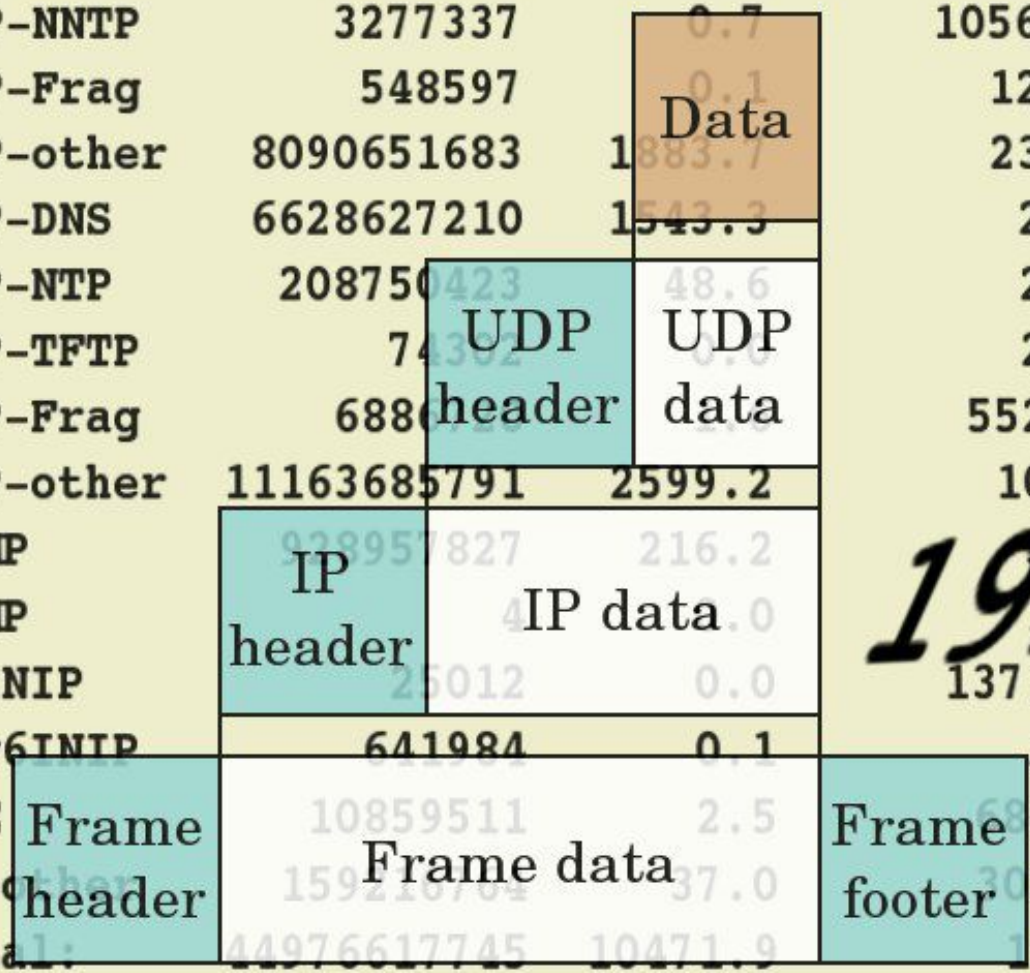
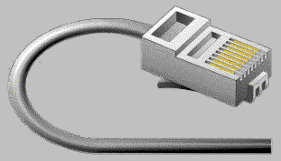
Protocol	Total Flows	Flows /Sec	Packets /Flow	Bytes /Pkt	Packets /Sec	Active(Sec) /Flow	Idle(Sec) /Flow
TCP-Telnet	3484677	0.8	87	111	70.9	23.6	22.7
TCP-FTP	127336721	29.6	20	66	599.2	7.0	27.6
TCP-FTPD	46489384	10.8	138	875	1493.7	2.1	29.3
TCP-WWW	15115628719	3519.3					
TCP-SMTP	2433340539	566.5					
TCP-X	43955166	10.2					
TCP-BGP	4179374	0.9	36	86	35.2	96.0	16.8
TCP-NNTP	3277337		1056	886	805.9	43.8	22.9
TCP-Frag	548597		12	170	1.6	7.1	25.6
TCP-other	8090651683		23	547	44836.9	8.0	24.9
UDP-DNS	6628627210		2	77	3290.9	2.0	30.0
UDP-NTP	208750		2	74	101.0	3.0	29.8
UDP-TFTP	74		2	214	0.0	1.3	29.3
UDP-Frag	688		552	588	886.1	34.5	23.9
UDP-other	11163685791	2599.2	10	272	28167.1	4.2	29.1
ICMP				77	788.2	5.4	28.0
IGMP			1	40	0.0	0.0	22.2
IPINIP			1371	137	7.9	43.8	21.2
IPv6INIP	641984	0.1	2	387	0.3	4.4	37.9
GRE	10859511	2.5	4	425	1731.7	73.3	19.3
IP-other			2	426	11222.5	56.3	21.0
Total:			16	538	167638.2	4.6	25.9

TCP/IP Protokoll Suite
Skript Kapitel 5ff



192.0.2.5/24



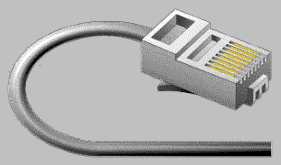
TCP/IP Protocol Suite

TCP/IP Protokoll-Sammlung

Überblick

welche Protokolle gehören dazu
welche Aufgaben haben diese Protokolle
welche Schichten decken diese Protokolle ab

Kapitel 4 / Seite 32

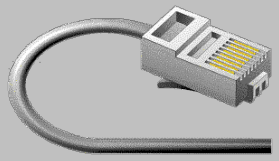


TCP/IP Protocol Suite

Die TCP/IP Protokoll Suite ist wie das OSI-Modell Layer basiert.

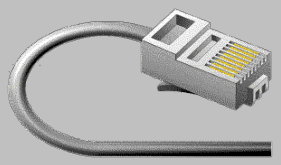
Die Layer 1 und 2 sowie die Layer 5 bis 7 sind jeweils zusammen gefasst

OSI Modell		TCP Modell
7	Application	Application Layer
6	Presentation	
5	Session	
4	Transport	Transport Layer
3	Network	Network Layer
2	Data-Link	Network Interface Layer
1	Physical	



TCP/IP Protocol Suite

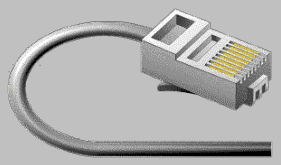
OSI Modell		TCP Modell	Protokolle
7	Application	Application Layer	HTTP, FTP, SMTP, POP3, IMAP4, Telnet, ssh, DNS, NTP, BGP,
6	Presentation		
5	Session		
4	Transport	Transport Layer	TCP, UDP, ICMP, ...
3	Network	Network Layer	IP
2	Data-Link	Network Interface Layer	ARP, RARP
1	Physical		



TCP/IP Protocol Suite; Layer 2

ARP: **Address Resolution Protocol** (**ARP**) wird verwendet um die Ethernet MAC-Adresse einer IP-Adresse zu finden.

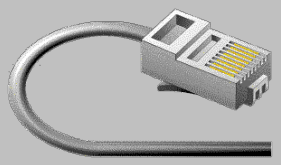
RARP: Ist eine Methode um einer Station eine IP anhand ihrer MAC-Adresse zu zuweisen. (RARP ist ein Vorgänger von BOOTP/DHCP)



TCP/IP Protocol Suite; Layer 3

IP: **Internet Protocol** (**IP**) ist ein **verbindungsloses** Protokoll, das verwendet wird, um Paket vom Transport Layer durch das Netz zu leiten.

IP ist ein routebares Protokoll.

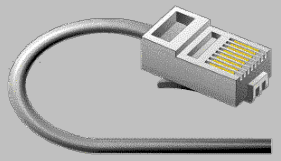


TCP/IP Protocol Suite; Layer 4

Im IP-Header ist eine Protokoll-Nummer enthalten, die angibt welches Protokoll die Daten im IP Paket angehören (analog dem Ethertype-Feld im Ethernet Header).

Protokoll-Nummern sind in der Datei `/etc/protocols` [1] abgelegt. Die Nummern werden von der IANA [2] vergeben und sind für alle IP Protokolle (IPv4 und IPv6) gültig.

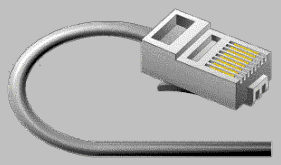
```
[1] windows: .../system/drivers/etc/protocol
[2] http://www.iana.org/assignments/protocol-numbers
```



TCP/IP Protocol Suite; Layer 4

ICMP: Internet Control Message Protocol (**ICMP**) (Protocol #1) ist ein **verbindungsloses** Protokoll, das verwendet wird um Information-, Status- oder Fehler-Meldungen zu übermitteln.

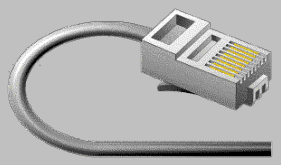
Mögliche Meldungen: Echo Reply, Destination unreachable, Source Quench, Echo Request, Time Exeeded, ...



TCP/IP Protocol Suite; Layer 4

TCP: Transmission Control Protocol (**TCP**) (Protocol #6) ist ein **verbindungsorientierts** Protokoll, das verwendet wird, um Daten gesichert durchs Netz zu transportieren.

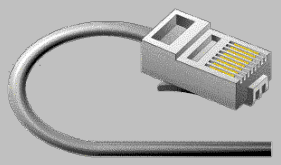
TCP garantiert, dass die Daten – in der gleichen Reihenfolge wie gesendet – ankommen.



TCP/IP Protocol Suite; Layer 4

UDP: User Datagram Protocol (**UDP**) (Protocol #17) ist ein **verbindungsloses** Protokoll, das verwendet wird, um Daten mit geringem Overhead durch das Netz zu transportieren.

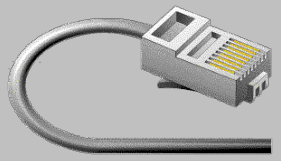
UDP kennt weder Flusskontrolle noch Fehlerkorrektur. Die Anwendungen müssen das selber erledigen!



TCP/IP Protocol Suite; Layer 4

Andere: Es gibt noch viele andere IP-Protokolle auf Layer 4.

Diese werden für spezielle Anwendungen verwendet:
Routing Protokolle (OSPF, EIGRP, ...),
IP-SEC (Encap Security Payload, Authentication Header),
vrrp, ...
Es ist für Firewall Konfigurationen nützlich zu wissen dass auch andere IP Protokolle als ICMP, UDP und TCP existieren!

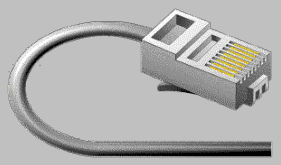


TCP/IP Protocol Suite; Layer 7

Applikationen:

Unzählige Applikationen verwenden IP ...

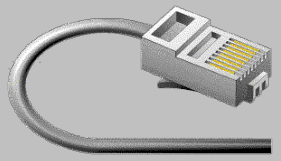
Jede Applikation muss – leider – selber dafür besorgt sein, dass der Empfänger die Daten richtig interpretieren kann!



TCP/IP Protocol Suite; Layer 7

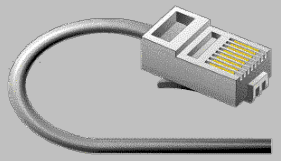
Applikationen:

Datentransfer:	FTP, TFTP, NFS, SMB/CIFS,
DruckDienste:	IPP, LPD
RemoteDienste:	Telnet, ssh, X11, RDP, ...
eM@il / News:	SMTP, POP3, IMAP4, NNTP
Web:	HTTP
Netzwerkdienste:	DHCP, BOOTP, DNS, NTP, Syslog, ...
Tunnel:	IPSEC, IPinIP, IPv6inIP, ...



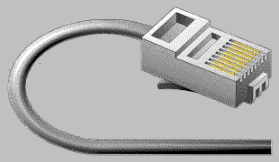
Verteilung der Protokolle

Protocol	Total Flows	Flows /Sec	Packets /Flow	Bytes /Pkt	Packets /Sec	Active(Sec) /Flow	Idle(Sec) /Flow
TCP-Telnet	2142021	0.4	22	163	11.1	34.4	25.4
TCP-FTP	69292174	16.1	25	57	417.7	5.7	26.9
TCP-FTPD	27762305	6.4	75	833	485.7	2.6	34.6
TCP-WWW	7684202068	1789.1	18	664	33002.4	4.1	29.9
TCP-SMTP	945875329	220.2	13	448	2985.4	7.2	29.1
TCP-BGP	2462947	0.5	24	101	13.8	112.5	19.4
TCP-NNTP	2043881	0.4	989	904	470.8	42.1	28.6
TCP-Frag	376749	0.0	4	250	0.3	5.5	30.6
TCP-other	4417559690	1028.5	18	525	19002.4	8.9	29.9
UDP-DNS	2088078323	486.1	2	76	1228.0	3.2	33.8
UDP-NTP	95496552	22.2	1	76	35.1	2.6	34.3
UDP-TFTP	165665	0.0	4	96	0.1	18.3	29.0
UDP-Frag	3223364	0.7	797	651	598.4	35.9	30.3
UDP-other	4579162977	1066.1	11	329	12189.0	4.9	32.9
ICMP	315821611	73.5	3	75	281.4	7.9	32.0
IGMP	9	0.0	1	34	0.0	5.9	32.0
IPINIP	5416	0.0	65	397	0.0	78.9	32.4
IPv6INIP	1482	0.0	4	313	0.0	1.4	42.3
GRE	3006667	0.7	609	393	426.7	106.7	23.2
IP-other	52845052	12.3	273	469	3364.7	67.6	25.1
Total:	**20308186365**	**4728.3**	**15**	**542**	**74554.4**	**5.6**	**31.0**



Paket Grösse

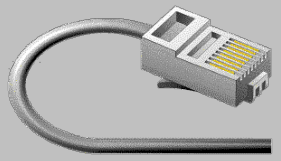
```
IP packet size distribution (720011M total packets):
   1-32   64   96  128  160  192  224  256  288  352
   .003 .395 .074 .038 .022 .011 .041 .006 .009 .004

    320  384  416  448  480  512  544  576 1024 1536
   .004 .004 .004 .004 .006 .006 .005 .015 .034 .306

   2048 2560
   .000 .000
```



Fragen ?

Didn’t we run out of IPv4 jokes?

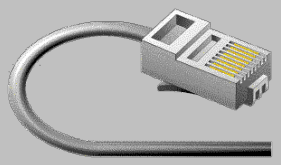
http://hardware.localhost.nl/



Internet Protokoll IP

Ziele

- Was sind routebare Protokolle
- IP-Adressen
  - Netzwerk-, IP-Adressen, Netzmasken
  - IP Mathematik



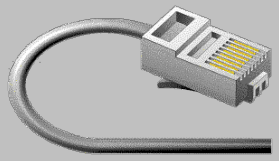
Routebare Protokolle

≠ Routing Protokolle!

Routebare Protokolle können zwischen lokalen und entfernten Adressen unterscheiden

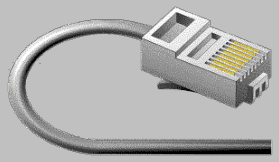
Routebare Protokolle kennen eine Netz-Hierarchie
Protokolle: IPv4, IPV6, Appletalk, IPX, ...

Nicht routebaren Protokollen fehlen diese Eigenschaften!
Protokolle: NetBEUI



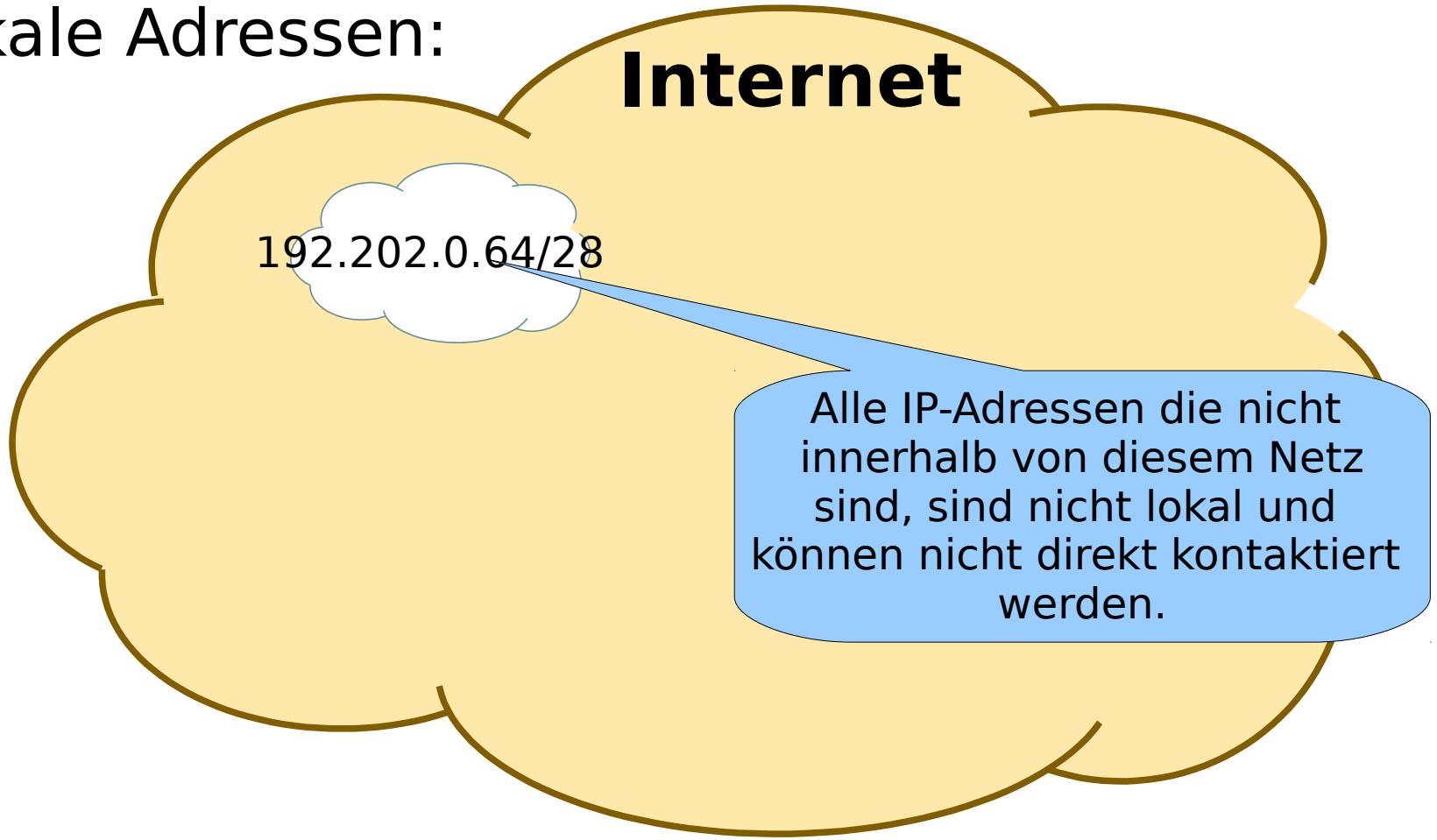
Internet Protokoll

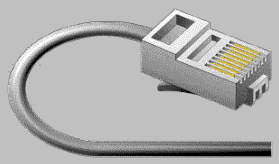
- Das Internet Protokoll IPv4 bzw. IPv6 ist route-bar.
- Routebare Protokolle unterteilen die Adressen in einen Netz-Teil und einen Host-Teil
- Der Host-Teil ist **lokal**, **direkt** erreichbar
- Der Netz-Teil ist **nur** via einem speziellen Gerät (Router, Gateway) erreichbar.
- Bei IPv4 / IPv6 ist die Trennung zwischen Netz- und Host-Teil variabel
- Bei IPv4 / IPv6 zeigt die Netzmaske wo die Trennung zwischen Netz- und Host-Teil liegt



