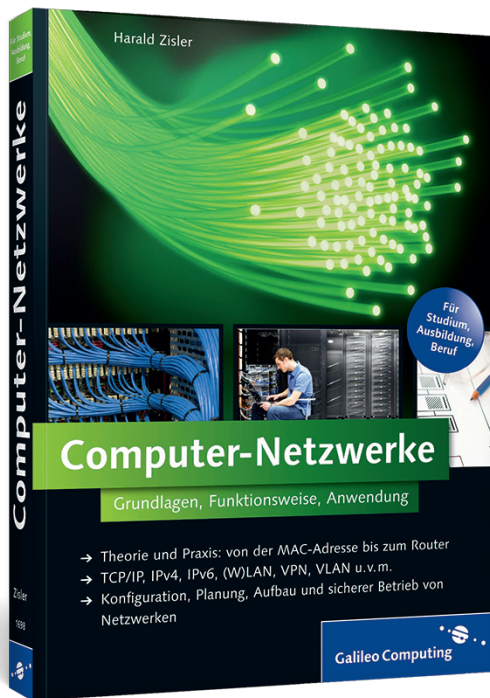


Harald Zisler

Computer-Netzwerke

Grundlagen, Funktionsweise, Anwendung



Auf einen Blick

1	Grundlagen moderner Netzwerke	17
2	Netzwerktechnik	27
3	Adressierung im Netzwerk – Theorie	75
4	MAC- und IP-Adressen in der Praxis	109
5	Steuer- und Fehlercodes mit ICMP und ICMPv6 übertragen	181
6	Datentransport mit TCP und UDP	187
7	Kommunikation und Sitzung	217
8	Standards für den Datenaustausch	255
9	Netzwerkanwendungen	259
10	Netzwerkpraxis	279
A	Fehlertafeln	327
B	Auflösungen Prüfungsfragen	335
C	Netzwerkbegriffe kurz erklärt	339

Inhalt

Geleitwort des Fachgutachters	13
Vorwort	15
1 Grundlagen moderner Netzwerke	17
1.1 Definition und Eigenschaften von Netzwerken	18
1.2 Die Netzwerkprotokollfamilie TCP/IP	20
1.3 OSI-Schichtenmodell und TCP/IP-Referenzmodell	21
1.4 Räumliche Abgrenzung von Netzwerken	24
1.5 Regel- und Nachschlagewerk für TCP/IP-Netze (RFCs)	25
1.6 Prüfungsfragen	26
2 Netzwerktechnik	27
2.1 Elektrische Netzwerkverbindungen und -standards	27
2.1.1 Netzwerke mit Koaxialkabeln	29
2.1.2 Netze mit Twisted-Pair-Kabeln	32
2.1.3 Aufbau, Bezeichnung und Kategorien von Twisted-Pair-Kabeln	33
2.1.4 Stecker- und Kabelbelegungen	36
2.1.5 Anschlusskomponenten für Twisted-Pair-Kabel	39
2.1.6 Herstellung von Kabelverbindungen mit der Schneid-Klemmtechnik (LSA)	41
2.1.7 Montage von RJ45-Steckern	44
2.1.8 Prüfen von Kabeln und Kabelverbindungen	48
2.1.9 Kennzeichnen, Suchen und Finden von Kabelverbindungen	52
2.1.10 Power over Ethernet (PoE)	54
2.2 Lichtwellenleiter, Kabel und Verbinder	54
2.2.1 Übersicht über die Netzwerkstandards mit Glasfaserkabel	56
2.2.2 Aufbau und Funktion von Glasfaserkabeln	57
2.2.3 Dauerhafte Glasfaserverbindungen	60
2.2.4 Lichtwellenleiter-Steckverbindungen	61
2.2.5 Umgang mit der LWL-Technik	64
2.2.6 Aufbau eines einfachen Leitungs- und Kabeltesters	67
2.2.7 Prüfen von LWL-Kabeln und -Verbindungen	67
2.3 Datenübertragung per Funktechnik	68

