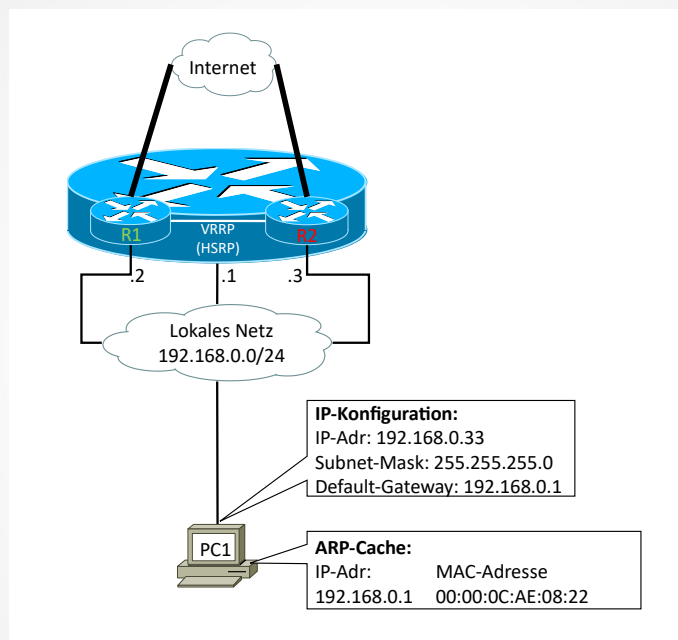
IPv4 PROXY ARP



IPv4 UNARP



IPv4 GLBP / HSRP / VRRP



Stand: 27.11.2022

Netztechnik Teil-9

Folie: 41:78

Situation:

R1 (192.168.0.2) ist Master-Router.

R2 (192.168.0.3) ist Backup-Router.

Die IP-Adresse des Virtuellen Routers ist 192.168.0.1.

Der Online-Router übernimmt zusätzlich zu seiner eigenen IP-Adresse noch die virtuelle IP-Adresse und auch die zugehörige virtuelle MAC-Adresse.

Der Master R1 sendet im Sekundenintervall Advertisements.

Fällt der Master-Router aus, übernimmt der Backup-Router die virtuelle IP-Adresse und die virtuelle MAC-Adresse innerhalb von 3 Sekunden.

Ablauf:

1. PC1 will eine Abfrage in das Internet senden. Dafür baut er einen Frame auf. Um den Frame aufzubauen benötigt er die MAC-Adresse seines Default-Gateways. Dazu sendet PC1 einen ARP-Request als Broadcast aus, in dem er sein Default-Gateway mit der IP-Adresse 192.168.0.1 bittet, seine MAC-Adresse mitzuteilen.

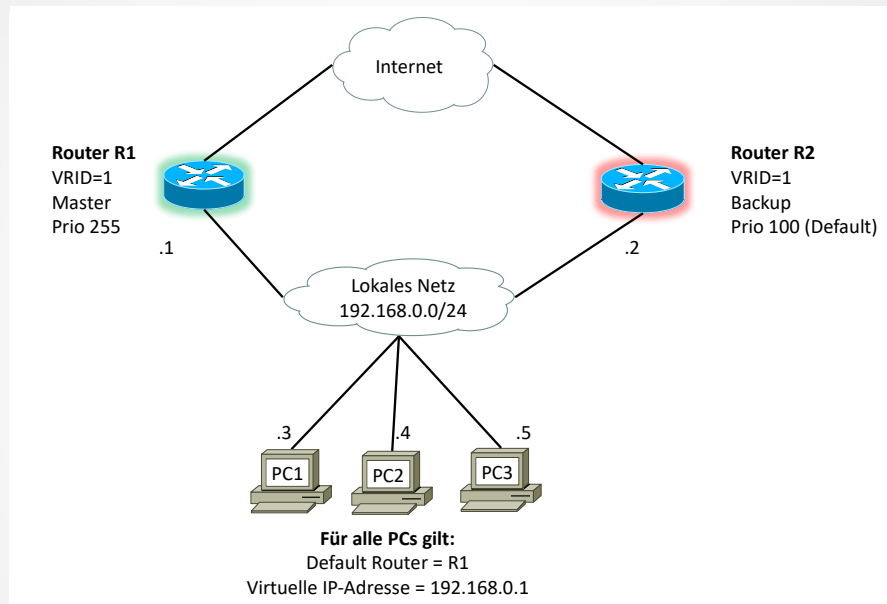
2. Der Master-Router (R1) sendet die virtuelle MAC-Adresse mit einem ARP-Reply an den PC1 zurück und dieser vermerkt die MAC-Adresse in seinem ARP-Cache.

3. Danach kann der PC1 seinen Frame in das Internet über den aktiven Router (R1) senden.

Der Vorteil dieses Aufbaus ist, dass nur eine Konfiguration auf den Routern erforderlich ist. Durch die Verwendung von virtuellen MAC-Adressen muss bei einem Router-Wechsel der ARP-Cache nicht aktualisiert werden.

Ein eventuelles Problem besteht darin, dass die Verbindung zwischen Routern ausfällt und jeder versucht Online-Router zu werden. Dies kann zu einer Split-Brain Situation führen

IPv4 VRRP-Beispiel-1



Stand: 27.11.2022

Netztechnik Teil-9

Folie: 42:78

Einfache Konfiguration zu Erhöhung der Router-Verfügbarkeit.

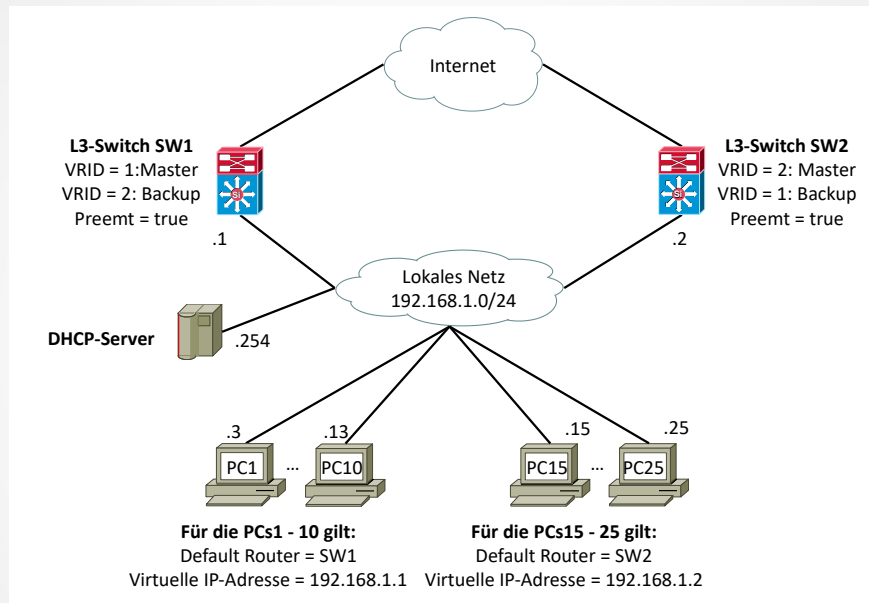
R1 ist Owner der IP-Adresse (.1) die gleichzeitig virtuelle IP-Adresse ist.

Die IP-Adresse wurde real an seine IP-Adresse gebunden. So bekommt der Router die Priorität 255 und ist damit Master, solange er aktiv ist.

Alle an das IP-Netzwerk 192.168.0.0/24 angeschlossenen Geräte nutzen R1 als Default Router. Dies bleibt so lange, wie der Router R1 aktiv ist. Erst im Fehlerfall übernimmt R2 die Masterfunktion.

Da normalerweise der Fehlerfall selten eintritt wird der Router R2 auch nur selten genutzt. Im Normalfall bleibt die Ressource R2 ungenutzt.

IPv4 VRRP-Beispiel-2



Stand: 27.11.2022

Netztechnik Teil-9

Folie: 43:78

Zur Verbesserung der Router-Auslastung führt das nächste Beispiel.
Anstelle von Routern werden hier Layer-3-Switches verwendet.

SW1 und SW2 haben die tatsächliche IP-Adresse als virtuelle IP-Adresse konfiguriert.

SW1 ist Owner der IP-Adresse .1 und damit Master für den VR mit der ID = 1.

SW2 ist Owner der IP-Adresse .2 und damit Master für den VR mit der ID = 2.

