Das Internet Protocol der Version 4

von Patrick Scheips

Das Internet Protocol der Version 4

I Das IP-Datagramm

II Die IP-Adresse

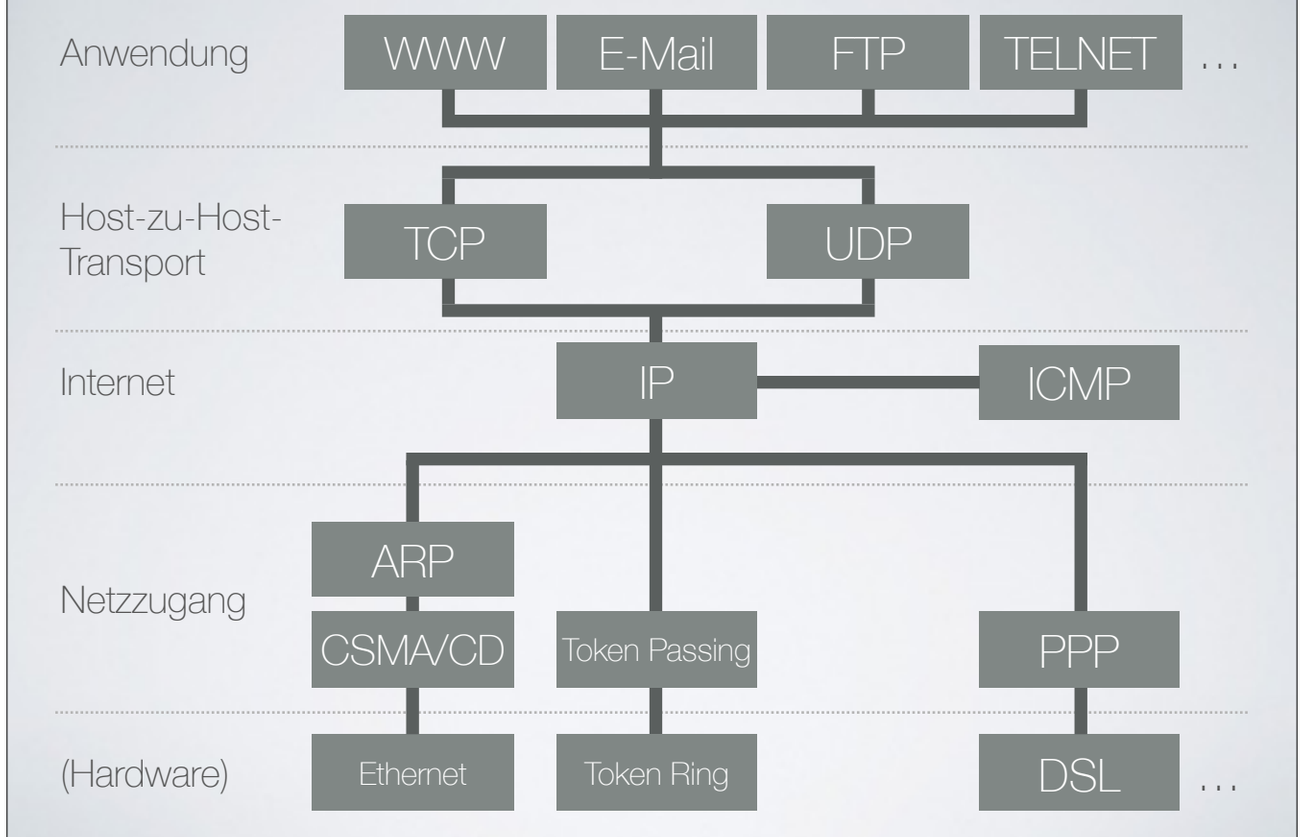
III Die IP-Adressklassen

- Kapitel 3 ist ziemlich umfangreich; Adressklassen sind überholt, dienen aber dem Verständnis u. A. für die Einführung des Nachfolgers CIDR
-

Das Internet Protocol der Version 4

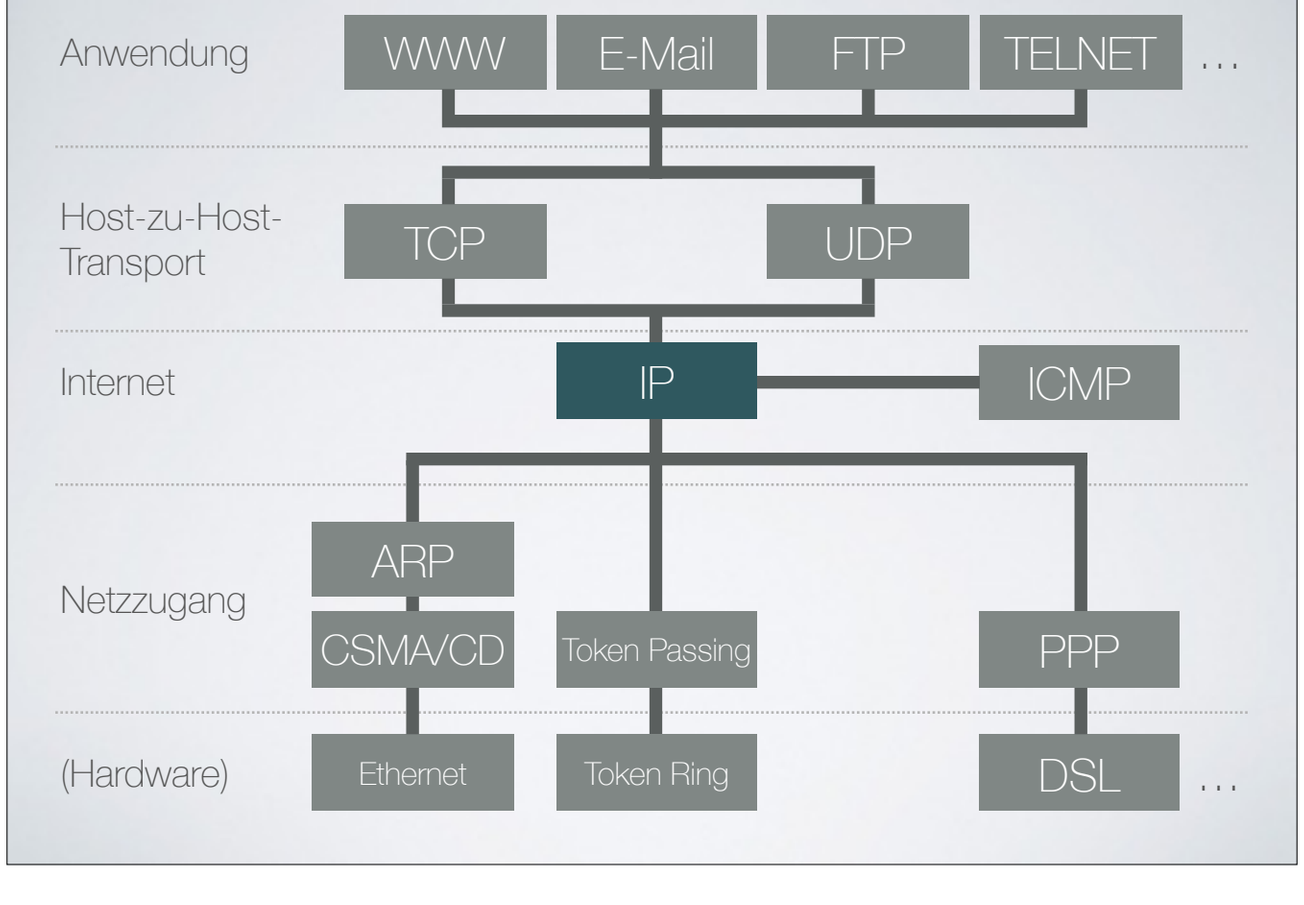
- Kapitel 4 ist auch ziemlich umfangreich; Thema ist, wie man überhaupt eine IP-Adresse erhält und welche Besonderheiten es bei IP-Adressnetzen gibt
- Kapitel 5 ist ebenfalls ziemlich umfangreich; Thema ist der Nachfolger von IP-Klassen