2.3.1	WLAN (Wireless LAN, Wi-Fi)	68
2.3.2	Datenübertragung über öffentliche Funknetze	70
2.3.3	Power-Line-Communication (PLC)	71
2.4	Technische Anbindung von Rechnern und Netzen	72
2.5	Weitere Netzwerkkomponenten	72
2.6	Zugriffsverfahren	73
2.6.1	CSMA/CD, Kollisionserkennung	73
2.6.2	CSMA/CA, Kollisionsvermeidung	73
2.7	Prüfungsfragen	74
3	Adressierung im Netzwerk – Theorie	75
3.1	Physikalische Adresse (MAC-Adresse)	75
3.2	Ethernet-Pakete (Ethernet-Frames)	77
3.3	Zusammenführung von MAC- und IP-Adresse	78
3.3.1	Adress Resolution Protocol (ARP), IPv4	78
3.3.2	Neighbor Discovery Protocol (NDP), IPv6	80
3.4	IP-Adressen	82
3.5	IPv4-Adressen	84
3.5.1	Netzwerkklassen im IPv4	84
3.5.2	Netz- und Subnetzmaske, Unterteilung von Netzen	85
3.5.3	Berechnungen	88
3.5.4	Private Adressen des IPv4	90
3.5.5	Zeroconf – konfigurationsfreie Vernetzung von Rechnern	90
3.5.6	Localnet und Localhost	92
3.5.7	Weitere reservierte Adressen	93
3.6	IPv6-Adressen	93
3.6.1	Adresstypen des IPv6	96
3.6.2	IPv6-Loopback-Adresse	98
3.6.3	Unspezifizierte Adresse	99
3.6.4	IPv4- in IPv6-Adressen und umgekehrt	99
3.6.5	Tunnel-Adressen	100
3.6.6	Kryptografisch erzeugte Adressen (CGA)	101
3.6.7	Lokale Adressen	102
3.6.8	Übersicht der Präfixe von IPv6-Adressen	102
3.6.9	Adresswahl und -benutzung	103
3.7	Internetprotokoll	104
3.7.1	Der IPv4-Header	105
3.7.2	Der IPv6-Header	107

3.8	Prüfungsfragen	108
3.8.1	Berechnungen	108
3.8.2	IP-Adressen	108
4	MAC- und IP-Adressen in der Praxis	109
4.1	MAC-Adressen	109
4.1.1	Ermitteln der MAC-Adresse	109
4.1.2	Ändern der MAC-Adresse	111
4.1.3	Manuelles Setzen und Ändern von MAC-Adressen mittels arp	112
4.1.4	ARP-Spoofing erkennen	112
4.2	IP-Adressen setzen	112
4.2.1	Netzwerkconfiguration von PCs	114
4.2.2	IP-Adresskonfiguration von weiteren Netzwerkgeräten	120
4.2.3	Zentrale IP-Adressverwaltung mit dem DHCP-Server	122
4.2.4	Zeroconf	129
4.3	Verwendung von Rechnernamen	129
4.3.1	Der Urtyp: Adressauflösung in der hosts-Datei	129
4.3.2	Der Domain Name Server (DNS) und seine Konfiguration	131
4.3.3	Einstellungen beim Client	141
4.4	Überprüfung der Erreichbarkeit und Namensauflösung von Hosts	143
4.4.1	Prüfung der Erreichbarkeit und Namensauflösung mit ping/ping6	143
4.4.2	Werkzeuge für Name-Server-Abfragen (nslookup, host, dig)	145
4.4.3	Mitschnitte von DNS-Abfragen mit Netzwerkdiagnoseprogrammen	146
4.5	Zentrale Netzwerkgeräte auf Sicherungs- und Vermittlungsebene	148
4.5.1	Bridges – Verbinden von Netzwerkteilen	148
4.5.2	Hubs – Sammelschiene für TP-Netze	149
4.6	Switches – Verbindungsknoten ohne Kollisionen	149
4.6.1	Funktionalität	150
4.6.2	Schleifen – Attentat oder Redundanz?	151
4.6.3	Verbindungen zwischen Switches (Link Aggregation, Port Trunking, Channel Bundling) ...	154