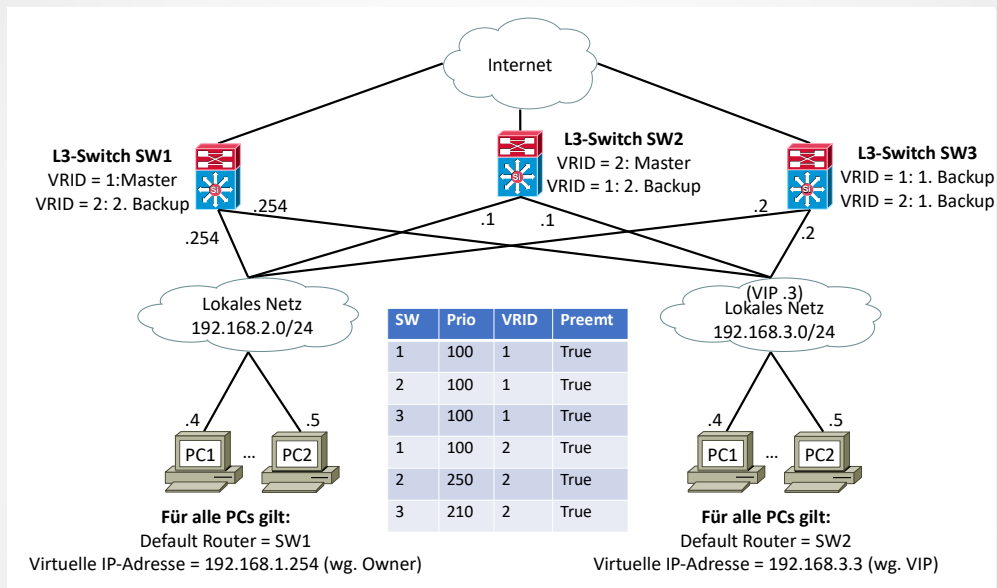
SW1 ist Backup für den virtuellen Router mit der ID = 2.

SW2 ist Backup für den virtuellen Router mit der ID = 1.

Per DHCP bekommt die eine Hälfte der Geräte SW1 als Default Router zugeteilt und die andere Hälfte den SW2 als Default Router zugewiesen.

Damit werden beide Wege in das Internet genutzt und die Netzlast ausgeglichen.

IPv4 VRRP-Beispiel-3



Stand: 27.11.2022

Netztechnik Teil-9

Folie: 44:78

In diesem Beispiel sind mehrere Netze an zwei Layer-3-Switches angebunden. Es soll hier gezeigt werden, dass Master und Backup entweder über Prioritäten (übersichtlicher und damit sicherer) oder IP-Adressen festgelegt werden können.

Beim virtuellen Router mit der ID = 1 haben alle Switches die Prio 100 (Default)
 SW1 bekommt als Owner der IP-Adresse 192.168.2.254 die Prio = 255 und wird somit zum Master im Netzwerk 192.168.2.0/24. Damit gibt es auch keine virtuelle IP-Adresse (VIP)
 SW3 wird aufgrund der höheren IP-Adresse (.3) als erster zum Backup falls SW1 ausfällt. SW2 wird aufgrund der niedrigeren IP-Adresse (.2) als letzter zum Backup, was auch gewünscht ist, da er bereits die Daten für das Netzwerk 192.168.3.0/24 transportiert.

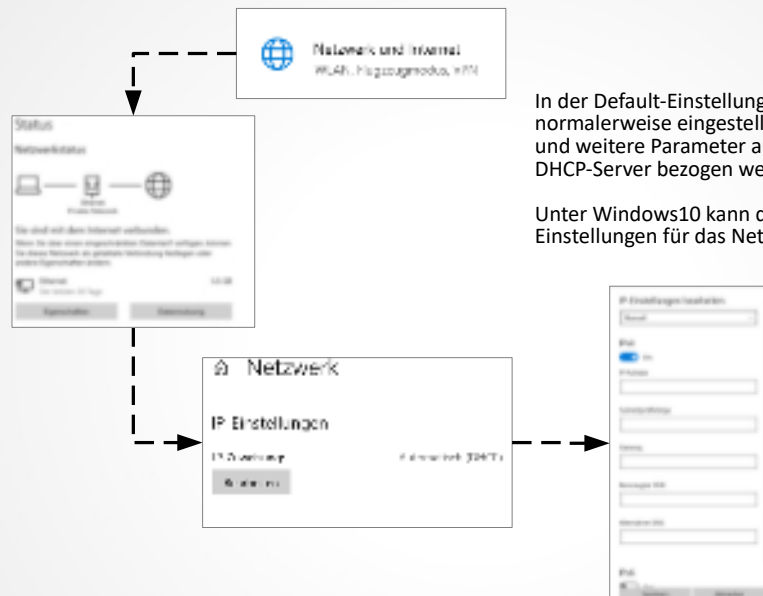
Beim virtuellen Router mit der ID = 2 wurden Prioritäten zugeteilt und die virtuelle IP-Adresse (VIP) = 192.168.3.3 eingerichtet. Keiner der Switches ist Owner dieser IP-Adresse. Damit greift die Prioritätsvergabe.

SW2 wird aufgrund der höchsten Priorität zum Master im Netzwerk 192.168.3.0/24.

SW3 wird aufgrund seiner Priorität als erster zum Backup falls SW2 ausfällt.

Da SW1 schon die Daten von 192.168.2.0/24 transportiert, wird er als letzter zum Backup.

IPv4 DHCP

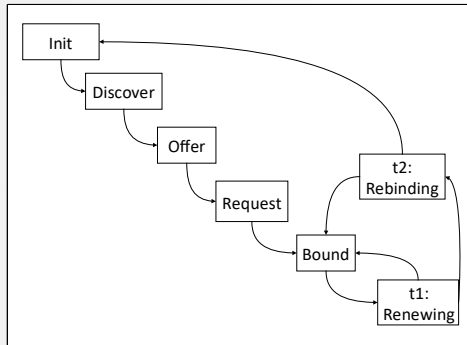


In der Default-Einstellung haben Clients normalerweise eingestellt, dass die IP-Adresse und weitere Parameter automatisch von einem DHCP-Server bezogen werden.

Unter Windows10 kann das unter den Einstellungen für das Netzwerk geändert werden.

IPv4 DHCP-Ablauf

Ablauf



DOS-Box-Kommandos

Informationsausgabe: `ipconfig /all`
Lease erneuern: `ipconfig /renew`
Lease freigeben: `ipconfig /release`

Lease-Erneuerung

Mit der Bestätigung des Lease wurde dem Client noch die Leasedauer mitgeteilt.

Aus der Leasedauer erzeugt der Client zwei Timer.
 $t1 = 0,5 * \text{Leasedauer}$

Nach dieser Zeit muss der Client die Leaserime erneuern und sendet einen DHCP-Request aus. Damit ist der Client im Zustand RENEWING. Empfängt der Client innerhalb einer Zeit $\leq t2$ einen DHCP-ACK, dann ist er wieder im Zustand BOUND.

$t2 = 0,875 * \text{Leasedauer}$

Empfängt der Client innerhalb der Zeit $t2$ keine Nachricht vom Server fällt er in den Zustand REBINDING. Dann versucht er es über einen DHCP-Request als Broadcast an alle verfügbaren DHCP-Server.

Bekommt der Client eine Antwort fällt er in den Zustand BOUND. Kommt allerdings keine Antwort oder er erhält ein DHCP-NAK, fällt er in den Zustand INIT.

Stand: 27.11.2022

Netztechnik Teil-9

Folie: 46:78

DHCP-Discover

Damit versucht der anfordernde Client den DHCP-Server zu finden und ihn aufzufordern, ein Adress-Angebot zu senden.

DHCP-Offer

Antwort des DHCP-Server auf eine DHCP-Discover-Nachricht.

DHCP-Request

Damit wird die angebotene IP-Adresse akzeptiert und alle anderen Angebote abgelehnt.

DHCP-ACK

Nachricht des DHCP-Servers mit dem gültigen Lease

DHCP-NAK

Nachricht des DHCP-Servers mit der Ablehnung des angeforderten Lease.

DHCP-Release

Nachricht des DHCP-Client an den DHCP-Server, dass die bisher genutzte IP-Adresse nicht mehr benötigt wird. Damit kann der DHCP-Server die Adresse wieder zur Verfügung stellen.

IPv4

Der DHCP-Server kann dem Client mit den Options eine Vielzahl von Parametern mitgeben.
Hier eine kleine Auswahl

Option Number	Name	Description
1	Subnet-Mask	Subnet-Mask
2	Time Offset	Time offset in seconds from UTC
3	Router	router addresses
4	Time-Server	time server addresses
5	Name-Server	IEN-116 server addresses
6	DNS-Server	DNS server adresse
7	LOG-Server	logging server address
8	Cookie-Server	quote server addresses
9	LPR Servers	printer server addresses
12	Host Name	Hostname string
15	Domain Name	The DNS domain name of the client
19	IP Layer Forwarding	Enable or disable IP forwarding
51	IP Address Lease Time	IP address lease time
58	Renew Time Value	DHCP renewal (T1) time
59	Rebinding Time Value	DHCP rebinding (T2) time

Eine detaillierte Liste gibt es z.B. bei:
<https://www.iana.org/assignments/bootp-dhcp-parameters/bootp-dhcp-parameters.xhtml#options>

IPv4 Zeroconf / APIPA

Ist entweder der DHCP-Server nicht vorhanden / erreichbar, oder ist der IP-Pool erschöpft, kann keine IP-Adresse zugewiesen werden.