I Das IP-Datagramm



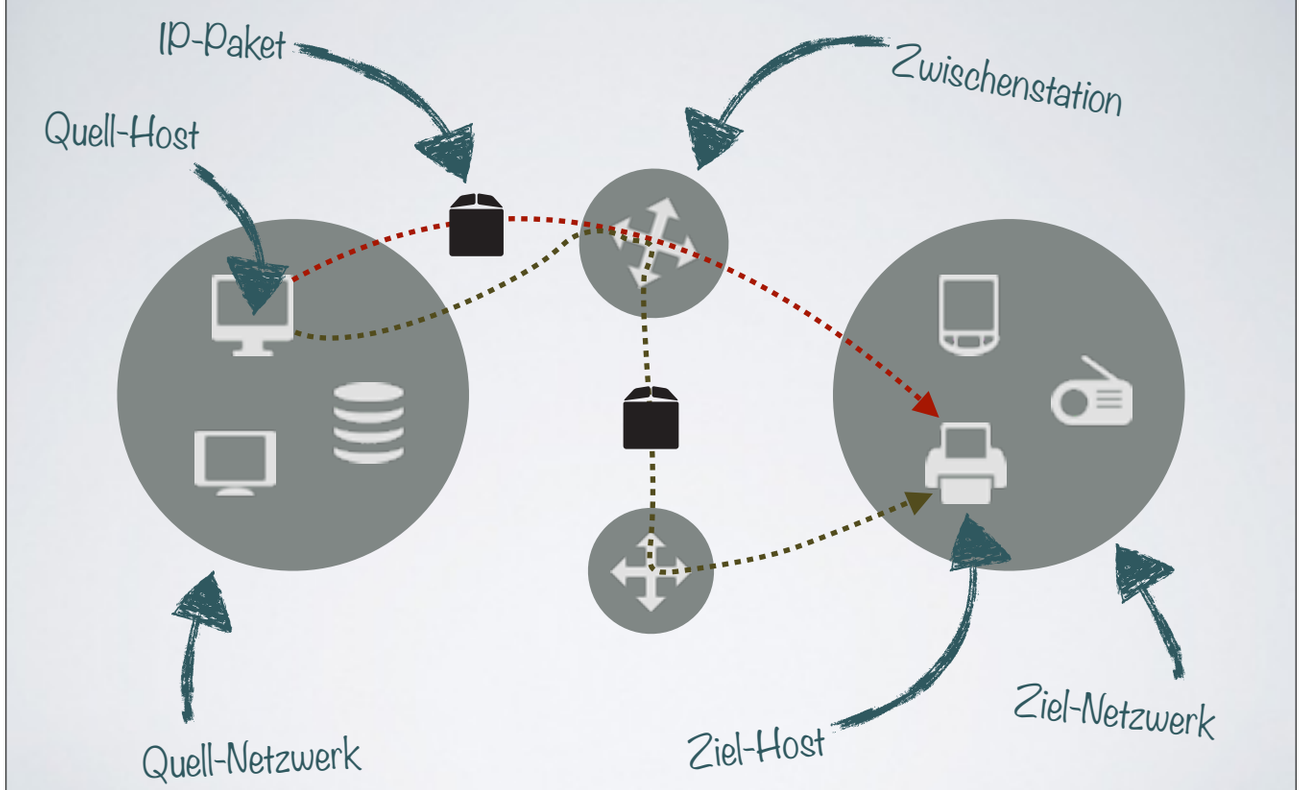
- TCP/IP-Protokollstapel (konkrete Implementierung des OSI-Referenzmodells)
  - Internetschicht-Protokolle regeln Rechneradressierung und Datenübertragung an korrekten Rechner; kümmern sich bei Bedarf um Weiterleitung von Daten in Teilnetze (Routing – das Thema wird hier nur angerissen => eigener Vortrag)
  - (Auf der Host-zu-Host-Transportschicht werden die Daten in Pakete unterteilt sowie mit der Information versehen, welche Anwendung auf dem einen Host diese Daten an welche Anwendung auf dem anderen sendet.)
- Hardware ist kein Teil des TCP/IP-Protokollstapels

I Das IP-Datagramm



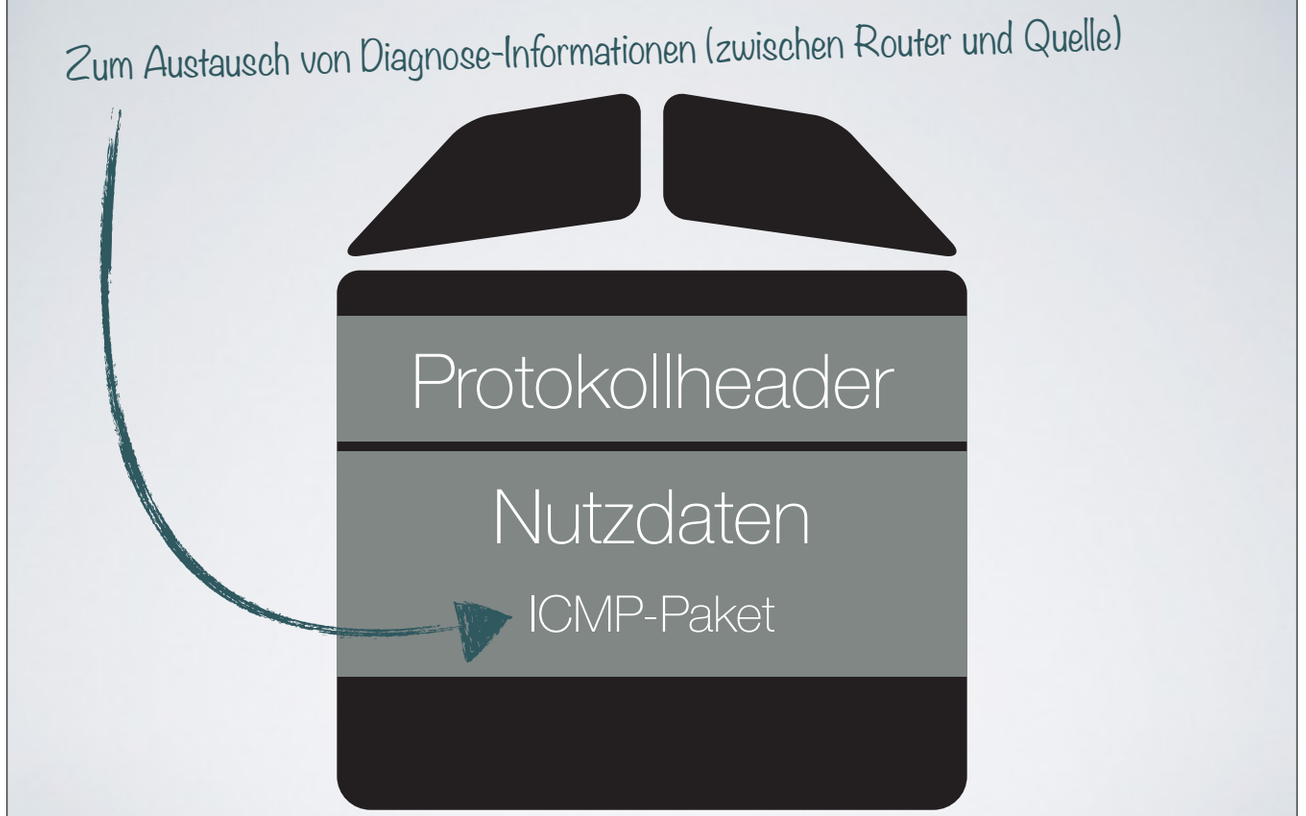
- TCP/IP-Protokollstapel (konkrete Implementierung des OSI-Referenzmodells)
  - Internetschicht-Protokolle regeln Rechneradressierung und Datenübertragung an korrekten Rechner; kümmern sich bei Bedarf um Weiterleitung von Daten in Teilnetze (Routing – das Thema wird hier nur angerissen => eigener Vortrag)
  - (Auf der Host-zu-Host-Transportschicht werden die Daten in Pakete unterteilt sowie mit der Information versehen, welche Anwendung auf dem einen Host diese Daten an welche Anwendung auf dem anderen sendet.)
- Hardware ist kein Teil des TCP/IP-Protokollstapels

I Das IP-Datagramm



- Netzinterner und netzübergreifender Datenaustausch zwischen Teilnehmer (Rechner) erfolgt über sog. IP-Datagramme
- Wahl des Weges dieser IP-Datagramme nennt man Routing (nicht Teil dieses Vortrags)
- Das Internetprotokoll (als Version 4 im Jahr 1981 definiert) dient zur Vermittlung (= Adressierung) solcher Datagramme
    - Dazu erhalten alle Stationen und Endgeräte im Netzwerk eine eigene Adresse, die die Station selbst und das Netz, in der sich die Station befindet, identifizieren
    - **Das Mapping von Adresse zu Name ist Aufgabe höherer Schichten (Host-zu-Host-Transport)**
- Das IP-Protokoll ist verbindungslos, d. h. es wird nicht überprüft, ob der Empfänger überhaupt erreichbar ist
- IP-Datagramme können **fragmentiert** werden (weitere Aufgabe vom IP-Protokoll!), wenn sie für Netzwerke, die sie auf der Route passieren, zu groß sind (Anzahl an Bytes, die eine Netzwerktechnologie transportieren kann, wird MTU – Maximum Transfer Unit – genannt)
    - Fragmentierung kann man auch verhindern, dazu gleich
- Jedes Datagramm wird unabhängig voneinander behandelt
- Das IP-Protokoll garantiert keine Reihenfolge der Ankunft von IP-Datagrammen beim Empfänger
- Datagramme können z. B. wegen Überlastung verloren gehen (später mehr dazu)
- Es gibt keine Empfangsbestätigung auf der IP-Schicht
- Wie solche IP-Datagramme aufgebaut sind (wichtig damit IP-Protokoll überhaupt funktioniert), sehen wir jetzt


Protokollheader
Nutzdaten



- ICMP = Internet Control Message Protocol
- ICMP ist verpflichtend für jeden Rechner und jeden Router

MTU ➜ Fragmentierung

Geschwindigkeit

Effizienz

Welche Informationen beinhaltet der IPv4-Protokollheader?