Internet Protokoll

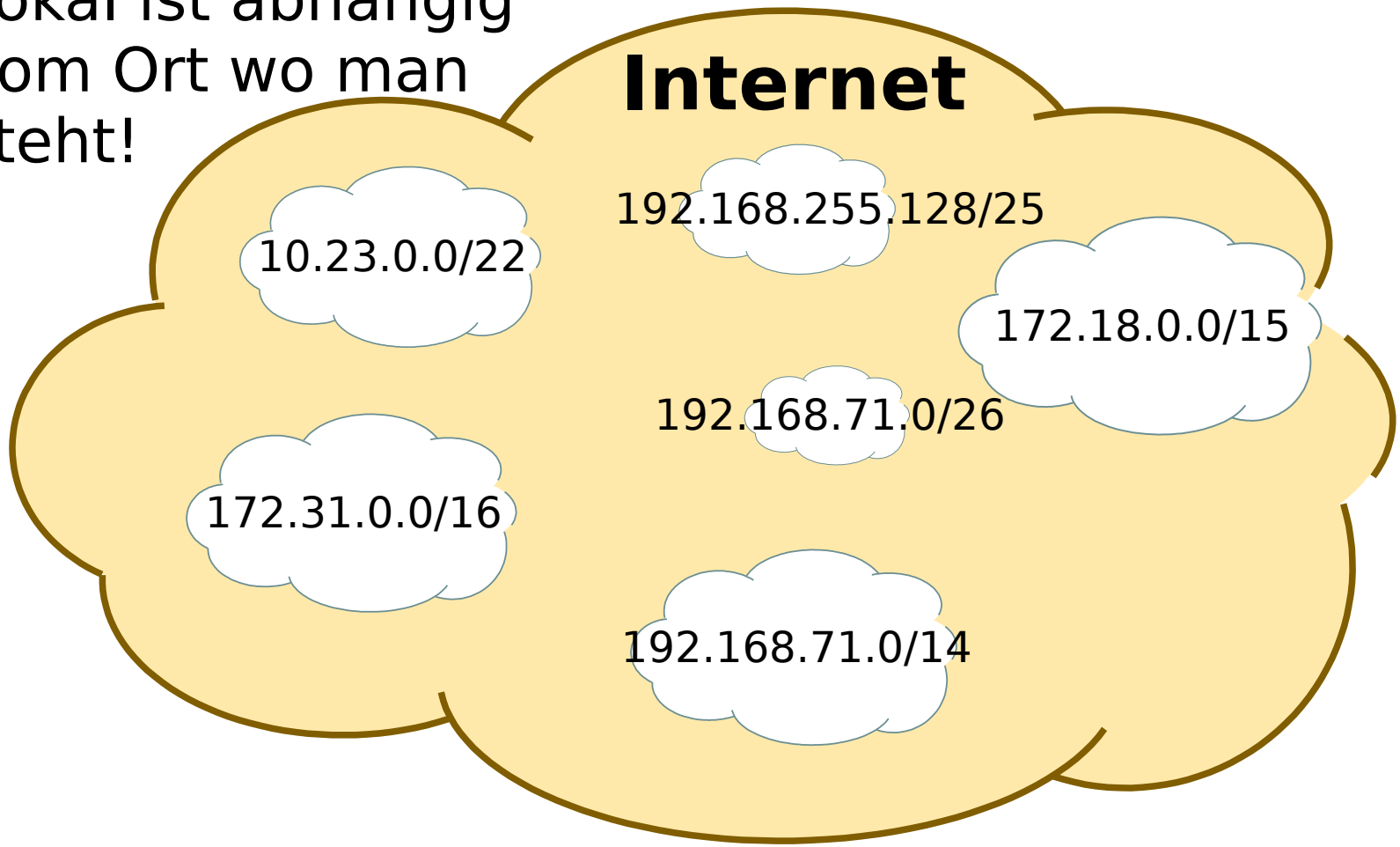
Lokale Adressen:

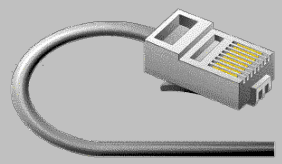




Internet Protokoll

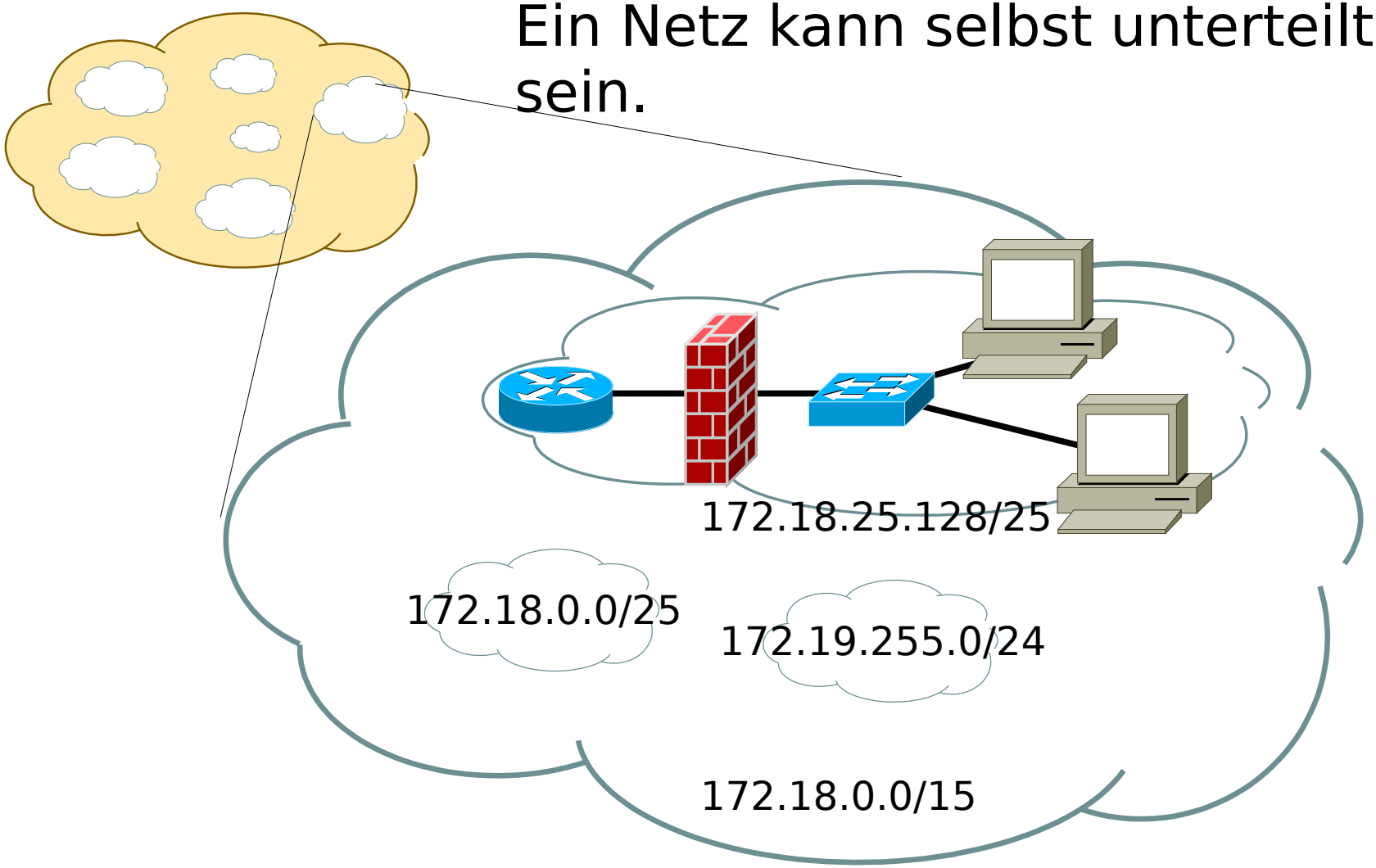
Lokal ist abhängig vom Ort wo man steht!

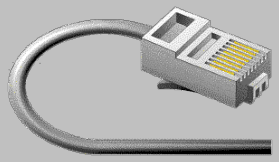




Internet Protokoll

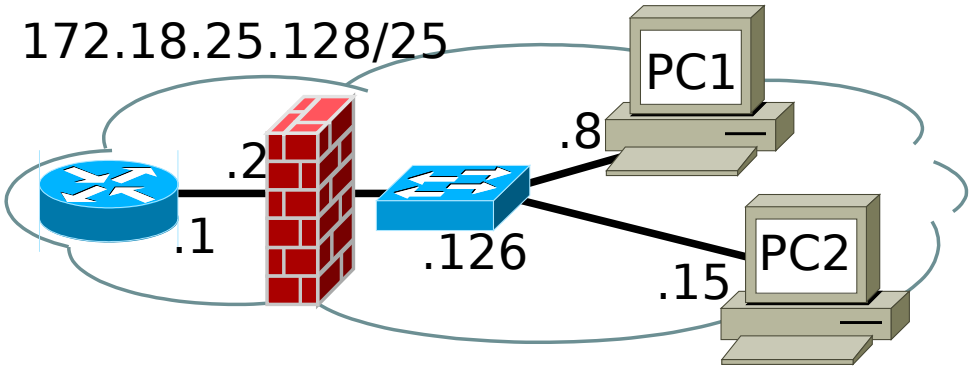
Ein Netz kann selbst unterteilt sein.





Internet Protokoll

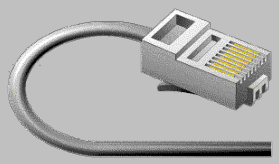
Die Host-Adresse adressiert den Host innerhalb des gegeben Netzwerkes



Router:	172.18.25.129/25
Firewall:	172.18.25.130/25
Switch:	172.18.25.254/25
PC1:	172.18.25.135/25
PC2:	172.18.25.143/25

Annahme: die Firewall ist transparent.

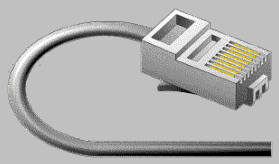
Die IP-Adresse wird aus der Netzwerk-Adresse und der Host-Adresse zusammen gesetzt!



Fragen ?

After dropping the packet the IP said it was my best effort.

http://hardware.localhost.nl/

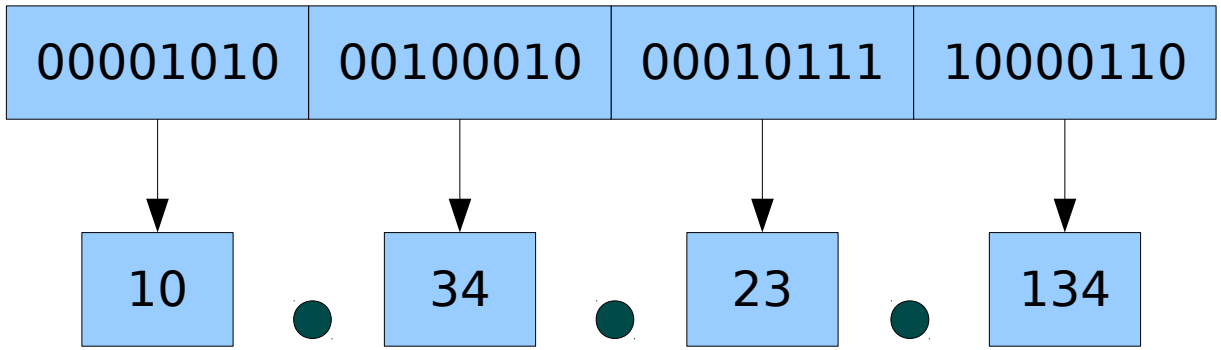


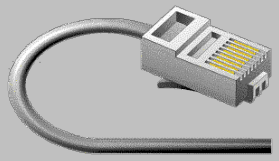
IP-Adressen

IPv4-Adressen sind 32Bit lang.

Jeweils 8Bit werden zusammen gefasst und als Dezimalzahl geschrieben.

Zwischen den Dezimalzahlen wird ein Punkt eingefügt.





Internet Protokoll

Zu Beginn wurden die Adressen in Klassen (A,B,C,D,E) unterteilt.

Die **Klassen A,B,C** werden für normale Anwendungen verwendet (mit Ausnahmen!).

Für jede Klasse (ABC) ist eine fixe Netzmaske definiert

1.0.0.0 – 126.255.255.255

128.0.0.0 – 191.255.255.255

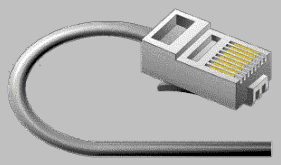
192.0.0.0 - 223.255.255.255

Die **Klasse D** ist für Multicast reserviert

224.0.0.0 - 239.255.255.255

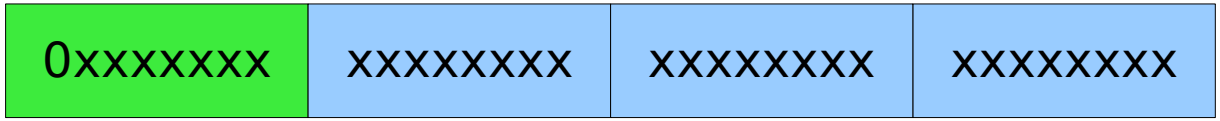
Die **Klasse E** ist für Experimente reserviert.

240.0.0.0 - 255.255.255.255



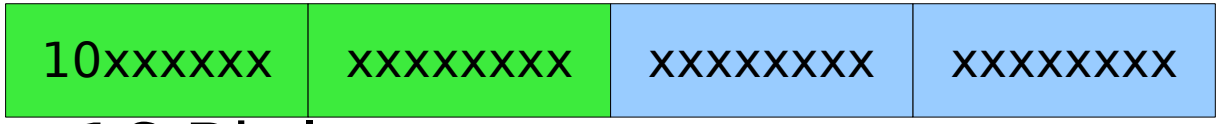
IPv4 Adressen – Classfull

Klasse A

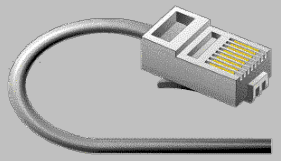


Die Netzadresse ist 8 Bit lang.
Die Hostadresse ist 24 Bit lang
Das erste Bit der IP-Adresse ist 0 (binär)
1.0.0.0 - 126.255.255.255
0.0.0.0 - 0.255.255.255 sowie 127.0.0.0 - 127.255.255.255 sind reserviert

Klasse B



Die Netzadresse ist 16 Bit lang.
Die Hostadresse ist 16 Bit lang
Die Netz-Adresse beginnt mit 10 (binär)
128.0.0.0 - 191.255.255.255

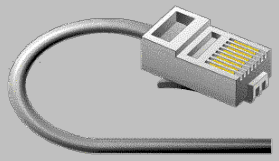


IPv4 Adressen – Classfull

Klasse C

110xxxxx	xxxxxxxx	xxxxxxxx	xxxxxxxx

Die Netzadresse ist 24 Bit lang.
Die Hostadresse ist 8 Bit lang
Das ersten Bits lauten 110 (binär)
192.0.0.0 - 223.255.255.255



Internet Protokoll – Classfull

Klasse D

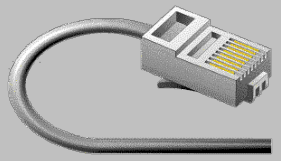
1110xxxx	xxxxxxxx	xxxxxxxx	xxxxxxxx

Das ersten Bits lauten 1110 (binär)
verwendet für Multicasts
Es gibt keine Netzmaske!
224.0.0.0 - 239.255.255.255

Klasse E

1111xxxx	xxxxxxxx	xxxxxxxx	xxxxxxxx

Die ersten Bits lauten 1111 (binär)
verwendet für Forschung / Experimente
Es gibt keine Netzmaske!
240.0.0.0 - 255.255.255.254

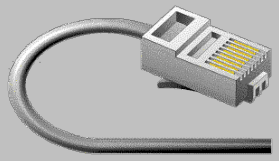


Internet Protokoll – Classfull

Übersicht

Class	Erstes Octet
A	1 - 126
B	128 - 191
C	192 - 223
D	224 - 239
E	240 - 255

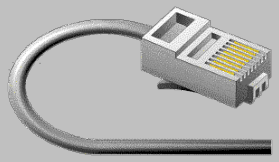
Das Netz 0.0.0.0/8 ist nicht verwendet!
Das Netz 127.0.0.0/8 ist für Loopback Interfaces und Loopback reserviert!



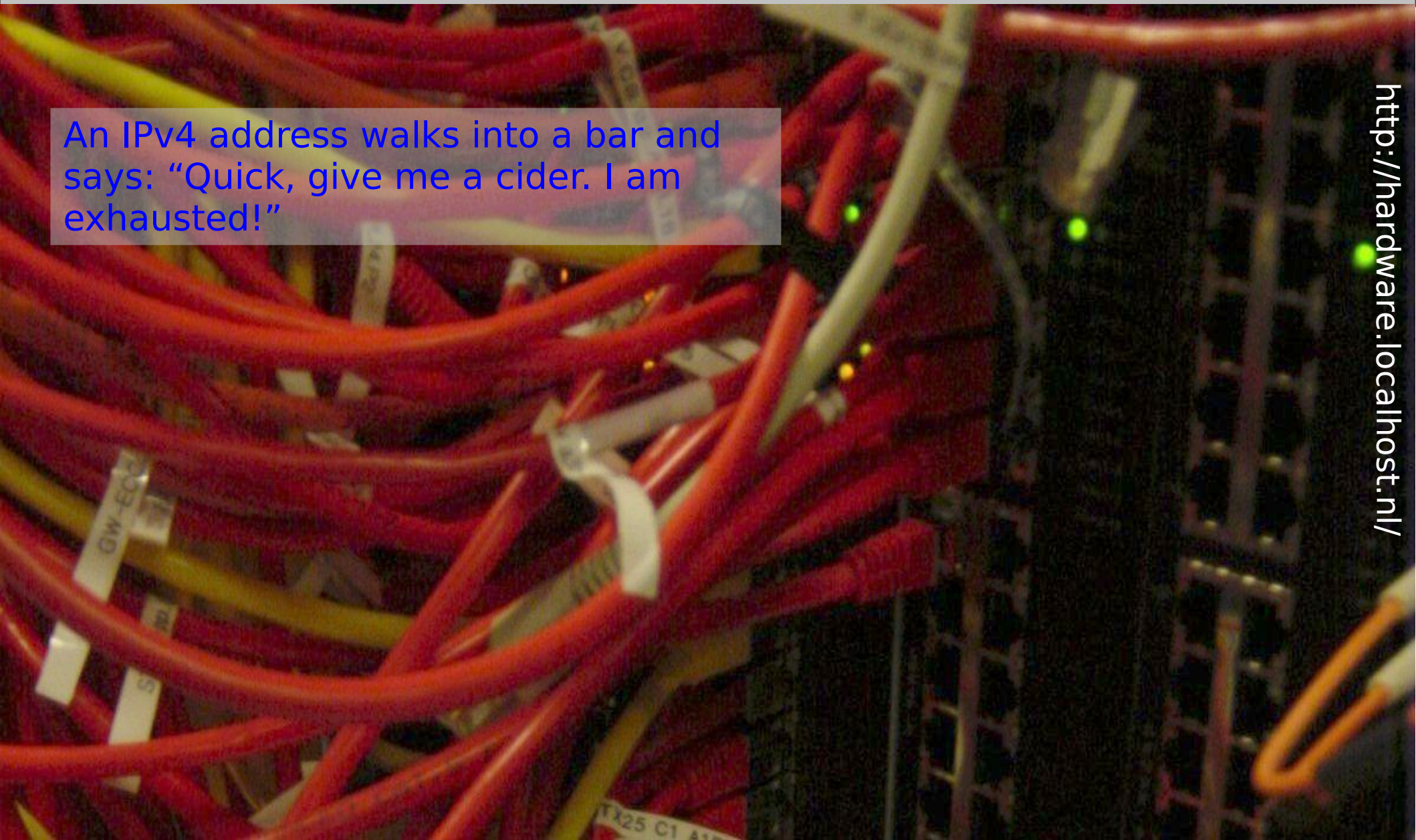
Internet Protokoll – Classfull

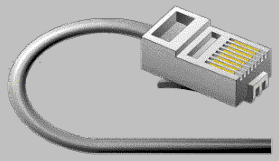
Übersicht

Class	Netze	Hosts
A	126	16'777'214
B	16'384	65'534
C	2'097-152	254
D	n/a	n/a
E	n/a	n/a



Fragen ?


An IPv4 address walks into a bar and says: “Quick, give me a cider. I am exhausted!”
http://hardware.localhost.nl/

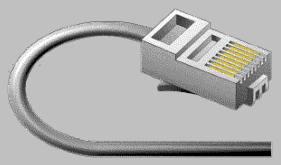


Internet Protokoll – Classless

Die starre Einteilung der Klassen hat sich als nitch zweckmässig erwiesen. Zu viele IP-Adressen sind blockiert und können nicht verwendet werden.

Die flexiblere Lösung **Classless Internet-Domain Routing** (CIDR) wurde 1993 eingeführt. Zu jedem Netz muss die Netzmaske bzw. die Grösse des Netzes angegeben werden.

CIDR und NAT/PAT hat den Verbrauch von IPv4 Adressen verlangsamt. Trotzdem steigt der IPv4 Bedarf weiterhin an.

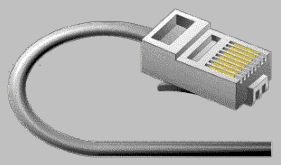


Internet Protokoll – Classless

CIDR erfordert, dass immer die Grösse des Netzes bzw. die Netzmaske angegeben wird – Dies ist notwendig, weil nicht mehr aufgrund der IP-Adresse alleine entschieden werden kann, wo die Grenze zwischen Netzwerk- und Host-Adresse liegt.