Damit ein Client dann trotzdem noch (wenigstens eingeschränkt) kommunizieren kann, gibt er sich über Zeroconf selbst eine IP-Adresse.

Dabei greift er auf einen hierfür reservierten IP-Adressbereich zurück 169.254.0.0/16

In diesem Netzwerk gibt er sich eine IP-Adresse. (z. B. 169.254.0.22/16)

Diese Adresse ist natürlich vor der Benutzung daraufhin zu testen ist, ob sie schon von einem anderen Client genutzt wird.

Bei Microsoft wird die Vorgehensweise als Automatic Private IP Addressing (APIPA) bezeichnet.

Bei Apple ist die Vorgehensweise im Rahmen des Bonjour-Protokolls realisiert.

Im RFC 3330 wird das Zeroconf-verfahren beschrieben.

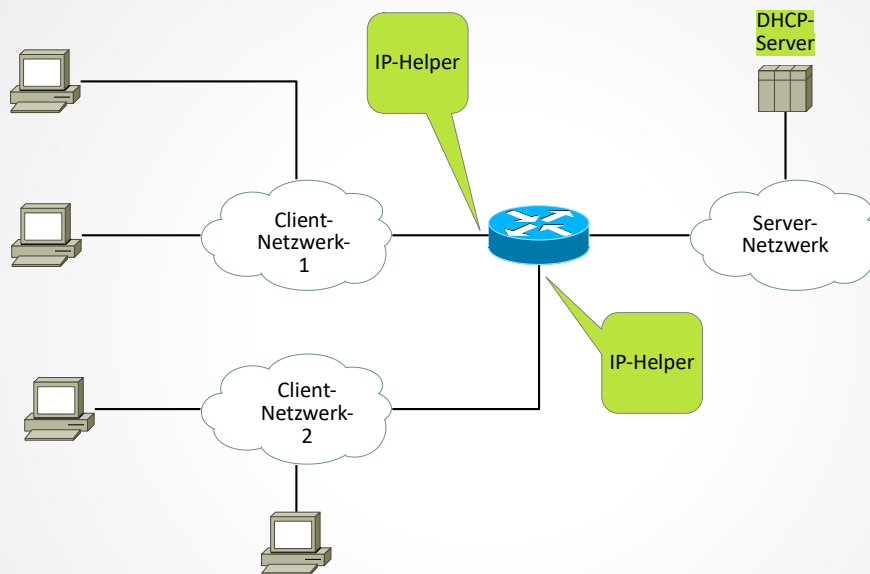
Standardisiert ist es unter dem Namen IPv4-Link-Local-Adresses (IPv4LL)

Adress-Bereich: 169.254.0.0 – 169.254.255.255

Es gibt auch eine automatische Erkennung von Netzwerk-Diensten:

- Bonjour (Apple) implementiert mit IPv4LL und Multicast DNS (mDNS)
- Avahi

IPv4 Iphelper



IPv4 ICMP

ICMP-Aufbau

Datenbits			
01234567	01234567	01234567	01234567
Type	Code	Checksum	
Data			
...			

IP kann selbst keine Fehlermeldungen erzeugen.
Dazu verwenden die Geräte, die IP nutzen, **ICMP**

Feld	Beschreibung
Type	Typenfeld, abhängig von der Art der ICMP-Nachricht
Code	Zusatzinformation zur ICMP-Nachricht
Checksum	Prüfsumme des gesamten ICMP-Paketes
Data	Abhängig von der Art des ICMP-Paketes können hier mehrere 32-Bit-Worte übertragen werden

Typ	Bedeutung
0	Echo reply
3	Destination unreachable
4	Source quench
5	Redirect (route change)
8	Echo Request
11	Time exceeded for datagram
12	Parameterproblem on datagram
13	Time stamp request
14	Time stamp reply
15	Information request
16	Information reply
17	Address mask request
18	Address mask response

z. B. Typ = 3

Code	Data
0 = Net unreachable	Not used
1 = Host unreachable	Not used
2 = Protocol unreachable	Not used
3 = Port unreachable	Not used
4 = Fragmentation needed and df (don't fragment) set	Not used
5 = source route failed	Not used

IPv4 Namensauflösung

Anwender und auch Applikationen verwenden normalerweise zur Bezeichnung von Zielen sprechende Namen wie z. B. www.Amazon.com
Dahinter stehen IP-Adressen, die etwas umständlicher zu merken und zu schreiben sind.
Zur Auflösung der Namen in IP-Adressen werden Name-Services verwendet.

Historisches:

Als die Anzahl der verwendeten Geräte noch übersichtlich war wurden die Namen in Listen verwaltet.
Z. B. unter Unix: `/etc/hosts` und unter Windows `C:/Windows/System32/drivers/etc/hosts`

Da dies mit steigender Geräteanzahl nicht mehr vernünftig aktuell zu halten war wurden Server mit dem Verwalten der Namens-IP-Adress-Zuordnung entwickelt.

Internet-Name-Server

Die erste Lösung mit einer solchen Eigenschaft heißt Internet Name Service und ist unter der Internet Engineering Note 116 (IEN 116) veröffentlicht.

Im Name Server File können bis zu drei Name-Server hinterlegt werden.

Es gibt einen so genannten Primary Name Server, der immer als erster angesprochen wird.

Ist der Primary Name Server nicht erreichbar wird die Anfrage an den Secondary Name Server gesendet.

Primary Name Server 192.1.2.1

Secondary Name Server 192.1.2.5

Der Abfragende Rechner sendet einen Name-Request und erhält vom Name-Server einen Name-Reply zurück. Zur Sicherstellung, dass die Antwort auch zur Anfrage passt wird im Reply-Paket der angefragte Name nochmals zusammen mit der ermittelten IP-Adresse übertragen.

IPv4

DNS: Namensauflösung-1

DNS hat eine dezentrale Verwaltung mit einer Baumstruktur für den Namensraum.
Weiterhin kann sichergestellt werden, dass Namen eindeutig sind und die Funktion erweitert werden kann.
Bei der Baumstruktur haben die Blätter (Knoten) werden als Labels bezeichnet.
Ein Label darf nur alphanumerische Zeichen und den Bindestrich (-) enthalten.
Der Bindestrich darf nicht am Ende stehen.
Ein kompletter Domainname besteht aus einer Verkettung aller Labels eines Pfades.
Ein Label ist eine Zeichenkette mit mindestens einem Byte und maximal 64 Bytes (RFC 2181).
Die Labels werden mit Punkten innerhalb eines Domainnamens miteinander verbunden/getrennt.

DNS nutzt UDP als Transportschicht und verwendet dort den Port 53.
TCP ist ebenfalls möglich und wird auf jeden Fall für die Zonentransfers (Verteilung der Informationsdateien) genutzt.

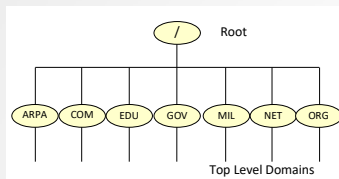
Der Service lässt sich in beiden Richtungen betreiben:

- Für einen Rechnernamen die zugehörige IP-Adresse ermitteln (lookup)
- Für eine IP-Adresse den zugehörigen Namen ermitteln (reverse lookup)

Das DNS besteht aus den drei Hauptkomponenten:

- Domain-Namensraum
- Nameserver
- Resolver

IPv4 DNS: Namensauflösung-2



Neben den TLDs gibt es noch Country-TLDs. Z. B.:

.de	Deutschland
.au	Österreich
.li	Lichtenstein
.lu	Luxemburg
.us	USA

Der Domain-Namensraum hat eine baumförmige hierarchischen Aufbau.
Von der Root ausgehend entwickelt sich der Baum.
Bei der Baumstruktur werden die Blätter (Knoten) als Labels bezeichnet.

Jede Verzweigung entspricht einer Zone.
Die erste / oberste Ebene wird als Top-Level-Domains (TLD) bezeichnet.
TLDs wurden vom Network Information Center (NIC) definiert.
Ein kompletter Domainnamen (FQDN = Fully Qualified Domain Name) wird mit einem Punkt abgeschlossen und darf inklusive aller Punkte 255 Byte lang sein.

Je weiter ein Label im Domainnamen rechts steht, desto höher steht es im Baum.
Deshalb wird ein Domain-Name immer von links nach rechts delegiert und aufgelöst.

