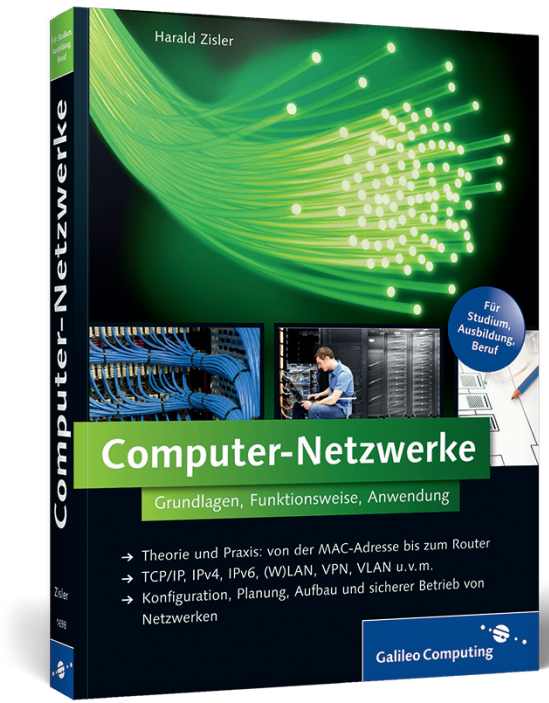
Harald Zisler

Computer-Netzwerke

Grundlagen, Funktionsweise, Anwendung



Galileo Press

Auf einen Blick

Inhalt

Hardware- und IP-Adresse verhalten sich wie Fahrgestellnummer und Autokennzeichen.

3 Adressierung im Netzwerk – Theorie

Bei modernen Computer-Netzwerken gelingt die Adressierung über Hardware- und Internetprotokoll-Adressen (IP-Adressen). In diesem Kapitel lernen Sie deshalb den Aufbau der Ethernet- und IP-Pakete kennen. Das hilft Ihnen bei der Fehlersuche, aber auch bei der Entwicklung eigener Anwendungen. Das Wissen um die verschiedenen Internetprotokoll-Versionen und deren Eigenheiten erleichtert Ihnen auch die damit verbundenen Umstellungsarbeiten. Mit Ihren Kenntnissen aus diesem Kapitel erkennen Sie auch umgekehrt Art und Zweck einer IP-Adresse.

Im ISO-Schichtenmodell finden Sie die physikalischen Adressen in der Ebene 2, die Adressen des Internetprotokolls im Layer 3. Das TCP/IP-Schichtenmodell ordnet die physikalischen Adressen der Netzzugangsschicht (Link Layer) und die IP-Adressen der Internetschicht (Internet Layer) zu.

3.1 Physikalische Adresse (MAC-Adresse)

Mit der (physikalischen) MAC-Adresse (Media Access Control) können Sie ein am Netzwerk angeschlossenes Gerät weltweit eindeutig identifizieren. Egal ob Netzwerkkarte, Printserver oder Webkamera, jedes Gerät verfügt über eine unverwechselbare MAC-Adresse. Sie entspricht der Fahrgestellnummer eines Kraftwagens und wird bei der Herstellung des Gerätes fest »eingeprägt«. Sie unterscheidet sich damit von den logischen Adressen des OSI-Layers 3 (z. B. IP-Adressen). Die MAC-Adresse wird in hexadezimaler Form angegeben und weist eine Länge von 6 Byte auf.

Anhand der ersten drei Bytes der MAC-Adresse können Sie den Hersteller identifizieren.

Aufbau von MAC-Adressen

`LL:LL:LL:XX:XX:XX`

LL: Herstellercode

XX: Identifikationsteil

Eine Trennung der Bytes kann auch durch »-« erfolgen.

Die hier gezeigte Schreibweise ist auch als kanonische Schreibweise bekannt (Norm IEEE 802.3). Im Gegensatz dazu gibt es auch die Bit-reverse-Darstellung, sie ist in RFC 2469 näher beschrieben.

Einige ausgewählte Herstellercodes bekannter Netzwerkgeräthersteller finden Sie in Tabelle 3.1.

Herstellercode	Hersteller
`00-05-5D`	D-Link Systems Inc.
`00-09-5B`	Netgear Inc.
`00-E0-4C`	Realtek Semiconductor Corp.
`00-E0-4F`	Cisco Systems Inc.
`00-E0-64`	Samsung Electronics

Tabelle 3.1 Auswahl von Herstellercodes in den MAC-Adressen

Sie können unter *http://standards.ieee.org/regauth/oui/index.shtml* den Herstellercode ermitteln oder die komplette aktuelle Liste herunterladen.

Broadcast-MAC-Adresse

Für das Rundsenden (Broadcast) an alle Teilnehmer innerhalb des erreichbaren Netzwerksegmentes wird die Adresse

`ff:ff:ff:ff:ff:ff`

verwendet. Sie wird vom Betriebssystem ausgegeben und ist geräteunabhängig.

Die Netzwerkprotokolle verwenden die MAC-Adresse nur innerhalb des gleichen Netzsegmentes.

Sicherheitshinweis

Die MAC-Adresse wird stets über das jeweilige Betriebssystem bzw. Microcontrollerprogramm weitergereicht. Damit besteht die Möglichkeit, beliebige MAC-Adressen zu verwenden oder die tatsächliche zu verändern. Für die eindeutig sichere Identifizierung von Geräten ist die MAC-Adresse daher nur sehr bedingt geeignet!

Sie können die MAC-Adresse für die Geräteverwaltung verwenden. Im Zusammenhang mit Datenbankanwendungen weisen Sie für PCs und Thin-Clients nicht nur die IP-Adressen, sondern auch Boot-Images oder weitere Zugangsmöglichkeiten zu. Allerdings müssen Sie den jeweiligen Gerätedatensatz nach einem Tausch der Netzwerkkarte ändern.

3.2 Ethernet-Pakete (Ethernet-Frames)

Ihre Daten transportieren Sie immer mit Hilfe der *Ethernet-Pakete*. Darin gehen Ihre in Einzelpakete zerlegten Daten vom Sender zum Empfänger, und das unabhängig vom verwendeten Netzwerkprotokoll.

Im Grunde würde Ihnen für Ihren Datentransport dieser einfache Paketmechanismus bereits ausreichen. Leider ist die Reichweite auf ein einziges, gemeinsames *Netzwerksegment* beschränkt. Sobald also Komponenten wie Switch, Bridge oder Router zwischen Ihrem Rechner und dem Zielgerät liegen, funktioniert mangels Adressierbarkeit die Kommunikation nicht. Für den segmentübergreifenden (und damit weltweiten) Datenverkehr benötigen Sie die Hilfe der höheren Netzwerkprotokolle. Diese enthalten die notwendigen Mechanismen.

Die *Ethernet-Frames* haben einen relativ einfachen Aufbau. Die Pakete haben eine Standardlänge von 1518 Byte (Tabelle 3.2) bzw. um das VLAN-Tag erweiterte 1522 Byte (Tabelle 3.3).

7 Byte	1 Byte	6 Byte	6 Byte	2 Byte	bis 1500 Byte	max. 46 Byte	4 Byte
Präambel	SFD	MAC-Adresse Ziel	MAC-Adresse Quelle	Typ	Nutzdaten	PAD	CRC (FCS)

Tabelle 3.2 Standard-Ethernet-Frame nach IEEE 802.3

7 Byte	1 Byte	6 Byte	6 Byte	4 Byte	2 Byte	bis 1500 Byte	max. 42 Byte	4 Byte
Präam-bel,	SFD	MAC-Adresse Ziel	MAC-Adresse Quelle	VLAN-Tag	Typ	Nutzdaten	PAD	FCS

Tabelle 3.3 Um das VLAN-Tag erweiterter Ethernet-Frame nach IEEE 802.1Q

Dieses VLAN-Tag kennzeichnet virtuelle Netzwerke (VLANs). Deren Mechanismen und Einsatzmöglichkeiten erkläre ich an anderer Stelle. Meist haben Sie es heute mit den um das VLAN-Tag erweiterten Ethernet-Frames zu tun.

Bestandteile des Ethernet-Frames mit VLAN-Tag

- **Präambel**: 7 Byte mit wechselnden Bits (»`10101010` ...«), zum Synchronsieren der Endgeräte, noch aus Kompatibilitätsgründen vorhanden
- **SFD**: Start-Frame-Delimiter, Bitfolge `10101011`, zum Synchronisieren und Anzeigen des Beginns des Frames, noch aus Kompatibilitätsgründen vorhanden
- **MAC-Adresse Ziel**
- **MAC-Adresse Absender**

- **VLAN-Tag**: Kennzeichnung für virtuelle Netzwerke
- **Typ**: Angabe über das von den Nutzdaten angewendete Netzwerkprotokoll. Einige wichtige Vertreter hiervon sind: `0x800` IPv4, `0x86DD` IPv6, `0x0806` Address Resolution Protokoll (ARP), `0x0842` Wake on Lan (WOL)
- **Nutzdaten**: maximal 1500 Bytes
- **Pad**: Dient zum Auffüllen auf die Mindestgröße des Ethernet-Frames von 64 Byte, wenn diese mit den Nutzdaten nicht erreicht wird.
- **FCS**: Frame Check Sequence, mittels 32-Bit-CRC-Prüfsumme wird die Übertragung auf Fehler überprüft.

3.3 Zusammenführung von MAC- und IP-Adresse

Sie wollen Ihre Datenpakete weltweit transportieren. Dazu benötigen Sie die Hilfe der Netzwerkprotokolle. Sie müssen die MAC-Adresse des Rechners mit seiner IP-Adresse zusammenführen. Hierbei helfen Ihnen die im Folgenden dargestellten Protokolle.

3.3.1 Adress Resolution Protocol (ARP), IPv4

Mit dem *Adress Resolution Protocol* (*ARP*) ermitteln Sie in IPv4-Netzen die MAC-Adresse zu einer IP-Adresse. Sie können damit auch einer MAC-Adresse eine IP-Adresse manuell zuweisen.

Normalerweise arbeitet das ARP-Protokoll ohne direkten Benutzereingriff unauffällig im Hintergrund. Daten sollen von A nach B geschickt werden, Sie geben jeweils die IP-Adresse auf dem OSI-Layer 3 an. Das ARP-Protokoll fragt alle erreichbaren Netzwerkteilnehmer, ob sie über die gesuchte IP-Adresse verfügen. Der Zielrechner antwortet entsprechend und gibt seine MAC-Adresse dem Fragesteller bekannt. Die Kommunikation zwischen den beiden wird nunmehr aufgebaut. Das Beispiel in Abbildung 3.1 zeigt Ihnen den Ablauf detailliert. Der linke Rechner sendet die ARP-Anfrage mit der eigenen IP- und MAC-Adresse (IP(S), MAC(S)), die IP-Adresse des Empfängers (IP(E)) und die Broadcast-Adresse `ff:ff:ff:ff:ff:ff`. Die erreichbaren Rechner prüfen, ob ihnen die angegebene Adresse gehört. Der angesprochene Zielrechner sendet daraufhin ein Paket mit seiner MAC-Adressangabe zurück (MAC(E)). Die anderen Rechner verwerfen das Paket.