▶ Fehlt die Netzmaske bei einer Adresse, so wird die Netzmaske der entsprechenden Klasse angenommen werden.

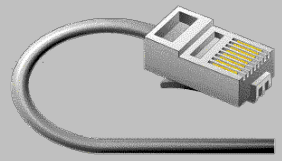
Geben sie **IMMER** die Netzmaske mit! Dadurch verhindern sie Fehler in den Konfigurationen!



CIDR Routen im Internet

In der globalen Routingtabelle sind vor allem CIDR Netze anzutreffen:

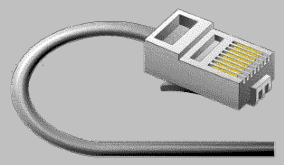
```
Network            Next Hop      Metric LocPrf Weight Path
* i3.0.0.0         139.4.71.37     9000    110      0 702 703 80 i
* i4.0.0.0         139.4.71.37     9000    110      0 702 701 3356 i
* i4.0.0.0/9       139.4.71.37     9000    110      0 702 701 3356 i
* i4.21.41.0/24    217.6.49.129   10000    100      0 3320 2914 16467 36806 i
* i4.36.200.0/21   217.6.49.129   10000    100      0 3320 3549 14135 i
* i4.67.64.0/22    217.6.49.129   10000    100      0 3320 6453 11608 19281 i
...
* i203.81.64.0/19  139.4.71.37     9000    110      0 702 701 2914 9988 i
* i203.81.96.0/21  139.4.71.37     9000    110      0 702 701 3491 9237 i
* i203.81.104.0/22 139.4.71.37     9000    110      0 702 701 3491 9237 i
* i203.81.108.0/22 139.4.71.37     9000    110      0 702 701 3491 9237 i
* i203.81.112.0/20 139.4.71.37     9000    110      0 702 701 4725 24289 i
* i203.81.128.0/19 139.4.71.37     9000    110      0 702 703 17608 i
* i203.81.160.0/20 217.6.49.129   10000    100      0 3320 2914 9988 18399 i
...
```



Netzmaske

Wie findet man die Netzwerk-Adresse von einer IP-Adresse?

- Die Netzwerk-Adresse ist immer am Anfang der IP-Adresse.
- Die Host-Adresse ist immer an Ende der IP-Adresse.
- Die Netzmaske gibt die Trennstelle zwischen Netz- und Host-Adresse an.



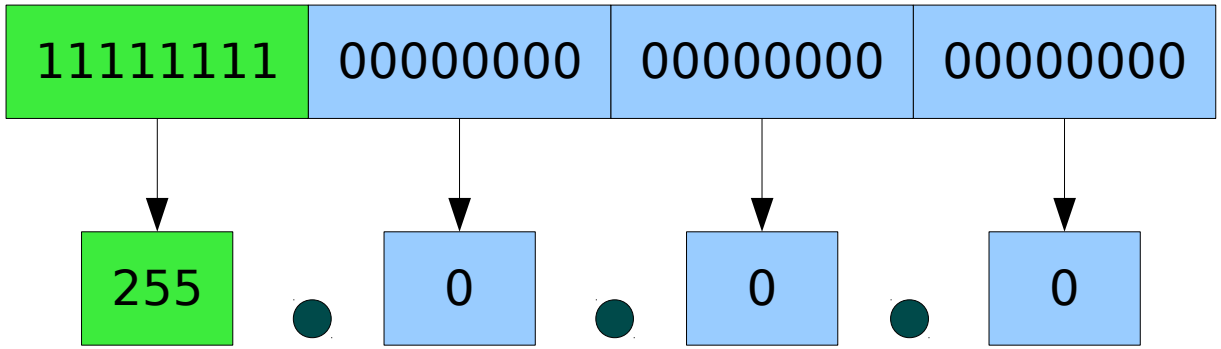
Netzmaske

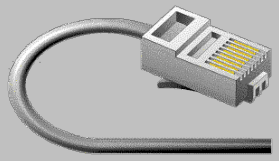
Die Netzmaske definiert wo die Grenze zwischen Netzwerk- und Host-Adresse liegt

Die Netzmaske ist wie die IPv4 Adresse 32Bit lang.

Der Netzwerk-Teil wird mit 1 markiert

Der Host-Teil wird mit 0 markiert



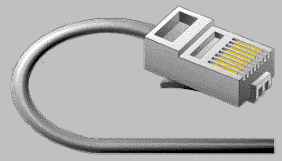


Netzmaske

Es gibt nur einen Netz- und einen Host-Teil.
Es darf nur einen Übergang von 1➔0 geben

11111111	00000000	00000000	00000000	OK
11111111	01111000	00000000	00000000	Falsch

Netzmasken können daher nur folgende Werte enthalten:
255, 254, 252, 248, 240, 224, 192, 128, 0



Netzmaske

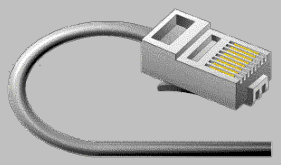
Die Netzmaske kann alternativ auch in der Slash-Notation angegeben werden.
Dazu werden die Anzahl der 1 in der Netzmaske hinter einem Slash (/) angegeben

11111111	1111	0000	00000000	00000000
11111111	00000000		00000000	00000000
11111111	11111111	11111111	11111111	

12x 1 ➔ **/12**

8x 1 ➔ **/8**

32x 1 ➔ **/32**



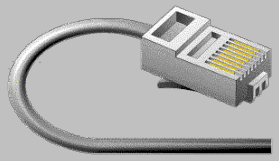
IP-Mathematik

Ist eine IP-Adresse und die dazugehörende Netzmaske bekannt, so können verschiedene Adressen berechnet werden.

$$NetzwerkAdresse = IPAdresse \wedge Netzmaske$$

$$BroadcastAdresse = IPAdresse \vee \neg Netzmaske$$

$$Anzahl\,Hosts = 2^{(32 - SlashNetzmaske)} - 2$$

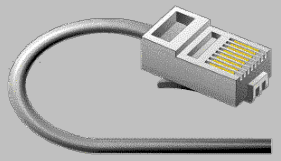


IP-Mathematik

Ein Host ist innerhalb eines Netzes, wenn seine

IP-Adresse zwischen der **Netzwerk-Adresse** und der **Broadcast-Adresse** liegt:

Netzwerk-Adresse < IP-Adresse < Broadcast-Adresse

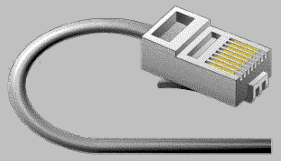


IPv4 Konfigurations Regeln

Die Netzwerk-Adresse zusammen mit der Netzmaske definiert ein IP-Netz eindeutig.

Die **Netzwerk**- oder die **Broadcast**-Adresse darf bei keinem **IPv4**-Host konfiguriert werden!

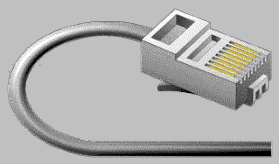
Pakete, die an die Netzwerk- oder Broadcast-Adresse gesendet werden, werden von allen Rechnern bearbeitet.



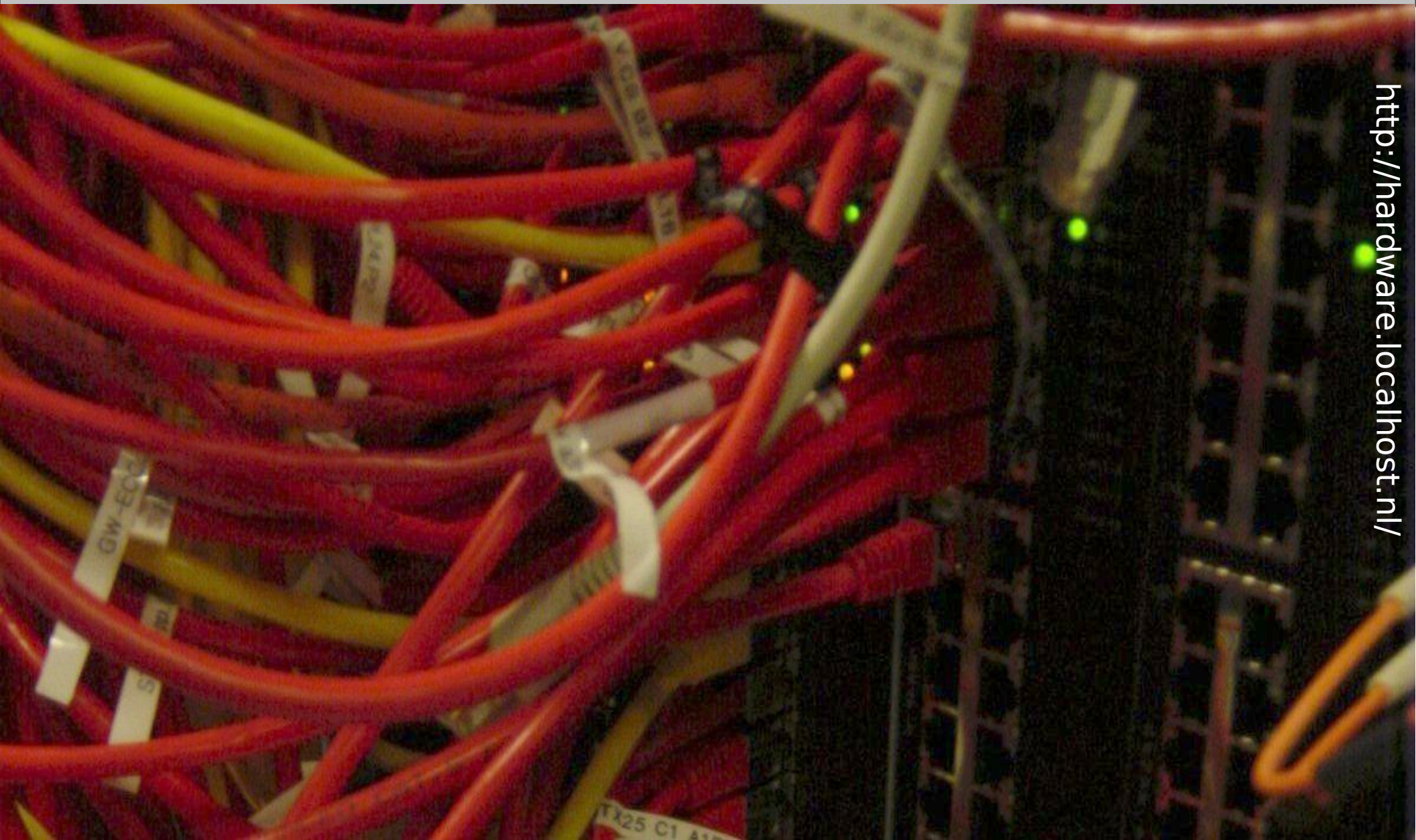
IPv4 Konfigurations - Regeln

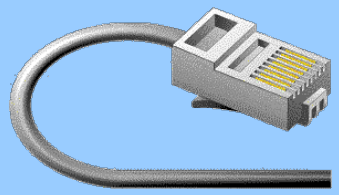
Jeder Host muss innerhalb eines Netzwerkes eine eindeutige IP-Adresse besitzen.
Muss der Host global ansprechbar sein, so muss eine weltweit eindeutige IP-Adresse verwendet werden.

Doppelt vergebene IP-Adressen bereiten grosse Probleme in einem Netzwerk!
Es ist möglich ein ganze Netzwerke so lahm zu legen!!!



Fragen?

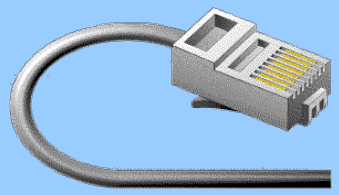




IP Math Hausaufgaben

1) Berechnen Sie die fehlenden Angaben der folgenden IP-Netzwerke.

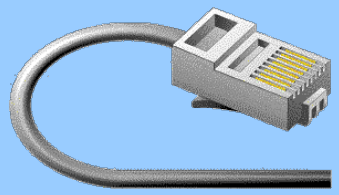
	IP	Netzwerk	Broadcast	Netzmaske	Hosts
a)	4.5.2.8/30				
b)	82.43.156.2				$2^{14}-2$
c)	195.226.2.21			255.255.248.0	
d)	/27		142.44.86.31		
e)	11.2.192.8			254.0.0.0	
f)	23.27.42.27				6
g)			212.55.197.239		14
h)		217.14.64.128	217.14.64.255		



IP Math Hausaufgaben

2) Bei folgenden Rechnern ist jeweils das angegebene IP-Netz konfiguriert. Der Administrator hat auch den angegebenen Default-Gateway konfiguriert.
Ist der Default-Gateway innerhalb des konfigurierten Netzes?

IP	Netzmaske	Gateway
212.55.196.74/28		212.55.196.65
192.168.5.3	255.255.255.32	192.168.5.1
172.16.25.210	255.255.255.240	172.16.25.208
14.67.54.240/26		14.62.54.254
62.12.130.66/28		62.12.130.79
217.14.65.35/30		217.14.65.33
223.54.25.4	255.255.255.224	223.54.25.1
172.16.58.5	255.255.254.0	172.16.58.225



IP Math Hausaufgaben

3) Berechnen Sie die kleinsten mögliche Netz für folgende IPs, so dass alle angegeben IPs innerhalb des Netzes liegen:

192.168.5.54, 192.168.5.65

172.16.54.0, 172.17.58.98

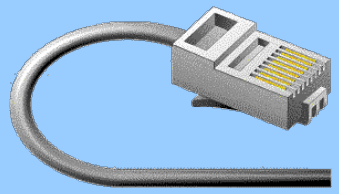
10.5.9.1, 10.2.45.58, 10.7.223.1

195.0.2.1, 195.0.2.2

183.57.1.33, 183.57.1.43

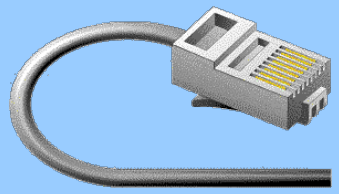
57.5.19.1, 57.5.19.128, 57.5.19.45

139.57.1.89, 138.57.5.84



IP Math Hausaufgaben

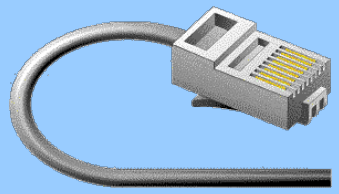
4) 179.29.21.96/xx ist eine Netzwerk-Adresse. Leider haben sie vergessen die Netzmaske aufzuschreiben.
Suchen sie alle möglichen und gültigen Netzmasken die dafür in Frage kommen.



IP Math Hausaufgaben

5) Sie müssen das Netzwerk der Firma Hype GmbH erstellen. Sie haben dazu folgende Angaben bekommen:
Die Firma hat 4 Abteilungen, die jede eine getrenntes Netz bekommen soll.
Die grösste Abteilung wird 20 PC und 10 Netzwerk-Drucker bekommen.
Die drei anderen Abteilungen werden mit Je 10 PCs und je 1 Netzwerk-Drucker auskommen. Die Firma erwartet, dass in der nächsten Zeit ca. 20% mehr PCs und Drucker angeschlossen werden müssen.

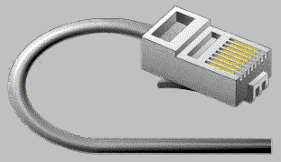
Als Netzwerk haben sie 172.24.0.0/23 bekommen. Definieren sie die notwendigen Netze so dass jeweils alle Rechner / Drucker einer Abteilungen ans Netz angeschlossen werden können und genügend Reservekapazität vorhanden ist.



IP Math Hausaufgaben

6) Ein Paket, das an die Broadcast-Adresse gesendet wird erreicht definitionsgemäss alle Rechner innerhalb des Netz- werkes.

a) Wie wird dies mit Ethernet sichergestellt?
b) Verifizieren sie das mit Wireshark, indem sie die lokale Broadcast-Adres- se anpingen und gleichzeitig den Verkehr aufzeichnen.
c) Was zeichnen sie mit Wireshark auf, wenn sie anstelle der Broadcast-Adresse die Netzwerk-Adresse anpingen?

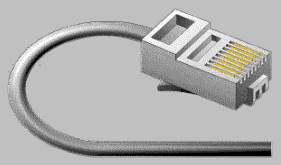


reservierte IP Adressen

Neben den Class D und Class E Adressen gibt es noch weitere IPv4-Adressen die für bestimmte Zwecke reserviert sind. Diese sind in den RFCs rfc1918, rfc5735, rfc5737 dokumentiert

RFC 1918: Private IP-Adressen
10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16 können für private Netze verwendet werden und sind im Internet nicht geroutet.
Diese Adressen sind weltweit **nicht** eindeutig.

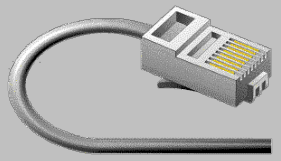
Bei VPN Tunnels zwischen privaten Netzen kann es zu komplizierten Setups kommen.



reservierte IP Adressen

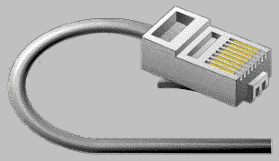
0.0.0.0/8 - Addresses in this block refer to source hosts on "this" network. Address 0.0.0.0/32 may be used as a source address for this host on this network; other addresses within 0.0.0.0/8 may be used to refer to specified hosts on this network.

127.0.0.0/8 - This block is assigned for use as the Internet host loopback address. A datagram sent by a higher level protocol to an address anywhere within this block should loop back inside the host. This is ordinarily implemented using only 127.0.0.1/32 for loopback, but no addresses within this block should ever appear on any network anywhere.



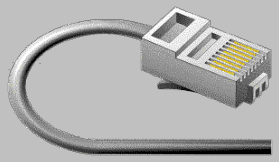
reservierte IP Adressen

169.254.0.0/16 - This is the "link local" block. It is allocated for communication between hosts on a single link. Hosts obtain these addresses by auto-configuration, such as when a DHCP server may not be found.



reservierte IP Adressen

192.0.2.0/24,
198.51.100.0/24,
203.0.113.0/24 - This blocks are assigned as "TEST-NET1", "TEST-NET2" and ""TEST-NET3" for use in documentation and example code. It is often used in conjunction with domain names *example.-com* or *example.net* in vendor and protocol documentation.
Addresses within this blocks should not appear on the public Internet.

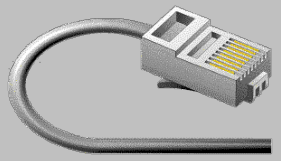


Fragen?

Didn’t we run out of IPv4 jokes?

Didn’t we run out of IPv4 jokes?

http://hardware.localhost.nl/



Wer vergibt die IP-Adressen?

Damit das Internet funktioniert müssen die IP-Adressen weltweit koordiniert werden.

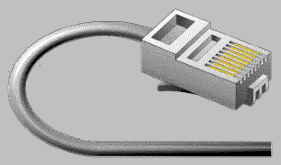
Die Vergabe der IP-Adressen erfolgt hierarchisch.

Als oberste Instanz koordiniert die Internet Assigned Numbers Authority (IANA) die IP-Adressen.

IANA vergab /8 Blocks an Regionale Internet Registraturen (RIR)[1].

IANA vergibt weiterhin IPv6 Blöcke![2]

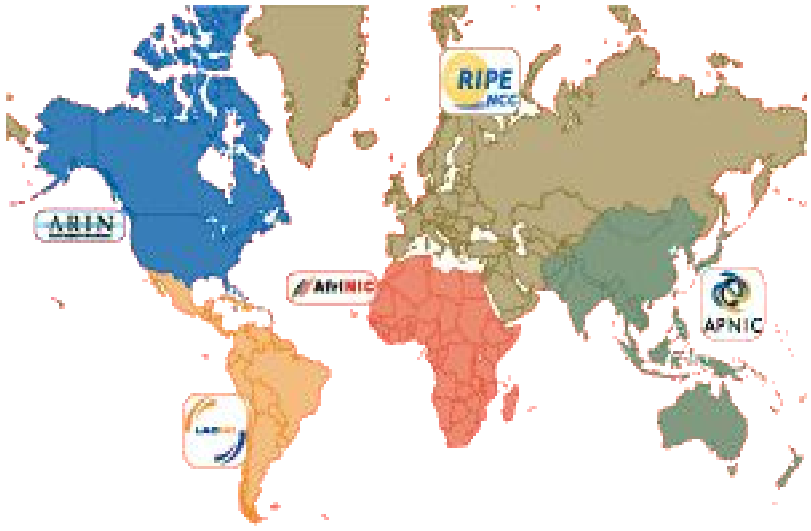
[1] http://www.iana.org/assignments/ipv4-address-space/ipv4-address-space.txt
[2] http://www.iana.org/assignments/ipv6-address-space/ipv6-address-space.txt

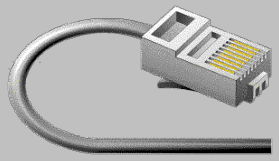


Wer vergibt IP-Adressen

Weltweit gibt es 5 RIRs:

AFRINIC	African Internet Numbers Registry
APNIC	Asia Pacific Network Information Centre
ARIN	American Registry for Internet Numbers
LACNIC	Latin American and Caribbean Internet Addresses Registry
RIPE	Réeseaux IP Européans





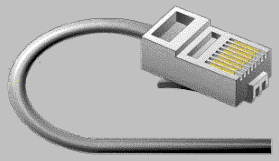
Wer vergibt IP-Adressen

Die RIRs allozieren IP-Adressen an die Local Internet Registry (LIR) – ihre Mitglieder.