Ein vollständiger Domain-Name wird auch Fully Qualified Domain Name (FQDN) genannt.
Beispiel für ein FQDN: `www.amazon.com.`
Der letzte Punkt gehört zum DNS-Namen, kann jedoch weggelassen werden.

Autoritative Server sind für eine Zone zuständig

Nicht autoritative Server beziehen die Zoneninformation von anderen Servern. Die Daten werden in einem Cache gehalten.
Ein TTL-Wert stellt sicher dass die Information aktuell ist.

IPv4 DNS: Namensauflösung-3

Die DNS-Objekte werden als Satz von Resource-Records in einer sogenannten Zonendatei (auch Zone genannt) gehalten und auf den autoritativen DNS-Servern über Zonentransfers abgeglichen.

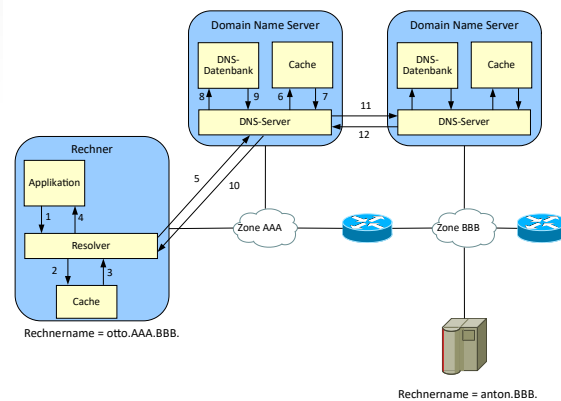
Resource Records

Die von den DNS-Servern verwalteten Informationen sind in den so genannten Resource Records (RR) hinterlegt. Die RR werden als ASCII-Datei in den Zonendateien oder in den DNS-Transport-Paketen in komprimierter Form verarbeitet.

Resource Records Format

Im ASCII-Format haben die RRs den folgenden Aufbau im ASCII-Format:

```
<name> [<ttl>] [<class>] <type> <rdata> <length>
<name>      Der Domänenname des Objekts, zu dem der Resource Record gehört (optional)
<ttl>       time to live (in Sekunden). Gültigkeit des Resource Records (optional)
<class>     Protokollgruppe, zu der der Resource Record gehört (optional)
<type>      beschreibt den Typ des Resource Records
<rdata>     (resource data) Daten, die den Resource Record näher beschreiben
              (zum Beispiel eine IP-Adresse für einen A-RR, oder einen Hostnamen für einen NS-RR)
<length>    Länge der folgenden Daten
```



Rekursiver Ablauf:

Falls ein DNS-Server die Info nicht hat, fragt er den nächsten DNS-Server.

Iterativer Ablauf:

Falls ein Server die Info nicht hat, gibt er eine negative Rückmeldung und der anfragende Resolver fragt den nächsten DNS-Server, der in der Rückmeldungen angegeben wurde.

IPv4 DNS: Resource-Record

Die Typen der Resource-Record sind vielfältig. Hier eine kleine Auswahl.

Typ	Bedeutung
A	IPv4-Adresse eines Hosts
AAAA	IPv6-Adresse eines Hosts
CERT	Resource Record für das Speichern von Zertifikaten (siehe RFC 4398)
CNAME	Kanonischer Name für einen Host (die Domain mit diesem RR ist ein Alias)
DNAME	ähnlich CNAME, aber für komplette Domains, siehe RFC 2672
DNSKEY	enthält einen dem Namen zugeordneten Public-Key – löste bei DNSSEC ab 2004 den Typ KEY ab.
DS	dient der Verkettung DNSSEC-signierter Zonen
MX	Mail Exchange – der für diese Domain zuständige Mailserver
NAPTR	Naming Authority Pointer – Erweiterung des A Resource Record
NSAP	Network Service Access Point
NS	Hostname eines autoritativen Nameservers. Verknüpfungen (Delegationen) der Server untereinander
PTR	Domain Name Pointer (für das Reverse Mapping, um IP-Adressen Namen zuzuweisen)
RRSIG	enthält eine digitale Unterschrift (wird seit 2004 von DNSSEC (=DNS Security) verwendet und ersetzt SIG)
SOA	Start of Authority
SPF	Sender Policy Framework
SRV	angebotener Dienst (Service)
SSHFP	SSH Fingerprint, zum Veröffentlichen der Fingerprints von SSH-Schlüsseln, siehe RFC 4255
TXT	fredefinierbarer Text, wird u. a. auch für Sender Policy Framework (SPF) verwendet. Wird auch oft genutzt für Google-Site Verification

Stand: 27.11.2022

Netztechnik Teil-9

Folie: 55:78

Wichtig:

SOA (Start of Authority)

A (Auflösung Name -> IPv4-Adresse)

AAAA (Quad A) (Auflösung Name -> IPv6-Adresse)

MX (Mail Exchange = Auflösung Mailserver-Name -> IPv4-Adresse)

PTR (Auflösung IP-Adresse → Name)

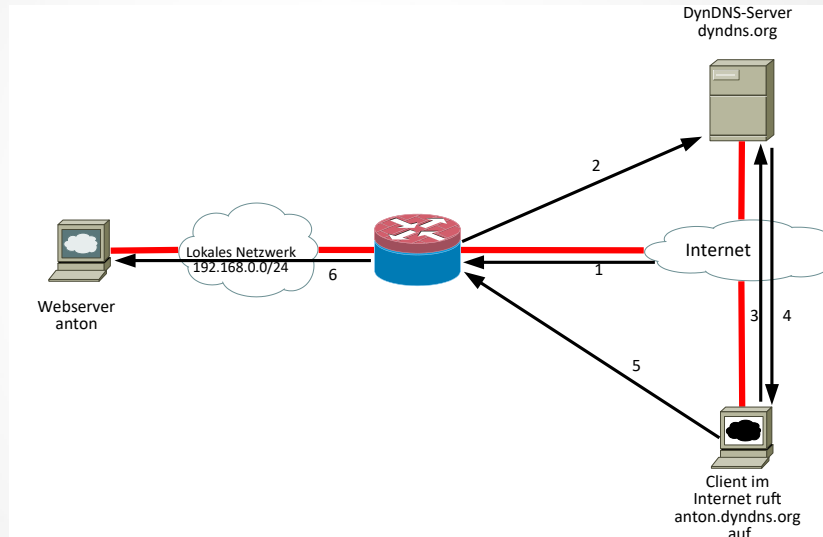
IPv4 DNS: SOA-Record

Der Start of Authority (SOA) -Resource-Record ist ein wichtiger Bestandteil einer Zonendatei. Er enthält Angaben zur Verwaltung der Zone und zum Zonentransfer. Er ist spezifiziert im RFC1035.

Typ	Bedeutung
Name	Zonen-Name
IN	Zonenklasse Internet
Primary	Zonenmaster. Bestimmt an wen dynamische Updates gesendet werden.
Mail-Address	Mailadresse des Administrators. Datei wird das @-Zeichen durch „.“ ersetztPunkte vor dem @-Zeichen werden durch „\“ ersetzt. Damit wird aus otto.huber@abc.com otto\huber.abc.com
Seriennummer	Wird bei jeder Änderung inkrementiert. Hat vorzugsweise das Format JJJJMMTTVV und ist ein Hinweis auf die letzte Änderungen
Refresh	Sekundenabstand in dem sekundäre Nameserver beim primären Nameserver die Seriennummer abfragen um Änderungen zu erkennen. RIPE-NCC-Empfehlung 86400 = 24 Stunden
Retry	Nach ausbleibender Antwort soll nach x Sekunden beim Primary Nameserver nachgefragt werden. Muss < als Refresh sein. RIPE-NCC-Empfehlung 7200 = 2 Stunden
Expire	Nach dieser Zeit in Sekunden soll bei ausbleibender Antwort vom Primary Nameserver nicht mehr auf Zonenabfragen geantwortet werden. Muss größer sein als 2 von Refresh + Retry
TTL	Time to Live für negatives Caching. RIPE-NCC-Empfehlung 172800 = 2 Tage

IPv4 DynDNS

Bei DDNS gibt es die Möglichkeit die Einträge des Name Servers dynamisch zu ändern oder zu ergänzen. Bei einer Serveranbindung über xDSL ergibt sich durch die dynamischen IP-Adresszuweisungen das Problem, dass alte DNS-Einträge auf dem Name Server ins Leere zeigen und bei der Namensauflösung die falschen Adressen zurück liefern.