4.6.4	Virtuelle Netze (VLAN)	155
4.6.5	Switch und Sicherheit	157
4.6.6	Geräteauswahl	159
4.6.7	Anzeigen und Anschlüsse am Switch	160
4.6.8	Konfiguration eines Switches allgemein	161
4.6.9	Spanning Tree am Switch aktivieren	161
4.6.10	VLAN-Konfiguration von Switches	162
4.6.11	Konfiguration von Rechnern für tagged VLANs	164
4.7	Routing – Netzwerkgrenzen überschreiten	167
4.7.1	Gemeinsame Nutzung einer IP-Adresse mit PAT	170
4.7.2	Festlegen des Standard-Gateways	170
4.7.3	Routing-Tabelle abfragen (netstat)	171
4.7.4	Routenverfolgung mit traceroute	172
4.7.5	Route manuell hinzufügen (route)	172
4.7.6	Route löschen (route)	175
4.8	Multicast-Routing	176
4.9	Praxisübungen	177
4.9.1	Glasfasern	177
4.9.2	TP-Verkabelung	177
4.9.3	Switches	177
4.9.4	MAC- und IP-Adressen	177
4.9.5	Namensauflösung	178
4.9.6	Routing	178
4.9.7	Sicherheit im lokalen Netz	178
5	Steuer- und Fehlercodes mit ICMP und ICMPv6 übertragen	181
5.1	ICMP-Pakete (IPv4)	182
5.2	ICMPv6-Pakete	183
6	Datentransport mit TCP und UDP	187
6.1	Transmission Control Protocol (TCP)	187
6.1.1	Das TCP-Paket	187
6.1.2	TCP: Verbindungsaufbau	190
6.1.3	TCP: Transportkontrolle	190
6.1.4	TCP: Verbindungssabbau	192
6.2	Das User Datagram Protocol (UDP)	193
6.2.1	UDP: Der UDP-Datagram-Header	193
6.3	Nutzung von Services mittels Ports und Sockets	194
6.3.1	Sockets und deren Schreibweise	196

6.3.2	Übersicht über die Port-Nummern	196
6.3.3	Ports und Sicherheit	198
6.4	Die Firewall	200
6.4.1	Integration der Firewall in das Netzwerk	202
6.4.2	Regeln definieren	203
6.5	Der Proxyserver	206
6.5.1	Lokaler Proxyserver	208
6.5.2	Proxyserver als eigenständiger Netzwerkteilnehmer	208
6.5.3	Squid, ein Proxyserver	209
6.6	Port and Address Translation (PAT), Network Address Translation (NAT)	209
6.7	Praxis	212
6.7.1	Verbindungsaufbau zu einem Dienst mit geänderter Port-Nummer	212
6.7.2	Durchführen von Portscans zum Austesten von Sicherheitsproblemen	213
6.7.3	Schließen von Ports	214
6.8	Prüfungsfragen	215
6.8.1	TCP-Protokoll	215
6.8.2	Ports und Sockets	215
6.8.3	Firewall	216
7	Kommunikation und Sitzung	217
7.1	SMB/CIFS (Datei-, Druck- und Nachrichtendienste)	217
7.1.1	Grundlagen	218
7.1.2	Freigaben von Verzeichnissen und Druckern unter Windows	218
7.1.3	nmbd und smbd unter Linux/FreeBSD	219
7.1.4	Samba-Konfigurationsdatei smb.conf	219
7.1.5	Testen der Konfiguration	223
7.1.6	Aufnehmen und Bearbeiten von Samba-Benutzern	224
7.1.7	Starten, Stoppen und Neustart der Samba-Daemons	224
7.1.8	Netzlaufwerk verbinden (Windows 7)	225
7.1.9	Client-Zugriffe unter Linux/FreeBSD	226
7.1.10	Zugriffskontrolle mit smbstatus	228
7.1.11	Die net-Befehle für die Windows- Batchprogrammierung	229