Jedes LIR vergibt dann die IP-Adressen an ihre Kunden gemäss deren Bedarf unter Berücksichtigung der Richtlinien vom entsprechenden RIR.

Wer ein LIR ist, kann bei RIPE öffentlich eingesehen werden[1]

[1] http://www.ripe.net/membership/indices/

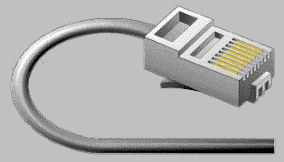


PI oder PA?

RIR vergeben zwei "Arten" von IP-Adressen:

PI Provider independent
Diese Adressen sind nicht an einen bestimmten Provider gebunden. Diese Adressen müssen angefordert und in jedem Fall gegenüber der RIR begründet werden!

PA Provider aggregatable
Diese Adressen sind an einen bestimmten Provider gebunden und können bei einem Wechsel vom Provider **nicht** mitgenommen werden!

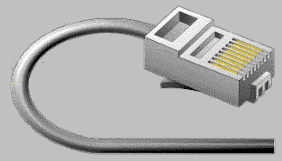


Whois

Die Whois Datenbank wird von den RIR und LIR gepflegt und können von öffentlich abgefragt werden.

Diese Datenbank dient dazu Inforationen zu Domainnamen und IP-Adressen und deren Besitzer abzulegen.

Whois ist - ähnlich wie DNS - eine verteilte Datenbank. Im Unterschied zum DNS gibt es keine 'Root'-whois Server. Der Client muss selber wissen bei welchem whois-Server er die gesuchte Informationen anfordern kann.

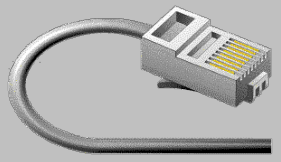


Whois

Mit dem Befehl **whois**[1] kann nachgesehen werden wem welche IP-Adresse zugeordnet wurde:

```
inetnum:        212.55.196.64 - 212.55.196.71
netname:        CH-MAX-MUSTER
descr:          BBI for Max Muster
country:        CH
admin-c:        MM3421-RIPE
tech-c:         MM3421-RIPE
status:         ASSIGNED PA
notify:         ripe@cyberlink.ch
mnt-by:         CYBERLINK-MNT
changed:        dvg@cyberlink.ch 20021107
source:         RIPE
```

[1] oder http://www.ripe.net/whois



IP Adressen

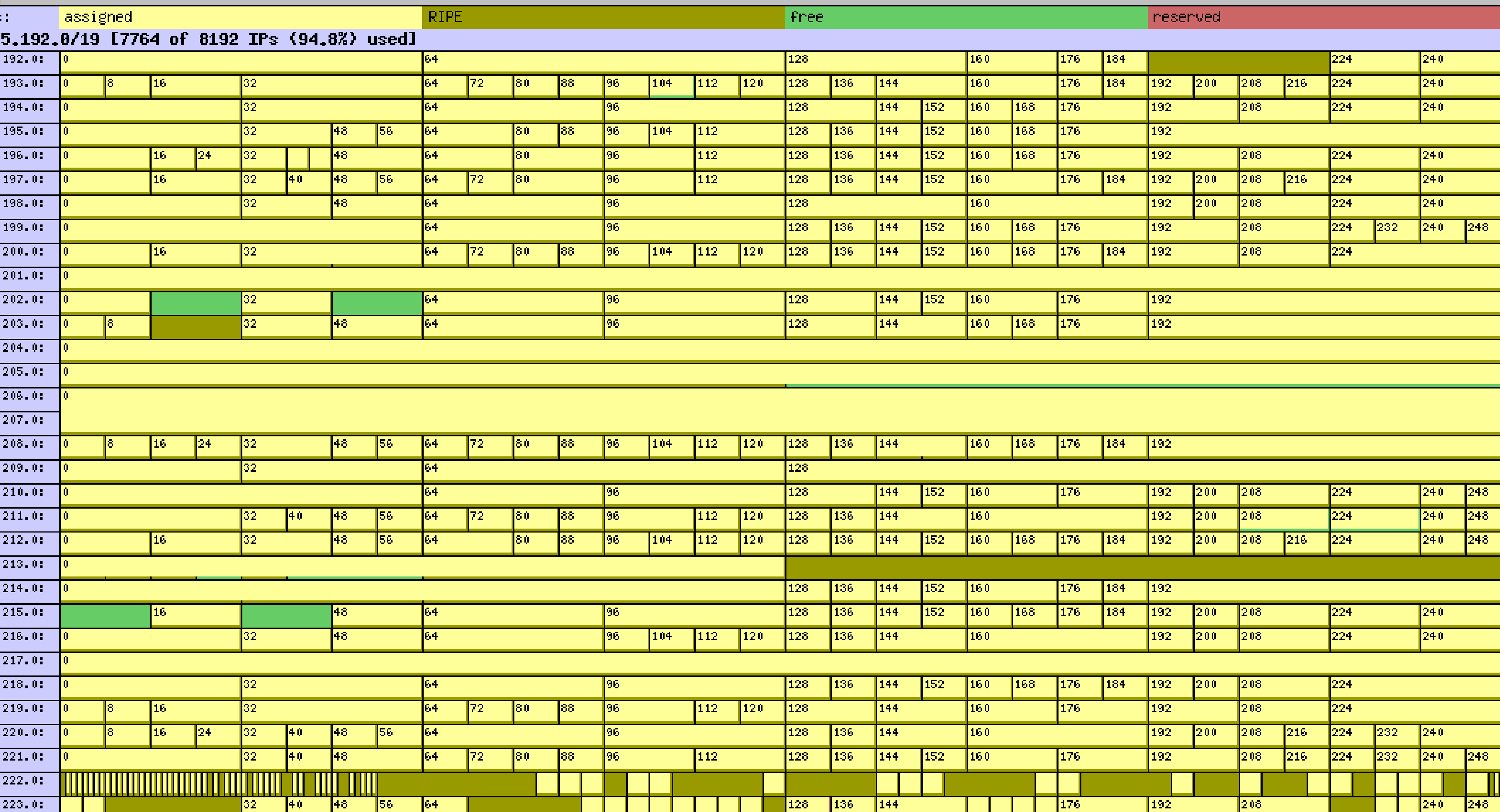
Wenn sie IP-Adressen benötigen, stellen sie sich folgende Fragen:

- Müssen die/alle Rechner weltweit erreichbar sein?
  Nein → RFC1918 Private Adressen.

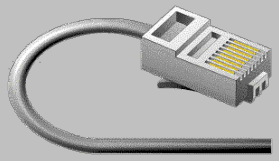
- Funktionieren Dynamische Adressen?
  Ja → ein einfaches Abo vom Provider meiner Wahl

- Brauche ich **PA** oder **PI** Adressen?
  PA → technischer, finanzieller Aufwand gering
  PI → technischer, administrativer Aufwand sehr hoch

IP-Tapete



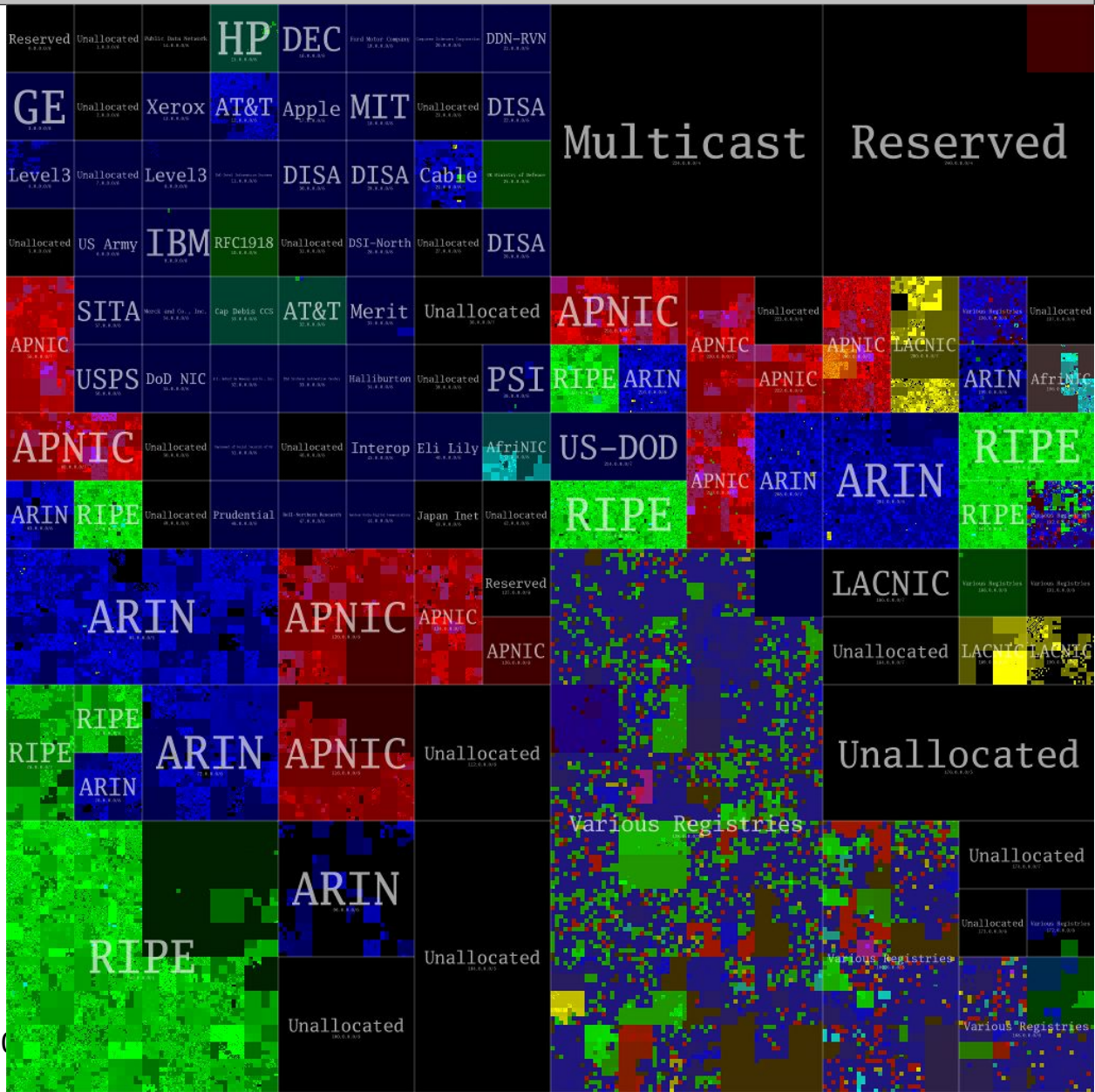
:: assigned RIPE free reserved
5.192.0/19 [7764 of 8192 IPs (94.8%) used]
192.0: 0 64 128 160 176 184 224 240
193.0: 0 8 16 32 64 72 80 88 96 104 112 120 128 136 144 160 176 184 192 200 208 216 224 240
194.0: 0 32 64 96 128 144 152 160 168 176 192 208 224 240
195.0: 0 32 48 56 64 80 88 96 104 112 128 136 144 152 160 168 176 192
196.0: 0 16 24 32 48 64 80 96 112 128 136 144 152 160 168 176 192 208 224 240
197.0: 0 16 32 40 48 56 64 72 80 96 112 128 136 144 152 160 176 184 192 200 208 216 224 240
198.0: 0 32 48 64 96 128 160 192 200 208 224 240
199.0: 0 64 96 128 136 144 152 160 168 176 192 208 224 232 240 248
200.0: 0 16 32 64 72 80 88 96 104 112 120 128 136 144 152 160 168 176 184 192 208 224
201.0: 0
202.0: 0 32 64 96 128 144 152 160 176 192
203.0: 0 8 32 48 64 96 128 144 160 168 176 192
204.0: 0
205.0: 0
206.0: 0
207.0:
208.0: 0 8 16 24 32 48 56 64 72 80 88 96 104 112 120 128 136 144 160 168 176 184 192
209.0: 0 32 64 128
210.0: 0 64 96 128 144 152 160 176 192 200 208 224 240 248
211.0: 0 32 40 48 56 64 72 80 88 96 112 120 128 136 144 160 192 200 208 224 240 248
212.0: 0 16 32 48 56 64 80 88 96 104 112 120 128 136 144 152 160 168 176 184 192 200 208 216 224 240 248
213.0: 0
214.0: 0 128 136 144 152 160 176 184 192
215.0: 16 48 64 96 128 136 144 152 160 168 176 184 192 200 208 224 240
216.0: 0 32 48 64 96 104 112 120 128 136 144 160 192 200 208 224 240
217.0: 0
218.0: 0 32 64 96 128 136 144 152 160 168 176 184 192 200 208 224
219.0: 0 8 16 32 64 72 80 88 96 112 120 128 144 160 176 192 208 224
220.0: 0 8 16 24 32 40 48 56 64 96 128 136 144 160 192 200 208 216 224 232 240
221.0: 0 32 40 48 64 72 80 88 96 112 128 136 144 152 160 176 192 208 216 224 232 240 248
222.0:
223.0: 32 40 48 56 64 128 136 144 176 192 208 240 248

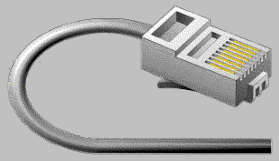


Fragen?

Netzverteilung
vom 1. Okt 2007

Jeder Pixel repräsen-
tiert ein /24 Netz.

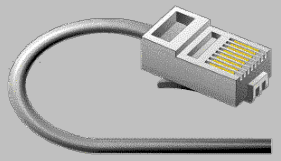




IP Pakete

Ziele:

- IP Pakete
- ICMP Pakete
- TCP Pakete verstehen
- 3 Way Handshake
- Sliding Window
- UDP Pakete verstehen
- Well known Port Numbers kennen



IP Pakete

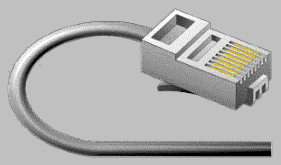
Repetition:

IP befindet sich auf dem Layer 3 des OSI-Modells.

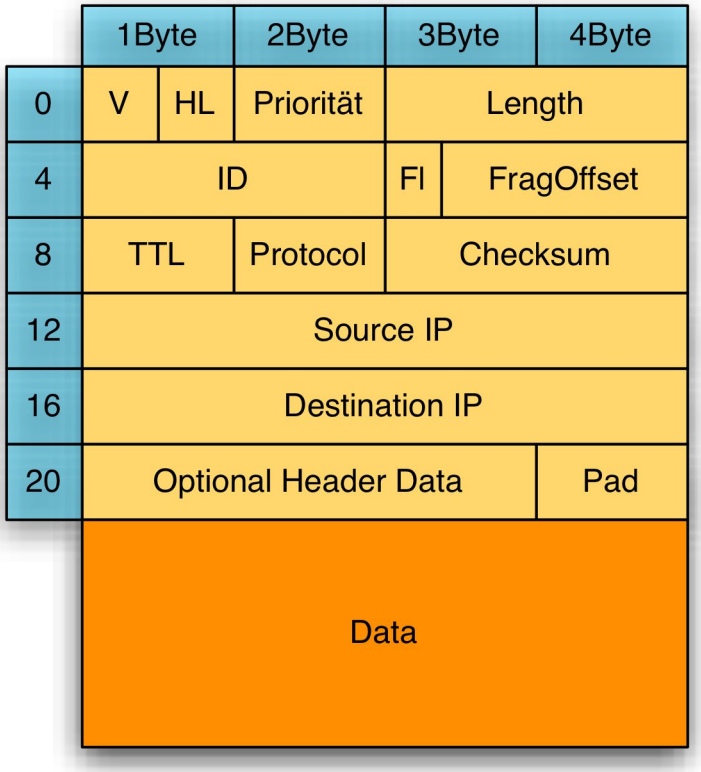
Alles was sie bis jetzt über die unteren Layer 1 und 2 gelernt haben ist weiterhin uneingeschränkt gültig!

Das bedeutet, dass IP-Pakete die Payload der Ethernet Frames sind und daher maximal 1500Byte[1] lang sein können!

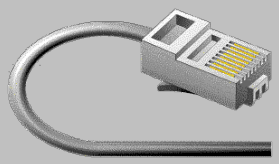
1) Gilt für 10/100Mbit Ethernet



IP Paket Header



V	Version
HL	HeaderLength in Words
Priorität	Priority Flags
Length	Länge des ganzen Flows
ID	Sequenznummer des Flows
Fl	Flags
FragOffset	Abstand des aktuellen Fragementes zum Anfang der Daten
TTL	Time to Live (Hops to Live)
Protocol	Protokoll der Daten
Checksm	Header Checksumme
Source IP	Source IP-Adresse
Destination IP	Destination IP-Adresse
Optional Header Data	Optionale Header Daten
PAD	Füllbytes, da der IP-Header n*32Bit lang sein muss (→ HeaderLength)
Data	Die Daten, die mittels IP übertrage werden



IP Paket

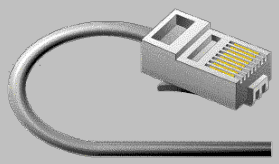
V Version (4Bit)
4 → IPv4

HL HeaderLength in Words (4Bit)
Die Länge des Headers in Worten (32Bit). Mögliche Werte sind 5 ... 16, entspricht einer Headerlänge von 20 bis 64Byte

Differentiated Services Field, Priority Flags
Bit 7... 2: Differentiated Services Codepoint
Bit 1: ECN-Cable Transport
Bit 0: ECN-CE

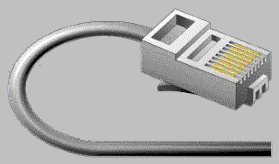
Length Länge des ganzen Pakets (16Bit)
Maximale Grösse eines IP-Paketes ist 2^{16} Byte

ID Identifikations Nummer des Flows
Jeder Flow hat eine eindeutige Nummer. Diese Nummer wird vom Absender vergeben.



IP Paket

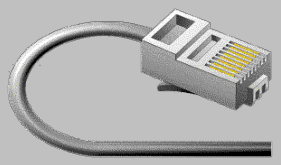
F	Flags Bit (7,6,5) Bit 7: Reserve Bit 6: Don't Fragment Bit 5: more Fragments
Frag	Abstand des aktuellen Fragments zum Anfang der Daten (13bit) * 8 Fragmente können daher nur ein mehrfaches von 8Byte betragen!
TTL	Time to Live (Hops to Live) Jeder Router, der das Paket verarbeitet verringert diesen Zähler. Wird der Wert 0 erreicht – und das Paket ist nicht am Ziel – wird das Paket verworfen und der Absender via einer ICMP-Meldung darüber informiert.
Proto	Protokoll der Daten IP-Protokoll Nummer, meistens (ICMP [1], TCP [6] oder UDP [17])



IP Paket

Checksm	Header Checksumme Quersumme über den ganzen Headerbereich
SrcIP	Source IP-Adresse
DestIP	Destination IP-Adresse
Optional	Optionale Header Daten Im Header können zusätzliche Felder eingefügt werden. Beispielsweise Authentication Header (RFC1826)…Mögliche Werte sind bei IANA [1] publiziert.
PAD	Füllbytes, da der IP-Header n*32Bit lang sein muss (→ HeaderLength)
Daten	Die Nutzdaten, die mittels IP übertragen werden. Diese müssen entsprechend den Angaben des Proto-Feldes interpretiert werden.