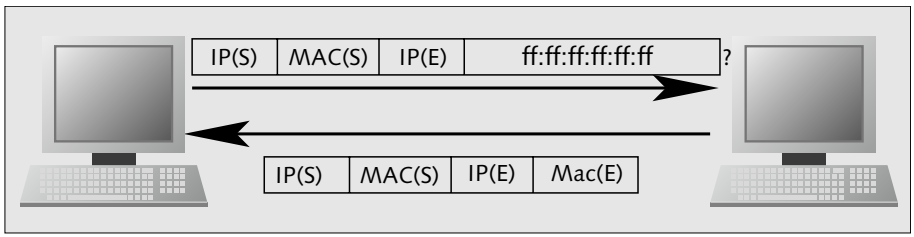


Abbildung 3.1 Schema ARP-Abfrage

Protokoll einer ARP-Anfrage

Rechner1 stellt Anfrage:

```
00:1e:33:0d:e9:f9 > ff:ff:ff:ff:ff:ff, ARP,
length 42: arp who-has 192.168.0.102 tell 192.168.0.103
```

Rechner1 erhält Antwort von Rechner2:

```
00:11:6b:62:93:2e > 00:1e:33:0d:e9:f9, ARP,
length 60: arp reply 192.168.0.102 is-at 00:11:6b:62:93:2e
```

Nach diesem Austausch steht der weiteren Datenübertragung nichts mehr im Wege.

Beide Rechner speichern normalerweise die erfolgreiche ARP-Anfrage im *ARP-Cache*. Wie lange die Informationen dort verbleiben, ist unterschiedlich. Gebräuchlich sind Zeiten zwischen 5 und 10 Minuten.

Inhalt der ARP-Caches der beteiligten Rechner

Cache Rechner1:

```
192.168.0.102 ether 00:11:6b:62:93:2e  C  eth0
```

Cache Rechner2:

```
? (192.168.0.103) at 00:1e:33:0d:e9:f9 on re0 expires in 1078 seconds [et
hernet]
```

Die verschiedenartige Darstellung der Cache-Inhalte resultiert aus der Verwendung verschiedener Betriebssysteme.

Ist die IP-Adresse unbekannt, können Sie mittels des *Reverse Adress Resolution Protocol* (*RARP*) einen zentralen Rechner kontaktieren und nach dieser abfragen. Dieses Netzwerkprotokoll ist aber kaum mehr von Bedeutung.

Proxy-ARP und Sicherheit: Im seltenen Fall, dass ein Router zwei Netze mit gleichem IP-Adressbereich verbindet, antwortet dieser anstelle des Zielrechners. Listet man den ARP-Cache auf, so taucht die IP-Adresse des Routers anstelle der des Zielrechners auf.

Proxy-ARP oder *ARP-Spoofing*: Wenn Sie den ARP-Cache des abfragenden Rechners auflisten und finden zu ein und derselben MAC-Adresse verschiedene IP-Adressen, so befindet sich entweder ein Proxy-ARP-Server im Netz, oder es liegt ARP-Spoofing vor. In diesem Fall hat ein Angreifer vor, den Netzwerkverkehr zu belauschen oder zu manipulieren!

Rechner versenden einen ARP-Broadcast mit der eigenen IP-Adresse als Absender und Ziel mit dem Zweck, die neue, eigene MAC-Adresse allen erreichbaren Rechnern des eigenen Netzwerksegmentes bekannt zu geben (*Gratuitous ARP*). Das ist beim Laden oder Netzwerkstart eines Rechners ganz normal. Die benachrichtigten Rechner ergänzen oder ändern daraufhin die entsprechenden Einträge des ARP-Caches. Wenn Sie zwei oder mehrere Rechner redundant betreiben, so wird damit allen anderen Teilnehmergeräten der Umstieg auf die Reserve, was das Netzwerk angeht, bekannt gemacht.

3.3.2 Neighbor Discovery Protocol (NDP), IPv6

Was Sie hier im Buch über das ARP-Protokoll für IPv4-Adressen gelesen haben, würde grundsätzlich auch mit IPv6-Adressen funktionieren. In der Praxis kommt aber stattdessen das *Neighbor Discovery Protocol* **(***NDP***)** zum Einsatz. Die Grundlagen hierfür finden Sie in den RFCs 3122 und 4861 hinterlegt. Auch dieses Protokoll arbeitet unbemerkt vom Benutzer und bedarf im Normalfall keinerlei Eingriffes.

Die Funktionen, Begriffe und Eigenschaften des NDP für IPv6

- **Neighbor Solicitation**: Anfrage nach MAC-Adresse
- **Neighbor Advertisement**: Antwort auf eine Anfrage nach der MAC-Adresse (Neighbor Solicitation)
- **Knoten**: Netzwerkteilnehmer
- **Finden** von Routern, welche Pakete in weitere Netzwerke weiterreichen
- **Duplikate IP Adress Detection**: Zwei Knoten (Netzwerkteilnehmer) können niemals die gleiche IP-Adresse bekommen.
- Kombination von **ARP** und **ICMP Router Discovery**: Auffinden von Routern im gleichen Netzwerk
- **Neighbor Unreachability Detection**: automatische Feststellung nicht erreichbarer Knoten im eigenen Netzwerk
- **Autokonfiguration** von Ipv6-Adressen
- **Wegfall** der Subnetzmasken
- neue **Sicherheit**sfunktionen

Bei der Fehlersuche hilft Ihnen die Tabelle 3.4 weiter. NDP verwendet mehrere verschiedene ICMPv6-Nachrichten. Allgemeines über ICMP-Nachrichten finden Sie in Kapitel 5, »Steuer- und Fehlercodes mit ICMP und ICMPv6 übertragen«.

Typ	Name	Zweck
133	Router Solicitation	Netzwerkteilnehmer, die nicht als Router fungieren, können von den Routern im gleichen Netzwerk ein Router Advertisement anfordern. Der oder die erreichbaren Router reagieren sofort und übersenden die gewünschte Nachricht.
134	Router Advertisement	Router verschicken diese Nachrichten in festen Intervallen oder nach Anforderungen des Typs 133 sofort. Sie geben ihre Anwesenheit im Netz damit bekannt.
135	Neighbor Solicitation	Rechner überprüfen damit die Erreichbarkeit des Nachbarn oder ermitteln die MAC-Adresse von diesem.
136	Neighbor Advertisement	Es handelt sich um die Antwort auf die Anfrage des Typs 135, der angefragte Rechner ist erreichbar.
137	Redirect Message	Router informieren damit andere Netzwerkteilnehmer, wenn es einen anderen, besseren Router zum Erreichen des gewünschten Zieles gibt.

Tabelle 3.4 Nachrichtentypen des NDP

Betrachten Sie den Ablauf einer Adressanfrage mit Antwort.

Protokoll einer Neighbor Solicitation mit Antwort

Anfrage Rechner1:

```
16:15:19.726208 IP6 fe80::211:6bff:fe62:932e > fe80::21e:33ff:fe0d:e9f9:
ICMP6, neighbor solicitation, who has fe80::21e:33ff:fe0d:e9f9, length 32
```

Antwort Rechner2:

```
16:15:19.726249 IP6 fe80::21e:33ff:fe0d:e9f9 > fe80::211:6bff:fe62:932e:
ICMP6, neighbor advertisement, tgt is fe80::21e:33ff:fe0d:e9f9, length 24
```

NDP bringt seine Informationen in verschiedenen Caches unter. Sie finden daher die Informationen besser geordnet.

Übersicht über die Caches des NDPs

- **Destination Cache**: Enthält Adressen, an welche erfolgreich Daten gesendet wurden, und die Angabe für den nächsten Hop, welche die Pakete benutzen sollen.
- **Default Router List**: Enthält für jeden Netzwerkanschluss die erreichbaren Router. Die Einträge enthalten Verfallsvorgaben.

- **Prefix List**: Beinhaltet Präfixe, welche im gleichen Netzwerk gültig sind, mit Verfallsvorgaben. Ausnahme: Angaben des eigenen Rechners (Link-Lokal)
- **Neighbor Cache**: Liste mit Netzwerkteilnehmern, mit welchen innerhalb einer festgelegten Zeitspanne erfolgreich kommuniziert wurde. Es werden die Uni-Cast-IP-Adresse, die MAC-Adresse, der Zustand, das »Alter« des Eintrages und der Netzwerkanschluss festgehalten.

Aus dem *Neighbor Cache* können Sie den Zustand des Eintrages bezüglich eines Verbindungseintrages auslesen. Sie können damit nicht nur protokollbedingte Netzwerkprobleme eingrenzen. Die Bedeutung dieser Angaben finden Sie in Tabelle 3.5.

Zustand	Bedeutung
Delay	Ablauf ReachableTime, Versand eines Datenpaketes innerhalb der Delay First Probe Time. Kommt innerhalb dieser Zeit keine Quittung, ändert sich der Zustand auf Probe, und eine Neighbor Solicitation wird abgesetzt.
Probe	Zustand während des Abwartens auf eine positive Quittung der Neighbor Solicitation. Der Cache-Eintrag verfällt, wenn die vorkonfigurierte Anzahl der Versuche ohne positives Ergebnis durchgeführt wurde.
Stale	Unbekannt, ob angegebener Nachbarrechner erreichbar ist. Zeitpunkt der letzten positiven Quittung liegt länger als die Reachable Time zurück. Zustand bleibt bis zum Versenden des nächsten Datenpaketes an den hier eingetragenen Rechner bestehen.
Incomplete	Zustand nach Absenden Neighbor Solicitation und Eintreffen Neighbor Advertisement
Reachable	Rechner ist erreichbar, da innerhalb der Reachable Time ein Neighbor Advertisement von diesem erhalten wurde.

Tabelle 3.5 Einträge für den Zustandswert im Neighbor Cache des NDP

3.4 IP-Adressen

In der OSI-Schicht 3 begegnen Ihnen *logische Adressen*. Damit haben Sie die Möglichkeit, Verbindungen mit Partnern außerhalb des eigenen Netzwerksegmentes aufzunehmen. Die logischen Adressen dürfen Sie durchaus mit dem amtlichen KFZ-Kennzeichen vergleichen, die MAC-Adresse entspräche der Fahrgestellnummer.