7.2	Network-File-System (NFS)	230
7.2.1	Konfiguration des NFS-Servers	230
7.2.2	Konfiguration des NFS-Clients	233
7.3	HTTP für die Informationen im Internet	234
7.3.1	Grundlagen des HTTP-Protokolls	234
7.3.2	Serverprogramme	238
7.3.3	Client-Programme	239
7.3.4	Webbrowser und Sicherheit	240
7.4	Mail-Transport	241
7.4.1	Grundlagen des SMTP/ESMTP-Protokolls	241
7.4.2	Konfigurationshinweise	245
7.4.3	Anhänge von E-Mails, MIME, S/MIME	246
7.5	Secure Shell (SSH) und Secure Socket Layer (SSL), Transport Layer Security (TLS)	250
7.5.1	Secure Shell (SSH)	250
7.5.2	SSL und TLS	251
7.6	Praxisübungen	253
7.6.1	Konfiguration Samba-Server	253
7.6.2	NFS-Server	253
7.6.3	HTTP, Sicherheit	253
7.6.4	E-Mail	253
8	Standards für den Datenaustausch	255
9	Netzwerkanwendungen	259
9.1	Datenübertragung	259
9.1.1	File Transfer Protocol (FTP), Server	259
9.1.2	File Transfer Protocol (FTP), Clients	260
9.1.3	Benutzerkommandos für FTP- und SFTP-Sitzungen ...	261
9.1.4	Secure Copy (scp), Ersatz für Remote Copy (rcp)	263
9.1.5	SSHFS: entfernte Verzeichnisse lokal nutzen	264
9.2	SSH, SFTP und SCP: Schlüssel erzeugen zur Erhöhung der Sicherheit oder zur kennwortfreien Anmeldung	265
9.3	Aufbau eines SSH-Tunnels	267
9.4	Fernsitzungen	269
9.4.1	Telnet	269
9.4.2	Secure Shell (SSH), nur Textdarstellung	269
9.4.3	Display-Umleitung für X11-Sitzungen	270
9.4.4	SSH zur Displayumleitung für X11	271
9.4.5	Virtual Network Computing (VNC)	272

9.4.6	Nomachine (NX)	275
9.4.7	Remote Desktop Protocol (RDP)	277
10	Netzwerkpraxis	279
10.1	Planung von Netzwerken	279
10.1.1	Bedarf ermitteln	279
10.1.2	Ermitteln des Ist-Zustandes	281
10.1.3	Berücksichtigung räumlicher und baulicher Verhältnisse	282
10.1.4	Investitionssicherheit	282
10.1.5	Ausfallsicherheiten vorsehen	283
10.1.6	Zentrales oder verteiltes Switching	284
10.2	Netzwerke mit Kupferkabeln	286
10.2.1	Kabel (Cat. 5 und Cat. 7)	287
10.2.2	Anforderungen an Kabeltrassen und Installationskanäle	287
10.2.3	Dosen und Patchfelder	288
10.3	Netzwerke mit Glasfaserkabeln	290
10.3.1	Kabeltrassen für LWL-Kabel	291
10.3.2	Dosen und Patchfelder	292
10.3.3	Medienkonverter	292
10.3.4	LWL-Multiplexer	292
10.4	Geräte für Netzwerkverbindungen und -Dienste	293
10.4.1	Netzwerkkarten	293
10.4.2	WLAN-Router und -Sticks	294
10.4.3	Router	295
10.4.4	Switches	296
10.4.5	Printserver	297
10.4.6	Netzwerkspeicher (NAS)	299
10.4.7	Modems für den Netzzugang	299
10.5	Einbindung externer Netzwerkteilnehmer	302
10.6	Sicherheit	303
10.6.1	Abschottung wichtiger Rechner	304
10.6.2	Netzwerkverbindung mit Virtual Private Network (VPN)	306
10.6.3	WLAN sicher konfigurieren	308
10.6.4	SSH-Tunnel mit Putty aufbauen	309
10.7	Prüf- und Diagnoseprogramme für Netzwerke	312
10.7.1	Rechtliche Hinweise	312
10.7.2	Verbindungen anzeigen mit netstat	312

10.7.3	Hosts und Ports finden mit nmap	313
10.7.4	Datenverkehr protokollieren (wireshark, tcpdump) ...	316
10.7.5	Netzaktivitäten messen mit darkstat	319
10.7.6	Netzlast erzeugen mit fping	321
10.7.7	Weitere Einsatzmöglichkeiten von fping	321
10.7.8	Erreichbarkeit von Hosts prüfen mit ping/ping6	323
Anhang		325
A	Fehlertafeln	327
B	Auflösungen Prüfungsfragen	335
C	Netzwerkbegriffe kurz erklärt	339
Index		355

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 »eingepreßt«. 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 Netzwerkgerätehersteller 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 Netzwerksegmentes.