[1] http://www.iana.org/assignments/ip-parameters

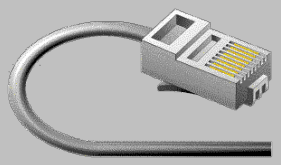


IP Paket

```
0000   00 0f 34 e7 8b ae 00 01   02 37 cc 95 81 00 00 03   ..4..... .7......
0010   08 00 45 08 00 72 11 42   40 00 3f 06 f7 9b d4 37   ..E..r.B @.?....7
0020   c4 4a d4 37 c5 e6 fd cf   0c ea 13 48 86 4d d6 86   .J.7.... ...H.M..
0030   a7 1b 80 18 ff ff 4c 53   00 00 01 01 08 0a 60 1d   ......LS ......`.
0040   a3 5e 15 43 0e df 3a 00   00 00 03 73 65 6c 65 63   .^.C..:. ...selec
0050   74 20 2a 20 66 72 6f 6d   20 4e 4f 5f 4f 46 5f 52   t * from  NO_OF_R
0060   41 54 49 4e 47 53 5f 50   45 52 5f 53 54 49 4d 55   ATINGS_P ER_STIMU
0070   4c 55 53 20 77 68 65 72   65 20 63 6f 75 6e 74 20   LUS wher e count
0080   3c 20 31 30                                        < 10
```

OSI 4, IP-Payload
OSI 3, IP-Header
OSI 1,2, Ethernet Header mit VLAN Tag

ACHTUNG: Der Ethertype vom Paket **muss** IP (0x0800) sein, sonst ist es KEIN IPv4 Paket!

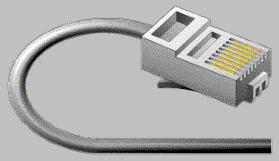


IP Paket im Detail

HexDump eines IP-Paketes

```
0000   00 0f 34 e7 8b ae 00 01   02 37 cc 95 81 00 00 03    ..4..... .7......
0010   08 00 45 08 00 72 11 42   40 00 3f 06 f7 9b d4 37    ..E..r.B @.?....7
0020   c4 4a d4 37 c5 e6 .. ..   .. .. .. .. .. .. .. ..    .J.7..
```

Offset	Wert	Bedeutung
0012:	45	Version 4, HeaderLength 5x4Byte = 20Byte
0013:	08	TOS/DSCP-Feld
0014:	0072	Total Length: 114
0016:	1142	ID: 4418
0018:	4000	Flag, FragOffset
001a:	3F	Time To Live
001b:	06	Protokoll: TCP
001c:	f79b	Header Checksum
001e:	d4.37.c4.4a	Source IP-Adresse (212.55.196.74)
0022:	d4.37.c5.e6	Destination IP-Adresse (212.55.197.230)

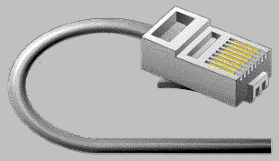


Fragmentierte Pakete

Sollen mehr Daten, als dass in ein Frame auf dem Link Platz hat, transportiert werden, muss die Übertragung in mehreren Frames erfolgen. Die Daten werden fragmentiert.

Die Daten werden in "schluckbare" Stücke verschnitten und dann einzeln zum Empfänger gesendet.

Jedes dieser Datenfragment bekommt den ursprünglichen Header (Mit Modifikationen bei den Fragment_Flags) vorangestellt.



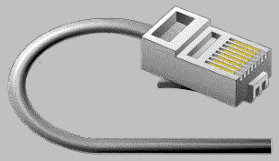
Fragmentierte Pakete

Der Empfänger kann die eintreffenden Fragmente an Hand der FragmentOffset Angaben ordnen.

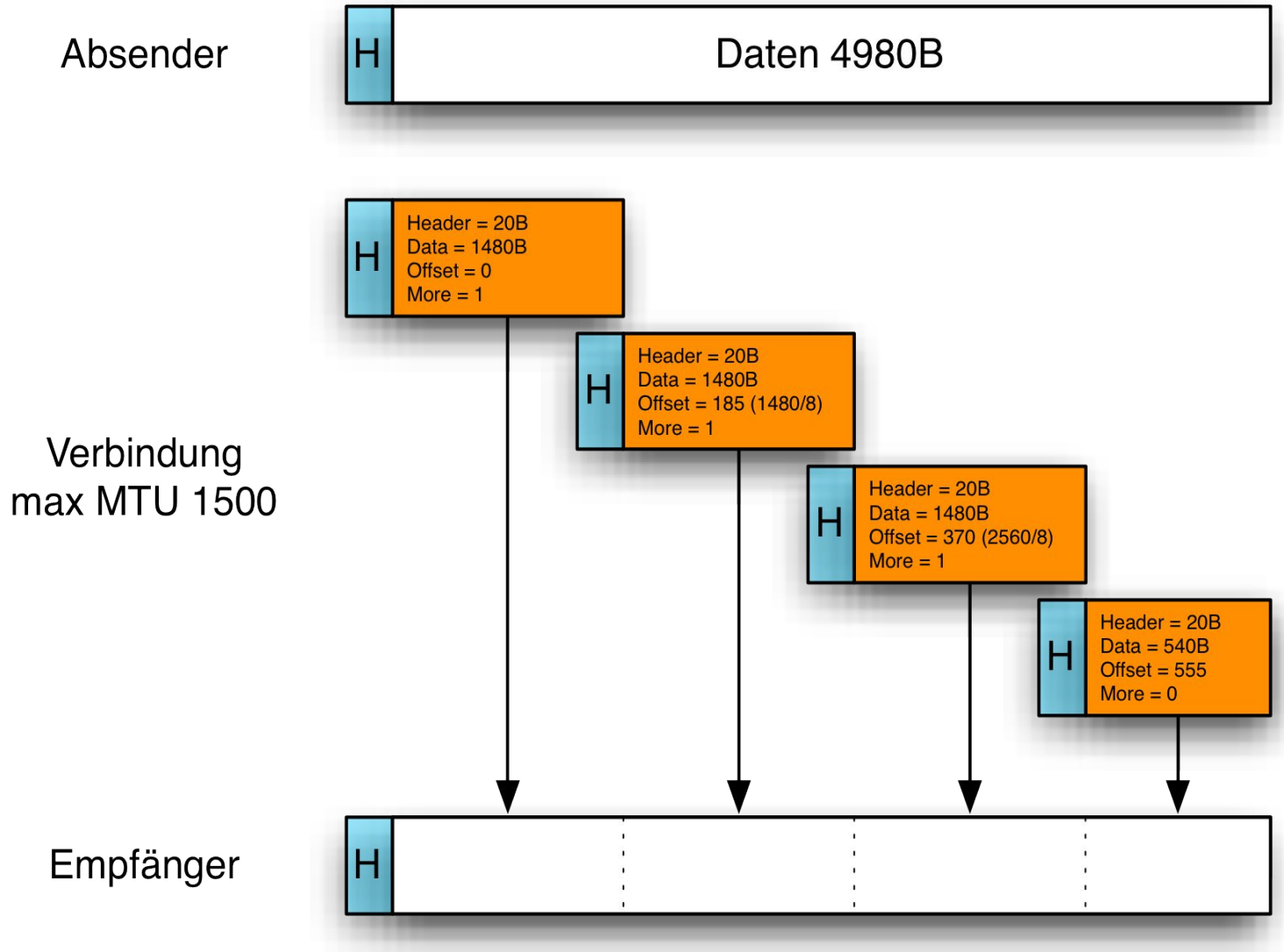
Anhand der Packet Grösse und dem MoreFragment Flags Weiss der Empfänger wieviele Fragments ankommen sollen.

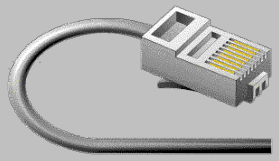
Der Empfänger wartet, bis alle Framgmente eingetroffen sind, und leitet die ganzen Daten dann an die obere Schicht weiter.

Geht ein Fragment verloren, so wird das ganze Paket verwerfen und eine ICMP Time Exceeded generiert.



Fragmentierte Pakete

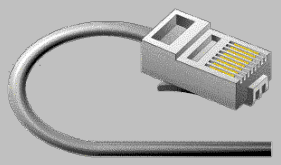




Fragen ?

The worst thing about protocol jokes is the ridiculous TTL.

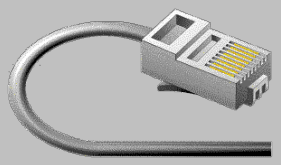
http://hardware.localhost.nl/



Internet Control Message Protocol, ICMP

ICMP Meldungen werden in verschiedenen Situationen versendet z.B. wenn ein Paket das Ziel nicht erreichen kann, wenn ein Router einen besseren Weg zu Ziel kennt, oder um die Erreichbarkeit eines Hosts zu testen.

Das Internet Protokoll (IP) ist so gebaut, dass der Ziel-Rechner mit grosser Wahrscheinlichkeit erreicht wird, eine Garantie, dass der Ziel Host erreicht werden kann, gibt es nicht!



Internet Control Message Protocol, ICMP

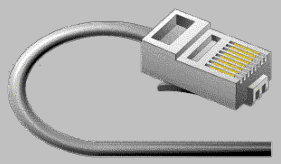
ICMP wird verwendet um dem Absender über Probleme bei der Übertragung zu informieren.

ICMP kann verwendet werden um Verbindungs-Probleme zu untersuchen.

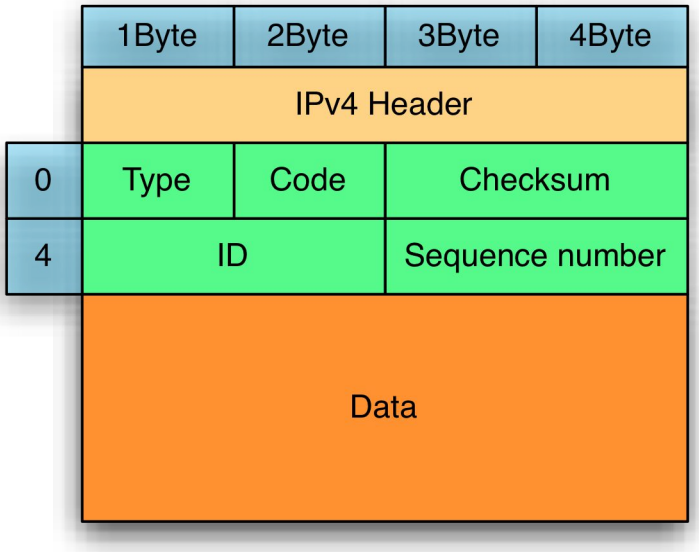
Um endlose ICMP-Loops zu vermeiden werden nie ICMP-Meldungen aufgrund von ICMP-Paketen erzeugt!

Jede IP-Implementierungen muss ICMP unterstützen.

ICMP ist ein sehr wichtiger Teil vom Internet Protokoll und darf nicht blockiert werden.

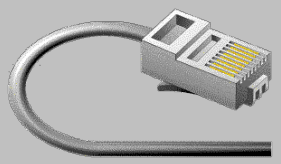


ICMP Paket



ICMP-Paket basiert auf IP, darum muss vor dem ICMP-Paket ein IP-Header stehen!

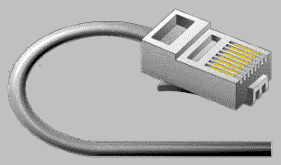
Type:	Art der ICMP Nachricht
Code:	Detaillierte Information zur Nachricht
Checksum:	Checksumme der ICMP Nachricht
ID:	Identifier
Sequenz#:	Sequenznummer
Data:	Weitere Daten (Dies ist meistens der Header vom Paket, das die Meldung verursachte)



ICMP Type

ICMP Typen:

0	**Echo Replay**
1	Reserved
2	Reserved
3	**Destination unreachable**
4	**Source quench**
5	**Redirect**
6	Alternate Host Address
7	
8	**Echo Request**
9	Router Advertisement
10	Router solitation
11	**Time exceeded**
12	Parameter Problem
13	Timestamp request
14	Timestamp replay
15	Information request
16	Infromation Replay
17	Address mask request
18	Address mask replay
19	Reserved
20 – 29	Reserved
30	Traceroute
31	Conversation error
32	Mobile Host Redirect
33	IPv6 Where are You
34	IPv6 I Am Here
35	Mobile Registration Request
36	Mobile Registration Replay
37	Domain Name request
38	Domain Name replay
39	SKIP Algorithm Discovery Protokoll
40	Photuris, Security failures
41	Experimental mobility protokoll
42 – 255	Reserved

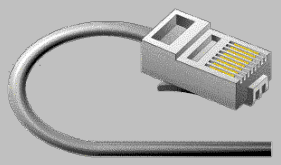


ICMP Paket

ICMP Pakete werden über IP versendet:

```
0000   00 01 02 37 cc 95 00 0f   34 e7 8b ae 08 00 45 c0   ...7.... 4.....E.
0010   00 38 54 08 00 00 ff 01   36 01 d4 37 c4 41 d4 37   .8T..... 6..7.A.7
0020   c4 4a 0b 00 f4 ff 00 00   00 00 45 a0 00 40 a1 49   .J...... ..E..@.I
0030   00 00 01 01 e5 33 d4 37   c4 4a d4 37 c5 e6 08 00   .....3.7 .J.7....
0040   dd f0 00 0f 1a 00                                  ......
```

Adresse / Offset	Wert	Bedeutung
0000 ... 0011:	Ethernet Header	EtherType muss **0x0800** sein!
0012 ... 0021:	IP Header	Protocoll muss ICMP (**0x01**)sein!
0022:	**0x0b**	Type: Time Exceeded
0023:	0x00	Code
0024:	0xf4ff	Checksumme
0026:	0x0000	Identifier: 0
0028:	0x0000	Sequenznummer: 0
002a:	0x45a0..	Hier folgt eine Kopie des Paketes, das das "Problem" auslöste

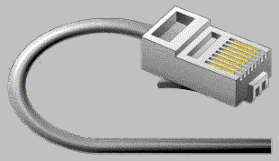


ICMP Echo Request

Wenn ein IP-Host eine **ICMP Echo Request** (08) Anforderung bekommt, so antwortet er mit einer **ICMP Echo Replay** (00) Meldung.

Damit kann getestet werden ob der Host IP mässig richtig konfiguriert ist.

ICMP Echo Requests können mit dem Befehl **`ping <IP-Adresse>`** erzeugt werden.

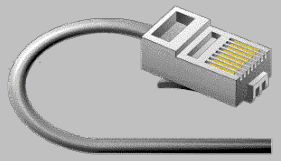


ICMP Destination unreachable

Dieser ICMP-Typ ist der wichtigste neben den Echo Request.

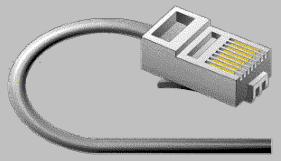
Destination unreachables (03) werden von Routern auf dem Weg zum Ziel oder vom adressierten Host erzeugt.

Der Grund warum das Ziel nicht erreichbar ist wird im Code Feld der ICMP-Meldung genauer angegeben:



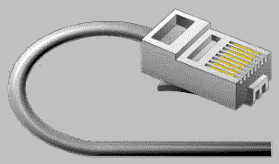
ICMP Destination unreachable

Code	Beschreibung
0	Network unreachable error
1	Host unreachable error
2	Protocol unreachable error. Das gewünschte Protokoll ist nicht unterstützt.
3	Port unreachable error. *Der gewünschte Port ist nicht erreichbar. In der Regel ist der Dienst hinter diesem Port nicht aktiv.*
4	The datagram is too big. *Das gesendete Paket ist zu gross*
5	Source route failed error.
6	Destination network unknown error.
7	Destination host unknown error.



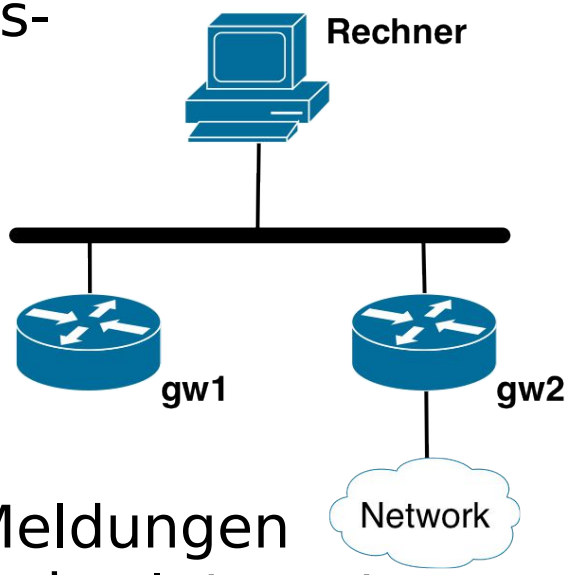
ICMP Destination unreachable

Code	Beschreibung
8	Source host isolated error. Obsolete.
9	The destination network is administratively prohibited. *Das Netzwerk ist gefiltert.*
10	The destination host is administratively prohibited. *Das Paket wurde vom Host ausgefiltert.*
11	The network is unreachable for Type Of Service.
12	The host is unreachable for Type Of Service.
13	Communication Administratively Prohibited. *Das Paket wurde auf einem Router gefiltert.*
14	Host precedence violation.
15	Precedence cutoff in effect.



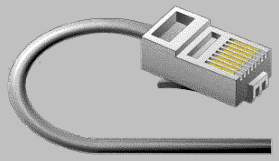
ICMP Redirect message

Router senden einem direkt angeschlossenen Rechner ICMP redirect (05) Meldungen, wenn der Ziel-Adresse besser über einen anderen localen Router erreicht werden kann.



Wenn der Rechner, gw1 als Default-Gateway verwendet, so kann gw1 dem Rechner mit einer ICMP redirect Meldungen mitteilen,dass er besser gw2 für Pakete ins Internet verwenden soll.

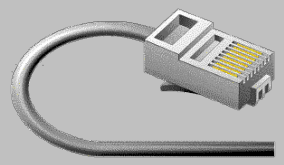
▶ ICMP-Redirect Meldungen sind problematisch, da diese nicht authentifiziert sind und so jeder Host diese Nachrichten erzeugen kann und dadurch den Traffic entsprechend umgeleitet werden kann!
Redirect Meldungen sollen nur von lokalen Router versendet werden (Achtung IP-Address Spoofing!)!



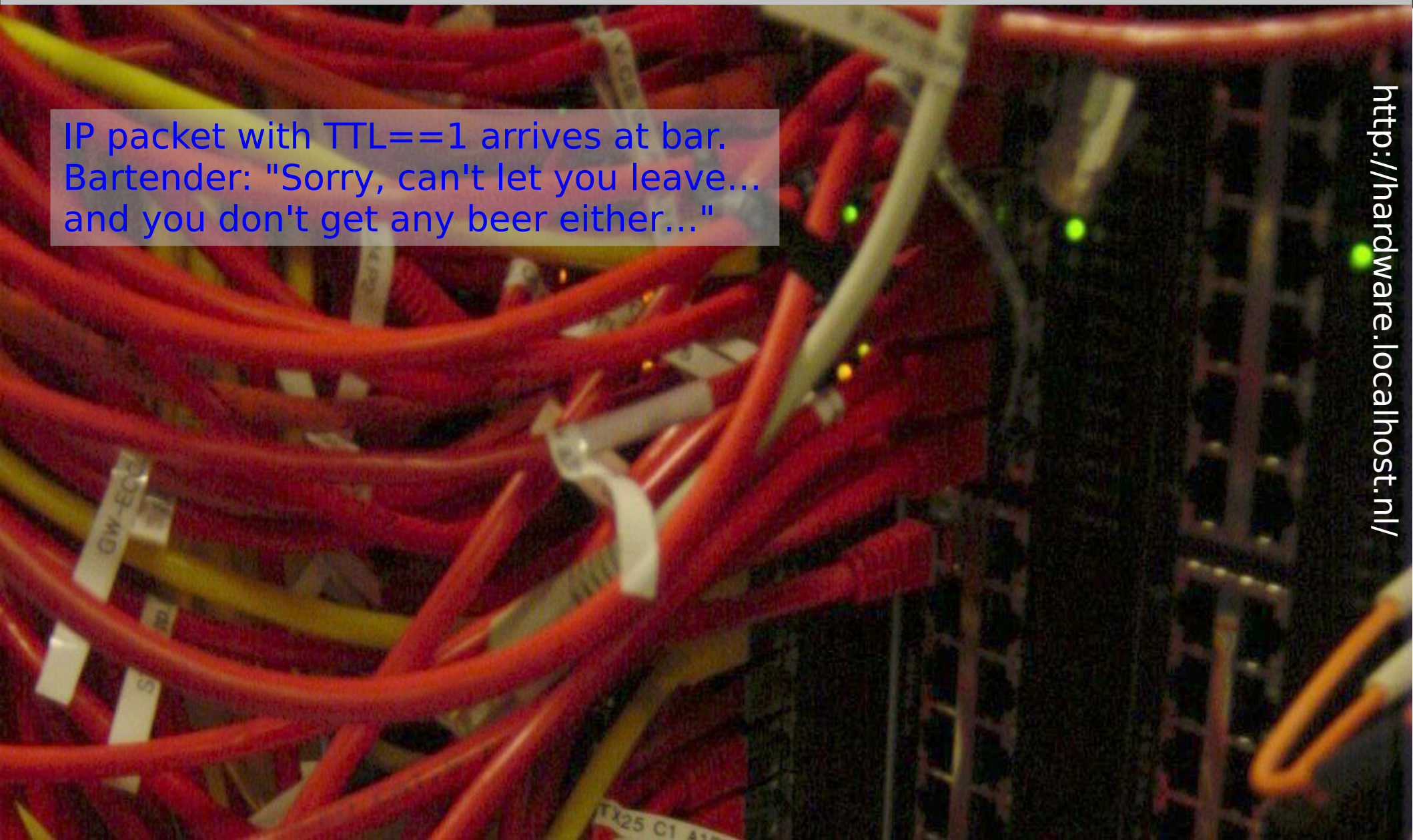
ICMP Time Exeeded

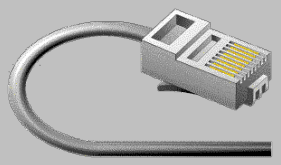
Es gibt 2 Time Exeeded (11) Meldungen

- Wenn in einem IP-Paket das TTL Feld == 0 wird, wird das Paket verworfen und eine Time to Live exceeded ICMP-Meldung an den Absender gesendet. Durch das Time to Live Feld können Layer 3 Loops verhindert werden.
- Ein Host sendet eine ICMP Time Exceeded Meldungen wenn der Host nicht alle notwendigen Fragmente eines fragmentierten Paketes innerhalb eine bestimmten Zeit bekommen hat.
  Der Host verwirft die erhaltenen Fragmente.