Die logischen Adressen kennzeichnen auch die IP-Pakete. Sie tauchen hier als Quell- und Zieladressen auf, unabhängig von der Hardware-Adresse der Ethernet-Frames.

Die Adressierung nach dem IP-Protokoll hat sich im Laufe der Jahre gegen herstellerspezifische Lösungen (Novell, DEC, Microsoft usw.) durchgesetzt. Es war und ist für die Anwender einfacher, einen offenen, allgemeingültigen Standard zu verwenden, der zudem von Geräten aller Größenordnungen beherrscht wird.

Sie werden – besonders hier im Kapitel – mit IP-Adressen nach dem IP-Protokoll Version 4, aber auch Version 6 konfrontiert. Das hat ganz einfach damit zu tun, dass sich der Vorrat an freien Adressen des IPv4 langsam dem Ende zuneigt (4.294.967.296 Adressen). Beim IPv6 treffen Sie nicht nur auf einen schier unerschöpflichen Adressvorrat (ca. $34 * 10^{38}$ Adressen), sondern auch auf einige interessante Neuerungen, die Sie nur hier finden.

Weltweit vergibt die *Internet Assigned Numbers Authority* **(***IANA***)** Adressblöcke an die regionalen Vergabestellen *Regional Internet Registry* **(***RIR***)** (Tabelle 3.6). Diese wiederum versorgen die *Local Internet Registry* **(***LIR***)** mit freien Adressen. Der nächsterreichbare LIR ist Ihr Internet-Service-Provider. Von ihm erhalten Sie entweder Ihre feste oder temporär gültige IP-Adresse.

Region	RIR
Afrika	**AfriNIC** (African Network Information Centre)
Asian-Pazifik	**APNIC** (Asia Pacific Network Information Centre)
Europa, Naher Osten, Zentralasien	**RIPE NCC** (Réseaux IP Européens Network Coordination Centre)
Lateinamerika, Karibik	**LACNIC** (Regional Latin-American and Caribbean IP Address Registry)
Nordamerika	**ARIN** (American Registry for Internet Numbers)

Tabelle 3.6 Regional Internet Registries

Die *Internet-Service-Provider* (*ISP*s) sind in der Regel Mitglied in der RIR.

In einem *privaten Netzwerk* vergeben Sie selbst die IP-Adressen.

Einzigartigkeit von IP-Adressen
Jede IP-Adresse darf innerhalb eines Netzwerkes nur ein einziges Mal vorkommen.

3.5 IPv4-Adressen

Die IPv4-Adressen bestehen aus 32 Bit, welche zu vier Blöcken (Oktetts) gruppiert werden (4 Byte). Die Werte werden als Dezimalzahlen geschrieben, mit einem zulässigen Bereich von 0 bis 255.

Aufbau von IPv4-Adressen

```
NNN.NNN.NNN.NNN
```

Eine IPv4-Adresse besitzt einen Netzwerk- und einen Teilnehmer-Anteil (»Host«). Welches der Bytes allerdings zu welchem Teil gehört, hängt wiederum von der Netzwerkklasse ab. Sollen Ihre Rechner alle miteinander kommunizieren, müssen deren IP-Adressen denselben Netzwerkteil aufweisen.

Die IPv4-Adressen sind seit 1981 in RFC **791** definiert. In RFC 1349 finden Sie einige Weiterentwicklungen und Verweise auf weitere beteiligte RFCs.

Mit IPv4 werden Sie noch lange arbeiten. Vor allem nicht öffentliche Bestandsnetze werden es sicher bis auf weiteres anwenden. Viele Netzwerkgeräte (z. B. Printserver) können nicht auf die neue IP-Version upgedated werden. Damit sollten Sie also die theoretischen Grundlagen dieser Version kennen.

3.5.1 Netzwerkklassen im IPv4

Anhand der IP-Adresse erkennen Sie normalerweise nicht mehr, wie weit sich der Netzwerkanteil erstreckt. Hierbei hilft Ihnen die (Sub-)Netzmaske.

Zusammen mit der (Sub-)Netzmaske, die hier später erklärt wird, können Sie Netze mit einer verschieden hohen Anzahl von Teilnehmern definieren. Allerdings gilt dies nur für private Netze. Wenn Sie Netze betreuen, welche »draußen« im Internet existieren, müssen Sie unbedingt die Vorgaben Ihres Providers (= LIR) einhalten, weil es sonst zu großen Störungen kommt. Konkret bedeutet dies, dass Sie nur »unterhalb«, also »rechts« vom Netzwerkanteil Ihre Einteilungen vornehmen dürfen.

Früher (Tabelle 3.7) konnten Sie einer IP-Adresse bereits ansehen, welcher Netzklasse sie angehörte. Das erste Byte zeigte dies an. Seit Längerem schon wurde diese Einteilung aufgehoben, um der Adressknappheit etwas abzuhelfen.

Klasse	Bereich	1. Byte binär	Nutzbare Adressen	Netzmaske
A	0.0.0.0 - 127.255.255.255	00000000	16777214	255.0.0.0
B	128.0.0.0 - 191.255.255.255	10000000	65534	255.255.0.0
C	192.0.0.0 - 223.255.255.255	11000000	254	255.255.255.0

Tabelle 3.7 Einteilung von Netzwerkklassen

Beachten Sie bitte einige Anmerkungen zur Einteilung in Netzwerkklassen (Tabelle 3.7):

- Die Zahl der mathematisch möglichen Adressen wird stets um zwei vermindert. Sie benötigen diese für die Netz- und Broadcast-Adresse (z. B. 192.168.0.0 und 192.168.0.255).
- Während Sie die Bereichsangaben als mehr oder weniger historisch betrachten müssen, ist die Einteilung hinsichtlich der nutzbaren Adressen und die Angabe der Subnetzmaske in der Tabelle weiterhin gültig.
- Die in der Tabelle nicht aufgeführte Klasse D dient Multicast-Zwecken (bei Datenstreams, z. B. Video). Hier klinken sich Rechner passiv ein. Die Klasse E dient Test- und Forschungszwecken. Sie werden in der Praxis in der Regel mit beiden Klassen kaum in Berührung kommen.

Zur Verdeutlichung der Aufteilung einer IP-Adresse betrachten Sie bitte folgende Angaben:

Anteile von Netz (N)- und Hostanteilen (H) nach Netzwerkklassen

Klasse A: `NNN.HHH.HHH.HHH`

Klasse B: `NNN.NNN.HHH.HHH`

Klasse C: `NNN.NNN.NNN.HHH`

3.5.2 Netz- und Subnetzmaske, Unterteilung von Netzen

Eine Netz- oder Subnetzmaske besteht wie die IPv4-Adresse aus vier Bytes. Mit ihr unterteilen Sie IP-Adressen in den Netzwerk- und Host-Anteil.

Die Unterteilung eines Netzes in Subnetze bringt Ihnen verschiedene Vorteile:

- Mit dadurch verkleinerten Broadcast-Domänen verringern Sie die Netzlast durch Rundsendungen (Broadcasts).
- Sie können organisatorische Gegebenheiten durch die aufgeteilten Adressräume abbilden

Sie können (in der Regel innerhalb privater Netze) durch die Netzmaske aber auch z. B. zwei Klasse-C-Netze nach alter Denk- und Sprachweise miteinander verbinden.

Netzmaske und Subnetzmaske

- Umfasst die Maske alle möglichen Adressen eines Netzes, so handelt es sich um eine **Netzmaske** (siehe 6).
- Unterteilt sie jedoch den Adressraum, spricht man von der **Subnetzmaske**.
- Technisch bestehen zwischen der Netzmaske und der Subnetzmaske keine Unterschiede.
- Der Netzanteil wird stets mit 1, die Host-Anteile mit 0 belegt.
- Netz- und Subnetzmasken bestehen somit stets aus **führend gesetzten Bits**. Es treten keine »0-Lücken« auf.
- Weitere Normen: RFCs **950**, 1518, 1519

Im Rahmen des *Classless Inter-Domain Routings* (*CIDR*) wurde auch eine neue Schreibweise für die Netzmaske eingeführt. Anstelle der byteweisen Angabe (z. B. 255.255.0.0) werden hier die führenden gesetzten Bits zusammengezählt und per Schrägstrich an die IP-Adresse angehängt.

Die Angabe `192.168.0.36/24` beinhaltet die Netzmaske `255.255.255.0`. Binär wird die Netzmaske in diesem Fall so dargestellt:

```
11111111.11111111.11111111.00000000
```

Zählen Sie die gesetzten Bits (oder rechnen Sie einfach 3 Oktets mal 8 Bits), so erhalten Sie hier die 24.

Für Ihre tägliche Arbeit sind die Angaben in den Tabellen 3.8 und 3.9 sicher nützlich. Sie finden eine Gegenüberstellung der binären, klassischen und der CIDR-Schreibweise. In Tabelle 3.9 ist die Anzahl der Adressen bzw. Hosts je Netzmaske angegeben.

(Sub-)Netzmaske		
Binär	**Dezimal**	**CIDR-Notation**
11111111.00000000.00000000.00000000	255.0.0.0	/8
11111111.10000000.00000000.00000000	255.128.0.0	/9
11111111.11000000.00000000.00000000	255.192.0.0	/10
11111111.11100000.00000000.00000000	255.224.0.0	/11
11111111.11110000.00000000.00000000	255.240.0.0	/12
11111111.11111000.00000000.00000000	255.248.0.0	/13
11111111.11111100.00000000.00000000	255.252.0.0	/14
11111111.11111110.00000000.00000000	255.254.0.0	/15
11111111.11111111.00000000.00000000	255.255.0.0	/16
11111111.11111111.10000000.00000000	255.255.128.0	/17
11111111.11111111.11000000.00000000	255.255.192.0	/18
11111111.11111111.11100000.00000000	255.255.224.0	/19
11111111.11111111.11110000.00000000	255.255.240.0	/20
11111111.11111111.11111000.00000000	255.255.248.0	/21
11111111.11111111.11111100.00000000	255.255.252.0	/22
11111111.11111111.11111110.00000000	255.255.254.0	/23
11111111.11111111.11111111.00000000	255.255.255.0	/24
11111111.11111111.11111111.10000000	255.255.255.128	/25
11111111.11111111.11111111.11000000	255.255.255.192	/26
11111111.11111111.11111111.11100000	255.255.255.224	/27
11111111.11111111.11111111.11110000	255.255.255.240	/28
11111111.11111111.11111111.11111000	255.255.255.248	/29
11111111.11111111.11111111.11111100	255.255.255.252	/30
11111111.11111111.11111111.11111110	255.255.255.254	/31
11111111.11111111.11111111.11111111	255.255.255.255	/32

Tabelle 3.8 Subnetzmasken

Die binäre Darstellung benötigen Sie bei der Berechnung von Netzadressen und Subnetzmasken.