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
Präambel,	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 Synchronisieren 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 Address Resolution Protocol (ARP), IPv4

Mit dem *Address 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.

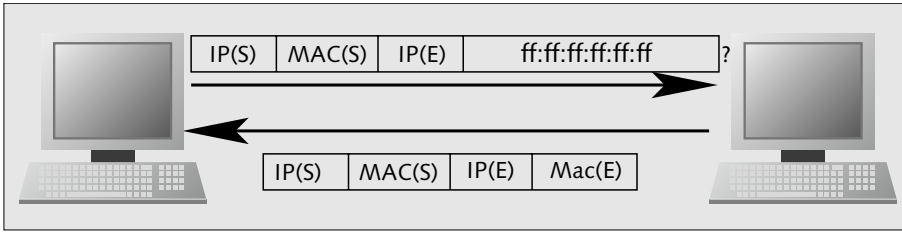


Abbildung 3.1 Schema ARP-Abfrage

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 Address 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 **Sicherheitsfunktionen**

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 Fahrge-stellnummer.

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. $34 \cdot 10^{38}$ 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 (ISPs)* sind in der Regel Mitglied in der RIR.

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

Einzigkeit 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 Netzwerkklassse 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 abzuhelpfen.

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 Beispiels.

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 Addressing (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 Netzwerk 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 Address 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 angeben.

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).

XX:XX:XX:XX:XX:XX:XX:XX			
Standort- Präfix	Teil- Netz- ID	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	reserviert	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:FFF::/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: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 Address 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 Addressing 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 »Besetztsymbol« 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 »Netzzlast« auf sich hat. Selbst für ein paar Byte brauchen Sie diesen ganzen Aufwand.

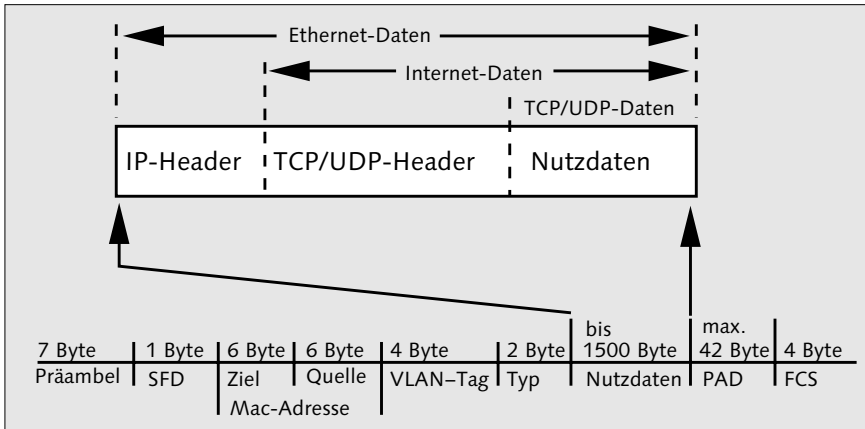


Abbildung 3.5 IP-Paket als Nutzlast des Ethernet-Frames

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.

Version	IHL	TOS	Länge	
Identifikation			Flags	Fragment Offset
TTL	Protokoll		Header-Prüfsumme	
Sender-IP-Adresse				
Ziel-IP-Adresse				
Optionen				Padding
Daten				

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.