Stand: 27.11.2022

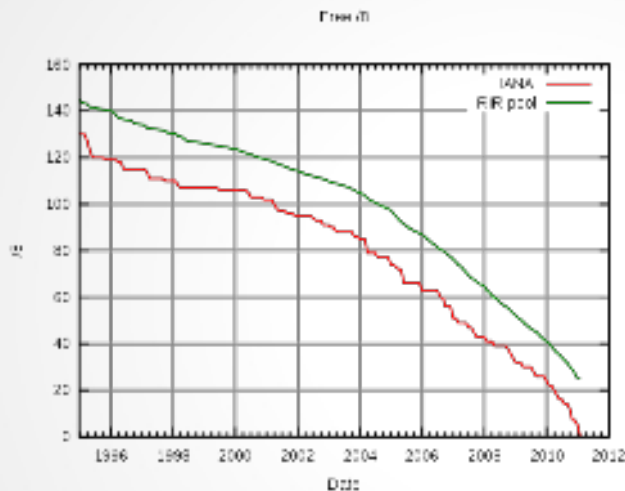
Netztechnik Teil-9

Folie: 57:78

1.
Der Provider Teilt dem Router seine im Internet gültige IP-Adresse mit.
2.
Der Router teilt seine neue IP-Adresse dem DynDNS-Server mit.
3.
Ein Client will auf anton.dyndns.org zugreifen.
Für die Namensauflösung wendet er sich an den DynDNS.
4.
Der DynDNS-Server teilt die aktuelle IP-Adresse dem Client mit.
5.
Nun kann der Client auf den Server über den Router mit Firewall zugreifen.
- (6.)
Wird dem Router eine neue IP-Adresse mitgeteilt, meldet er diese wiederum an den DynDNS-Server.

IPv6 Einführung

$2^{32} = 4.294.967.296$ IPv4-Adressen
 $2^{128} = 340.282.366.920.948.463.374.607.431.768.21.456$ IPv6-Adressen



Seit 2009 gibt es beim RIPE NCC unter dem Link <http://www.ripe.net/ripe/docs/ripe-373.html> die Möglichkeit providerunabhängige IPv6-Adressblöcke (IPv6 End User Site Assignment Request Form) zu beantragen.

Stand: 27.11.2022

Netztechnik Teil-9

Folie: 58:78

- Außer der Lösung der Adressenverknappung gibt es weitere Vorteile, die durch den Einsatz von IPv6 zum Tragen kommen:
Wegfall von NAT und allen in diesem Zusammenhang stehende Probleme
- Effizientere Ausnutzung von Netzwerkressourcen durch kürzere
- Paketbearbeitungszeiten und verbesserte Fragmentierungsregeln.
- Durch den bereits implementierten Einsatz von IPsec wird die Sicherheit verbessert.
- Erweiterung der Always-On-Funktionalität erhöht für mobile Enduser die Erreichbarkeit
- Durch die Einführung von Flow-Labels wird QoS (Quality of Service) ermöglicht, was den Einsatz von Multimedia-Anwendungen wie z.b. interaktives internetbasiertes Fernsehen.
- Autokonfiguration von Endgeräten
- Flexible Sensornetze für z. B. Krisensituationen oder Gebäudemanagement
- Internet der Dinge (Z. B. Vehicle-to-X)

IPv6 Terminologie

Das **Internet4** ist der über IPv4 erreichbare Teil des Internets und das **Internet6** ist der über IPv6 erreichbare Teil.

Ein **Node** ist ein Gerät, das über ein oder mehrere **Interfaces**, an einem oder mehreren Netzwerken angeschlossen ist.

Ein **Router** ist ein spezieller Node.

Er besitzt Routing-Eigenschaften und kann damit den Netzwerk-Verkehr über Netzwerk-Grenzen hinweg ermöglichen.

Ein **Host** ist ein Node ohne Routing-Eigenschaften.

Ein **Interface**, oder auch **Link**, ist die Verbindung zum Netzwerk.

Alle weiteren an diesen Link angeschlossenen Nodes sind **on-link** und damit Nachbarn (**Neighbours**).

Nodes, die nicht direkt erreicht werden können (etwa nur über eine Router), sind **off-link**.

IPv6 Header

Version (4Bit)	Traffic Class (8Bit)	Flow-Label (20Bit)	
Payload (16Bit)		Next Header (8Bit)	Hop Limit (8Bit)
Source Address (128Bit)			
Destination Address (128Bit)			
Data			

Name	Länge in Bit	Bedeutung
Version	4	Versionskennung. Hat immer den Wert 6
Traffic Class	8	Die Traffic Class entspricht dem TOS (Type of Service unter IP-V4). Werte von 0 bis 7 werden für den lastgesteuerten Datenverkehr verwendet. Werte von 8 bis 15 sollen für Echtzeit Datenverkehr verwendet werden
Flow Label	20	Dient zur Kennzeichnung eines „Flows“
Payload Length	16	Gibt die Datenmenge in Bytes an, die den Header folgen. Hier ist eine Datenmenge bis 64 kByte möglich. Die Jumbo Payload-Option erlaubt Datagramme bis 4 GByte
Next Header	8	Hier wird die nächsthöhere Protokollschicht angegeben.
Hop Limit	8	Der Inhalt dieses Feldes wird bei jeder Übertragung durch Router um 1 decrementiert. Wird der Wert 0 erreicht, dann wird das Paket verworfen.
Source-Adresse	128	Quell-Adresse. Der Adress-Aufbau folgt.
Destination-Adresse	128	Ziel-Adresse. Der Adress-Aufbau folgt.
Data		Zu übertragene Daten, die dem Header folgen

IPv6

Unterschiede im Header im Vergleich zu IPv4

Fragmentation/Reassembly

Eine Fragmentierung gibt es bei IPv6 nicht.

Zu große Pakete werden von den Routern verworfen und müssen deshalb bereits beim Sender richtig dimensioniert werden.

Dazu sendet der Router ein ICMPv6-Paket an den Absender und teilt ihm mit, dass die Paketgröße kleiner zu wählen ist.

Die minimale MTU-Size wird von 576 Bytes bei IPv4 auf 1280 bei IPv6 angehoben.

Die Ermittlung der maximal möglichen MTU-Size, also der MTU-Size entlang des gesamten Weges vom Sender zum Ziel, dem so genannten MTU-Path, gewinnt hiermit an Bedeutung.

Checksumme

In der unterlagerten Schicht wurde bereits eine Checksumme bearbeitet.

Dies wäre eine redundante Bearbeitung. Die Checksummen-Bearbeitung müsste jedes mal, wenn der Next-Hop-Wert dekrementiert wird, ebenfalls durchlaufen werden.

Dies reduziert die Latenzzeiten (Durchlaufzeit vom Empfang bis zum weiter senden) in den Routern.

Optionen

Optionen werden durch einen Extension-Header möglich der im Next Header Feld eingetragen wird.

IPv6 Optionen

Optionen werden durch einen Extension-Header möglich, der im Next Header Feld eingetragen wird.

Name	Typ	Größe	Beschreibung	RFCs
Hop-By-Hop Option	0	variabel	Enthält Optionen, die von allen IPv6-Geräten, die das Paket durchläuft beachtet werden müssen. Wird für Jumbograms verwendet.	2460 2675
Routing	43	variabel	Durch diesen Header kann der Weg des Paketes durch das Netz beeinflusst werden. Anwendungsfall Mobile IPv6.	2460 3775 5095
Fragment	44	64 Bit	Parameter für eine Fragmentierung	2460
Authentication Header (AH)	51	variabel	Enthält Daten zur Sicherstellung der Vertraulichkeit des Paketes	4302
Encapsulation Security Payload (ESP)	50	variabel	Dient zur Verschlüsselung des Paketes	4302
Destination Options	60	variabel	Enthält Optionen die vom Zielrechner des Paketes beachtet werden müssen.	2460
No Next Header	59	leer	Platzhalter für den letzten Extension-Header	2460

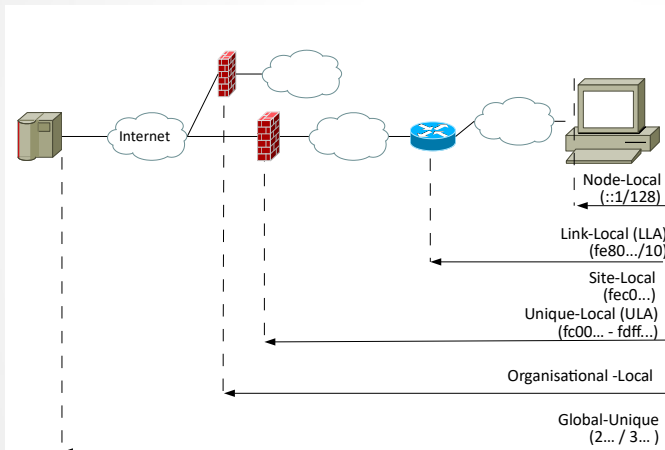
IPv6 Scope

Scope

Im Unterschied zu IPv4 haben IPv6-Nodes mehrere IP-Adressen.