CIDR-Notat.	Adressen	Nutzbare Hostadr.	CIDR-Notat.	Adressen	Nutzbare Hostadr.
/8	16777216	16777214	/21	8 x 256	2046
/9	128 x 65536	8388606	/22	4 x 256	1022
/10	64 x 65536	4194302	/23	2 x 256	510
/11	32 x 65536	2097150	/24	256	254
/12	16 x 65536	1048574	/25	128 x 1	126
/13	8 x 65536	524286	/26	64 x 1	62
/14	4 x 65536	262142	/27	32 x 1	30
/15	2 x 65536	131070	/28	16 x 1	14
/16	65536	65534	/29	8 x 1	6
/17	128 x 256	32766	/30	4 x 1	2
/18	64 x 256	16382	/31	2 x 1	0
/19	32 x 256	8190	/32	1 x 1	1
/20	16 x 256	4094	–	–	–

Tabelle 3.9 Subnetzmaske und Adressräume

3.5.3 Berechnungen

Sie können einen (zugewiesenen) Adressbereich in Teilsegmente unterteilen, allerdings in dem in Tabelle 3.9 gezeigten Mengenraster. Die Unterteilung zeige ich Ihnen anhand eines Beispieles.

Ihr Netz soll in zwei Teile segmentiert werden. In einem werden sich künftig 19 Teilnehmer aufhalten, im anderen 80. Sie verwenden das Netzwerk `192.168.1.0`. Sie wollen unter anderem wissen, in welches der Teilnetze das Gerät mit der IP-Adresse `192.168.1.25` gehört. Außerdem interessiert Sie natürlich der IP-Adressbereich, der vergeben werden kann. Bei den Berechnungen verwenden Sie die **logische Addition** (**AND**). Sie hat folgende Regeln (Wahrheitstabelle):

Logische Addition (AND)

```
0 + 0 = 0
0 + 1 = 0
1 + 0 = 0
1 + 1 = 1
```

Wenn bei zwei Binärzahlen also jeweils die `1` aufeinandertreffen, bekommen Sie wiederum eine `1` als Ergebnis.

Sehen Sie zunächst den manuellen Lösungsweg zur Frage, wohin `192.168.1.25` gehört:

Manuelle Berechnungen

- Entnehmen Sie aus der Tabelle die passende Netzmaske, hier: `/27`, ausgeschrieben 255.255.255.224.
- Schreiben Sie die IP-Adresse und Netzmaske binär untereinander, und führen Sie die logische Addition durch:

```
11000000.10101000.00000001.00011001  192.168.0.25
11111111.11111111.11111111.11100000  255.255.255.224
11000000.10101000.00000001.00000000  192.168.1.0
```

Die Netzadresse lautet also `192.168.1.0`, in welchem `192.168.1.25` Mitglied ist.

Sie können natürlich auch ein Rechenprogramm wie ipcalc für die IP-Adressen und Netzmasken benutzen. Die Ausgaben einer Berechnung für die beiden Teilnetze sehen Sie in Abbildung 3.2. Es soll dabei der Rechner mit der IP-Adresse `192.168.1.25` dem ersten, kleineren Netz zugehören.

```
harald@ZE4:~$ ipcalc 192.168.1.0/27
Address:   192.168.1.0          11000000.10101000.00000001.000 00000
Netmask:   255.255.255.224 = 27 11111111.11111111.11111111.111 00000
Wildcard:  0.0.0.31             00000000.00000000.00000000.000 11111
=>
Network:   192.168.1.0/27       11000000.10101000.00000001.000 00000
HostMin:   192.168.1.1          11000000.10101000.00000001.000 00001
HostMax:   192.168.1.30         11000000.10101000.00000001.000 11110
Broadcast: 192.168.1.31         11000000.10101000.00000001.000 11111
Hosts/Net: 30                    Class C, Private Internet

harald@ZE4:~$ # 2. Berechnung, um die Startadresse für das 2. Teilnetz zu erhalten
harald@ZE4:~$ ipcalc 192.168.1.0/25
Address:   192.168.1.0          11000000.10101000.00000001.0 0000000
Netmask:   255.255.255.128 = 25 11111111.11111111.11111111.1 0000000
Wildcard:  0.0.0.127            00000000.00000000.00000000.0 1111111
=>
Network:   192.168.1.0/25       11000000.10101000.00000001.0 0000000
HostMin:   192.168.1.1          11000000.10101000.00000001.0 0000001
HostMax:   192.168.1.126        11000000.10101000.00000001.0 1111110
Broadcast: 192.168.1.127        11000000.10101000.00000001.0 1111111
Hosts/Net: 126                   Class C, Private Internet

harald@ZE4:~$ # 3. Berechnung für das zweite Teilnetz
harald@ZE4:~$ ipcalc 192.168.1.128/25
Address:   192.168.1.128        11000000.10101000.00000001.1 0000000
Netmask:   255.255.255.128 = 25 11111111.11111111.11111111.1 0000000
Wildcard:  0.0.0.127            00000000.00000000.00000000.0 1111111
=>
Network:   192.168.1.128/25     11000000.10101000.00000001.1 0000000
HostMin:   192.168.1.129        11000000.10101000.00000001.1 0000001
HostMax:   192.168.1.254        11000000.10101000.00000001.1 1111110
Broadcast: 192.168.1.255        11000000.10101000.00000001.1 1111111
Hosts/Net: 126                   Class C, Private Internet
```

Abbildung 3.2 Berechnungen für die beiden Teilnetze

Um nun herauszubekommen, ab welcher Adresse das zweite Teilnetz beginnt, führen Sie die Berechnung für die Netzadresse `192.168.1.0` zweimal aus, einmal mit der zutreffenden Netzmaske `255.255.255.224` und für das zweite Teilnetz mit `255.255.255.128`. Sie können dann die höchste vorkommende Adresse ablesen (`Broadcast`). Deren Wert erhöhen Sie um 1 und nehmen das Ergebnis als Startwert für die dritte Berechnung. Zusammen mit der richtigen Netzmaske (`/25`) erhalten Sie alle notwendigen Angaben für das zweite Teilnetz mit den 80 Teilnehmern.

Im Ergebnis erhalten Sie jeweils die Netzadresse, die niedrigste und höchste für Netzwerkteilnehmer verwendbare Adresse (`HostMin` und `HostMax`), deren Anzahl (`Hosts/Net`) und die Broadcast-Adresse.

3.5.4 Private Adressen des IPv4

Für den Aufbau Ihrer privaten, nicht mit dem Internet direkt verbundenen Netze benutzen Sie die durch `RFC 1918` definierten Adressbereiche (Tabelle 3.10). Diese Adressen werden auch nicht in das öffentliche Internet weitergeleitet.

Adressbereich	Anzahl IP-Adressen
`10.0.0.0-10.255.255.255`	ein Netz mit 16.777.216 Adressen, Netzmaske 255.0.0.0 10.0.0.0/8
`172.16.0.0-172.31.255.255`	16 Netze mit 65.536 Adressen, Netzmaske 255.255.0.0 172.16.0.0/16–172.31.0.0/16
`192.168.0.0-192.168.255.255`	256 Netze mit 256 Adressen, Netzmaske 255.255.255.0 192.168.0.0/24–192.168.255.0/24

Tabelle 3.10 Adressbereiche privater Netzwerke

3.5.5 Zeroconf – konfigurationsfreie Vernetzung von Rechnern

Neben den drei klassischen IPv4-Privatnetzen stehen Ihnen auch noch die Adressen von `169.254.1.0` bis `169.254.254.255` zur Verfügung. Auch sie werden nicht in das Internet durchgeroutet. In diesem reservierten Bereich, genannt *Zeroconf*, können Sie Rechner ohne weitere Konfiguration vernetzen. Sie müssen weder manuell noch per DHCP eine IP-Adresse zuweisen. Die Nutzung von DHCP widerspricht sogar dem Wesen von Zeroconf und darf deshalb nicht angewendet werden. Der reservierte Adressbereich ist für das *Automatic Private IP Adressing* (*APIPA*) nach RFC 3927, auch bekannt als Zeroconf oder *Auto-IP*, reserviert. Die Netzmaske lautet

255.255.0.0, die ersten und letzten 256 Adressen dürfen nicht verwendet werden. Somit verbleiben Ihnen immerhin 65.024 Adressen zur Nutzung.

Die automatische Adresskonfiguration greift dabei auch auf die Sicherungsschicht (Layer 2) des OSI-Modells zu. Wenn Sie Ihren Rechner einschalten, berechnet er zunächst aus seiner MAC-Adresse zusammen mit einem Zufallsgenerator seine IP-Adresse. Weil eine IP-Adresse in einem Netz nur einmal vorhanden sein darf, prüft Ihr Rechner, ob die Adresse nicht schon von einem anderen Gerät benutzt wird. Er bildet dazu ein ARP-Paket (ARP-Probe), bei dem die Absenderadresse mit 0.0.0.0 und als Empfängeradresse die eigene angegeben wird. Ihr Rechner sendet das Paket insgesamt dreimal alle 1 bis 2 Sekunden aus. Erhält Ihr Rechner bis nach 2 Sekunden nach dem Absetzen der letzten ARP-Probe ein ARP-Paket, bei dem die errechnete IP-Adresse mit der Absenderadresse übereinstimmt, muss er nochmals eine neue berechnen. Befinden sich zum gleichen Zeitpunkt besonders viele Rechner am Netz, welche ihre Adressen berechnen, so müssen Sie mit solchen Adresskonflikten rechnen. Damit das Netzwerkwerk nicht mit zu vielen ARP-Paketen überfrachtet wird, werden die sich gerade konfigurierenden Rechner nach zehn Fehlversuchen nur noch einen Versuch je Minute starten. Für Sie und die anderen Benutzer können also durchaus fühlbare Wartezeiten auftreten.

Gehört Ihrem Rechner »seine« Adresse, macht er diese allen anderen per doppeltem ARP-Announcement im Abstand von 2 Sekunden bekannt. Hierbei verwendet er als Absender- und Empfänger-IP diese eben berechnete Adresse. Im Zeroconf-Netz herrscht hinsichtlich der IP-Adresse trotzdem eine trügerische Ruhe für Ihren Rechner. Er muss jetzt ständig auf Adresskonflikte, die durch andere Rechner verursacht werden, achten. Diesen Fall erkennt er, wenn ARP-Pakete von anderen Teilnehmern eintreffen, welche »seine« Adresse als Absenderadresse benutzen.