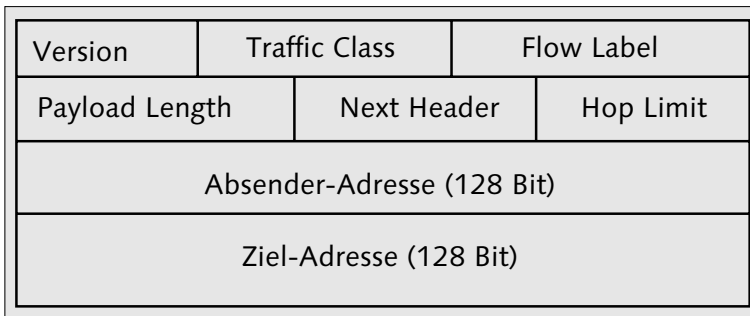


Abbildung 3.7 IPv6-Header

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 ICMPv6-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

/etc/defaults/nfs-common 231
/etc/defaults/nfs-kernel-server 231
/etc/exports 231
/etc/fstab 231, 234
/etc/host.conf 142
/etc/hosts.allow 232
/etc/hosts.deny 232
/etc/network 116
/etc/nsswitch.conf 142
/etc/rc.conf 118
/etc/resolv.conf 136
1000Base-LX 57
1000Base-SX 57
1000Base-T 33
100Base-FX 56
100Base-SX 56
100Base-TX 33
10BASE-5 29
10Base-5 31
10Base-FL 56
10Base-T 33
10GBase-ER 57
10GBase-LR 57
10GBase-LX4 57
10GBase-SR 57
10GBase-T 33
10Gigabit Media Independent Interface
→ 10G-MII
10G-MII 72
6to4-Adressen 100

A

Abmantler 41
Abschottung wichtiger Rechner 304
Active Directory 218
Address Resolution Protocol → ARP
Adressierung im Netzwerk
MAC-Adresse 75
Media Access Control 75
physikalische Adresse 75
Adressierung 19
Adressierung im Netzwerk 75
Hardware- und IP-Adressen 75

AES-Verschlüsselung 308
alive 323
Analog-Modem
Beschaffung 300
Anspießen 62
Anwendungsschicht/Application Layer
23–24
Anycast-Adressen 96
Anzeigen und Anschlüsse am Switch 160
Apache 238
APIPA 129
Arbeitsgruppen-Konfiguration 218
Arbeitsnetz 304
Architekturunabhängigkeit 20
ARP 78
arp 110
ARP-Broadcast 80
ARP-Cache 79
ARP-Spoofing 80
ARP-Spoofing erkennen 112
Attachment Unit Interface → AUI
Attachment Units Interface → AUI
Auflösungen Prüfungsfragen 335
Aufnehmen und Bearbeiten von
Samba-Benutzern 224
AUI 30, 72
Ausfallsicherheiten
Netzplanung 283
Außenmantel 58
Auto-MDI(X) 38
Autonomes System 169
avahi 129

B

Benutzerkommandos für FTP- und
SFTP-Sitzungen 261
Beschriftung von Kabeln 52
Bestandsbauten
Netzwerkplanung 282
Bestandsnetze
Netzplanung 287
Betriebssystemermittlung
nmap 315

Betriebsvereinbarung 304
bonjour 129
Border Gateway Protocol, BGP 169
BPDU 153
Brandabschnitt 288
Brandschott 288
Bridge 148
Bridge Protocol Data Unit → BPDU
Bridgedevice 149
Broadcast-Domänen 86
Broadcast-MAC-Adresse 76
browseable 222
Bündelader 58

C

Canonical Format Indicator 157
Carrier Sense Multiple Access/Collision
Detection → CSMA/CD
CGA 101
Cheapernet 31
Checkliste Ist-Zustand für Netzwerk-
planung 281
Checkliste Netzwerkplanung 279
Chipsatz, Netzwerkkarte 293
CIDR 86
CIFS 217
Classless Inter-Domain Routing → CIDR
Coatings 58
Common Internet File System → CIFS
Cookies 241
create mask 221
Crimpzange 45
Cross-over-Kabel 38–39
CSD 70
CSMA/CA 73
CSMA/CD 31, 73