Netzwerkübergreifende Kommunikation

Anwendungszwecke

- Datagramm ist der Bezeichnung eines Datenpaketes auf der Internetschicht des TCP/IP-Protokollstapels, auf der das IP arbeitet

I Das IP-Datagramm

RFC 791

Byte	0		1	2	3
0	Version	IHL	DSCP & ECN	Paket-Gesamtlänge	
4	Identifikation			Flags	Fragment-Offset
8	Time to Live		Protokoll	Header-Prüfsumme	
12	Quelladresse				
16	Zieladresse				
20	Optionen				Padding
...	evtl. weitere Optionen				

- IP-Header enthält Steuerdaten, welche das Internet Protocol zu einem Datenpaket hinzufügt, das ihm vom übergeordneten Transportprotokoll übergeben wird
- Minimale Länge des IP-Headers beträgt 20 Byte
- Es können bis zu 40 Byte Optionen dazukommen

Das IP-Datagramm

RFC 791

Byte	0		1	2	3
0	Version	IHL	DSCP & ECN	Paket-Gesamtlänge	
4	Identifikation			Flags	Fragment-Offset
8	Time to Live		Protokoll	Header-Prüfsumme	
12	Quelladresse				
16	Zieladresse				
20	Optionen				Padding
...	evtl. weitere Optionen				

- Version des Internet Protocols (hier 4)
- Protokoll = Nummer die angibt, für welches Transportprotokoll (wie TCP oder UDP) der Inhalt dieses Datagramms bestimmt ist

I Das IP-Datagramm

RFC 791

Byte	0		1	2	3
0	Version	IHL	DSCP & ECN	Paket-Gesamtlänge	
4	Identifikation			Flags	Fragment-Offset
8	Time to Live		Protokoll	Header-Prüfsumme	
12	Quelladresse				
16	Zieladresse				
20	Optionen				Padding
...	evtl. weitere Optionen				

- „Internet Header Length“ als Vielfaches von 32 Bit
  - Maximalwert: 1111 Binär (15 Dezimal) * 32 Bit = 480 Bit = 60 Byte
  - Minimalwert: 5 * 32 Bit = 160 Bit = 20 Byte (festgelegt in der RFC 791)
- Die Gesamtlänge des Paketes inklusive Header und Nutzdaten

I Das IP-Datagramm

RFC 791

Byte	0		1	2	3
0	Version	IHL	DSCP & ECN	Paket-Gesamtlänge	
4	Identifikation			Flags	Fragment-Offset
8	Time to Live		Protokoll	Header-Prüfsumme	
12	Quelladresse				
16	Zieladresse				
20	Optionen				Padding
…	evtl. weitere Optionen				

- Früher Type of Service: Informationen, die zur Priorisierung von IP-Paketen genutzt werden können (z. B. wenn geringe Latenz wie bei VoIP notwendig ist), seit 2011 (RFC 3168):
  - Differentiated services code point: Ein Zahlenwert-Code (von der IANA verwaltet) klassifiziert ein Paket, d. h. legt Netzwerkrichtlinien und -regeln fest, nicht aber die Priorität selbst. Diese wird vom Router selbst vergeben, indem er ein Weiterleitungsverhalten (PHB, Per Hop Behaviour) vergibt, welches u. a. über die Bandbreite und Verhalten für den Verlust von Paketen regelt
  - Explicit Congestion Notification: Ein Router kann durch Setzen dieses Bits im IP-Header kennzeichnen, dass im Netz eine Überlastung droht. Erreicht ein Paket das Ziel, kann es so der Quelle über diese Überlastung informieren sodass diese die Datenrate reduzieren kann. Folge: Weniger wegen Überlastung verworfene Pakete
- Anekdote: 1999 bot die c’t angeblich [als Aprilscherz] ein Tool zum Download an, mit dem man die Quality-of-Service-Informationen manipulieren könne, um die Geschwindigkeit von Internetverbindungen zu erhöhen.

I Das IP-Datagramm

RFC 791

Byte	0		1	2	3
0	Version	IHL	DSCP & ECN	Paket-Gesamtlänge	
4	Identifikation			Flags	Fragment-Offset
8	Time to Live		Protokoll	Header-Prüfsumme	
12	Quelladresse				
16	Zieladresse				
20	Optionen				Padding
...	evtl. weitere Optionen				

- Ein durch den Absender Identifikationswert, um fragmentierte Datagramme zusammensetzen zu können
- Dieser Wert muss eindeutig sein für Quelle-Ziel-Paar und Protokoll solange das Paket oder seine Fragment im Internet „leben“

I Das IP-Datagramm

RFC 791

Byte	0		1	2	3
0	Version	IHL	DSCP & ECN	Paket-Gesamtlänge	
4	Identifikation			Flags	Fragment-Offset
8	Time to Live		Protokoll	Header-Prüfsumme	
12	Quelladresse				
16	Zieladresse				
20	Optionen				Padding
...	evtl. weitere Optionen				

- Kontrollflags zur Regelung der Paketfragmentierung:
  - Das erste Bit muss immer 0 sein
  - Das zweite Bit sagt, ob das Paket fragmentiert werden darf (1) oder nicht (0)
    - wenn nicht, wird das Paket ggf. verworfen, wenn es zu „enge“ Netzwerke passiert
  - Das dritte Bit sagt, ob noch ein weiteres Fragment folgt (1) oder es sich um das letzte handelt (0)
- Anekdote: Am 1. April 2003 wurde [als Aprilscherz] von Steven Bellovin (amerikanischer Sicherheitsforscher bei AT&T) in der RFC 3514 vorgeschlagen, das freie Bit zur einfacheren Erkennung von schädlichen IP-Datenpaketen zu verwenden.

I Das IP-Datagramm

RFC 791

Byte	0		1	2	3
0	Version	IHL	DSCP & ECN	Paket-Gesamtlänge	
4	Identifikation			Flags	Fragment-Offset
8	Time to Live		Protokoll	Header-Prüfsumme	
12	Quelladresse				
16	Zieladresse				
20	Optionen				Padding
...	evtl. weitere Optionen				

- Gibt an, an welcher Stelle in einem Gesamtpaket sich dieses Paket befindet, sofern es sich um ein Fragment handelt
- Das erste Fragment oder ein nicht-fragmentiertes Paket erhält den Wert 0

I Das IP-Datagramm

RFC 791

Byte	0		1	2	3
0	Version	IHL	DSCP & ECN	Paket-Gesamtlänge	
4	Identifikation			Flags	Fragment-Offset
8	Time to Live		Protokoll	Header-Prüfsumme	
12	Quelladresse				
16	Zieladresse				
20	Optionen				Padding
...	evtl. weitere Optionen				

- Falls die Empfängerstation nicht gefunden wird, sorgt der TTL dafür, dass das Paket nach einer bestimmten Anzahl (üblich: 30 bis 64) an Hops (Weiterleitungen durch Router) verworfen wird. Dazu zieht jeder Router, der das Datagramm weiterleitet, den Wert 1 ab. Ist 0 erreicht, so wird das Paket verworfen.
- Ursprünglich wurde der TTL in Sekunden angegeben, das hat sich in der Praxis aber nicht durchgesetzt

I Das IP-Datagramm

RFC 791

Byte	0		1	2	3
0	Version	IHL	DSCP & ECN	Paket-Gesamtlänge	
4	Identifikation			Flags	Fragment-Offset
8	Time to Live		Protokoll	Header-Prüfsumme	
12	Quelladresse				
16	Zieladresse				
20	Optionen				Padding
...	evtl. weitere Optionen				

- Eine Prüfsumme für eine Plausibilitätsprüfung. Ist die Prüfsumme falsch, wird das Paket nicht akzeptiert und muss erneut gesendet werden
- Es wird nur der Header überprüft, da sich die Headerdaten ständig ändern und so nicht immer zeitraubend die Prüfsumme des ganzen Paketes berechnet werden muss

I Das IP-Datagramm

RFC 791

Byte	0		1	2	3
0	Version	IHL	DSCP & ECN	Paket-Gesamtlänge	
4	Identifikation			Flags	Fragment-Offset
8	Time to Live		Protokoll	Header-Prüfsumme	
12	Quelladresse				
16	Zieladresse				
20	Optionen				Padding
...	evtl. weitere Optionen				

- Variable Länge, maximal 40 Byte, immer in 32 Bit aufgeteilt, wird bei Bedarf mit Nullen aufgefüllt (Padding)
- Werden selten verwendet, da alle auf dem Weg zum Ziel befindlichen Router diese Optionen unterstützen müssen
- Möglich sind Sicherheits-, Debugging- und Statistik-Features

I Das IP-Datagramm

RFC 791

Byte	0		1	2	3
0	Version	IHL	DSCP & ECN	Paket-Gesamtlänge	
4	Identifikation			Flags	Fragment-Offset
8	Time to Live		Protokoll	Header-Prüfsumme	
12	Quelladresse				
16	Zieladresse				
20	Optionen				Padding
...	evtl. weitere Optionen				

- IP-Adressen von Sender und Empfänger
- Mehrere Empfänger = EINE Unicast-Adresse