Ihr Rechner reagiert darauf auf verschiedene Weise. Hat er offene TCP-Verbindungen und noch keine kollidierenden ARP-Pakete empfangen, also nur ein ARP-Probe, sendet er ein klarstellendes ARP-Announcement. In allen anderen Fällen wird er sich eine neue Adresse berechnen und damit eine »Schlacht um die IP-Adresse« mit viel Netzlast durch Endlosschleifen vermeiden.

Zeroconf bietet eine eigene Namensauflösung und Diensterkennung an, was an späterer Stelle hier im Buch gezeigt wird.

Zeroconf finden Sie bei allen gängigen Betriebssystemen. Für Apple-Rechner ist es unter *bonjour* bekannt, Linux und Unix-Derivate verwenden hauptsächlich den *avahi-Daemon*. Microsoft nennt das Verfahren *Automatic Private IP Addressing* (*APIPA*).

Fakten zu Zeroconf

- **automatische Adresszuweisung** ohne DHCP-Server
- **Namensauflösung** ohne DNS-Server
- **automatische Erkennung von Netzwerkdiensten**
- **Sicherheit**: Die automatische Konfiguration greift tief in das jeweilige Betriebssystem ein. Vom Einsatz in sicherheitsrelevanten Umgebungen wird deshalb abgeraten.
- **Norm**: RFC 3927

3.5.6 Localnet und Localhost

Moderne Betriebssysteme benötigen ein »internes Netzwerk« zur Erledigung verschiedener Aufgaben. Im Bereich Unix/Linux greifen unter anderem die Druckdienste und das X11- bzw. Xorg-Grafiksystem darauf zurück. Sie finden für diese *Loopback-Adressen* den Adressbereich von `127.0.0.0` bis `127.255.255.255` reserviert. Für jede Netzwerkkarte Ihres Rechners wird diese (zusätzliche) Adresse mehr oder weniger von selbst vergeben. Datenpakete an eine Adresse aus diesem Bereich werden nicht in das Netzwerk geleitet, sondern wieder zurück an den Rechner.

Sie können für viele kritische Anwendungen die Sicherheit erheblich erhöhen, wenn diese ausschließlich auf dieser *Loopback-Adresse* »lauschen«. Natürlich ist das nur sinnvoll, wenn diese Anwendung ausschließlich für diesen einzigen Rechner ihre Dienste anbieten soll, z. B. ein eigener, rechnerlokaler Name-Server oder eine Datenbank. Angriffe hierüber mittels des lokalen Netzwerkes sind damit ausgeschlossen.

Auch für den Test von Serveranwendungen greifen Entwickler gerne auf den `localhost` zurück. Sie vermeiden Netzlast und natürlich auch den Zugang durch Sicherheitslücken in den noch unfertigen Anwendungen.

Auszug der Ausgabe von ifconfig für die superprivate Adresse

```
lo
Link encap:Lokale Schleife
inet Adresse:127.0.0.1  Maske:255.0.0.0
inet6-Adresse: ::1/128 Gültigkeitsbereich:Maschine
UP LOOPBACK RUNNING  MTU:16436  Metrik:1
RX packets:433140 errors:0 dropped:0 overruns:0 frame:0
TX packets:433140 errors:0 dropped:0 overruns:0 carrier:0
Kollisionen:0 Sendewarteschlangenlänge:0
RX bytes:50267351 (47.9 MiB)  TX bytes:50267351 (47.9 MiB)
```

Auf diesem Linux-Rechner wird das Loopback-Gerät als `lo` bezeichnet. Vergleichen Sie die Angaben zu den gesendeten (`TX`) und empfangenen (`RX`) Daten. Sie zeigen stets die gleichen Werte.

Die RFCs 5735 und 2606 beschreiben den Einsatz dieses besonderen Adressbereiches.

3.5.7 Weitere reservierte Adressen

Sie finden in Tabelle 3.11 weitere reservierte Adressbereiche (RFC 5735). Die Anwendungen sind sehr unterschiedlich. So finden Sie IP-Bereiche, die Sie für Anleitungen und Dokumentationen verwenden können, ohne damit Betriebs- und Sicherheitsgeheimnisse auszuplaudern.

Adressbereich	Netzmaske	Zweck	RFC
0.0.0.0 – 0.255.255.255	255.0.0.0	aktuelles Netz (nur als Quelladresse zulässig)	3232
192.0.0.0 – 192.0.0.255	255.255.255.0	noch reserviert, aber Vergabe vorgesehen	
192.0.2.0 – 192.0.2.255	255.255.255.0	Test-Net-1, Dokumentation und Beispielcode	5737
192.88.99.0 – 192.88.99.255	255.255.255.0	Weiterleitungspräfix für 6to4-Anycast	3068
198.18.0.0 – 198.19.255.255	255.254.0.0	Benchmark-Tests	2544
198.51.100.0 – 198.51.100.255	255.255.255.0	Test-Net-2, Dokumentation und Beispielcode	5737
203.0.113.0 – 203.0.113.255	255.255.255.0	Test-Net-3, Dokumentation und Beispielcode	5737
224.0.0.0 – 239.255.255.255	weitere Unterteilungen	Multicasts	3171
240.0.0.0 – 255.255.255.255	weitere Unterteilungen	reserviert	1112 Sect.4
255.255.255.255	255.255.255.255	Broadcast	0919 und 0922

Tabelle 3.11 Weitere reservierte IPv4-Adressbereiche

3.6 IPv6-Adressen

Sie werden mehr und mehr mit dem Nachfolger des IPv4 zu tun haben. IPv6 wird IPv4 ablösen (müssen). Die maximal 4.294.967.296 Adressen des IPv4 sind bald komplett vergeben. Eine Adressknappheit bedeutet aber eine Stagnation beim weiteren Ausbau des Internets. Schon lange wurde deshalb am Nachfolgeprotokoll gearbeitet. Die Netzgemeinde profitiert bei IPv6 nicht nur vom erweiterten

Adressraum. Das IPv6 besitzt auch neue Leistungsmerkmale, welche unter IPv4 nicht oder nur mit externen Erweiterungen verfügbar waren.

Kenndaten des IPv6

- Anzahl der Adressen: 2^{128}
- zustandslose automatische Konfiguration von Adressen
- integrierte Verschlüsselung von IP-Paketen (*Ipsec*)
- Verwirklichung des Ende-zu-Ende-Prinzips (Wegfall von Verfahren wie *Network Adress Translation* (*NAT*))
- IP-Adressen für mobile Geräte
- Vereinfachung von Techniken wie *Quality of Service* und *Multicast*
- Wichtige Normen: RFCs **2460** und **4291**, Updates: RFCs 5095, 5722, 5871, 5952, 6052

IPv6-Adressen bieten Ihnen einen anderen Anblick. Durch ihre Länge von 128 Bit und der hexadezimalen Schreibweise sind sie schwerer lesbar als die gewohnten IPv4-Adressen. Rechner haben allerdings weniger Schwierigkeit mit der Umwandlung von Hexadezimalzahlen in Binärzahlen als mit der von Dezimalzahlen in Binärzahlen.

Eine IPv6-Adresse wird wegen ihrer Länge anders dargestellt. Sie wird in acht durch »:« getrennte Blöcke zu 16 Bit unterteilt, die Werte in hexadezimaler Schreibweise angegeben.

Schreibweisen von IPv6-Adressen

- **Grundform**: `fe80:0000:0000:0000:0223:54ff:fe5b:869d`
- **Nullen**: Sie dürfen führende Nullen innerhalb eines Blockes auslassen.
- **Blöcke mit Wert 0**: Sie dürfen aufeinanderfolgende Blöcke, deren Wert 0 beträgt, auslassen und durch einen Doppelpunkt ersetzen. Sie dürfen das innerhalb einer Adresse allerdings nur einmal durchführen.
- **Beispiel** nach dem Entfernen führender Nullen und von zusammenhängenden Blöcken mit 0: `fe80::223:54ff:fe5b:869d`
- **URL**: IPv6-Adressen werden in eckige Klammern eingeschlossen: `http://[fe80::223:54ff:fe5b:869d]/`
- **Port-Nummern**: Sie werden außerhalb der Klammerung angefügt: `http://[fe80::223:54ff:fe5b:869d]:8080/`

(Sub-)Netzmasken in der klassischen Form sind bei IPv6 nicht gebräuchlich, vielmehr benutzen Sie hier die CIDR-Notation. Die Größe eines zu vergebenden

Netzwerkes muss einer Zweierpotenz entsprechen, ein einzelner Host trägt die `/128`. Abbildung 3.3 zeigt Ihnen die Zergliederung einer IPv6-Adresse.

Byte	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	x 8
=Bits (Länge)	8	16	24	32	40	48	56	64	72	80	88	96	104	112	120	128	
Adresse	fe	80	00	00	00	00	00	00	02	23	54	ff	fe	5b	86	9d	

Abbildung 3.3 Zergliederung einer IPv6-Adresse

Sie geben ein Netz in der Form `fe80:0000:0000:0000:0223/80` an. Die Netzadresse lautet damit `fe80:0000:0000:0000:0223:0000:0000:0000`, die Adressen für die Hosts gehen von `fe80:0000:0000:0000:0223:0000:0000:0001` bis `fe80:0000:0000:0000:0223:ffff:ffff:ffff`, was 281.474.976.710.655 Adressen ergibt.

Ihr Internet-Provider bezieht normalerweise die ersten 48 Bits des Netzes von seiner *Regional Internet Registry* (*RIR*). Diesen Bereich teilt er weiter in Teilnetze auf. Die Teilnetz-ID ist normalerweise 16 Bit lang. Sie selbst bekommen ein Teilnetz `/64`. Nun kennen Sie bereits die ersten beiden Teile Ihrer Adressen, das Standort-Präfix und die Teilnetz-ID. Der dritte Teil besteht aus dem 64 Bit langen *Interface Identifier*. Dabei wird entweder die MAC-Adresse der Netzwerkkarte zur Berechnung mit herangezogen, oder Sie vergeben diesen Teil der IPv6-Adresse selbst (Abbildung 3.4, RFC 4291).

Bestandteile von IPv6-Adressen

- **Präfix**: Kennzeichnet den Adressraum, wird in CIDR-Schreibweise angegeben.
- **Subnet-ID**: Organisationen unterteilen damit die ihnen zugewiesenen Bereiche. Sie erhalten ein `/48`-Präfix und verwenden 16 Bit für die Kennzeichnung ihrer Subnetze.
- **Interface-ID**: Kennzeichnet die Schnittstelle (Schnittstellen-ID).