D

darkstat 319
Darstellungsschicht/Presentation Layer
23
Datei-, Druck- und Nachrichtendienste
217
Dateiattribute 222
Dateiendung 255

Dateiformate 255
Dateityp 255
Datenaustausch
Standards 255
Datenpakete 18
Datenverkehr protokollieren 316
Default Router List 81
demilitarisierte Zone 201
Destination Cache 81
DHCP 122
dhcpd.conf 125
dhcpdump 127
DHCP-Server 122
Konfiguration 125
dig 146
directory mask 221
Display-Umleitung für X11-Sitzungen 270
DMZ 201
DNS 131
Domain Name Server → DNS
Domain-Name 132
Domänen-Prinzip 217
Dosenkörper 41
DSL-Modem
Beschaffung 300
Dual-Speed Hub 149
Duplicate Address Detection 102
Dynamic Host Configuration Protocol
→ DHCP
Dynamisches Routing 168

E

EDGE 70
EIA/TIA T568 A 37
EIA/TIA T568 B 37
Eigenschaften von Netzwerken
Adressierung 19
Fehlererkennung 19
Fehlerkorrektur 19
Flusssteuerung 19
Netzwerkprotokoll 18
paketorientiert 18
transaktionssichernde Maßnahmen 20
transparent 18
übertragungssichernde Methoden 20
verbindungslos 19
verbindungsorientiert 19

Eigenschaften von Netzwerken (Forts.)
Verbindungssteuerung 19
 Einbindung externer Netzwerk-
 teilnehmer 302
 Einwahlrechner 302
 elinks 239
 E-Mail-Anhänge 246
 Erreichbarkeit von Hosts prüfen 323
 Ersatzverbindung
 Switch 153
 ESMTP 241
 Ethernet-Frames 77
 Aufbau 77
 Ethernet-Pakete 77
 exim 241
 Extended Simple Mail Transport Protocol
 → ESMTP

F

Farbkennzeichnung/Adernfarbe 37
 FCS 78
 Fehlererkennung 19
 Fehlerkorrektur 19
 Fehlersuche 100BASE-T-Netz
 keine schnelle Verbindung möglich 327
 Fehlersuche DHCP
 Host bekommt keine Adresse zugewiesen
 327
 Fehlersuche im Kupfernetz
 Host ohne Verbindung 327
 Fehlersuche im LWL-Netz
 Host ohne Verbindung 327
 Fehlertafeln 327
 Ferrule 61
 File Transfer Protocol → FTP
 file-Kommando 255
 findsmb 226
 Firefox 239
 Firewall 200, 304
 Integration 202
 Firewall-Regeln 203
 allow 203
 block 203
 deny 203
 drop 203
 iptables 204
 pass 203

Firewall-Regeln (Forts.)
 reject 203
 Flags 106
 Flags in Multicast-Adressen 97
 Flow Label 107
 Flussteuerung 19
 fping 321
 FQDN 132
 Fragment-Offset 106
 freeSSHd 251
 Freigabe 218
 Freigaben von Verzeichnissen und
 Druckern unter Windows 218
 Fremdes Wartungspersonal 303
 FTP 259
 aktiver Modus 259
 passiver Modus 260
 Verbindung beenden 262
 FTP-Clients 260
 FTP-Server 259
 Fully Qualified Domain Name → FQDN
 Funkmodem
 Beschaffung 301

G

Gefälschte Frames 158
 Gemeinsame Nutzung einer IP-Adresse
 170
 Geräteauswahl
 Switch 159
 Gigabit Media Independend Interface
 → GMII
 Glasfaserabschnitte 65
 Glasfaser-Steckverbindungen 61
 Glasfaserverbindungen
 dauerhafte 60
 Glaskern 58
 Glasmantel 58
 Globale Unicast-Adressen 96
 GMII 72
 GPRS 70
 Group Identifier 98