Das Internet Protocol der Version 4

I — Das IP-Datagramm

II — Die IP-Adresse

III — Die IP-Adressklassen

IV — Verteilung von IP-Adressen

V — CIDR, Super- & Subnetting

VI — Zusammen-fassung

IP-Adresse

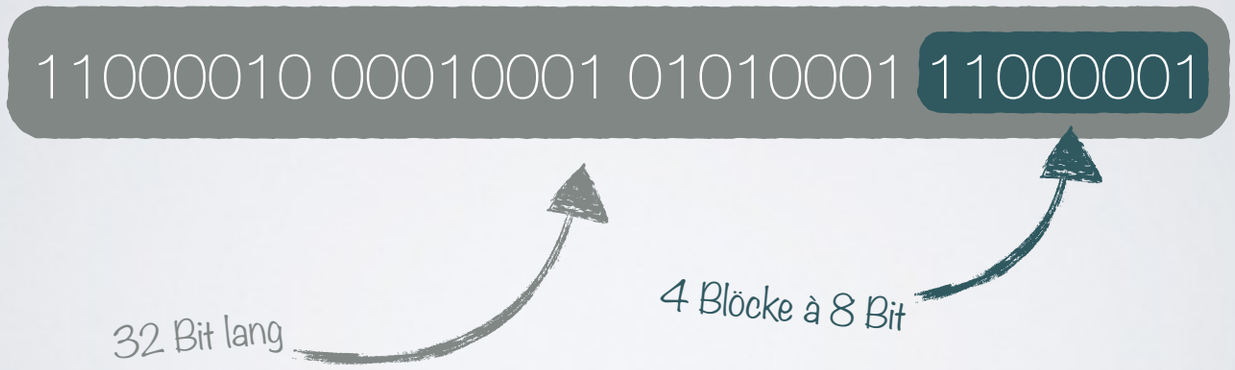
der Version IPv4

- Eine IP-Adresse identifiziert einen Host und das Netzwerk, in dem sich dieser befindet, eindeutig
- Solche IP-Adressen sind also prinzipiell einmalig

RFC 791

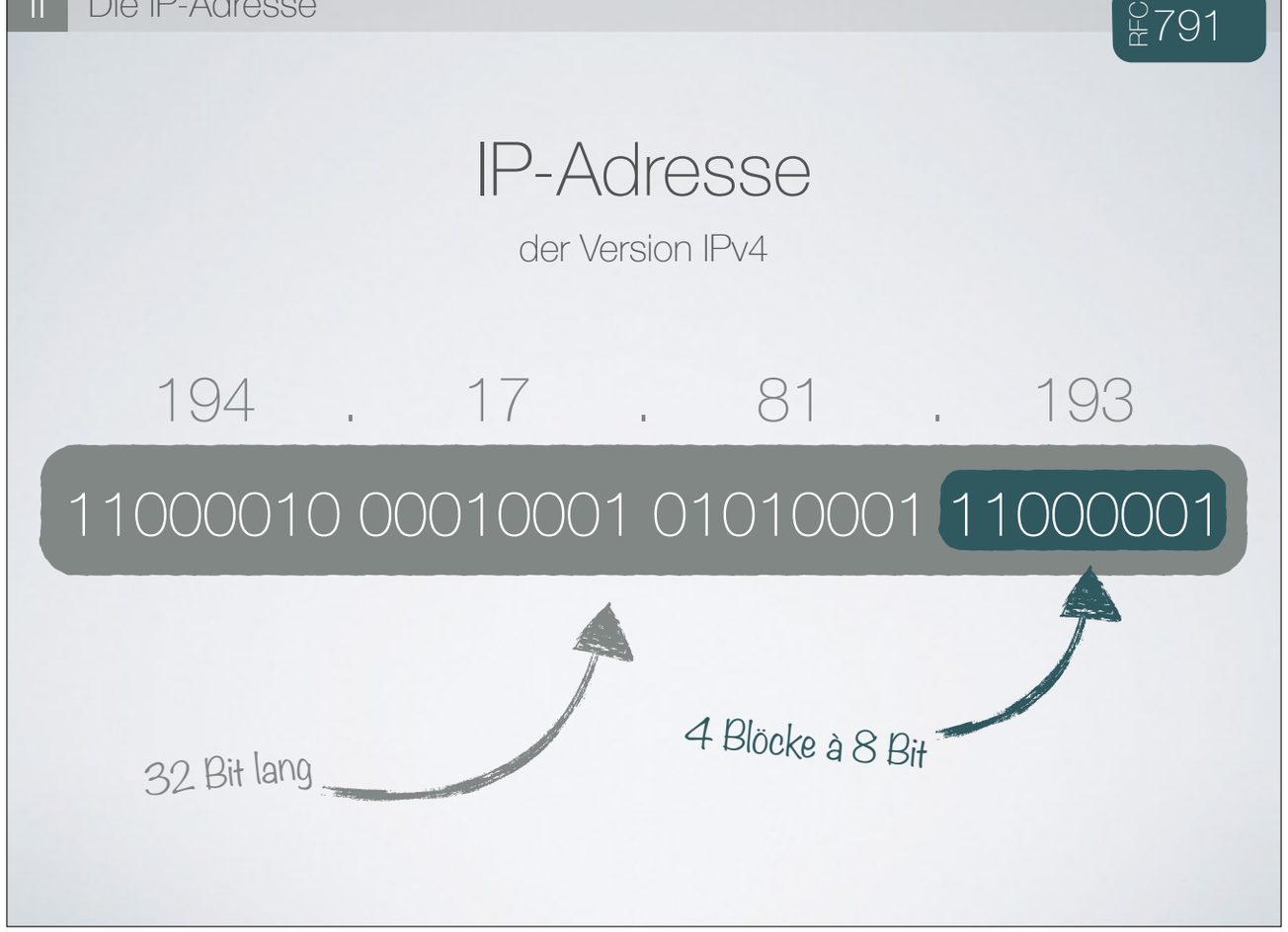
IP-Adresse

der Version IPv4



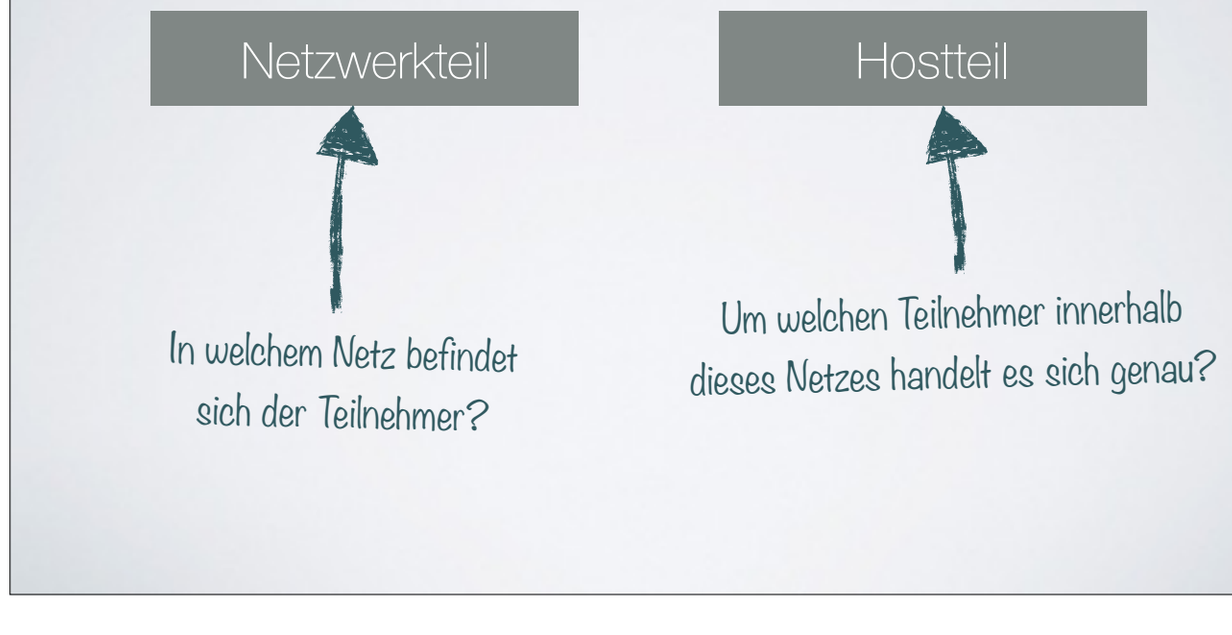
- In der Version 4 des IP-Protokolls ist eine IP-Adresse ein 32-Bit-Code, der in 4 Blöcke à 8 Bit unterteilt ist

RFC 791



- Typischerweise werden IP-Adressen – für und von uns Menschen – in vier durch Punkte getrennte Blöcke bestehend aus Dezimalzahlen zwischen 0 und 255 notiert – und nicht in Binärschreibweise
- IP-Adressklassen lassen sich an in Binär dargestellten IP-Adressen aber besser erklären, daher sind diese Beispiele nicht im Dezimalsystem notiert
- Da solch eine IP-Adresse – wie gesagt – einen Host in einem Netz eindeutig identifiziert, muss sie natürlich eine gewisse Struktur besitzen um diese Informationen zu kodieren. [KLICK]

RFC 791



- Dazu werden IP-Adressen in zwei Teile unterteilt: Einem Netzwerkteil und einem Hostteil
- Das Konzept hinter dieser Unterteilung hat sich spätestens Anfang der 90er verändert
- Wir betrachten zunächst das ursprüngliche (inzwischen veraltete und praktisch nicht mehr verwendete) Konzept der IP-Adressklassen [KLICK]

Das Internet Protocol der Version 4

I

Das IP-Datagramm

II

Die IP-Adresse

III

Die IP-Adressklassen

IV

Verteilung von IP-Adressen

V

CIDR, Super- & Subnetting

VI

Zusammen-fassung

III Die IP-Adressklassen

RFC 791 veraltet/abgelöst!