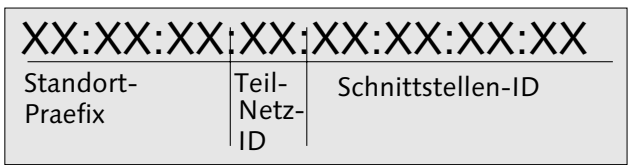


Abbildung 3.4 Unterteilung von IPv6-Adressen

3.6.1 Adresstypen des IPv6

Sie treffen beim IPv6 auf drei Arten von Adressen. Die Ihnen vom IPv4 her bekannten Broadcast-Adressen sind hier ungebräuchlich und wurden teilweise durch die *Multicast-Adressen* ersetzt.

Grundregeln zur IPv6-Adressvergabe

- Für jede Netzwerkschnittstelle (Interface) müssen Sie mindestens eine Unicast-Adresse vergeben.
- Sie können für jede Netzwerkschnittstelle mehrere IPv6-Adressen zuweisen.
- Sie können für jede Netzwerkschnittstelle gleichzeitig Unicast-, Multicast- und Anycast-Adressen verwenden.
- Sie können eine Unicast-Adresse mehreren Netzwerkschnittstellen eines Rechners zuweisen, um darüber eine Lastverteilung zu ermöglichen.
- Sie können einen Knoten über jede der Unicast-Adressen ansprechen.

Die drei Adresstypen Unicast, Multicast und Anycast erfüllen alle bestimmte Zwecke und haben ihre Besonderheiten, auf die Sie achten müssen.

Unicast-Adressen

- Dienen der eindeutigen Identifizierung eines Interfaces eines Knotens (Netzwerkteilnehmers).
- **Globale Unicast-Adressen** sind weltweit gültig und werden über das Internet geroutet. Ihr Präfix lautet `2000::/3`.
- **Link-local Unicast-Adressen** gelten nur im lokalen Netz und werden nicht in das Internet weitergeroutet. Ihr Präfix lautet `FE80::/10`.
- Jede Netzwerkschnittstelle benötigt eine eigene *Link-local* Adresse, um im privaten Netzwerk den Rechner (Knoten) gegenüber anderen Knoten zu identifizieren. Dies ist für das Funktionieren der automatischen Adresskonfiguration und des *Neighbor Discovery Protokolls* (*NDP*) notwendig.

Wenn Sie eine Unicast-Adresse mehreren Netzwerkschnittstellen zuordnen, haben Sie eine *Anycast-Adresse* geschaffen.

Anycast-Adressen

- Verfügen über das gleiche Präfix wie Unicast-Adressen.
- Werden aus dem Unicast-Adressbereich entnommen.
- Dienen zur Lastverteilung und Bildung von Redundanzen.
- Bei einer Routergruppe mit gemeinsamer Anycast-Adresse werden Pakete an den nächsterreichbaren Router gesendet.
- Absender hat keine Möglichkeit, die Empfangsschnittstelle auszuwählen. Das Zielgerät wird durch das Routingprotokoll bestimmt.

- Beim Interface Identifier der Adresse sind alle Bits auf 0 gesetzt.
- Reservierte Subnetz-Anycast-Adressen verwenden eine Anycast-ID mit 7 Bit Länge. Diese vermindert die Bitzahl beim Interface Identifier entsprechend. Der Interface-Identifier-Anteil beim EUI-64-Format ist damit nur 57 Bit lang.
- Norm: RFC 2526

Die Anycast-IDs von `00-7D` und `7F` sind reserviert, `7E` ist dem *Mobile IPv6 Home Agent Anycast* vorbehalten.

Multicast-Adressen benötigen Sie, um gleichzeitig viele Rechner anzusprechen, z. B. beim Internetradio, NTP-Server (Zeitserver).

Multicast-Adressen

- Mit der Multicast-Adresse erreichen Sie eine Gruppe von Netzwerkschnittstellen.
- Ein Paket an eine Multicast-Adresse erreicht alle Netzwerkschnittstellen mit dieser Adresse und wird von diesen verarbeitet.
- Eine Netzwerkschnittstelle kann mehrere Multicast-Adressen haben.
- Multicast-Adressen erkennen Sie am Präfix `FF00::/8`.
- Multicast-Adressen enthalten einen Group Identifier anstelle des Interface Identifiers (Tabelle 3.12).

8 Bit	4 Bit	4 Bit	8 Bit	8 Bit	64 Bit	32 Bit
FF	Flags ORPT	Scope	reser-viert	plen	IID	Group Identifier

Tabelle 3.12 Zusammensetzung der Multicast-Adresse nach RFC 4489

Die Werte für die Flags (Tabelle 3.13) und Scope (Tabelle 3.14) zeigen Ihnen weitere Eigenschaften der Multicast-Adresse auf.

Flag	Einträge
O	reserviert, muss mit 0 belegt werden
R	Rendezvous-Point nach RFC 3956
P	dynamisch zugewiesene Präfix-Information gemäß RFC 3306
T	0 = fest von IANA zugewiesen, 1 = temporäre Multicast-Adresse

Tabelle 3.13 Flags in Multicast-Adressen

Im Scope-Feld finden Sie Angaben, die die Reichweite der Multicast-Adresse beschränken.

Wert(e)	Zuweisung
0, 3, F	reserviert
6, 7, 9, A, B, C, D	nicht zugewiesen
1	Interface-local Scope
2	Link-local Scope
4	Admin-local Scope
5	Site-local Scope
8	Organisation-local Scope
E	Global Scope

Tabelle 3.14 Einträge Scope-Feld

Die nachfolgenden acht Bits sind reserviert, Sie müssen sie mit `0` belegen. Den Bereich `plen` müssen Sie mit `FF` belegen (nach RFC 4489).

Das `IID`-Feld ersetzt das 64-Bit-Präfix gemäß RFC 3306. Sie halten damit die einzelnen Knoten auseinander. Der *Group Identifier* kennzeichnet eine Multicast-Anwendung. Ferner stellt er sicher, dass diese nur einmal auf dem Host vorhanden ist.

Beispiele für bekannte Multicast-Adressen

`FF01:0:0:0:0:0:0:1` All-Nodes-Adresse, Interface-local, Scope

`FF01:0:0:0:0:0:0:2` All-Router-Adresse, Interface-local, Scope

`FF02:0:0:0:0:0:0:1` All-Nodes-Adresse, Link-local, Scope

`FF02:0:0:0:0:0:0:2` All-Router-Adresse, Link-local, Scope

3.6.2 IPv6-Loopback-Adresse

Die Ihnen schon vom IPv4 bekannte Loopback-Adresse wird auch im IPv6 verwendet. Sie lautet `0:0:0:0:0:0:0:1`, in Kurzform `::1`. Auch hier müssen Sie beachten, dass Sie diese Adresse niemals Netzwerkschnittstellen zuweisen dürfen und können.

Loopback-Adresse bei einem Linux-Rechner mit IPv4 und IPv6

```
lo
Link encap:Lokale Schleife
inet Adresse:127.0.0.1  Maske:255.0.0.0
inet6-Adresse: ::1/128 Gültigkeitsbereich:Maschine
...........
```

Beachten Sie die CIDR-Schreibweise (/128) mit der ein einzelner Host gekennzeichnet wird. Manche Systeme, wie FreeBSD, vergeben zusätzlich noch eine Link-local Unicast-Adresse.

Loopback-Adresse bei einem FreeBSD-System mit IPv4 und IPv6

```
lo0: flags=8049<UP,LOOPBACK,RUNNING,MULTICAST> metric 0 mtu 16384
        options=3<RXCSUM,TXCSUM>
        inet 127.0.0.1 netmask 0xff000000
        inet6 ::1 prefixlen 128
        inet6 fe80::1%lo0 prefixlen 64 scopeid 0x5
.............
```

3.6.3 Unspezifizierte Adresse

Diese Adresse verwendet Ihr Rechner unter anderem während des Ladevorganges als Absenderadresse. Empfängt er in dieser Phase eine Anfrage zur Adresskonfiguration von einem anderen Knoten, zeigt er damit an, dass er (noch) nicht über eine gültige IP-Adresse verfügt.

Die *All-Zero-Adresse* sollten Sie nie in Zieladressen verwenden. Die Adresse wird 0:0:0:0:0:0:0:0 ausgeschrieben oder als :: abgekürzt.

3.6.4 IPv4- in IPv6-Adressen und umgekehrt

Der Wechsel von IPv4 nach IPv6 geschieht allmählich, so dass Sie mit beiden Protokollfamilien parallel arbeiten werden.

Sie werden beim Stöbern in älterer Fachliteratur auf die *Ipv4-kompatible IPV6-Adresse* stoßen. Diese speziellen Unicast-Adressen transportierten Ipv6-Pakete über ein Ipv4-Netz. Die letzten 32 Bits enthielten die IPv4-Adresse. Dieser Adresstyp wird nicht mehr verwendet und auch nicht mehr unterstützt (RFC 4291, abgelöst durch RFC 6052).

Mit der Verwendung einer *Ipv4-mapped IPv6-Adresse* stellen Sie die Adresse eines IPv4-Hosts als IPV6-Adresse dar. Nach RFC 6052 wird empfohlen, den IPv4-Adressteil an den Schluss zu hängen (/96). Damit können Sie den IPv4-Teil vor allem auch in der gewohnten Schreibweise verwenden. Von rechts nach links gesehen (Tabelle 3.15), füllen Sie nach dem IPv4-Teil die nächsten 16 Bits mit FFFF auf. Damit wurde eine Länge von 48 Bit erreicht. Die weiteren Stellen werden mit 0-Bits aufgefüllt. Sie erhalten damit ein Präfix 0:0:0:0:0:FFFF::/96.

80 Bit	16 Bit	32 Bit
0:0:0:0:0	FFFF	IPv4-Adresse

Tabelle 3.15 IPv4-mapped IPv6-Adresse

Schreibweisen von IPv4-mapped IPv6-Adressen

IPv4-Adresse: `192.168.1.200`
IPv6-Adresse: `0:0:0:0:0:FFFF:C0A8:01C8`
Kurzschreibweisen: `::FFFF:C0A8:01C8, ::FFFF:192.168.1.200`

3.6.5 Tunnel-Adressen

Während der Übergangsphase reisen Ihre Datenpakete durch IPv4- und IPv6-Netze. Dabei müssen sich die Adressen anpassen. Ihnen begegnen dabei verschiedene Tunnel-Adressen.

Sie benötigen *6to4-Adressen*, wenn Sie Pakete Ihrer IPv6-Knoten über ein IPv4-Netzwerk zu anderen IPv6-Knoten leiten wollen und dabei aber nicht auf einen statisch konfigurierten Tunnel zurückgreifen können. Hier wird die IPv4-Adresse nicht am Schluss angehängt, sondern in den führenden Stellen. Soll die Reise über das öffentliche Internet gehen, dürfen Sie dabei keine privaten IP-Adressen verwenden.