Das sind sowohl Unicast als auch Multicast-Adressen.

Jede dieser Adressen hat einen Scope, um zu beschreiben, in welchen Teilnetzen oder Netzbereichen die Adresse ihren Gültigkeitsbereich und damit auch ihre Reichweite, hat. Dieser Scope kann die folgenden folgende Bereiche festlegen:



Der Scope kann die folgenden folgende Bereiche festlegen:

- Node Local Scope
- Link Local Scope
- Site Local Scope
- Unique Local Scope
- Unique Globally Scope

Stand: 27.11.2022

Netztechnik Teil-9

Folie: 63:78

Node Local Scope

Diese Adressen gelten nur innerhalb des Nodes.

Link Local Scope

Diese Adressen sind nicht routebar und haben nur am Netzwerk-Link eine Bedeutung. Sie sind durch den Präfix: **fe80::/10** zu erkennen.

Site Local Scope

Diese Adressen sind routebar, allerdings nur bis zum Border-Router der Site. Damit entsprechen sie den RFC1918-Adressen von IPv4.

Ursprünglich war für diese Adressen der Präfix: **fec0::/10** vorgesehen. Wegen Problemen sollten sie allerdings nicht mehr im Einsatz sein (siehe RFC3879). Ihren Platz nehmen die Unique Local Adressen (ULAs) ein.

Unique Local Scope (ULA, RFC 4193)

Diese Adressen sind im Internet routebar und habenden Präfix: **fc00::/7**. Darin ist eine 40 Bit lange Global ID enthalten. Um Kollisionen zwischen den ULA-Netzen zu vermeiden, müssen Site Local Scope Adressen unterschieden werden können. Dazu muss die Global ID zufällig gesetzt sein.

Unique Globally Scope

Diese Adressen werden im Internet geroutet und können dort auch verwendet werden.

IPv6 Aufbau der Adresse

Der wichtigste und gebräuchlichste Adress-Aufbau ist der in RFC 3587 beschriebene globale Unicast-Adresse, der eine Adresse in einer allgemeinen Form beschreibt.

64 - n Bits	n Bits	64 Bits
Global Routing Präfix	Subnetz-ID	Interface ID

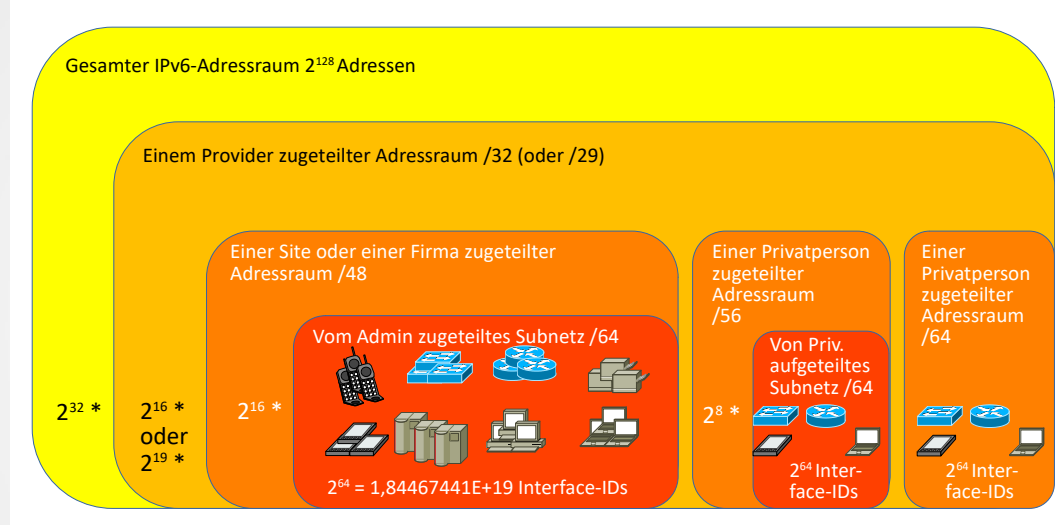
Der Global Routing Präfix entspricht dem Netzwerk-Teil einer IPv4-Adresse und legt ein international eindeutig gültiges, an ein weltweites Internet anschließbares Netzwerk fest.

Die Subnetz-ID bestimmt die Unterteilung in interne Sub-Netze, die für das öffentliche Internet ohne Belang sind.

In der Praxis hat sich die Real-World-Struktur durchgesetzt dabei ist der Global Routing Präfix auf 48 Bit festgelegt und die Subnetz-ID auf 16 Bit. Die Interface-ID hat 64 Bits.

48 Bits	16 Bits	64 Bits
Global Routing Präfix	Subnetz-ID	Interface ID

IPv6 Aufteilung der Adressen



Stand: 27.11.2022

Netztechnik Teil-9

Folie: 65:78

Derzeit steht ein Achtel der möglichen Adressen zur Verteilung zur Verfügung. Der Rest ist einer künftigen Verteilung vorbehalten.

Ein Internet Service Provider (ISP) bekommt normalerweise ein /32-Bereich zugeteilt. In begründeten Fällen ist auch ein /29-Bereich möglich.

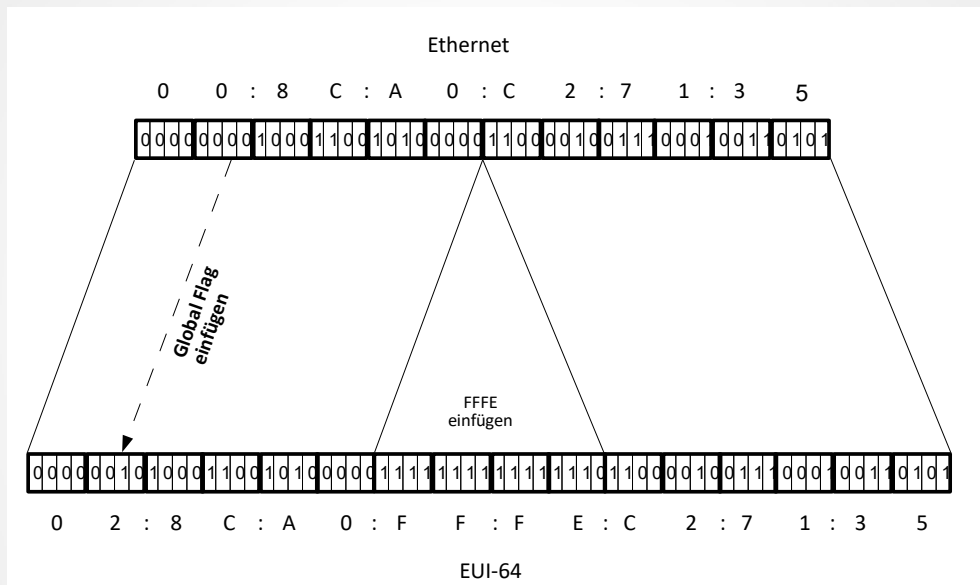
Vergibt der Provider seinem Kunden ein /48-Bereich kann er (falls er einen /29-Bereich bekommen hat) 2^{19} Kunden mit Netzwerken ausstatten.

Vergibt ein Provider einer Privatperson einen /56-Bereich könnte er 2^{27} Privatpersonen mit Netzwerken ausstatten.

Letztendlich stehen in jedem Subnetz 2^{64} Interface-IDs zur Verfügung, die direkt miteinander kommunizieren können.

IPv6

Aufbau der EUI-64-MAC-Adresse



IPv6

Unterschiede bei den IP-Adressen

Es gibt keine Broadcast-Adressen mehr!

Die Funktionalität der IPv6-Broadcast-Adressen wurden von der IPv6-Multicast-Adresse Link-Local-All-Nodes-Multicast-Address ff02::1 übernommen.

In IPv6 sind „All-0“ = „**All Zeros**“ und „All-1“ = „**All Ones**“ zunächst **zulässige Werte für Adressen**.
Die vollständige „All-0“ und „All-1“ über alle Felder sind nach wie vor ungültig!

Speziell Präfixe (also die vorderen Teile einer Adresse) können Felder mit Nullen enthalten.
Wichtig für den Beginn der Datenkommunikation ist die Interface ID innerhalb der IPv6-Adresse.
Sie wird aus der MAC-Adresse gebildet.
Alle anderen vorangestellten Teile lassen sich später ermitteln.

IPv6-Adressen werden den Schnittstellen (Interfaces) zugewiesen. Nicht den Knoten (Nodes)!

Da jede Schnittstelle zu einem Knoten gehört, kann jede Schnittstellen-Unicast-Adresse dazu verwendet werden den Knoten zu bezeichnen.