Fragen ?


IP packet with TTL==1 arrives at bar.
Bartender: "Sorry, can't let you leave...
and you don't get any beer either..."
http://hardware.localhost.nl/



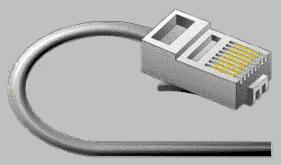
TCP / UDP Paket

TCP

- Verbindungsorientiert
- Zuverlässig
- Garantierte Reihenfolge der Daten
- Flexibilität in der Bandbreiten-Nutzung

UDP

- Verbingsloses Protokoll
- kleiner Overhead
- Schnell
- Reihenfolge der Daten ist **nicht** garantiert



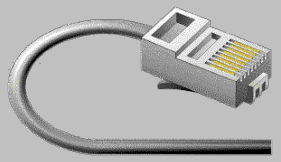
Transmission Control Protocol (TCP)

TCP ist verbindungsorientiert.

Das bedeutet, das bevor Daten ausgetauscht werden können, eine Verbindung aufgebaut werden muss.

Der Verbindungsaufbau erfolgt in 'Three-way-Handshake'

Eingesetzt wird TCP wo garantiert sein muss, dass die Daten ankommen und die Reihenfolge der Daten wichtig ist:
Web (http), Mail (smtp, pop3, imap4), Telnet, ssh, ...



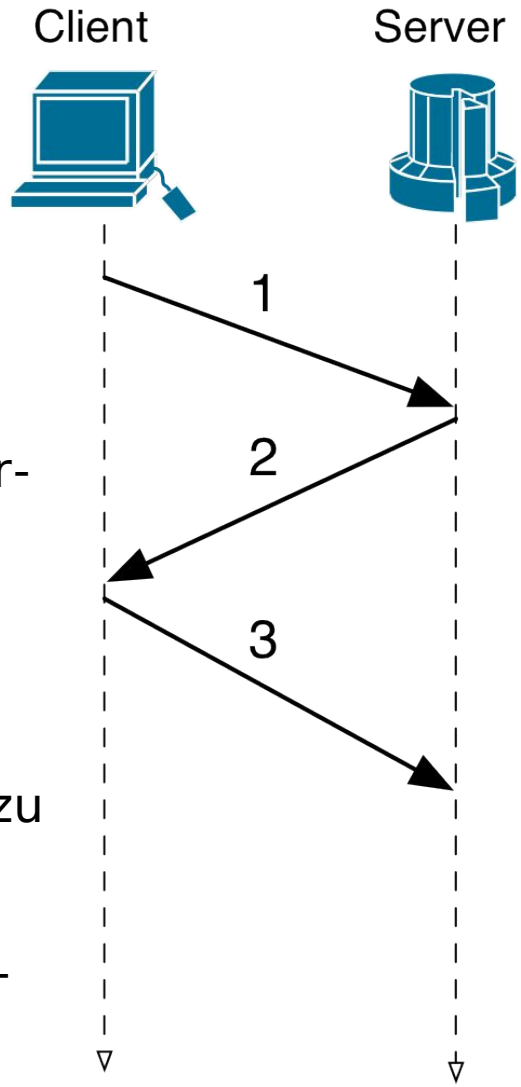
Three way Handshake

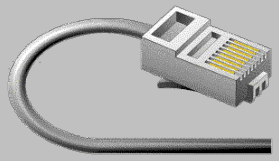
Verbindungsaufbau:

1) Der Client sendet dem Server eine TCP Paket mit dem SYN-Bit gesetzt, und einer beliebigen Sequenz-Nummer X.

2) Der Server bestätigt das Paket, in dem er das ACK-Flag setzt und die Sequenz-Nummer X um 1 erhöht. Gleichzeitig setzt der Server auch das SYN-Flag und erzeugt eine eigene Sequenz-Nummer Y

3) Der Client sieht, dass der Server seine Sequenz-Nummer X bekommen hat und richtig verarbeitet hat. Die Verbindung Client -> Server ist damit geöffnet.
Der Client muss das Paket vom Server bestätigen. Dazu erhöht er die Sequenz-Nummer Y um 1 und setzt das ACK-Flag.
Wenn der Server das Paket bekommt, ist auch die Verbindung Server -> Client geöffnet





Three way Handshake

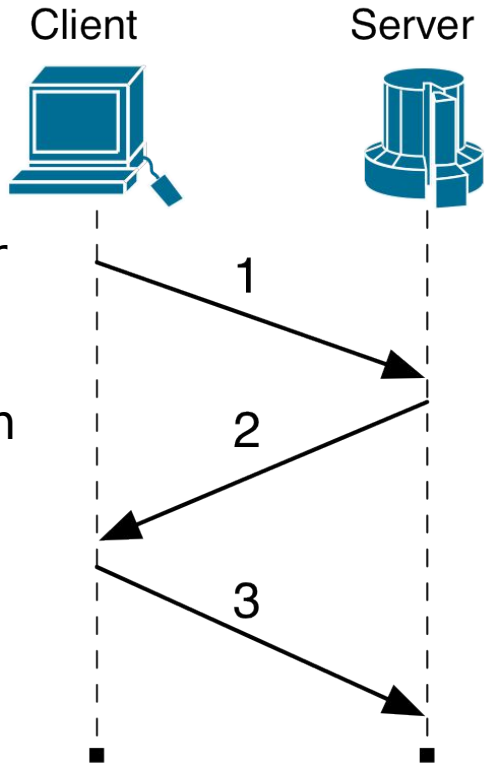
Verbindunsabbau

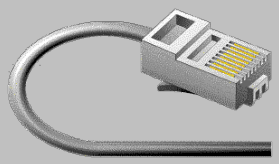
1) Wenn ein Verbindungspartner die Verbindung abbauen will, so sendet er ein Pakt mit der richtigen Sequenz-Nummer und dem gesetzten FIN-Flag. (hier im Beispiel initiiert der Client den Abbau)

2) Das Paket wird mit einem gesetzten ACK-Flag vom Server bestätigt. Gleichzeitig verlangt auch der Server, dass die Verbindung terminiert wird, in dem er das FIN-Flag setzt.

3) Diese Paket wird vom Client mit einem ACK Paket bestätigt.

Wichtig: Der Verbindungsabbau kann auch vom Server initiiert werden! (Es muss nur ein Paket mit der richtigen Sequenz-Nummer und den entsprechenden Flags gesendet werde)





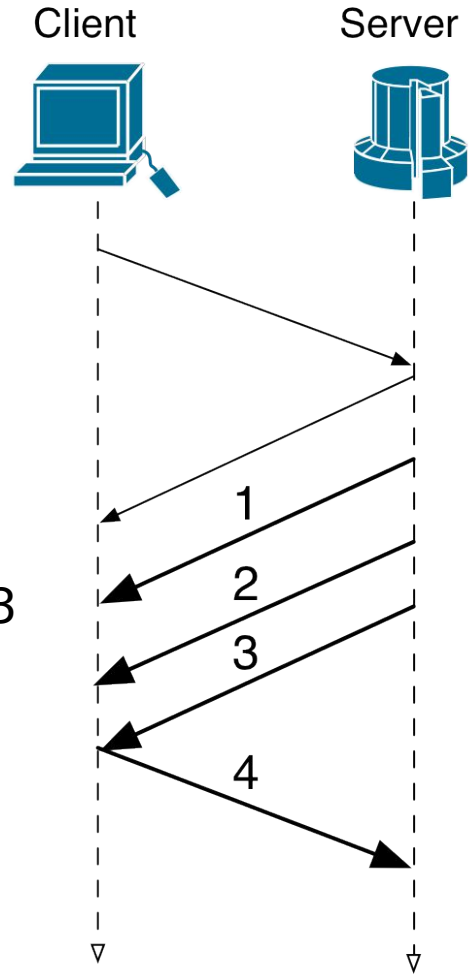
Datentransfer

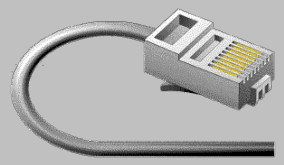
Datentransfer:

In der Regel wird jedes Datenpaket bestätigt. Dadurch wird sichergestellt, dass die Daten auch beim Empfänger angekommen sind. Fehlt eine Bestätigung, so muss der Sender das Paket nochmals senden

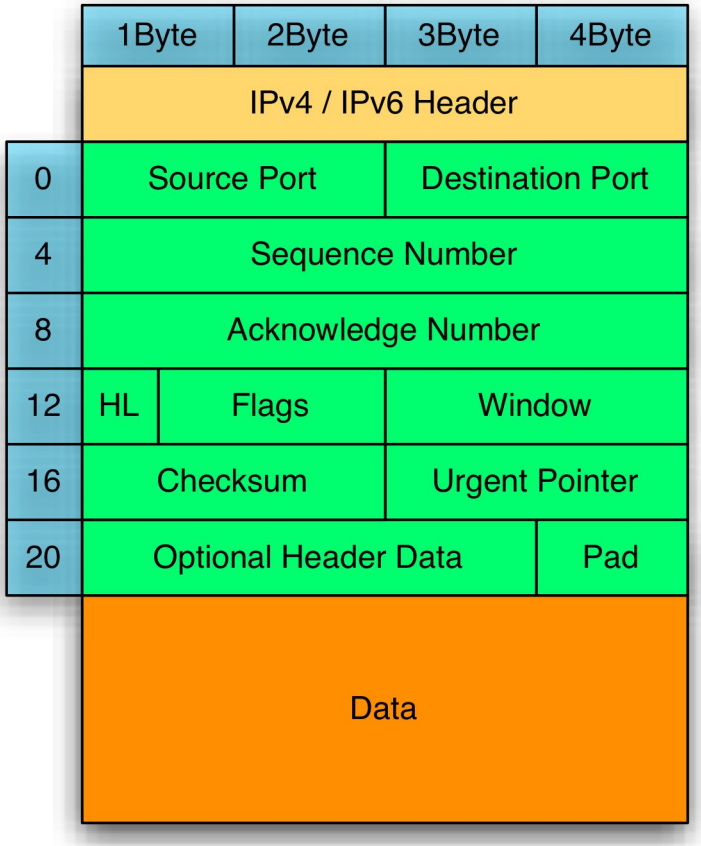
Um die Anzahl der Bestätigungen zu reduzieren, können auch mehrere Paket miteinander bestätigt werden. Mit dem Paket 4 werden die Paket 1,2 und 3 miteinander bestätigt.

Die Kommunikationspartner sprechen sich ab wie viele ausstehenden Bestätigungen sie unterstützen. Je nach Auslastung vom Netzwerk kann sich die Anzahl angepasst werden. (**sliding window**)



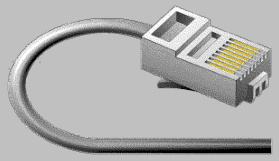


TCP Paket



TCP-Paket basiert auf IP, darum muss vor dem TCP-Paket ein IPv4 oder IPv6-Header stehen!

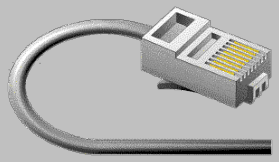
Src Port:	Source Port
Dst Port:	Destination Port
SeqNumber:	eigene Sequenz-Nummer
AckNumber:	Acknowlage Sequenz-Nummer
HL:	4Bit Header Length in 32bit Worten
Flags:	12Bit Verschiedene Flags
Window:	Windowsize in 32Byte 'Paketen'
Checksum:	Checksumme der TCP Nachricht
UrgentPoint:	Dieser Pointer zeigt auf das Ende der Dringenden Daten hin.
Optionen:	Optionale TCP Header
Pad:	Fülldaten, damit der Header die spezifizierte Headerlänge bekommt.



TCP Flags

Im Moment sind folgende TCP Flags (≠IP Flags) definiert:

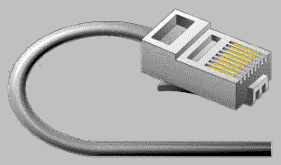
Fin:	Verlangt, dass die Verbindung beendet wird
Syn:	Aufbau ein Verbindung
Reset:	Zurücksetzen einer Verbindung
Push:	Die Daten sollen sofort verarbeitet werden ohne dass diese gepuffert werden.
Acknowledgment:	Der Header enthält eine gültige ACK-Sequenz-Nummer
Urgent:	Der UrgentPointer enthält eine gültige Angabe
ECN-ECHO:	verwendet für ECN
Congestion Window Reduce:	verwendet für ECN



Fragen ?

In high society, TCP is more welcome than UDP. At least it knows a proper handshake.

http://hardware.localhost.nl/

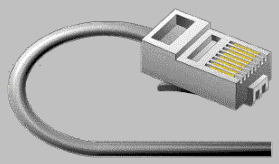


User Datagram Protocol (UDP)

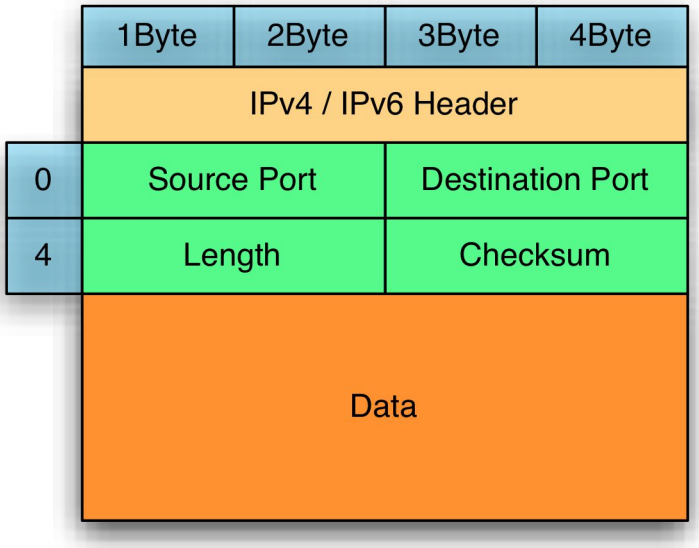
UDP

Verbingsloses Protokoll
kleiner Overhead
Schnell
Vermeiden redundanten Transportkontrollen

Eingesetzt wird UDP vor allem für Dienste die Pakete ohne grossen Protokoll overhead versenden müssen:
Namensauflösung (DNS), DateiSysteme (NFS, SMB, ...), VoIP, BOOTP, DHCP, SNMP

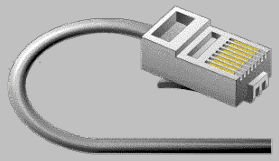


UDP Paket



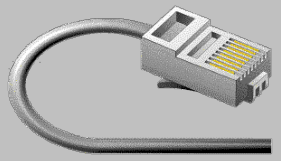
UDP-Paket basiert auf IP, darum muss vor dem UDP-Paket ein IP-Header stehen!

SrcPort:	Source Port
Dst Port:	Destination Port
Length:	Länge des UDP Paketes
Checksum:	Checksumme der UDP Nachricht



UDP, TCP Portnummern

- UDP und TCP verwenden Portnummern um den Service zu adressieren.
- Bekannte Services haben fixe Portnummern (well known port number), welche von der IANA verwaltet werden.
- Ein Service kann – muss aber nicht – über beide Protokolle UDP oder TCP implementiert werden:
- DNS funktioniert sowohl über UDP als auch TCP.
- HTTP funktioniert nur über TCP.
- DHCP funktioniert nur als UDP, ...

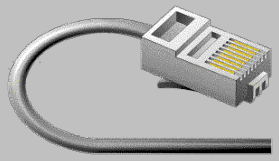


Portnummern, die man kennt

Einige Portnummern sind so verbreitet, dass man diese kennen sollte:

```
ftp-data 20/tcp
ftp      21/tcp
ssh      22/tcp
telnet   23/tcp
smtp     25/tcp
domain   53/udp  # dns
domain   53/tcp  # dns
bootps   67/udp  # dhcp
bootpc   68/udp  # dhcp
www      80/tcp
pop3     110/tcp
sunrpc   111/udp portmapper
sunrpc   111/tcp portmapper
imap     143/tcp
snmp     161/udp
snmp-trap        162/udp
```

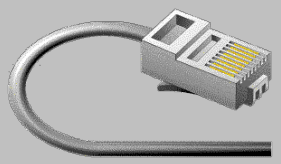
In der Datei /etc/services sind die Portnummern aufgelistet.



Fragen ?

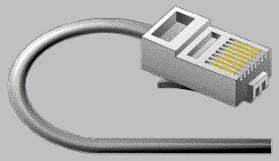
The problem with UDP jokes: I don’t get half of them.

http://hardware.localhost.nl/



IPv6

The bad thing about IPv6 jokes is that nobody wants to tell them first.



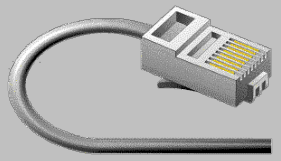
Wozu IPv6?

Der Adressraum ist bei IPv4 ist zu klein.

Es sind maximal $2^{\wedge 32}$ (~4.2Mia) Adressen möglich.

Da ein Teil Adressen für Multicast und Experimente (Class E) reserviert sind, können effektiv weniger Adressen verwendbar.
(Damit ist es nicht möglich, dass jeder Mensch eine IP-verwende kann!)

CIDR und NAT haben den Verbrauch von IPv4 Adressen verlangsamt, aber nicht gestoppt. So ist der IPv4 Adress-Pool bei der IANA seit dem Februar 2011 leer



IPv6 128bit Adressen

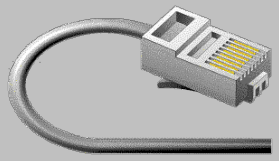
IPv6 erweitert den Adressraum von 32Bit auf 128Bit.

Das ergibt theoretisch 2^128 mögliche Adressen.
Oder ausgeschrieben sind das

340'282'366'920'938'463'463'374'607'431'768'211'456

Adressen

340 Sextillionen 282 Quintilliarden 366 Quintillionen 920 Quadrilliarden 938 Quadrillionen 463 Trilliarden 463 Trillionen 374 Billiarden 607 Billionen 431 Milliarden 768 Millionen 211 Tausend und 456



IPv6 Notation

Jeweils 4 Bit werden als HexZahl (0-9a-f) geschrieben.
4 dieser HexZahlen werden gruppiert und mittels Doppelpunkten getrennt

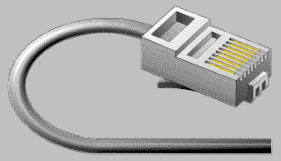
2001:0db8:0000:1234:0000:0000:0000:0001

führende Nullen können weggelassen werden:

2001:db8:0:1234:0:0:0:1

eine einzige Sequenz von :0:0: kann durch :: ersetzt werden

2001:db8:0:1234::1 **nicht aber** ~~**2001:db8::1234::1**~~

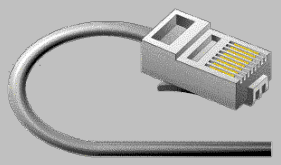


IPv6 Netzmasken

IPv6 ist classless, d.h. es gibt keine Netzklassen wie bei IPv4. Eine Angabe der Netzmaske ist zwingend notwendig. Die Netzmaske wird immer in der Slash-Notation geschrieben

2001:db8:0:1234::1**/64**

Gebräuchlich sind folgende Netzmasken
/128 eine einzelne IPv6 Adresse
/64 Ein einzelnes IPv6 Netz
/48 Mehrere Subnetze (65536 Netze)
/32 Kleinstes Netz, das von den RIRs an Provider vergeben wird

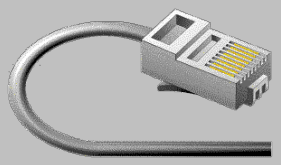


IPv6 Adress Arten

IPv6 kennt folgende Adress Arten:

Global Unicast Adressen
Global Multicast Adressen
Link Local Unicast Adressen
Link Local Multicast Adressen

Es gibt **keine** Broadcast Adresse in IPv6. Anstelle von Broadcasts werden Multicasts eingesetzt.