6to4-Adressen tragen das Präfix `2002`. Die eingebettete IPv4-Adresse wird hexadezimal dargestellt (Tabelle 3.16).

16 Bit	32 Bit	16 Bit	64 Bit
2002	IPv4-Adresse	Teilnetz-ID	Interface-ID
Präfix	48 Bit		

Tabelle 3.16 Aufbau von 6to4-Adressen

Beispiel einer 6to4-Adresse

IPv4-Adresse: `85.88.3.146`
IPv6-Adresse: `2002:5558:0392:0001:0:0:0:8`

Sie haben einen Rechner, der mit seiner privaten IPv4-Adresse mittels eines Routers mit dem Internet verbunden ist. Der Router führt die übliche *Network Adress Translation* (*NAT*) durch. Ihr Rechner soll sich in ein entferntes IPv6-Netz einfügen. Um diese Verbindung zu realisieren, müssen Sie den *Teredo-Mechanismus* benutzen. Dieser tunnelt das IPv6 in UDP über Teredo-Relais. Der Teredo-Dienst besteht aus diesen Relais, Clients und Servern.

Teredo stammt aus dem Hause Microsoft. In der Unix-Welt ist der Dienst unter dem Begriff *Miredo* bekannt. Der Dienst umgeht die üblicherweise vorhandene IPv4-Firewall, so dass Sie die Anwendung als Sicherheitsproblem betrachten müssen.

Die Teredo-Adressen (Tabelle 3.17) besitzen das Präfix `2001:0000:/32`. Die Pakete werden über den UDP-Port 3544 geleitet (Erklärungen zu Ports finden Sie in Abschnitt 6.3, »Nutzung von Services mittels Ports und Sockets«). Die genauen Definitionen finden Sie in RFC 4380 und, was die Sicherheit von Teredo betrifft, in RFC 5991.

32 Bit	32 Bit	16 Bit	16 Bit	32 Bit
2001:0000 Präfix	IPv4-Adresse Server	Flags	Port	IPv4-Adresse Client

Tabelle 3.17 Aufbau von Teredo-Adressen

Wenn Sie den Wunsch haben, über ein IPv4-Netzwerk zwei IPv6-Hosts ohne Zuhilfenahme von Routern kommunizieren zu lassen, so hilft Ihnen dabei das *Intra Site Automatic Tunnel Adressing Protocol* (*ISATAP*).

In RFC 5214 ist festgeschrieben, dass die Adressen im modifizierten EUI-64-Format (nach RFC 4291) gehalten sind. Damit ergibt sich ein Aufbau nach Tabelle 3.18.

64 Bit	32 Bit	32 Bit
Präfix	private IPv4-Adresse 0000:5EFE öffentl. IPv4-Adresse 0200:5EFE	IPv4-Adresse

Tabelle 3.18 Aufbau einer ISATAP-Adresse

Die ersten 64 Bits einer ISATAP-Adresse entsprechen jenen einer gewöhnlichen Unicast-Adresse. Von den folgenden 32 Bits dienen 24 Bits dem *IEEE Organizationally Unique Identifier* (*OUI*). Davon sehen Sie in den ersten 16 Bits wiederum, ob es sich um eine private IPv4-Adresse (`0000`) oder um eine öffentliche (`0002`) handelt. Mit der Kennung `FE` zeigt die Adresse an, dass sie eine IPV4-Adresse enthält.

3.6.6 Kryptografisch erzeugte Adressen (CGA)

Durch die Anwendung von kryptografisch erzeugten Adressen (Secure Neighbor Discovery (SEND)) können Sie die Sicherheit bei der Neighbor Discovery (ND) erhöhen. Sie können damit sicherstellen, dass der Absender von NDP-Paketen auch der »rechtmäßige« Inhaber der IP-Adresse ist.

Die Interface-ID wird hierbei durch zusätzliche Parameter und Hash-Funktionen berechnet. In den RFCs 3972, 4581 und 4982 finden Sie darüber Erläuterungen zu den eingesetzten Verfahren. Insbesondere verhüten Sie durch den Einsatz dieser so berechneten Adressen Spoofing-Attacken gegen das Neighbor- und Router Solicitation und -Advertisement. Auch gegen DOS-Attacken der *Duplicate Address Detection* (*DAD*) und Massen-Antworten sind Sie damit geschützt.

3.6.7 Lokale Adressen

Auch im IPv6 treffen Sie auf lokale Adressen. Diese werden keinesfalls in das Internet weitergeleitet, sie dienen dem Datentransport in Ihrem privaten Netzwerk.

Die *Site-local Unicast-Adressen* sind nach RFC 3879 obsolet. Stattdessen können Sie die *Unique-local Unicast-Adressen*, wie sie das RFC 4193 beschreibt, frei innerhalb Ihres lokalen Netzes verwenden. Sie erkennen diese Adressen am Präfix `FD00::/8` bzw. `FC00/8`. Ihren Aufbau finden Sie in Tabelle 3.19 beschrieben.

Bereich	8 Bit	40 Bit	16 Bit	64 Bit
privat administriert	FD00	Global ID	Subnet-ID	Interface-ID
reserviert für Registrierung	FC00 Präfix			

Tabelle 3.19 Aufbau Unique-local Unicast-Adressen

Das Präfix `FD00` wenden Sie bei privater, nicht öffentlicher Administration des lokalen Netzes an. `FC00` ist für die in der Zukunft einmal mögliche Registrierung eigener privater Adressbereiche vorgesehen.

3.6.8 Übersicht der Präfixe von IPv6-Adressen

Zusammenfassend finden Sie eine Übersicht über die wichtigsten Präfixe im IPv6 (Tabelle 3.20).

Präfix	Zugewiesen für
`FF00/8`	Multicast-Adressen
`FD00/8`	Unique-local Unicast-Adressen, privat verwaltet
`FC00/8`	Unique-local Unicast-Adressen, reserviert für später mögliche Registrierung
`FE80 /10`	Link-local Unicast-Adressen
`2000::/3`	Global Unicast-Adressen

Tabelle 3.20 IPv6-Adresspräfixe

Präfix	Zugewiesen für
2001::/32	Teredo-Adressen
2001:db8::/32	nur für Dokumentationszwecke, werden nicht im Internet weitergeleitet
2002:::/16	6to4
0:0:0:0:0:FFFF::/96	IPv4-mapped IPv6-Adresse
0:0:0:0:0:0:0:0 ::	All-Zero-Adresse
0:0:0:0:0:0:0:1 ::1/128	Localhost, Loopback-Adresse

Tabelle 3.20 IPv6-Adresspräfixe (Forts.)

3.6.9 Adresswahl und -benutzung

Bei den alten IPv4-Adressen reicht eine einzige für die Netzwerkkarte aus, damit Sie mit Ihrem Rechner im Netz »mitmischen« können. Unter IPv6 hingegen benutzt Ihr Rechner (teilweise für jede Netzwerkschnittstelle) die Link-local Adresse, die eventuelle zugewiesenen Uni- und Anycast-Adressen und die Loopback-Adresse. Ferner kennt er die All-Nodes-Multicast-Adresse und die Solicited-Node-Multicast-Adressen. Fungiert er zusätzlich als Router, gehören die Subnet-Router-Anycast-Adresse(n), die Anycast-Adressen und die All-Router-Multicast-Adressen dazu. Welche Adresse Ihr Rechner in welcher Situation benutzt, wird in RFC 3484 definiert, RFC 5220 hierzu ist informeller Natur. Internet-Draft RFC3484 Revise bereitet auf eine Neufassung von RFC 3484 vor.

Der Wegfall von *Site-local Unicast-Adressen* (nach RFC 3879) und die dafür neu hinzugekommenen *Unique-local Unicast-Adressen* (RFC4193) bewirken einige Änderungen auf das Wie und Wann der Anwendung der jeweiligen Adressen.

Einige wichtige Regeln zur Adressbenutzung

- Kleinerer Scope-Wert hat Vorrang: Damit werden lokale Adressen vor anderen bevorzugt, Pakete mit Ziel im eigenen, lokalen Netz werden mit diesen lokal gültigen Adressen transportiert.
- Benutzung des möglichst gleichen Scope-Wertes oder Link-Typs
- Mobile-IP: Home-Adressen gehen vor Care-of-Adressen.

Als Netzwerkadministrator sind Sie damit in der Regel nicht behelligt, wohl aber als Programmentwickler. Halten Sie sich über die entsprechenden RFCs über *http://www.ietf.org* unbedingt auf dem Laufenden!

3.7 Internetprotokoll

Das Internetprotokoll stellt für Sie nur die grundlegenden Transportmechanismen bereit, die für die Sendung von Datagrammen über Netzwerkgrenzen hinweg benötigt werden. Das Internetprotokoll arbeitet verbindungslos. Es wird, anders als bei verbindungsorientierten Verfahren, keine Verbindung im technischen Sinne aufgebaut, gesichert und abgebaut. Vielmehr sendet Ihr Rechner die Datagramme auf gut Glück in das Netz, in der Hoffnung, diese mögen ihr Ziel erreichen. Damit haben Sie auch schon eine besondere Stärke kennengelernt. Sie und Ihr Rechner müssen sich nicht um Verbindungswege und dergleichen kümmern. Und Sie werden auch kein »Besetztzeichen« erhalten. Wenn viele Rechner gleichzeitig Daten für ein Ziel senden, geht es einfach langsamer (oder, wenn es einfach zu viel wird, gar nicht mehr).

Es ist durchaus normal, dass die Datagramme nicht in der Reihenfolge ihrer Aussendung am Ziel eintreffen, nicht oder unvollständig ankommen. Das IP-Protokoll verfügt für solche Situationen über keinerlei Mechanismen. Diese sind vielmehr eine OSI-Schicht darüber angesiedelt (TCP-Protokoll, siehe Kapitel 6, »Datentransport mit TCP und UDP«).

Ihre IP-Pakete reisen mittels der Ethernet-Frames durch das Netz. Die IP-Header stehen vor den TCP- bzw. UDP-Headern, welche die Nutzdaten selbst aufnehmen. Details über die Ethernet-Frames finden Sie in Abschnitt 3.2, »Ethernet-Pakete (Ethernet-Frames)«.