Alle Schnittstellen müssen mindestens eine „Link-Local-Unicast-Adresse“ haben.

Damit kann eine Schnittstelle mehrere Adressen von jedem Typ (Uni-, Any- oder Multicast) oder Scope haben.

Unicast Adressen mit mehr als der Link-Scope-Adresse werden als Ziel- oder Quell-Adresse nicht benötigt.

Damit kann innerhalb eines Netzwerks kommuniziert werden.

Dies ist vor allem für Punkt-zu-Punkt-Verbindungen angenehm.

Ausnahme:

Eine Unicast-Adresse oder reine Menge von Unicast-Adressen können zu mehreren Schnittstellen zugewiesen werden, wenn die Implementierung für alle darüber liegenden Schichten die Schnittstellen als eine einzige Schnittstelle behandelt.

Dies ist nützlich für Loadsharing (deutsch: Last-Teilung) über mehrere physikalische Schnittstellen.

IPv6 Aussehen einer Adresse

Die bevorzugte Form

x:x:x:x:x:x:x

wobei x eine 16Bit-Hexadezimalzahl ist. Buchstaben (a,b,c,d,e,f) werden immer klein geschrieben.

So sieht eine IPv6-Adresse beispielsweise so aus.

fedc:ba98:7654:3210:fedc:ba98:7654:3210

oder

1080:0:0:0:8:800:200c:417a

Führende Nullen innerhalb eines 16-Bit-Feldes können weggelassen werden.

Darstellung langer 0-Ketten

Bei langen 0-Ketten ist es möglich, eine beliebig lange Folge von Nullen mit „::“ zu beschreiben

Diese Möglichkeit besteht pro Adresse jedoch nur einmal!

Damit sind folgende Adress-Beispiele mit unterschiedlichen Schreibweisen möglich.

Ausgeschriebene Form	Komprimierte Form	Bedeutung
1080:0:0:0:8:800:200C:417a	1080::8:800:200C:417a	Unicast-Adresse
ff01:0:0:0:0:0:0:101	ff01::101	Multicast-Adresse
0:0:0:0:0:0:0:1	::1	Loopback-Adresse
0:0:0:0:0:0:0:0	::	Unspezifizierte Adresse

IPv6

Aussehen einer IPv4-Adresse

Unter IPv6 genutzte IPv4 -Adressen

x:x:x:x:d.d.d.d

x entspricht einem 16-Bit-Hexadezimalwert (0 – FFFF) auf der höherwertigen Seite der Adresse.

d entspricht einem 8-Bit-Dezimalwert (0 – 255) auf der niederwertigen Seite der Adresse.

Diese Schreibweise dient nur der internen Darstellung und wird nie als Quell- oder Zieladresse versendet!

0:0:0:0:0:d.d.d.d

Beispiel:

::abba:815 = 0:0:0:0:0:171.186.8.21 = ::171.186.8.21

IPv4-mapped IPv6-Adresse

Hierbei sind die ersten 80 Bits auf 0 gesetzt.

Danach werden die nächsten 16 Bits auf 1 gesetzt.

Beispiel:

Ausgeschriebene Form

0:0:0:0:0:ffff.129.144.52.38

Komprimierte Form

::ffff.129.144.52.38

IPv6 Adress-Präfix

Bedeutung

Mit einem Präfix oder Format-Präfix werden Adressen näher spezifiziert.
So können Klassen oder Typen näher beschrieben werden.

Adress-Präfix-Schreibweise

Die Schreibweise entspricht der aus IPv4 bekannten CIDR-Schreibweise mit dem Schrägstrich.
Dargestellt wird die Adresse sowie eine Längenangabe getrennt mit dem Schrägstrich:

<IPv6-Adresse> / <Präfixlänge in Bits>

IPv6 Adress-Präfix

Bedeutung	Präfix in Binärschreibweise	Präfix in Hexadezimal
Unspezifizierte Adresse (RFC4291)	0000 0000	::/128
Loopback-Adresse (Entspricht 127.0.0.1 in IPv4) (RFC4291)	0000 0001	::1/128
Reserviert oder spezifisch	0000 0000	0000::/8
Reserviert für NASP Belegung	0000 0010	0200::/8
Nicht zugewiesen (ehemals für IPX reserviert)	0000 0100	0400::/8
Aggregierbare globale Unicast-Adresse	0010	2000::/3
Teredo (RFC 4380)	0010 0000 0000 0001 0000 0000 0000 0000	2001::/32
Benchmarking	0010 0000 0000 0001 0000 0000 0000 0010 0000 0000 0000 0000	2001:2::/48
ORCHID (RFC4843)	0010 0000 0000 0001 0000 0000 0001 0000	2001:10::/28
Documentation (RFC 3849)	0010 0000 0000 0001 1101 1011 0001 0000	2001:db8/32
6to4-Adresse	0010 0000 0000 0010	2002::/16
Unique Local (Entspricht den RFC 1918-Adressen in IPv4) (RFC 4193)	1111 1100	fc00::/7
Link-Local Unicast-Adresse entspricht 169.254.0.0 unter IPv4 (APIPA) (RFC4291)	1111 1110 1000 0000	fe80::/10
Site-Local Unicast-Adresse	1111 1110 1100 0000	fec0::/10
Multicast-Adresse entspricht 224.0.0.0/4 bei IPv4 (RFC4291)	1111 1111 0000 0000	ff00::/8
IPv4-Mapped-Adresse (RFC4038)	0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 1111 1111 1111 1111 0000 0000	::ffff:0:0/96
IPv4 compatible Adresse (RFC 4291)	0000 0000	::/96

Stand: 27.11.2022

Netztechnik Teil-9

Folie: 71:78

Übersicht der vorgeschriebenen Adressen

Laut RFC 4291 muss jeder Node, an jedem Interface, die folgen den Adressen erkennen können:

- Loopback-Adresse
- Eine Link-Local-Adresse
- Die Link-Local-All-Nodes-Multicast-Adresse
- Alle Unicast- oder Anycast-Adressen, die dem Interface zugewiesen wurden
- Für jede Unicast- oder Anycast-Adressen die zugehörige Link-Local-Solicited-Node-Multicast-Adresse
- Die Multicast-Adressen denen das Interface angehört

Für Router gilt zusätzlich:

- Die Subnet-Router-Anycast-Adresse für jedes Interface mit Routing-Funktionalität
- Alle Anycast-Adressen für die der Router konfiguriert wurde
- Die Link-Local- und die Site-Local-All-Routers-Multicast-Adresse (ff02::2 und ff05::2)

IPv6 Multicast-Adressen

Aufbau von Multicast-Adressen

Laut RFC4291 bauen sich Multicast-Adressen unter IPv6 folgendermaßen auf:

ff0s:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX

Dabei steht s für den Scope:

Wert (s)	Scope	Bedeutung
1	Node Local	Multicast Loopback
2	Link Local	Nicht routebar. Nur am betreffenden Link gültig
4	Administration Local	Administrativ zusammenhängende Netzwerke innerhalb einer Site
5	Site Local	Alle Netzwerke eine Site
8	Organisational Local	Alle Netzwerke einer Organisation
e	Global	Global Routing fähig

Ausschnitt:

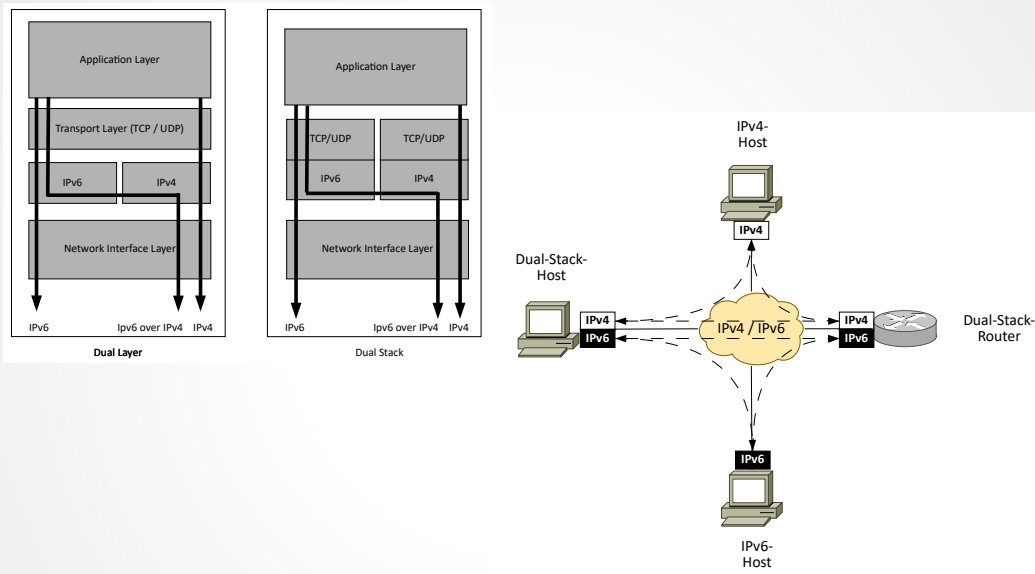
Wert (X)	Bedeutung	Gültig in Scope			
		1 (Node Local)	2 (Link Local)	5 (Site Local)	X (All Scopes)
::1	All Nodes	X	X		
::2	All Routers	X	X	X	
::4	DVMRP-Routers		X		
::5	OSPF/IGMP		X		
::6	OSPF/IGMP Designated Routers		X		
::7	ST Routers		X		
::8	ST Hosts		X		
::9	RIP Routers		X		
::A	EIGRP Routers		X		