Geklammerte Werte stellen praktisch nutzbare Netzwerkangaben dar (d. h. abzüglich Startbits)

Klasse	Startbits	Adressbereich	Netzwerk-Bits	Host-Bits	Anzahl Netze	Adressen pro Netz
A	0	0.0.0.0 bis 172.255.255.255	8 (7)	24	128	16,7 Mio.
B	10	128.0.0.0 bis 191.255.255.255	16 (14)	16	16.384	65.536
C	110	192.0.0.0 bis 223.255.255.255	24 (21)	8	2.097.152	256
D	1110	224.0.0.0 bis 239.255.255.255	Spezieller Bereich der Multicast-Adressen			
E	1111	240.0.0.0 bis 255.255.255.255	Reserviert für zukünftige Anwendungen			

Die ersten 1 bis 4 Bits geben an, zu welcher Klasse eine IP-Adresse gehört

- Erste Bits = Adressklassen-ID = 1. Quad
- Klasse-A-Netze sind die größten Netze (unpraktikabel groß) [TEASER FÜR CIDR]
    - Im RFC 791 wird das Konzept der Adressklassen „hübsch umworben“: Demnach sei für jeden Fall die passende Adressklasse dabei und das System sei flexibel – stimmte damals wohl auch
- „Zu Multicast-Adressen kommen wir gleich noch“
- Adressen pro Netz ergeben sich aus: 2^(Host-Bits)
    - Tatsächlich stehen zwei Hostadressen weniger zur Verfügung … [KLICK]

RFC 791

Innerhalb eines jeden einzelnen Netzes, egal welcher Klasse, gibt es **zwei spezielle IP-Adressen**:

Broadcast-Adresse

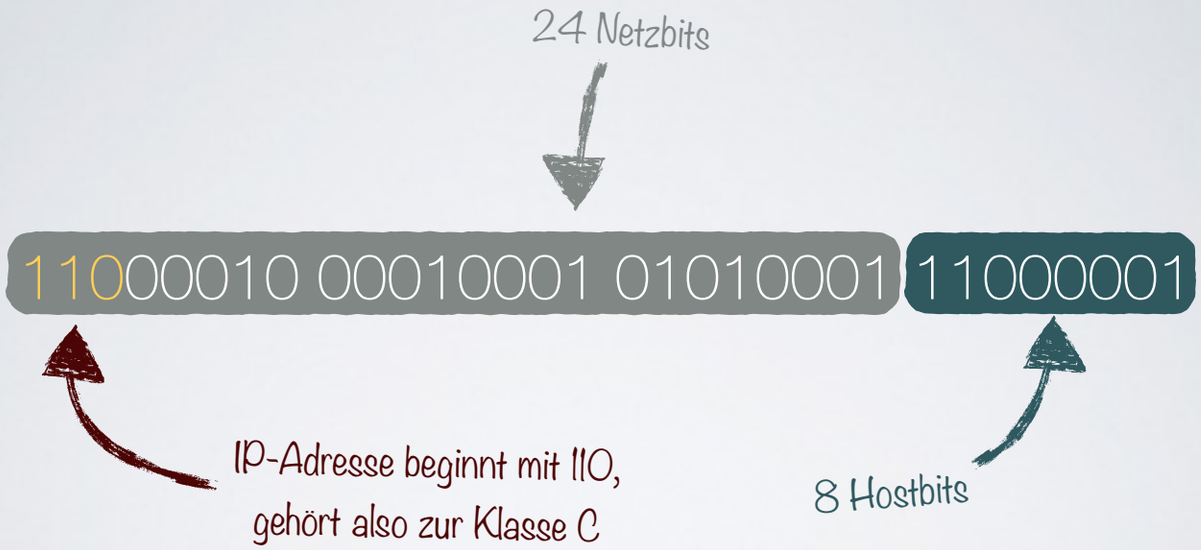
An die **höchste mögliche Adresse** geschickte Datenpakete werden von **jedem Host empfangen**.

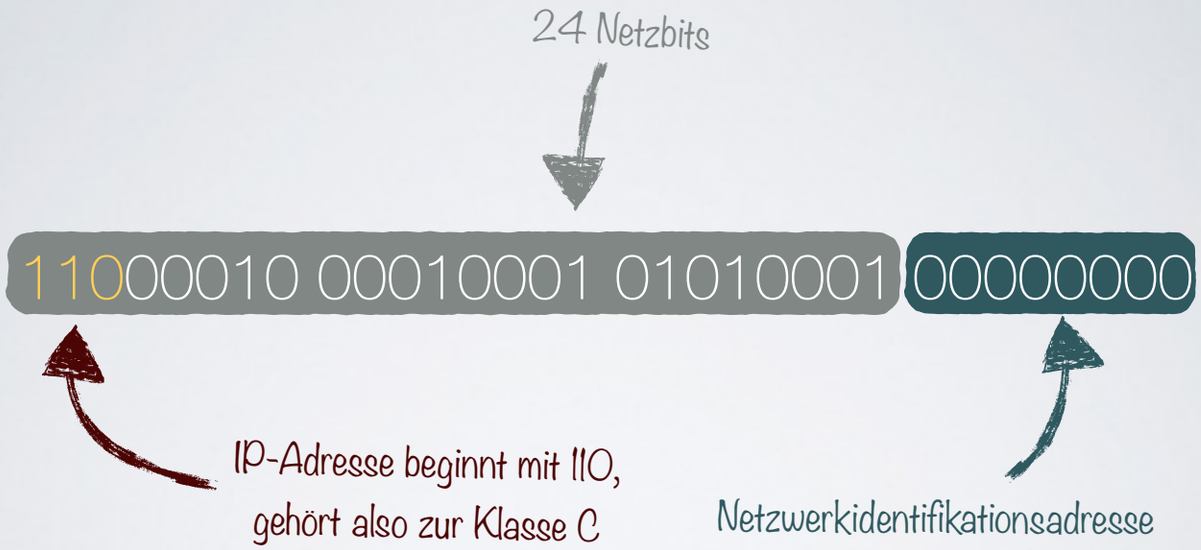
Netz-ID-Adresse

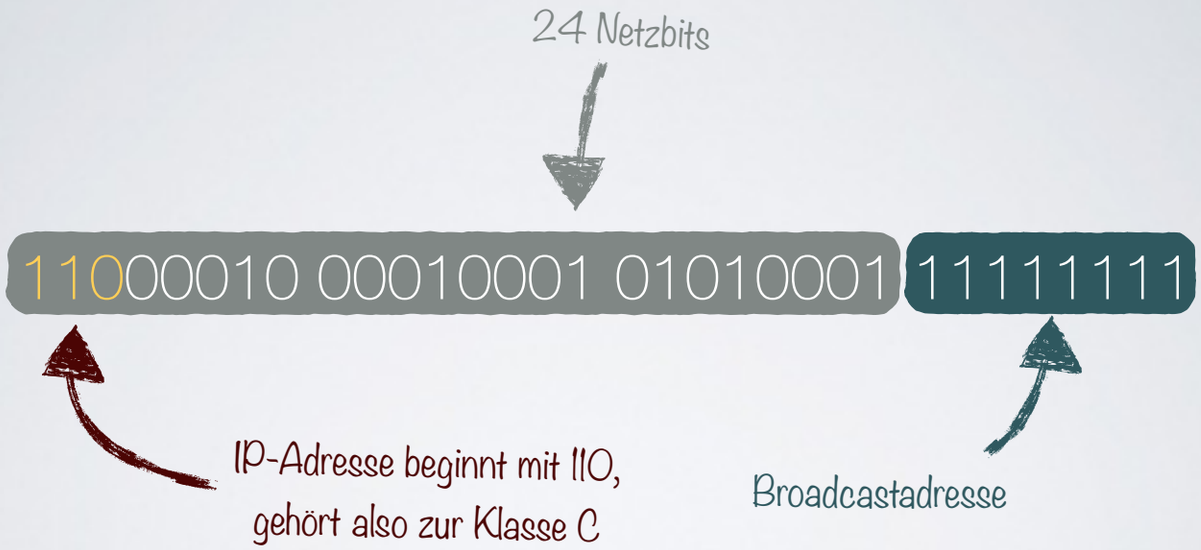
Die **niedrigste mögliche Adresse identifiziert** das **gesamte Netz** als solches nach außen hin.

Broadcast- und Netzwerkidentifikationsadressen stehen **nicht** als Host-Adressen zur Verfügung.