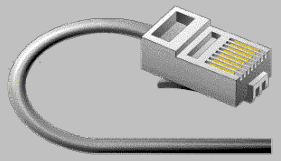


IPv6 und Ethernet

IPv6 und IPv4 können gleichzeitig verwendet werden.

Ein Ethernetframe verwendet als Type 0x86dd als Protokollangabe.

```
▷ Frame 1067: 160 bytes on wire (1280 bits), 160 bytes captured (1280 bits
▽ Ethernet II, Src: AsustekC_9d:b9:9a (e0:cb:4e:9d:b9:9a), Dst: Cisco_5d:a
  ▷ Destination: Cisco_5d:a0:33 (00:1b:0c:5d:a0:33)
  ▷ Source: AsustekC_9d:b9:9a (e0:cb:4e:9d:b9:9a)
    Type: IPv6 (0x86dd)
▷ Internet Protocol Version 6, Src: 2001:8a8:30:11::2 (2001:8a8:30:11::2),
▷ Transmission Control Protocol, Src Port: 41460 (41460), Dst Port: xmpp-c
▷ Jabber XML Messaging
```



IPv6 / IPv4

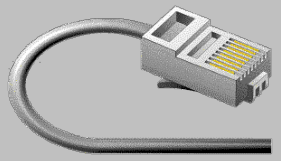
IPv6 und IPv4 können gleichzeitig verwendet werden:

```
heuer$ host heuer.org
heuer.org has address 62.48.3.35
heuer.org has IPv6 address 2001:4bf8:3::35
```

Kennt der Rechner beide Protokolle (IPv6 und IPv4), so wird meistens IPv6 bevorzugt.

Aktuell werden verschiedene Methoden erforscht wie das Umschalten zwischen IPv4 und IPv6 erfolgen kann beispielsweise happy eyeballs [1].

[1] https://tools.ietf.org/html/draft-ietf-v6ops-happy-eyeballs-02



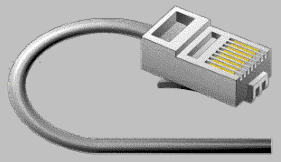
IPv6 im DNS

IPv6 Adressen können im DNS hinterlegt werden. Als Rescource Record wird ein AAAA-Record verwendet (eine IPv4 Adresse wird in einem A-Record abgelegt. Da die IPv6 Adresse viermal länger als eine IPv4 Adresse ist wurde der entsprechende Record als AAAA-Record definiert).

Die Reverse Auflösung für IPv6 erfolgt analog den Regeln von IPv4 in der **`ip6.arpa`** Domain

heuer@guybrush:~ host -t aaaa guybrush.maillink.ch
guybrush.maillink.ch has IPv6 address 2001:8a8:30:11::2

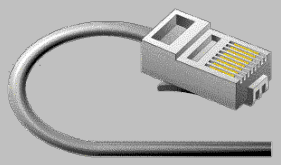
heuer@guybrush:~ host 2001:8a8:30:11::2
2.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.1.1.0.0.0.3.0.0.8.a.8.0.1.0.0.2.ip6.arpa domain name pointer guybrush.maillink.ch.



Spezielle IPv6 Adressen

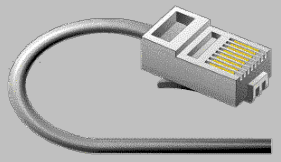
Wie bei IPv4 gibt es bei IPv6 spezielle Adressen:

::/0	entspricht der Default Route
::/128	entspricht der Adresse 0.0.0.0 Unspezifizierte Adresse, Der Host darf irgend eine seiner lokalen IPv6 Adressen verwenden.
::1/128	entspricht der loopback-Adresse



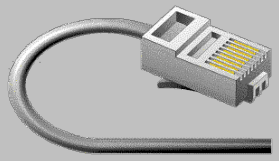
IPv6 Adressen

2000::/3	beinhaltet alle z.Z. gültigen IPv6 Adressen. Alle anderen IPv6 Adressen dürfen **NICHT** verwendet werden.
fe80::/10	Link Local Adressen
::1/128	entspricht der loopback-Adresse



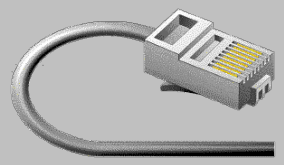
Spezielle IPv6 Netze

::ffff:0:0/96	ipv4 to ipv6 mapping. IPv4 Adressen können in IPv6 Adressen abgebildet werden. z.b. 192.168.1.1 -> ::ffff:192.168.1.1
fe80::/10	Link-Local Adresse. Diese Adressen sind nur auf einem Link gültig.
fc00::/7	Unique local unicast (RFC4193) fc00:... müssen registriert werden. fd00:... können autonom vergeben werden.

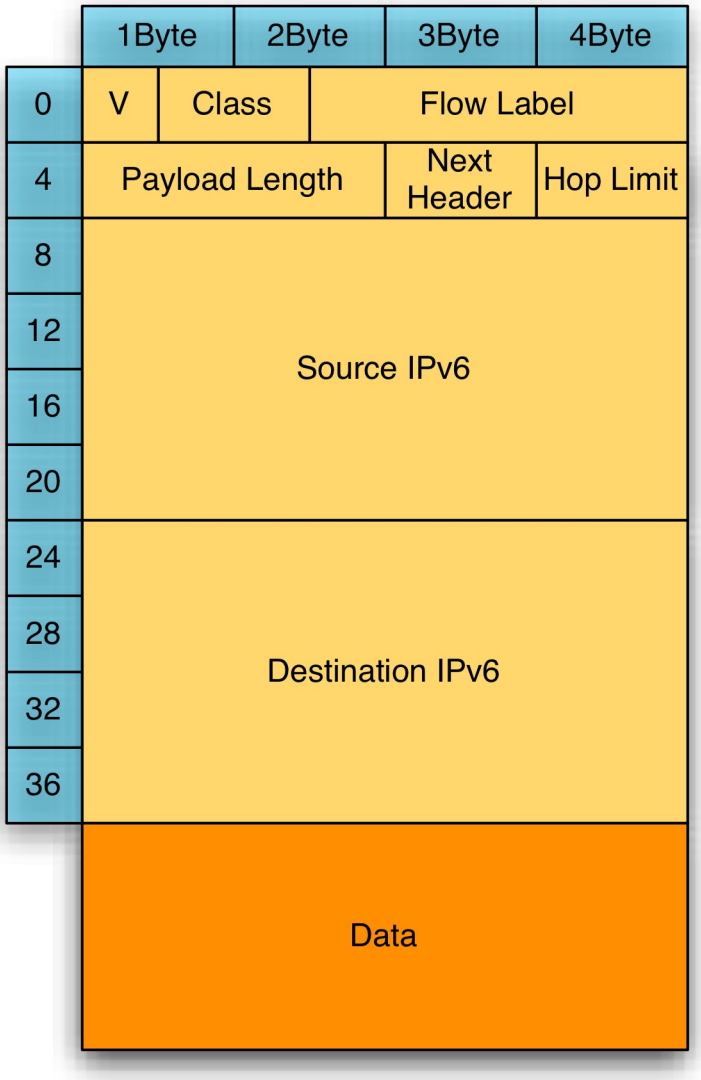


Spezielle IPv6 Netze

2001::/32	Teredo Tunneling
2001:db8::/32	Dieses Netz wird für Dokumentationen verwendet. Das Netz wird nicht geroutet.
2002::/16	6to4 Address Range



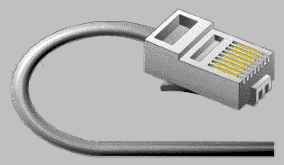
IPv6 Header



Die Felder im IPv6-Header wurden gegenüber dem IPv4-Header vereinfacht:

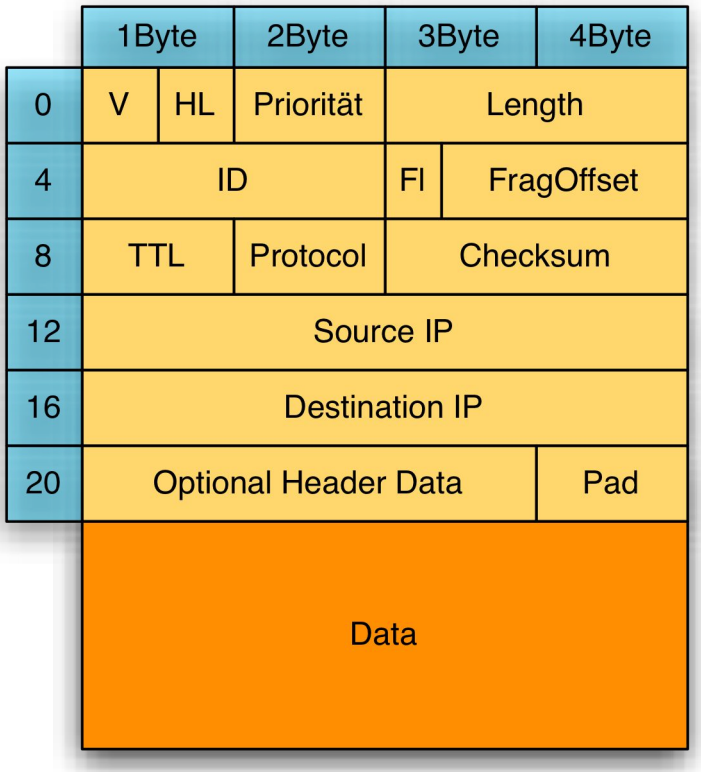
V	Version 6
Class	Traffic Class
Flow Label	Flow Label (Id)
PL-Len	Payload Length
NH	Zeiger zum Next Header
HL	Hop Limit
Src Addr	Source Adresse
Dst Addr	Destination Adresse

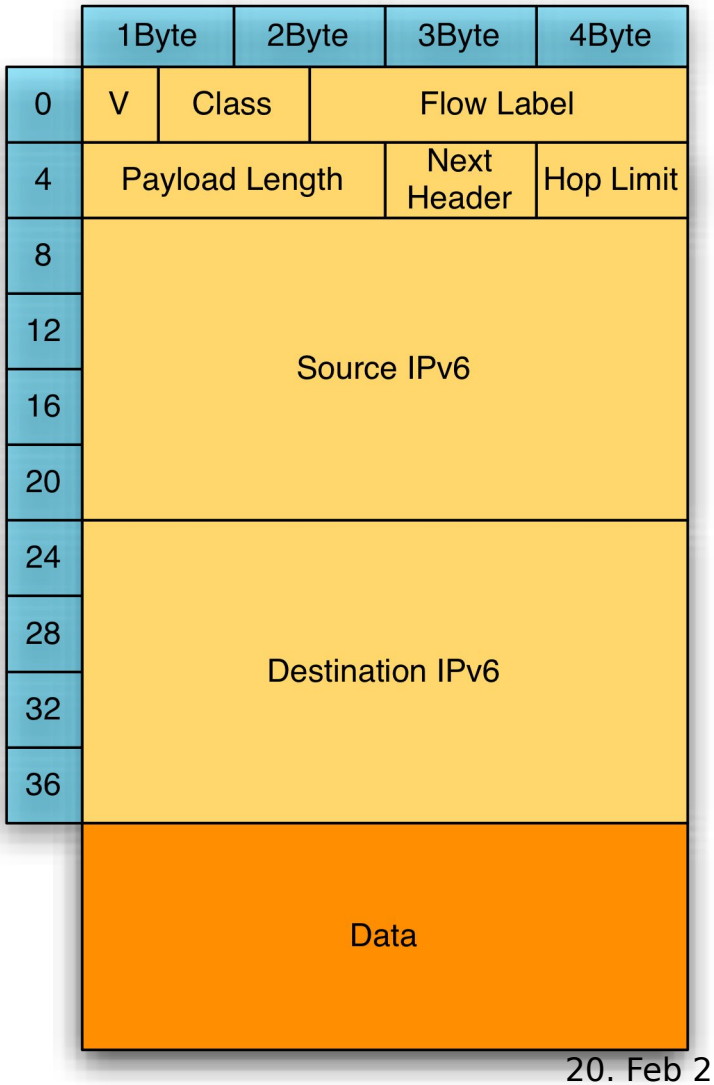
Im Paket kann die IPv6 Adresse nicht verkürzt eingetragen werden!

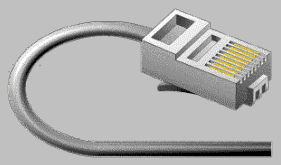


IPv4 / IPv6 Header

Vergleich vom IPv4 und IPv6 Header (ohne Headeroptionen)

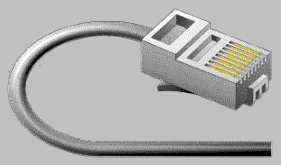






IPv4- versus IPv6-Header

IPv6	Beschreibung	IPv4
Version	Version	Version
Class	Traffic Class	~ Prio
Flow Label	Flow Label (Id)	ID/Sequenz
PL-Len	Payload Length	~ Length
NH	Zeiger zum Next Header	~ HeaderLength / Proto / Optional Header
HL	Hop Limit	TTL
Src Addr	Source Adresse	Src Addr
Dst Addr	Destination Adresse	Dst Addr
N Header	Weitere Header	n/a
n/a		Checksumme, Flags, Fragments

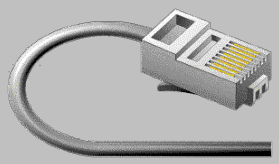


IPv6 Next Header

Mittels des **Next Header** Feldes kann dem IPv6 Header weitere optionale Informationen angehängt werden.

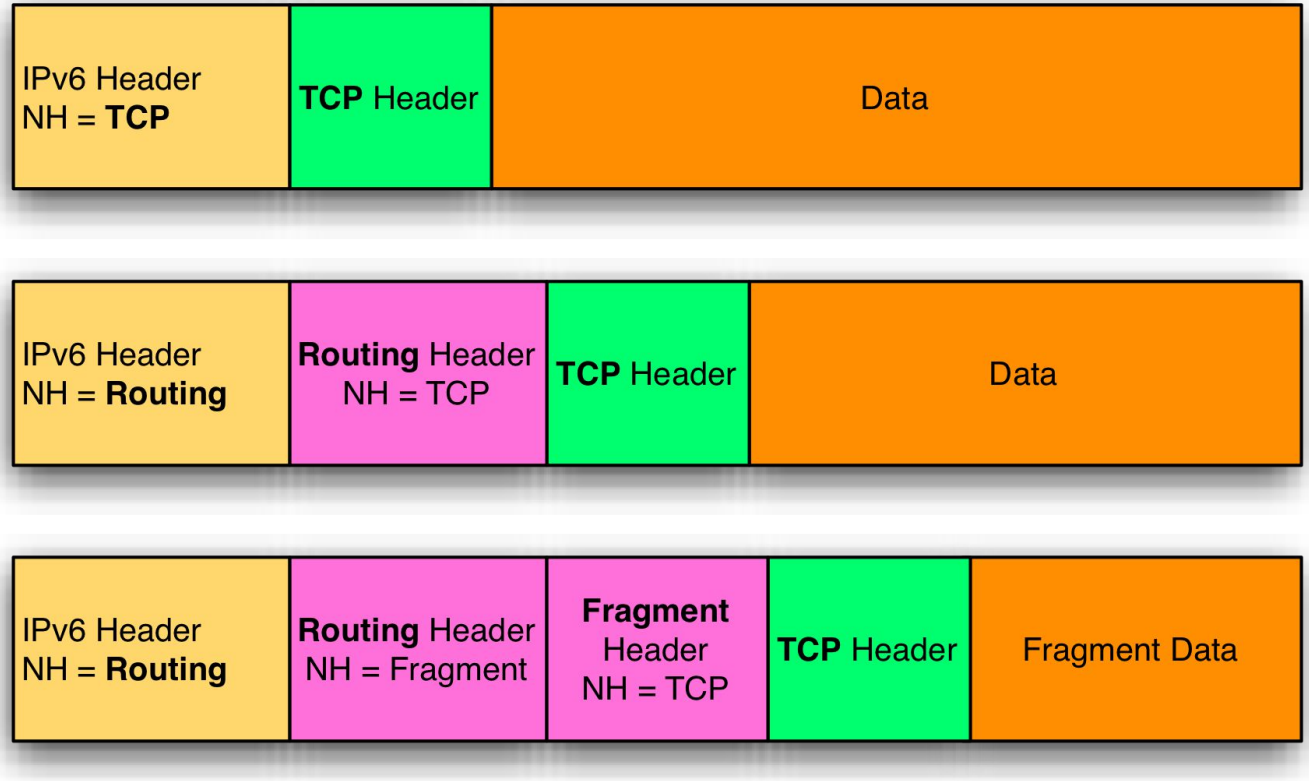
So kann der IPv6 Header nach bedarf erweitert werden.

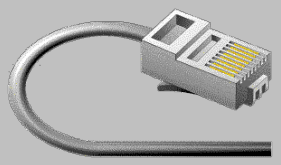
Die Header Extension werden nach dem IPv6 Header und vor dem Upper Layer Header eingefügt



IPv6 Next Header

Logischerweise bleibt für die Payload (Data) mit mehr Headern immer weniger Platz übrig.

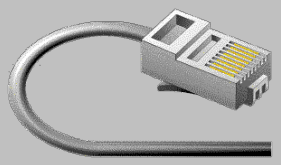




IPv6 Header

Beispiel eines IPv6 Paketes. Der Next Header ist grün markiert:

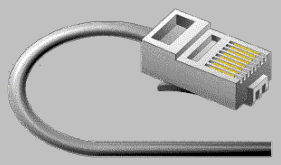
```
▸ Frame 15570: 581 bytes on wire (4648 bits), 581 bytes captured (4648 bits)
▸ Ethernet II, Src: Cisco_5d:a0:33 (00:1b:0c:5d:a0:33), Dst: AsustekC_9d:b9:9a
▾ Internet Protocol Version 6, Src: 2001:4dd0:fd76::4 (2001:4dd0:fd76::4), Dst:
  ▸ 0110 .... = Version: 6
  ▸ .... 0000 0000 .... .... .... .... .... = Traffic class: 0x00000000
    .... .... .... 0000 0000 0000 0000 0000 = Flowlabel: 0x00000000
    Payload length: 527
    Next header: TCP (0x06)
    Hop limit: 54
    Source: 2001:4dd0:fd76::4 (2001:4dd0:fd76::4)
    Destination: 2001:8a8:30:11::2 (2001:8a8:30:11::2)
▸ Transmission Control Protocol, Src Port: http (80), Dst Port: 50099 (50099),
▸ [4 Reassembled TCP Segments (4119 bytes): #15562(1208), #15564(1208), #15568(
▸ Hypertext Transfer Protocol
▸ Portable Network Graphics
```



IPv6 Next Header

Beispiel eines fragmentierten IPv6 Paketes. Der Fragment Header ist grün markiert:

```
▷ Frame 312055: 206 bytes on wire (1648 bits), 206 bytes captured (1648 bits)
▷ Ethernet II, Src: AsustekC_9d:b9:9a (e0:cb:4e:9d:b9:9a), Dst: Cisco_5d:a0:33 (00:1b:0c:5d:a0:3
▽ Internet Protocol Version 6, Src: 2001:8a8:30:11::2 (2001:8a8:30:11::2), Dst: 2001:4bf8:3::35
  ▷ 0110 .... = Version: 6
  ▷ .... 0000 0000 .... .... .... .... .... = Traffic class: 0x00000000
    .... .... .... 0000 0000 0000 0000 0000 = Flowlabel: 0x00000000
    Payload length: 152
    Next header: IPv6 fragment (0x2c)
    Hop limit: 64
    Source: 2001:8a8:30:11::2 (2001:8a8:30:11::2)
    Destination: 2001:4bf8:3::35 (2001:4bf8:3::35)
  ▽ Fragmentation Header
      Next header: ICMPv6 (0x3a)
      0000 1011 0011 0... = Offset: 358 (0x0166)
      .... .... .... ...0 = More Fragment: No
      Identification: 0x68e1c6f7
  ▷ [3 IPv6 Fragments (3008 bytes): #312053(1432), #312054(1432), #312055(144)]
▽ Internet Control Message Protocol v6
    Type: Echo (ping) request (128)
```

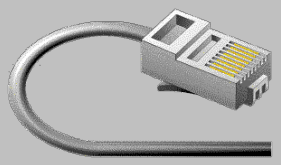


IPv6 Next Header

Folgende Next Header sind für IPv6 definiert.