Anhand des folgenden Gedankenmodells sehen Sie die Zusammenhänge klarer: Eine Fabrik versendet einen Traktor. Für den Versand wird er in eine Kiste (TCP- oder UDP-»Verpackung«) verpackt. Diese Umverpackung ist aber keine geeignete Transporthülle, also wird die Kiste in einen Container gestellt. Der Container enthält ein Dokument mit der Absender- und Zielangabe (IP-Header). Der Container wird auf einen Eisenbahnwaggon gestellt. Der Waggon hat unabhängig von den Angaben auf dem Container die Angabe eines Abgang- und Zielbahnhofes (Ethernet-Frame, Quell- und Ziel-MAC-Adresse). Der Waggon gelangt zum Zielbahnhof, einem Güterverkehrszentrum (Router). Der Container wird vom Waggon abgeladen und anhand des Frachtdokumentes auf das nächste Verkehrsmittel geladen, welches die Zielrichtung als Nächstes ansteuert. Auf diesem Weg wird der Container sicher noch öfter zwischen den verschiedenen Verkehrsträgern (Ethernet-Frames) umgeladen, bis er schließlich beim Empfänger landet. Dort wird er wieder vom Waggon genommen (Herauslösung aus dem Ethernet-Frame). Der Container wird geöffnet und die Kiste herausgeholt (Herausnahme aus der Transportverpackung, IP-Header). Die Kiste (TCP- oder UDP-Paket) wird geöffnet und schließlich der Traktor (Nutzlast) von ihr befreit.

Dieses Beispiel ist sehr ausführlich, Sie erkennen darin aber den kompletten Grundzug des Datentransportes über Netzwerke. Oft wird auf den notwendigen Zusammenhang von Ethernet-Frame und IP-Paket nicht eingegangen (Abbildung 3.5). Wenn Sie nun betrachten, was sich damit alles an »Overhead« zusammenballt, bekommen Sie ein Verständnis dafür, was es mit dem Begriff »Netzlast« auf sich hat. Selbst für ein paar Byte brauchen Sie diesen ganzen Aufwand.

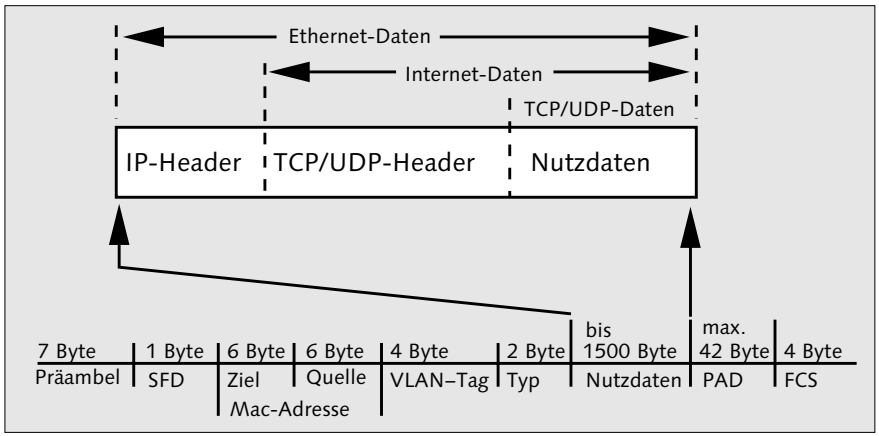


Abbildung 3.5 IP-Paket als Nutzlast des Ethernet-Frames

3.7.1 Der IPv4-Header

Im Header (Abbildung 3.6) finden Sie die Informationen für den Transport von Datagrammen. Je Zeile beträgt die Datenmenge 32 Bit.

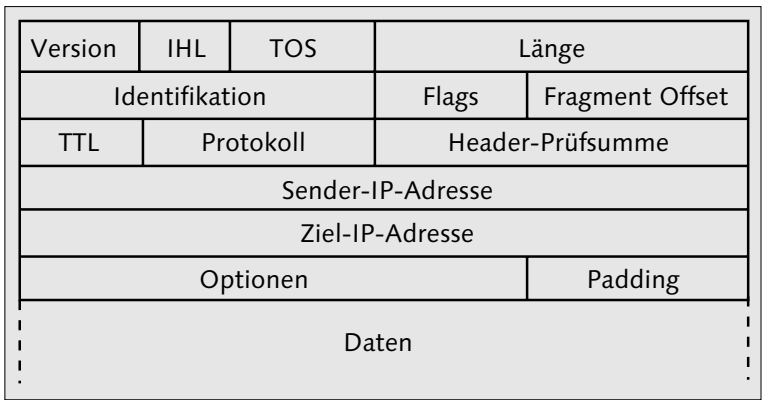


Abbildung 3.6 IPv4-Header

Die Bedeutung der einzelnen Felder des Headers finden Sie in Tabelle 3.21. Weitere Informationen finden Sie in den RFCs 3168 und 3260.

Feld	Länge (Bits)	Inhalt
Version	4	IP-Protokollversion (IPv4)
IHL	4	Internet Header Length, Länge des IP-Headers
TOS	8	Type of Service, Angabe zu Priorität und Eigenschaften des Paketes. Dieses Feld wird heute auch für die Angabe des QoS (Quality of Service) benutzt (RFC 3168), wobei nur die ersten sechs Bits benutzt werden: 0 für Best Effort, 40 für Expedited Flow (VoiP-Datenstrom) und 46 für Expedited Forwarding (VoiP-Datenstrom).
Länge	16	Total Length, maximal 64 kByte
Identifikation	16	Laufende Nummerierung der Pakete, dient zum Bilden der richtigen Reihenfolge beim Empfänger.
Flags	3	Bit 0: 0 (fest) Bit 1: 0: Fragmentierung erlaubt 1: Fragmentierung verboten Bit 2: 0: letztes Fragment, 1: weitere Fragmente folgen Diese Anweisung betrifft Router. Ist die Fragmentierung nicht erlaubt und das Paket größer als der Maximum Transport Unit (MTU), verfällt das Paket. Im IPv4 beträgt die Standardgröße für die Nutzlast 1500 Byte.
Fragment-Offset	13	Positionsangabe für Fragmente
TTL	8	Time to live: Lebensdauer eines Paketes in Sekunden, der Standardwert beträgt 64. Bei jedem Router, welchen das Paket durchläuft, vermindert sich der Wert um (mindestens) 1. Router verwerfen ein Paket mit der TTL 0. Dieser Mechanismus verhindert »unzustellbaren Datenmüll« und kreisende Nachrichten im Internet.
Protokoll	8	Angabe des Upper Layer Protocols, des eine OSI-Schicht höher liegenden Protokolls. Die Werte sind gemäß RFC 3232 in einer Datenbank hinterlegt. Beispiele: 6: TCP, 17: UDP, 1: ICMP
Header-Prüfsumme	16	Prüfsumme (gilt ausschließlich für den Header, nicht für die folgende Nutzlast)
Sender-IP-Adresse	32	IP-Adresse des Absenders
Ziel-IP-Adresse	32	IP-Adresse des Empfängers
Optionen	2	Angaben zu Routing und Diagnosezwecken

Tabelle 3.21 Inhalt des IPv4-Headers

Feld	Länge (Bits)	Inhalt
Padding	*	eventuell notwendige Füllbits zum Erreichen der vorgeschriebenen Bitzahl

Tabelle 3.21 Inhalt des IPv4-Headers (Forts.)

3.7.2 Der IPv6-Header

Der IPv6-Header (Abbildung 3.7) unterscheidet sich deutlich vom älteren IPv4-Format. So hat er eine feste Größe von 320 Bit. Weitere Informationen finden in dem erweiterten Kopfdaten-Bereich ihren Platz, welcher sich zwischen dem Header und dem Nutzdatenbereich befindet.

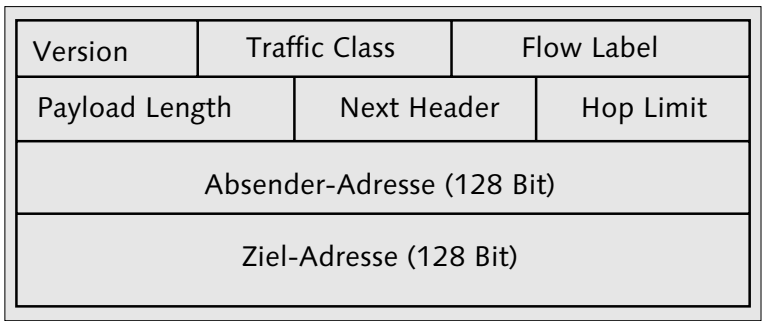


Abbildung 3.7 IPv6-Header

Die Tabelle 3.22 erläutert Ihnen die einzelnen Felder des IPv6-Headers. Einzelheiten zur IPv6-Adresse sind in den RFCs **2460**, 5095, 5722 und 5871 niedergeschrieben.

Feld	Länge (Bits)	Inhalt
`Version`	4	IP-Protokollversion (6)
`Traffic Class`	8	Quality of Service (QoS), Kennzeichnung der Priorität
`Flow Label`	20	Markieren von Paketen gleicher Verwendung und Behandlung (QoS). Zufallswerte, möglicher Bereich von `00001` bis `FFFFF`. Pakete ohne Eintrag durch Absender führen alle Bits mit 0. Pakete desselben Flows müssen stets die gleiche Absender- und Empfängeradresse tragen, sonst wird das Flow-Label nicht ausgewertet. Weitere Informationen finden Sie in RFC 3697 und dem noch in Diskussion befindlichen Nachfolge-Draft.

Tabelle 3.22 IPv6-Header

Feld	Länge (Bits)	Inhalt
`Payload Length`	16	Länge der Daten nach dem IPv6-Header (maximal 64 KB, Ausnahme Jumbogramm nach RFC 2675)
`Next Header`	8	Angabe des Folgeprotokolls (6 für TCP, 17 für UDP). Die Datenbank finden Sie unter *http://www.iana.org/assignments/protocol-numbers/protocol-numbers.xml*.
`Hop Limit`	8	Anzahl der maximalen Router-Sprünge (Hops). Wird der Wert überschritten, wird das Paket verworfen, und der Absender erhält eine ICPMv6-Nachricht. Bei jedem Hop vermindert sich der Wert um 1.
`Absenderadresse`	128	Angabe zwingend
`Zieladresse`	128	Kann auch nur die Adresse des nächsten Hops enthalten.

Tabelle 3.22 IPv6-Header (Forts.)

3.8 Prüfungsfragen

Die Auflösungen finden Sie in Abschnitt B, »Auflösungen Prüfungsfragen«.

3.8.1 Berechnungen

Ein Host hat die Adressangabe 192.168.5.65/23.

1. Über wie viele Hosts kann dieses Netz maximal verfügen?
2. Wie lautet die Netzwerkadresse dieses Netzes?
3. Wie lauten die erste und letzte IP-Adresse für Hosts in diesem Netz?

3.8.2 IP-Adressen

Warum gelingt der direkte Zugriff auf die Adresse

```
fe80::218:e7ff:fe16:7130/64
```

aus dem Internet nicht?

Index

A

B

C

D

E

F

G

H

I

J

K

L

M

N

O

P

Q

R

S

T

U

V

W

Y

Z