- Netz-ID-Adresse entspricht Postleitzahl
- Es folgt: Beispiel für Adressklassen


24 Netzbits
11000010 00010001 01010001 11000001
IP-Adresse beginnt mit 110,
gehört also zur Klasse C
8 Hostbits


24 Netzbits
11000010 00010001 01010001 00000000
IP-Adresse beginnt mit 110,
gehört also zur Klasse C
Netzwerkidentifikationsadresse


24 Netzbits
11000010 00010001 01010001 11111111
IP-Adresse beginnt mit 110,
gehört also zur Klasse C
Broadcastadresse

Das Internet Protocol der Version 4

I

Das IP-Datagramm

II

Die IP-Adresse

III

Die IP-Adressklassen

IV

Verteilung von IP-Adressen

V

CIDR, Super- & Subnetting

VI

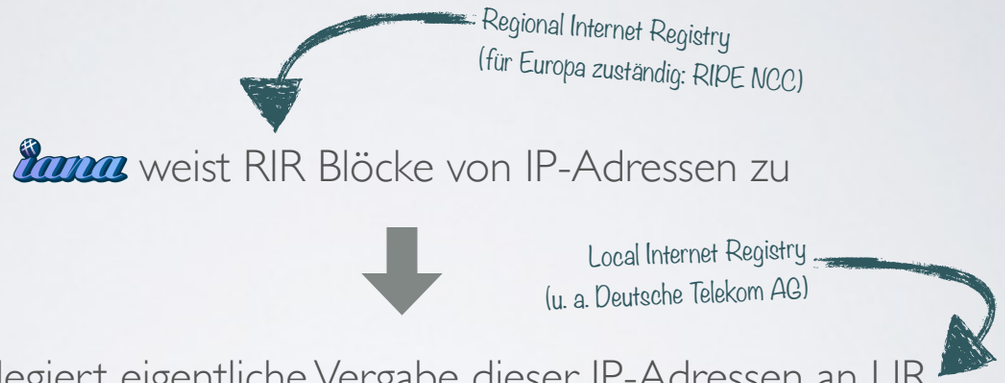
Zusammen-fassung

Internet Assigned Numbers Authority

IV Verteilung von IP-Adressen

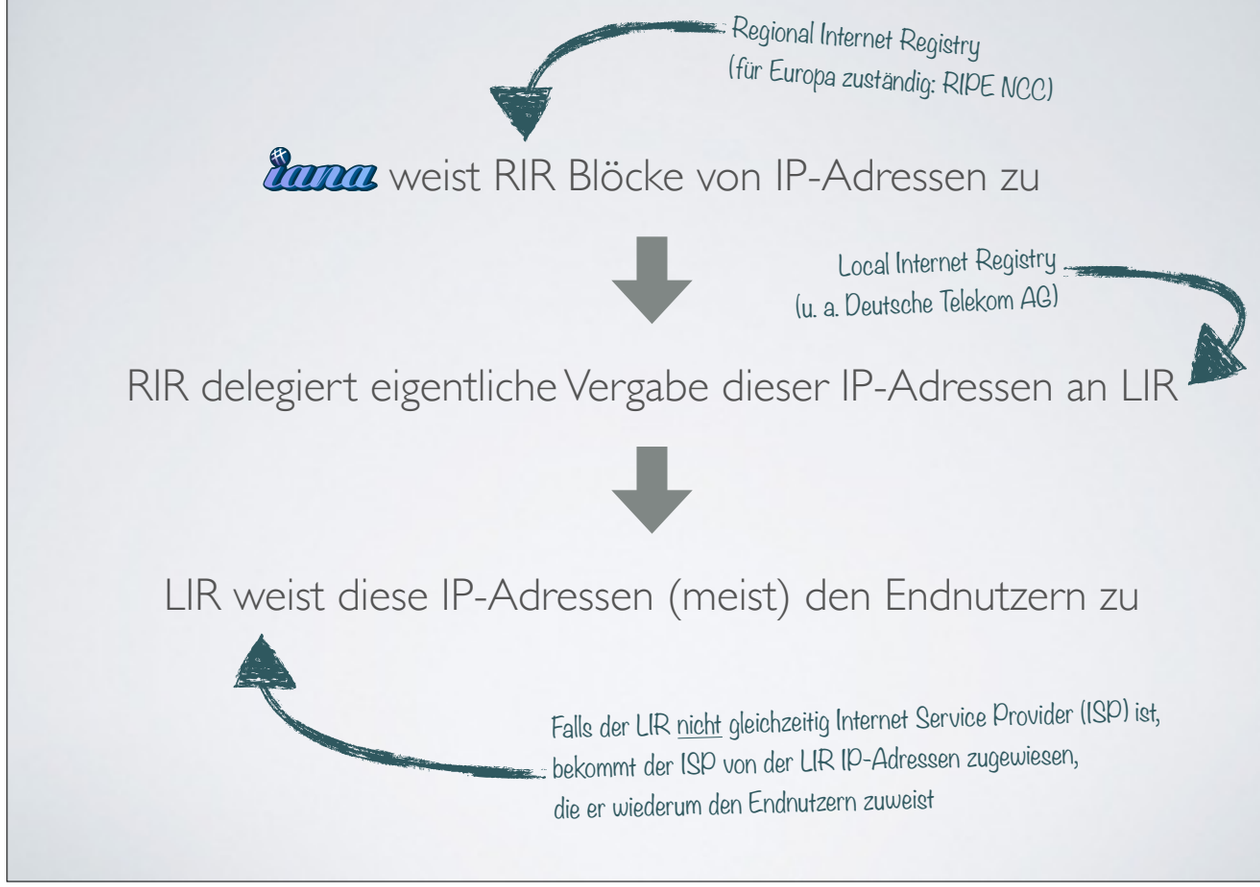
- RIPE NCC zuständig für Europa, Naher Osten und Zentralasien
  - Non-Profit-Organisation
  - finanziert sich aus Beiträge angeschlossener Mitglieder (ISP, Hochschulen, Großunternehmen)

IV Verteilung von IP-Adressen



- LIR ist meistens ISP

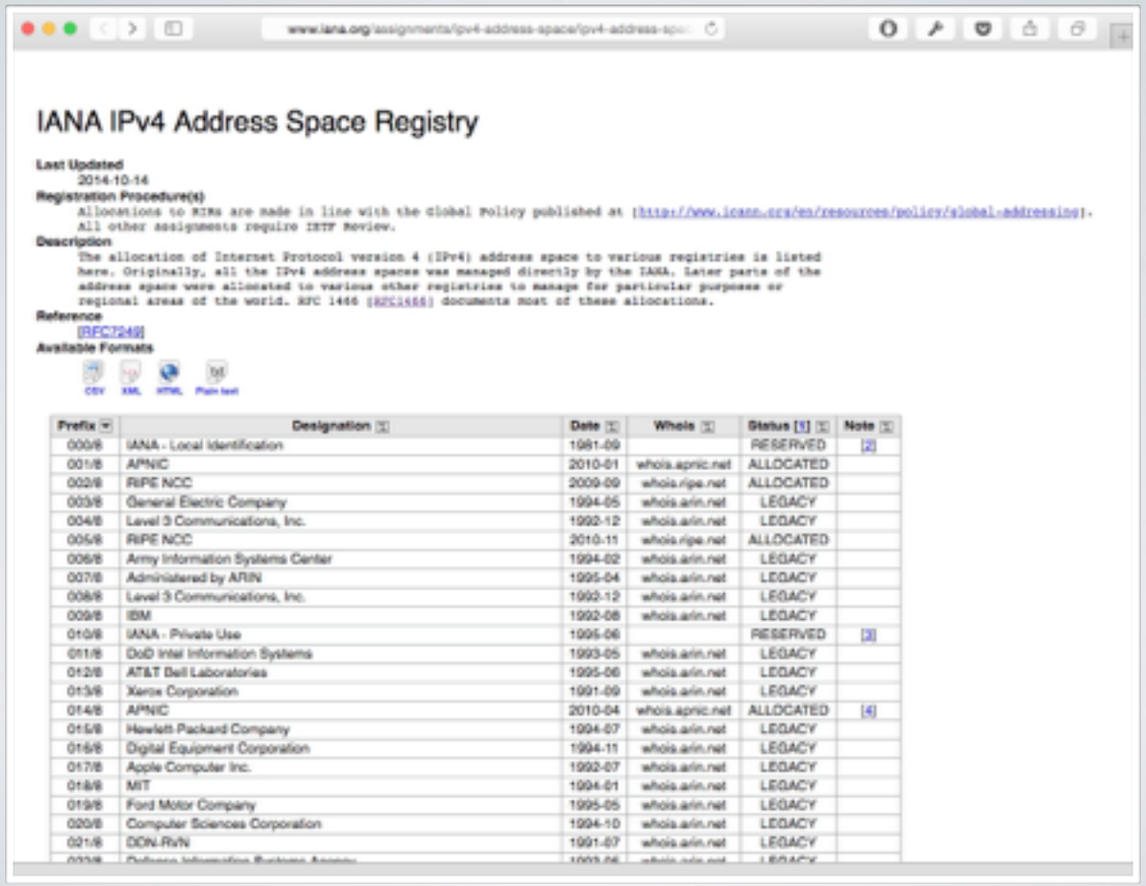
IV Verteilung von IP-Adressen



- Statt Endnutzer können die IPs vom LIR auch an weitere Provider zugewiesen werden
- In den Anfangszeiten des Internets hat die IANA IP-Adressen direkt an große Unternehmen und Unis vergeben:
    - Klasse-A-Netz 18.0.0.0 bzw. 18/8 gehört dem MIT, 19.0.0.0 Ford, 17.0.0.0 Apple