0	Hop by Hop Option
43	Routing Header
44	Fragment Header
50	ESP Header
51	Authentication Header
59	No Next Header
60	Destination Option Header
135	Mobility Header

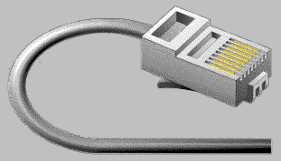
Entspricht der Eintrag nicht einer dieser Nummern ist der Next Header ein Upper Protocol (TCP, UDP, ...) Header



IPv6 Upper Layer Protokolle

Die meisten Layer 4 Protokolle sind unverändert:

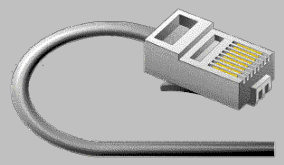
- **UDP**, **TCP** sind unverändert
- ICMP ist als **ICMPv6** implementiert
- IPSec ist ein integraler Bestandteil von IPv6 und kann mittels zusätzlichen Header realisiert werden.



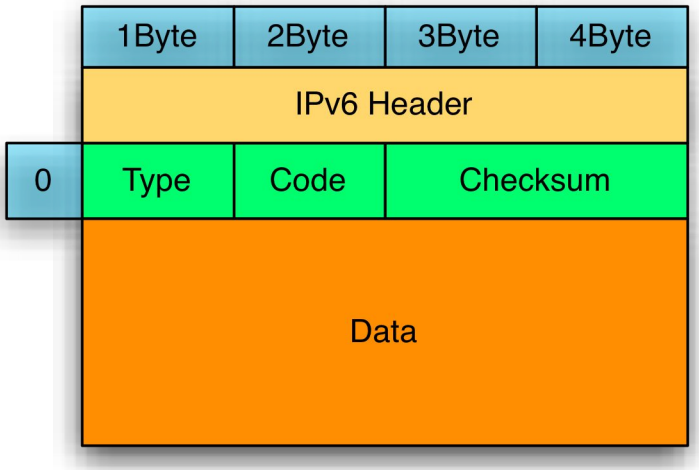
IPv6 ICMP

IPv6 verwendet wie IPv4 ICMP Meldungen um den Absender über spezielle Bedingungen zu informieren.
Dazu verwendet IPv6 eigene ICMP Meldungen, die im Protokoll ICMPv6 spezifiziert sind.

Der Aufbau vom ICMPv6 Header ist gegen über den ICMPv4 Header etwas vereinfacht.

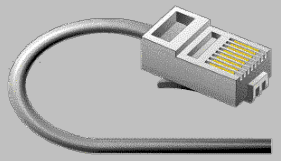


ICMPv6 Paket



ICMP-Paket basiert auf IP, darum muss vor dem ICMP-Paket ein IP-Header stehen!

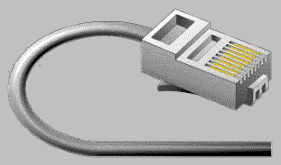
Type:	Art der ICMP Nachricht
Code:	Detaillierte Information zur Nachricht
Checksum:	Checksumme der ICMP Nachricht
Data:	Weitere Daten (Dies ist meistens der Header vom Paket, das die Meldung verursachte)



ICMPv6 Type

Im Vergleich zu ICMPv4 verwendet ICMPv6 eigene Werte!

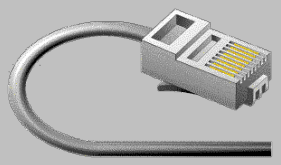
Wert	Bedeutung
1	**Destination unreachable**
2	Packet too big
3	**Time exceeded**
4	Parameter Problem
128	**Echo Request**
129	**Echo Replay**
130	Multicast Listener Query
131	Multicast Listener Report
132	Multicast Listener Done
133	Router Solicitation
134	Router Advertisement
135	Neighbour Solicitatioin
136	Neighbour Advertisment



ICMPv6 Echo request / replay

```
▷ Frame 37: 1462 bytes on wire (11696 bits), 1462 bytes captured (11
▷ Ethernet II, Src: AsustekC_9d:b9:9a (e0:cb:4e:9d:b9:9a), Dst: Cisc
▷ Internet Protocol Version 6, Src: 2001:8a8:30:11::2 (2001:8a8:30:1
▽ Internet Control Message Protocol v6
    Type: Echo (ping) request (128)
    Code: 0
    Checksum: 0x16e5 [correct]
    Identifier: 0x3289
    Sequence: 1
    [Response In: 38]
  ▽ Data (1400 bytes)
      Data: 0a51674f00000000b8fb060
      [Length: 1400]
```

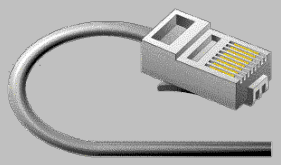
```
▷ Frame 38: 1462 bytes on wire (11696 bits),
▷ Ethernet II, Src: Cisco_5d:a0:33 (00:1b:0c:
▷ Internet Protocol Version 6, Src: 2001:4bf8
▽ Internet Control Message Protocol v6
    Type: Echo (ping) reply (129)
    Code: 0
    Checksum: 0x15e5 [correct]
    Identifier: 0x3289
    Sequence: 1
    [Response To: 37]
    [Response Time: 3.528 ms]
  ▽ Data (1400 bytes)
      Data: 0a51674f00000000b8fb0600000000010
      [Length: 1400]
```



IPv6 neighbor discovery

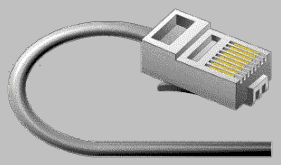
IPv6 Hosts können verschiedene Netzwerkparamter aus dem Netzwerk ziehen:

- Router Discovery
- Prefix Discovery
- Address Autoconfiguration
- Address Resolution
- Neighbor unreachability Detection
- Duplicate Address Detection
- Redirection



IPv6 Router Discovery

Bei IPv4 muss der Default-Router entweder per DHCP oder manuell konfiguriert werden.
Bei IPv6 kann ein Host mittels der ICMPv6 Router Solicitation Meldung nach einem Router fragen.
Ist ein Router im entsprechenden Netzwerksegment aktiv, sendet er eine Router Advertisement Meldung an den Host zurück.
Die Router senden periodisch Router Advertisement Meldungen aus.



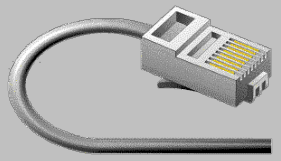
IPv6 Router Discovery

In der Router Advertisement Meldung Sind verschiedene Netzwerk Parameter enthalten:

- Link-Adresse
- MTU
- Prefix

```
▷ Frame 2412: 122 bytes on wire (976 bits), 122 bytes captured (97
▷ Ethernet II, Src: Cisco_5d:a0:33 (00:1b:0c:5d:a0:33), Dst: IPv6m
▷ 802.1Q Virtual LAN, PRI: 0, CFI: 0, ID: 5
▷ Internet Protocol Version 6, Src: fe80::21b:cff:fe5d:a033 (fe80:
▽ Internet Control Message Protocol v6
    Type: Router Advertisement (134)
    Code: 0
    Checksum: 0x61ea [correct]
    Cur hop limit: 64
  ▷ Flags: 0x00
    Router lifetime (s): 1800
    Reachable time (ms): 0
    Retrans timer (ms): 0
  ▷ ICMPv6 Option (Source link-layer address : 00:1b:0c:5d:a0:33)
  ▷ ICMPv6 Option (MTU : 1500)
  ▷ ICMPv6 Option (Prefix information : 2001:8a8:30:13::/64)
```

Mit diesen Werten kann eine Host sich selbst eine IPv6 Adresse zuweisen (stateless address autoconfiguration).

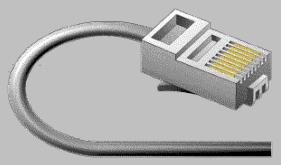


IPv6 und ARP?

ARP hat mit IPv6 nichts am Hut. Ein neues Protokoll, das die Verbindung zwischen den IPv6- und MAC-Adressen herstellt ist notwendig.

Dies ist in ICMPv6 integriert.

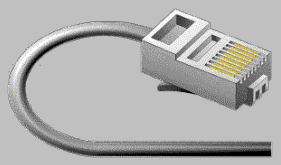
Der Mechanismus funktioniert ähnlich wie bei ARP.
Der eine Rechner sendet einen ~~Broadcast~~ Multicast.
Der gesuchte Host anwortet mit einem Unicast.



IPv6 Neighbour Solicitation

Der Host, der die MAC-Adresse eines anderen Hosts benötigt sendet eine Neighbour Solicitation (ICMPv6 Type 135) an die Multicast-Adresse (ff02::1:ff00:0/104 und rechte 3 Octets der Ziel-IP).

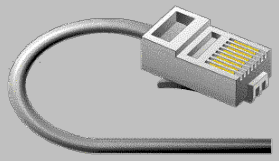
```
▷ Frame 163606: 90 bytes on wire (720 bits), 90 bytes captured (720 bits)
▷ Ethernet II, Src: AsustekC_9d:b9:9a (e0:cb:4e:9d:b9:9a), Dst: IPv6mcast_ff:00:00:01
▷ 802.1Q Virtual LAN, PRI: 0, CFI: 0, ID: 3
▷ Internet Protocol Version 6, Src: fe80::e2cb:4eff:fe9d:b99a Dst: ff02::1:ff00:1 (ff
▽ Internet Control Message Protocol v6
    Type: Neighbor Solicitation (135)
    Code: 0
    Checksum: 0x7f2a [correct]
    Reserved: 00000000
    Target Address: 2001:8a8:30:11::1 (2001:8a8:30:11::1)
  ▽ ICMPv6 Option (Source link-layer address : e0:cb:4e:9d:b9:9a)
      Type: Source link-layer address (1)
      Length: 1 (8 bytes)
      Link-layer address: AsustekC_9d:b9:9a (e0:cb:4e:9d:b9:9a)
```



IPv6 Neighbour Advertisement

Der gesuchte Host - sofern er online ist - anwortet mit einer Neighbour Advertisement (ICMPv6 Type 136) Unicast Meldung an den Fragesteller.

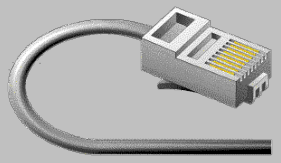
```
▷ Frame 163607: 90 bytes on wire (720 bits), 90 bytes captured (720 bits)
▷ Ethernet II, Src: Cisco_5d:a0:33 (00:1b:0c:5d:a0:33), Dst: AsustekC_9d:b9:9a (e0:cb:4e:9d:b9:9a)
▷ 802.1Q Virtual LAN, PRI: 0, CFI: 0, ID: 3
▷ Internet Protocol Version 6, Src: 2001:8a8:30:11::1 (2001:8a8:30:11::1), Dst: fe80::e2cb:4eff:fe9
▽ Internet Control Message Protocol v6
    Type: Neighbor Advertisement (136)
    Code: 0
    Checksum: 0xae9c [correct]
  ▷ Flags: 0xe0000000
    Target Address: 2001:8a8:30:11::1 (2001:8a8:30:11::1)
  ▽ ICMPv6 Option (Target link-layer address : 00:1b:0c:5d:a0:33)
      Type: Target link-layer address (2)
      Length: 1 (8 bytes)
      Link-layer address: Cisco_5d:a0:33 (00:1b:0c:5d:a0:33)
```



Duplicate Address Detection DAD

Wenn eine IPv6 Adresse bei einem Interface konfiguriert wird, so sendet das Interface zuerst eine **Neighbour Solicitation** Meldung für die eigene Adresse aus.

Wenn nun eine Meldung zurück kommt, bedeutet das, das die IPv6 Adresse schon von einem anderen Host verwendet wird und daher nicht selber verwendet werden darf.



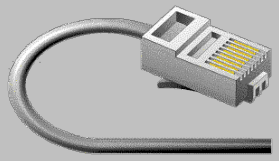
IPv6

Bei einem Broswer gibt es Problem wenn man eine IPv6 Adresse da der Doppepunkt verwendet wird um die Portangabe abzutrennen:

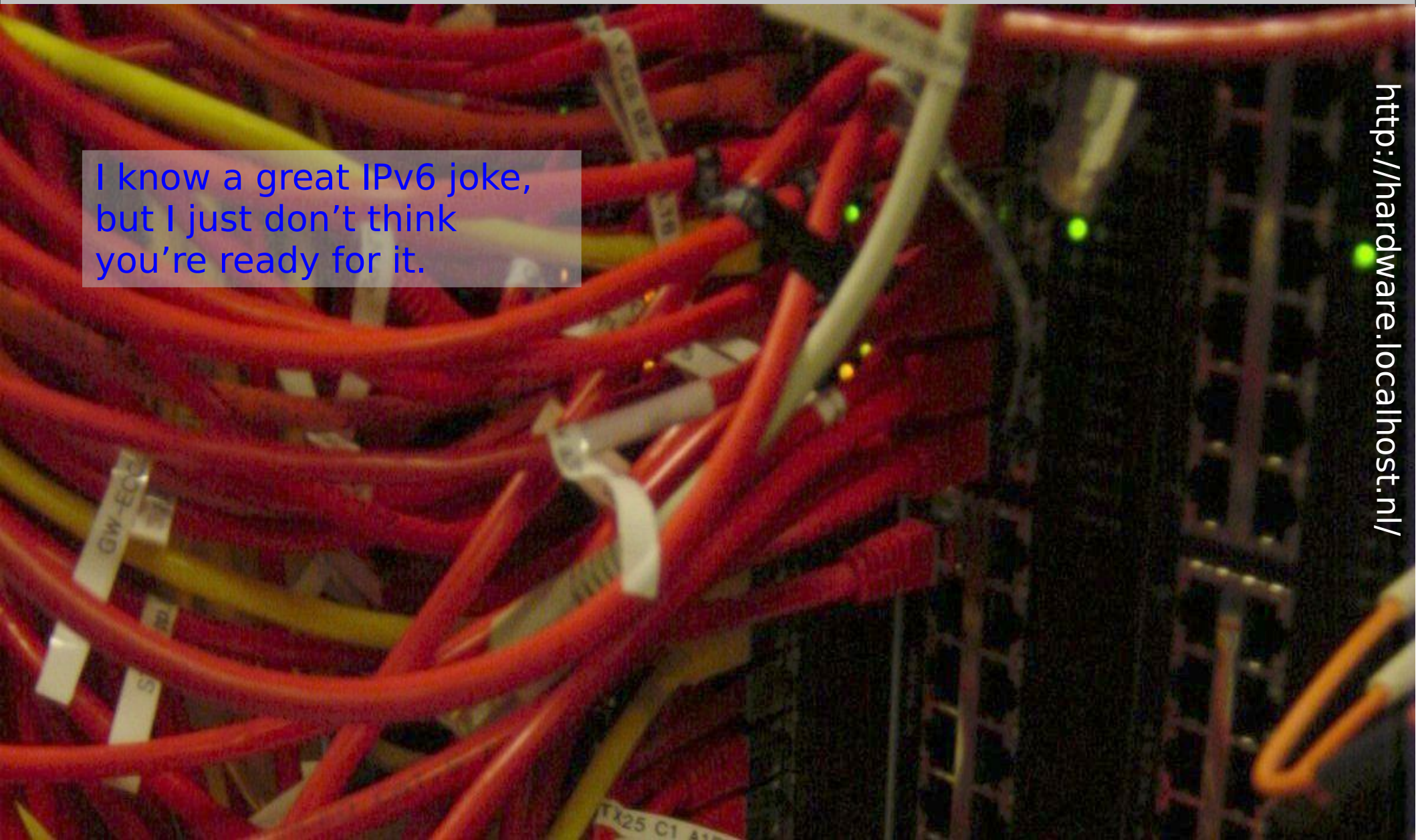
```
scheme://domain:port/path?query_string#fragment_id
```

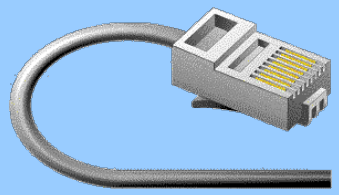
Um die Interpretation der IPv6 Adresse sicherzustellen, wird die IPv6-Adresse in eckigen Klammern notiert:

```
http://[2001:db8::cafe:80]:8080/
```



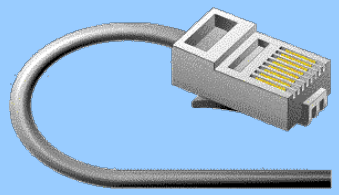
Fragen?


I know a great IPv6 joke,
but I just don’t think
you’re ready for it.
http://hardware.localhost.nl/



IPv6 Hausaufgaben

1) Untersuchen sie, wie der Rechner die IPv6-Link-Local-Adresse aus der MAC-Adresse bildet.

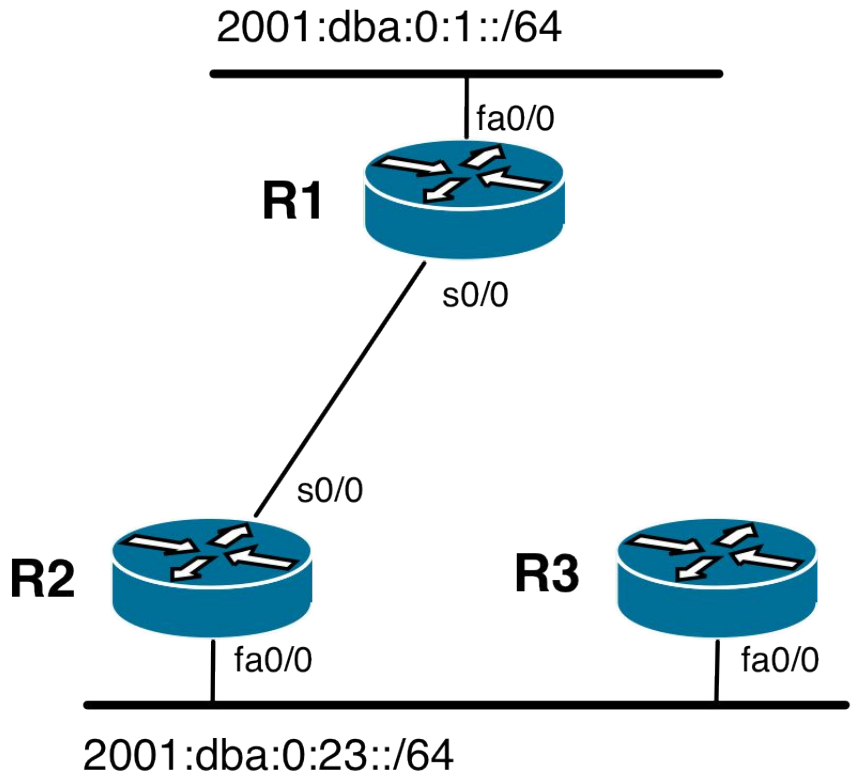


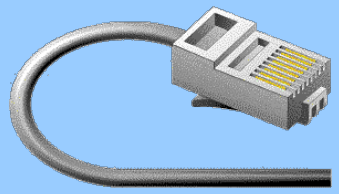
IPv6 Hausaufgaben

2) Konfigurieren sie in der Workbench folgendes Netzwerk und verifizieren sie die Konnektivität.

Für den Seriellen Link zwischen R1 und R2 dürfen nur link local Adressen verwendet werden.

IPv6 routen können mit dem Befehl
ipv6 route <netz/mask> [interface] <target>
konfiguriert werden.





IPv6 Hausaufgaben

3) Sie müssen das Netzwerk der Firma Hype GmbH erstellen. Sie haben dazu folgende Angaben bekommen:
Die Firma hat 4 Abteilungen, die jede eine getrenntes Netz bekommen soll.
Die grösste Abteilung wird 20 PC und 10 Netzwerk-Drucker bekommen.
Die drei anderen Abteilungen werden mit Je 10 PCs und je 1 Netzwerk-Drucker auskommen. Die Firma erwartet, dass in der nächsten Zeit ca. 20% mehr PCs und Drucker angeschlossen werden müssen.

Als Netzwerk haben sie vom Provider 2001:db8:old1:::/48 bekommen.
Definieren sie die notwendigen Netze so dass jeweils alle Rechner / Drucker einer Abteilungen ans Netz angeschlossen werden können und genügend Reservekapazität vorhanden ist.

Wo liegt der Unterschied der IPv6 Lösung gegenüber der IPv4 Lösung dieser Aufgabe?