IPv6

Weitere Protokolle im Umfeld von IPv6

Protokoll	Beschreibung
ICMPv6	Internet Control Message Protocol RFC2463. Diesem Protokoll kommt eine zentrale Bedeutung zu. Es darf von Firewalls nicht mehr geblockt werden wie bei IPv4.
DNSv6	Domain Name Service RFC3596
NDP	Neighbour Discovery Protocol. Damit wird das ARP-Protokoll abgelöst.
DHCPv6	Dynamic Host Configuration Protocol RFC3315
RIPng for IPv6	Routing Information Protocol RFC2080
OSPF for IPv6	Open Shortest Path First RFC2740

Übergang von IPv4 zu IPv6



ICMPv6

ICMPv6 wurde als Ergänzung für IPv6 entwickelt.
Ihm kommt mehr Bedeutung und Funktionalität als bei der IPv4-Version zu.
So wurden die Protokolle ARP und RARP in ICMPv6 integriert.
Deshalb dürfen ICMPv6-Pakete nicht mehr grundsätzlich von Firewalls geblockt werden.

Folgende Funktionen werden behandelt:

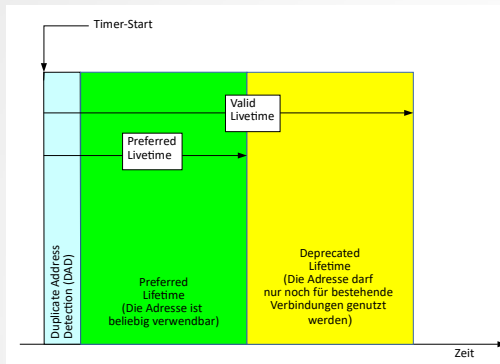
- Fehlermeldungen
- Informationsmeldungen

Typ-Feld-Wert	Fehlermeldung	Code-Feld-Wert
1	Destination unreachable	0 = No Route to Destination 1 = Communication administratively prohibited 2 = Not Assigned 3 = Address unreachable 4 = Port unreachable
2	Packet too big	0
3	Time Exceeded	0 = Hop-Limit exceeds 1 = Fragment-Reassembly-Time exceeded
4	Parameter-Problem	0 = Fehlerhaftes-Header-Feld 1 = Unbekannter Next-Header 2 = Unbekannte IPv6-Option

Typ-Feld-Wert	Information
128	Echo Request
129	Echo Reply
130	Multicast Listener Query
131	Version 1 Multicast Listener Report
132	Multicast Listener done
133	Router Solicitation Message
134	Router Advertisement Message
135	Neighbour Solicitation Message
136	Neighbour Advertisement Message
137	Redirect Message
138	Router Renumbering
139	ICMP Node Information Query
140	ICMP Node Information Response
141	Inverse Neighbour Discovery Solicitation Message
142	Inverse Neighbour Discovery Advertisement Message
143	Version 2 Multicast Listener Report
144	Home Agent Address Discovery Request Message

.....

DHCPv6



Über RAs erzeugte IP-Adressen haben einen Valid-Lifetime. Das entspricht der Lease-Time von mit DHCP erzeugten IP-Adressen.

Die Valid-Lifetime ist die gesamte Gültigkeitsdauer von der Erzeugung bis zum Löschen.

Innerhalb dieses Zeitraums ist eine Adresse zuerst preferred danach deprecated.

Während der Preferred-Lifetime verwendet der Rechner diese IP-Adresse. Danach (während der Deprecated-Lifetime) wird die IP-Adresse nur noch für bestehende Verbindungen genutzt.

Nach Ablauf der Valid-Lifetime wird die IP-Adresse gelöscht.

Mit der Absender-Adresse des Routers wird gleichzeitig auch das Default Gateway festgelegt.

Unterstützen Router und Client die RDNS-Option (Recursive DNS Server) wie im RFC 6106 beschrieben, kann die Adresse des DNS-Servers auch über die RAs mitgeteilt werden.

Damit ist die Autokonfiguration mittels der Router-Advertisements (RA) abgeschlossen. Da die IP-Adressen der Clients nirgendwo gespeichert / verwaltet werden, heißt dieses Verfahren Stateless Address Autoconfiguration (SLAAC).

Die Router senden in regelmäßigen Zeitabständen die RAs an die Link-Local-All-Nodes-Multicast-Adresse (ff02::1), damit die Clients die Konfiguration auf dem neuesten Stand halten können.

Stand: 27.11.2022

Netztechnik Teil-9

Folie: 76:78

Das Dynamic Host Control Protocol musste im Rahmen des Umstiegs von IPv4 auf IPv6 eine Renovierung über sich ergehen lassen und bekam, passend zur Nummerierung von IP, auch die Version 6.

Ziel der Konzeption von IPv6 war eine automatische Vergabe von IP-Adressen, um eine rudimentäre Kommunikation zu ermöglichen. Dies wird in einem Autokonfigurationsvorgang durchgeführt.

Im Gegensatz zur Vorgängerversion von IP, ist für die Vergabe von IP-Adressen um im lokalen Netzwerk zu kommunizieren, ist kein DHCP-Service erforderlich. Dafür übernehmen die Router für die grundlegende Kommunikation eine aktive Rolle.

Autokonfiguration

Wird ein Client eingeschaltet, so durchläuft er die folgenden Schritte, um sich mit IP-Adressen zu versorgen.

Senden einer Router-Solicitation-Nachricht an die Link-Local-All-Routers-Multicast Adresse (ff02::2).

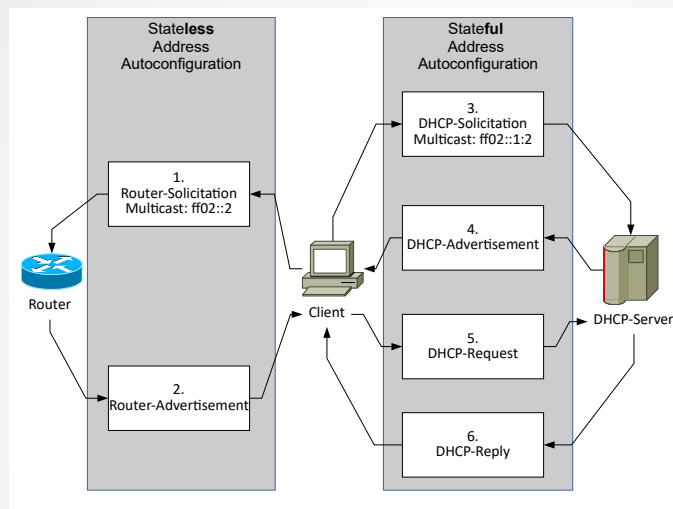
Ist ein Router im Netzwerk vorhanden, wird er mit einer Router-Advertisement Nachricht antworten.

Darin ist der globale IPv6-Präfix enthalten. Aus diesem Präfix kann der Client zusammen mit seiner MAC-Adresse und dem EUI-Verfahren (Extended Unique Identifier) seine global gültige IP-Adresse aufbauen.

Verwendet der Client die Privacy Extensions, wird zusätzlich zur globalen IP-Adresse (mit EUI-64-MAC-Adresse) eine temporäre IP-Adresse erzeugt. Dabei kommt anstelle der MAC-Adresse, ein vom Betriebssystem zufällig ermittelter Wert, für den Interface-Teil der IPv6-Adresse zum Einsatz.

Um sicher zu stellen, dass eine zufällig erzeugte IP-Adresse nicht bereits im Netzwerk existiert, wird mittels einer Duplicate Address Detection (DAD) die neu erzeugte IP-Adresse überprüft, bevor sie verwendet werden kann.

DHCPv6



Behandelte Themen

- Protokollfunktionen
- IPv4 (Protokoll / ARP / RARP / NAT / DHCP / ICMP / DNS)
- IPv6 (Protokoll / Unterschiede zu v4 / Übergänge von v4 zu v6 / ICMPv6 / DHCPv6)