IV Verteilung von IP-Adressen

http://www.iana.org/assignments/ipv4-address-space/ipv4-address-space.xhtml



IANA IPv4 Address Space Registry

Last Updated
2014-10-14
Registration Procedure(s)
Allocations to RIRs are made in line with the Global Policy published at [http://www.icann.org/en/resources/policy/global-addressing].
All other assignments require IETF Review.
Description
The allocation of Internet Protocol version 4 (IPv4) address space to various registries is listed here. Originally, all the IPv4 address spaces was managed directly by the IANA. Later parts of the address space were allocated to various other registries to manage for particular purposes or regional areas of the world. RFC 1466 [RFC1466] documents most of these allocations.
Reference
[RFC7249]
Available Formats
CSV XML HTML Plain text

Prefix	Designation	Date	Whois	Status [1]	Note
000/8	IANA - Local Identification	1981-09		RESERVED	[2]
001/8	APNIC	2010-01	whois.apnic.net	ALLOCATED	
002/8	RIPE NCC	2009-09	whois.ripe.net	ALLOCATED	
003/8	General Electric Company	1994-05	whois.arin.net	LEGACY	
004/8	Level 3 Communications, Inc.	1992-12	whois.arin.net	LEGACY	
005/8	RIPE NCC	2010-11	whois.ripe.net	ALLOCATED	
006/8	Army Information Systems Center	1994-02	whois.arin.net	LEGACY	
007/8	Administered by ARIN	1995-04	whois.arin.net	LEGACY	
008/8	Level 3 Communications, Inc.	1992-12	whois.arin.net	LEGACY	
009/8	IBM	1992-08	whois.arin.net	LEGACY	
010/8	IANA - Private Use	1995-06		RESERVED	[3]
011/8	DoD Intel Information Systems	1993-05	whois.arin.net	LEGACY	
012/8	AT&T Bell Laboratories	1995-06	whois.arin.net	LEGACY	
013/8	Xerox Corporation	1991-09	whois.arin.net	LEGACY	
014/8	APNIC	2010-04	whois.apnic.net	ALLOCATED	[4]
015/8	Hewlett-Packard Company	1994-07	whois.arin.net	LEGACY	
016/8	Digital Equipment Corporation	1994-11	whois.arin.net	LEGACY	
017/8	Apple Computer Inc.	1992-07	whois.arin.net	LEGACY	
018/8	MIT	1994-01	whois.arin.net	LEGACY	
019/8	Ford Motor Company	1995-05	whois.arin.net	LEGACY	
020/8	Computer Sciences Corporation	1994-10	whois.arin.net	LEGACY	
021/8	DDN-RVN	1991-07	whois.arin.net	LEGACY	

- (Video)

IV Verteilung von IP-Adressen

http://www.heise.de/netze/meldung/IPv4-Adresspool-ausgeschoepft-1181351.html

heise Netze

News Artikel Foren

Netze > 7-Tage-News > 2011 > KW 5 > IPv4-Adresspool ausgeschöpft

News-Meldung vom 01.02.2011 10:47 « Vorige | Nächste »

IPv4-Adresspool ausgeschöpft

vorlesen / MP3-Download

Die für die Vergabe von IP-Adressen zuständige IANA (Internet Assigned Numbers Authority) hat heute dem Asia-Pacific Network Information Centre (APNIC) zwei /8-IPv4-Adressblöcke zugeteilt, gab die regionale Internet-Registry (RIR) für Asien und Australien heute in einer Mitteilung bekannt. Die beiden Blöcke 39/8 und 106/8 waren damit die letzten beiden, für die die IANA das alte Vergabeverfahren angewandt hat.

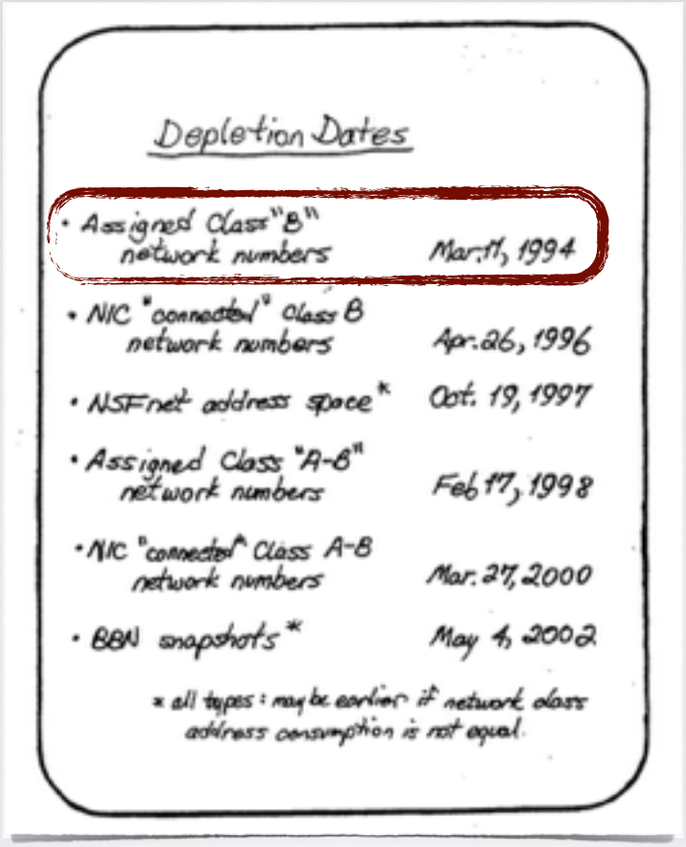
Für die noch verbleibenden fünf /8-Blöcke an IPv4-Adressen im IANA-Pool greift nun ein gesondertes Vergabeverfahren. Je einer der noch freien Blöcke wird automatisch für jede der fünf RIRs reserviert und muss ihnen von der IANA zugewiesen werden (Exhaustion Phase), was laut der IANA-Liste und der diversen IPv4-Adress-Counter bislang noch nicht passiert ist.

Voraussichtlich starten IANA und ICANN die Exhaustion Phase erst am Donnerstag und weisen dabei die letzten fünf Blöcke an die RIRs zu. **[Update]**:Dies ist mittlerweile auch geschehen, wie die IANA am 3. Februar mitteilte. (rek)

- Am 31. Januar 2011 wurde von der IANA der letzte IPv4-Adressblock vergeben
- Die Standford University hat einen ihnen zugewiesenen IPv4-Adressblock zurückgegeben
- Die IANA führt ein „Recovery Pool“, in welchem solche zurückgegebenen Adressblöcke aufbewahrt werden und dann neu vergeben werden
- Tatsächlich wäre der Vorrat an IPv4-Adressräumen schon sehr viel früher verbraucht gewesen, wenn man nicht „lebenserhaltende Maßnahmen“ gesucht und gefunden hätte (IPv6, NAT, …)

IV Verteilung von IP-Adressen

http://www.ietf.org/old/2009/proceedings/prior29/IETF18.pdf



- So hat man 1992 (Frank Solensky) auf einem Treffen der Internet Engineering Task Force (IETF) prognostiziert, dass bei der damals geltenden Vergabepolitik (nämlich über Netzklassen) die IPv4-Adressen des Klasse-B-Netzes im Jahr 1994 verbraucht sein würden
- „Erschöpfungsdaten“
- Gründe, die man gefunden hat, waren enorm anwachsende Routing-Tabellen (siehe extra Vortrag), ein möglicherweise zu kleiner Adressraum (hat man später mit IPv6 versucht zu lösen, siehe extra Vortrag) und eben ein enormer Verbrauch an insbesondere Klasse-B-Netzen
- Eines der Hauptprobleme, welches zu dieser schnellen Erschöpfung des Adresspools geführt hat, war [KLICK]

III Die IP-Adressklassen

RFC 791

veraltet/abgelöst!

Geklammerte Werte stellen praktisch nutzbare Netzwerkangaben dar (d. h. abzüglich Startbits)

Klasse	Startbits	Adressbereich	Netzwerk-Bits	Host-Bits	Anzahl Netze	Adressen pro Netz
A	0	0.0.0.0 bis 172.255.255.255	8 (7)	24	128	16,7 Mio.
B	10	128.0.0.0 bis 191.255.255.255	16 (14)	16	16.384	65.536
C	110	192.0.0.0 bis 223.255.255.255	24 (21)	8	2.097.152	256
D	1110	224.0.0.0 bis 239.255.255.255	Spezieller Bereich der Multicast-Adressen			
E	1111	240.0.0.0 bis 255.255.255.255	Reserviert für zukünftige Anwendungen			

Die ersten 1 bis 4 Bits geben an, zu welcher Klasse eine IP-Adresse gehört

IP-Adressklassen sind ineffizient

- Insbesondere bei Klasse-A-Netzen bleiben viele der 16,7 Millionen möglichen Adressen ungenutzt, da ein solches Netz auch umpraktikabel groß wäre. Somit werden IP-Adressen verschwendet.

IP-Adressklassen sind ineffizient

Oft sind Netze insbesondere der Klasse A überdimensioniert, sodass viele **Hostadressen ungenutzt** bleiben und somit verschwendet werden

- Insbesondere bei Klasse-A-Netzen bleiben viele der 16,7 Millionen möglichen Adressen ungenutzt, da ein solches Netz auch umpraktikabel groß wäre. Somit werden IP-Adressen verschwendet.

RFC 1918

IP-Adressklassen sind ineffizient

Oft sind Netze insbesondere der Klasse A überdimensioniert, sodass viele **Hostadressen ungenutzt** bleiben und somit verschwendet werden

↓

Freigabe von Adressbereichen für die ausschließliche Verwendung in privaten Netzwerken:

A	10.0.0.0	B	172.16.0.0 – 172.31.0.0	C	192.168.0.0 – 192.168.255.0

- Über NAT teilen sich die Rechner in einem privaten Netzwerk dann eine externe IP (das ist heutzutage Standard)

RFC 6890

Auswahl weiterer spezieller Netze:

RFC 1122	Aktuelles Netz	0.0.0.0/8
RFC 3927	link local 169.254.0.0/16	Möglichkeit, sich bei temporärer Nichterreichbarkeit von DHCP selbst automatisch eine IP-Adresse zuzuweisen
RFC 1122	Loopback-Adressbereich 127.0.0.0/8	Virtuelle Netzwerk-Schnittstelle (Loopback-Interface), über die sich ein Host selbst per IP erreicht 127.0.0.1 ist der De-Facto-Standard für den „local host“
RFC 919 RFC 922	Limited Broadcast 255.255.255.255	An diese Adresse geschickte Pakete werden von allen Hosts im selben Netzwerk empfangen Diese Broadcasts werden vom Router nicht weitergeleitet

- localhost nützlich bei Netzwerkprogrammierung, da so zum Testen Client = Server sein kann
- Universeller Broadcast = Limited Broadcast
  - Ziel liegt immer im selben Netz, wird vom Router nicht weitergeleitet
  - Unterschied zum directed Broadcast: Diese werden vom Router weitergeleitet, falls Quell- und Zielnetz nicht identisch sind und dann erst im Zielnetz in einen Broadcast umgesetzt (wenn Zielnetz = Quellnetz => limited Broadcast)
  - Universelle Broadcasts sind wichtig, wenn Schnittstellen ihre IP-Adresse dynamisch beziehen und somit bei Inbetriebnahme noch gar nicht wissen, zu welchem Netz sie gehören; universelle Broadcasts ermöglichen dann Anfrage zur Zuteilung einer Adresse

Das Internet Protocol der Version 4

I

Das IP-Datagramm

II

Die IP-Adresse

III

Die IP-Adressklassen

IV

Verteilung von IP-Adressen

V

CIDR, Super- & Subnetting

VI

Zusammen-fassung

Classless Inter-Domain Routing

(CIDR)

- Die (vorübergehende) Lösung: CIDR, 1993 eingeführt um das Konzept der Netzklassen abzulösen
- CIDR soll eine Übergangslösung darstellen und wurde damals für eine Dauer von etwa fünf Jahren ausgelegt – ist aber jetzt noch in Verwendung

RFC 1519

Classless Inter-Domain Routing

ermöglicht Setzung der Trennlinie zwischen Netzbits
und Hostbits an einer beliebigen Stelle

RFC 1519

Classless Inter-Domain Routing

ermöglicht Setzung der Trennlinie zwischen Netzbits
und Hostbits an einer beliebigen Stelle

Erste Bits der Adresse sagen nichts mehr über die
Größe des Netzes aus

RFC 1519

Classless Inter-Domain Routing

ermöglicht Setzung der Trennlinie zwischen Netzbits
und Hostbits an einer beliebigen Stelle

↓

Erste Bits der Adresse sagen nichts mehr über die
Größe des Netzes aus

↓

Notieren der Anzahl der Netzbits per
Suffix oder Teilnetzmaske

Suffix
(CIDR-Adresse)

Die Anzahl der Netzbits werden direkt nach einem Slash hinter der Netzwerkadresse notiert

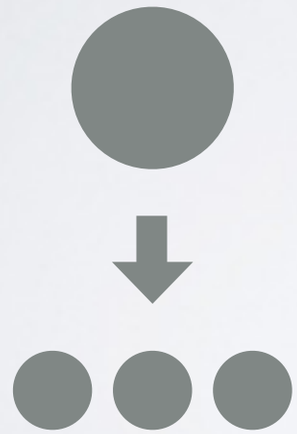
Beispiel: Das Klasse-A-Netz 14.0.0.0 wird zu 14.0.0.0**/8**

Teilnetzmaske
(Subnet Mask)

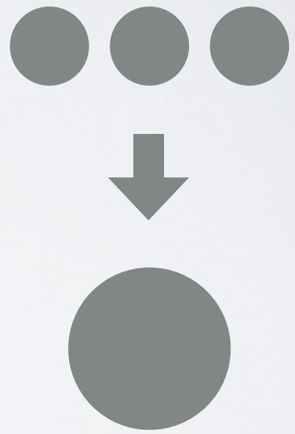
Für jedes Netzbit wird eine 1 und für jedes Hostbit eine 0 notiert. Diese werden dann zusammen in vier (dezimalen) 8-Bit-Blöcken geschrieben, der Teilnetzmaske.

Beispiel: Für das Klasse-A-Netz 14.0.0.0 lautet die **Teilnetzmaske 255.0.0.0**

Subnetting



Supernetting



Das Internet Protocol der Version 4

I

Das IP-Datagramm

II

Die IP-Adresse

III

Die IP-Adressklassen

IV

Verteilung von IP-Adressen

V

CIDR, Super- & Subnetting

VI

Zusammen-fassung

IPv4-Datagramme und -Header, IPv4-Adresse

- IP-Protokoll ist paketbasiert, d. h. Daten werden in Paketen durch das Internet transportiert
- Diese IP-Pakete (genau: Datagramme) können u. U. **fragmentiert**, d. h. aufgeteilt werden
- IPv4-Pakete werden mit einem sog. **IPv4-Header** versehen, welcher u. a. Auskunft über Quelle, Ziel, Paketgröße gibt und Fragmentierungsinformationen enthält
- IPv4-Adressen sind **32 Bit lang** und dienen der **eindeutigen Kennzeichnung von Teilnehmern** in einem IPv4-Netzwerk
- IPv4-Adressen bestehen aus **Netz- und Hostteil** werden meist in **Dezimalschreibweise** notiert und in **vier durch Punkte getrennte Oktetten** gegliedert

Netzklassen, CIDR, Subnetting, Supernetting

- Bis 1993 wurden **Netzklassen** (A bis E) verwendet, um den IPv4-Adressbereich zu unterteilen
- 1993 wurden Netzklassen durch **CIDR** abgelöst, welches durch eine flexiblere Aufteilung von Netz- und Hostteil eine effizientere Ausnutzung des IPv4-Adressbereichs ermöglicht
- **Teilnetzmasken bzw. CIDR-Suffixe** drücken die Aufteilung einer IPv4-Adresse in Netz- und Hostteil aus
- CIDR ermöglicht Subnetting und Supernetting
- **Subnetting** meint die Unterteilung eines IPv4-Netzes in mehrere kleinere IPv4-Netze
- **Supernetting** meint das Zusammenfassen mehrerer IPv4-Netze zu einem großen IPv4-Netz

- CDIR = Classless Inter-Domain Routing

Broadcast, Multicast, IANA

- In einem IPv4-Netz ist die niedrigste IPv4-Adresse für die **Netzwerkkennung** und die höchste für **Broadcasts** reserviert
- Broadcasts erreichen jeden Host im IPv4-Netzwerk
- Multicast-Adressen ermöglichen den Versand desselben Datenstroms an mehrere Empfänger
- Die **IANA** ist die **zentrale Stelle für die Vergabe von IPv4-Adressen** (Endkunden erhalten IPv4-Adressen allerdings über den Umweg über einen LIR/ISP
- Bestimmte IPv4-Adressbereiche sind inzwischen für besondere Zwecke reserviert (= IANA vergibt diese nicht)
  - Private Adressbereiche, Limited Broadcast, link local, …

- IANA = Internet Assigned Numbers Authority

Das Internet Protocol der Version 4

I

Das IP-Datagramm

II

Die IP-Adresse

III

Die IP-Adressklassen

IV

Verteilung von IP-Adressen

V

CIDR, Super- & Subnetting

VI

Zusammen-fassung

Das Internet Protocol der Version 4

I

Das IP-Datagramm

II

Die IP-Adresse

III

Die IP-Adressklassen

IV

Verteilung von IP-Adressen

V

CIDR, Super- & Subnetting

VI

Zusammen-fassung

Das Internet Protocol der Version 4

mit Material von

- Sascha Kersken: „IT-Handbuch für Fachinformatiker“. Galileo Computing, 3. Auflage 2008
- Thomas Schmidt. Carl-Severing-Berufskolleg für Metall- und Elektrotechnik, Bielefeld 2011
- http://de.wikipedia.org und http://en.wikipedia.org (Artikel zu *IPv4*, *CIDR*, *IP-Adresse*, *Netzklasse*; Abrufdatum: 19.10.2014)
- http://www.iana.org/numbers (Abrufdatum: 19.10.2014)
- diverse RFC-Dokumente (siehe Hinweise auf einzelnen Folien)