H

Halbduplex 32
 Hardware-Firewall 200
 Header-Prüfsumme 106
 Herstellercode 75
 Hohlader 58
 Hop Limit 108
 host 145
 Host to Network 24
 Host-Anteil 85
 Hosts und Ports finden mit nmap 313
 hosts-Datei 129
 HSCD 70
 HSDPA 70
 HTML 234
 HTTP 234
 Apache 238
 Cookies 241
 elinks 239
 Firefox 239
 get 235
 head 235
 HTTP 234
 HTTP/1.0 234
 HTTP/1.1 234
 HTTP-Clients 239
 HTTP-Requests 235
 HTTPS 234
 HTTP-Statuscodes 236
 Iceweasel 239
 Internet Explorer 239
 Internet Information Services (IIS) 238
 Internet-Café 241
 Java/Java-Skript 240
 lighthttpd 238
 lynx 239
 Masterpasswort 241
 Opera 239
 post 235
 Sicherheit für Webbrowser 240
 Statuscode 235
 thttpd 238
 trace 235
 w3m 239
 HTTP-Serverprogramme 238
 Hubs 73, 149
 Hypertext Markup Language → HTML
 Hypertext Transfer Protocol → HTTP

I

Iceweasel 239
 ICMP 181
 ICMP freischalten 206
 ICMP-Meldungen 181
 ICMP-Pakete 181
 ICMP-Pakete (IPv4) 182
 ICMPv6 181
 ICMPv6-Nachrichten 81
 ICMPv6-Pakete 183
 Identifikation 106
 IEEE-Standards 28
 IETF 25
 ifconfig 110, 117
 IGMP 176
 IHL 106
 Interface-ID 95, 102
 interfaces 116, 221
 Intermediate System to Intermediate System Protocol, IS-IS 169
 Internet 24
 Internet Explorer 239
 Internet Group Management Protocol → IGMP
 Internet Information Services (IIS) 238
 Internetanwendungsserver 305
 Internet-Café 241
 Internetprotokoll 104
 Internetschicht/Internet Layer 24
 Intra Site Automatic Tunnel Addressing Protocol → ISATAP
 Intranet 24, 200
 Intranetzugang per Internet 302
 Inventur eines lokalen Netzwerkes
 nmap 314
 Inventur-Scan 315
 ip 117
 ip link show 110
 ip neigh 110
 IP-Adresse zuweisen 112
 IP-Adressen 82
 IP-Adressen setzen
 /etc/rc.conf 118
 Adresse zuweisen 112
 avahi 129
 Berechnung Subnetzmaske mit ipcalc 113
 bonjour 129
 Debian-Linux 116

IP-Adressen setzen (Forts.)

dhcpcd.conf 125
dhcpcdump 127
DHCP-Server 122
FreeBSD 118
ifconfig 117
ip 117
IP-Adresskonfiguration von weiteren Netzwerkgeräten 120
Linux 116
Netzplanung 112
Netzwerkkonfiguration von PCs 114
Windows 7 114
Zeroconf 129

ipcalc 113

ipconfig 110

IP-Protokoll 83

iptables 204

IPv4 78

IPv4-Adressen 84

IPv4-Header 105

IPv4-mapped IPv6-Adresse 99

IPv6 80

IPv6-Adressen 93

Adresstypen 96

Bestandteile 95

Präfixe 102

Regeln zur Adressbenutzung 103

Schreibweisen 94

IPv6-Header 107

IPv6-Kenndaten 94

IPv6-Loopback-Adresse 98

ISATAP 101

ISDN-Modem

Beschaffung 300

Ivestitionssicherheit

Netzwerkplanung 282

J

Java/Java-Skript 240

K

Kabelbelegung 36

Kabelkategorien 35

Kabel-Modem

Beschaffung 300

Kabelrinne 287

Kabeltrassen für LWL-Kabel 291

Kabeltrassen und Installationskanäle

Anforderungen 287

Kabelverbindungen prüfen 48

Klebetchnik 62

Klimatisierung 283

Koaxialkabel 29

Kollisionsbereich 150

Kollisionserkennung 73

Kollisionsvermeidung 73

Kommunikation 217

Kommunikationsschicht/Session Layer 23

Kompaktader 58

Konfiguration

Switch 161

Kryptografisch erzeugte Adressen 101

Kupferteknik

Netzplanung 286

L

L2TP 307

LACL 154

LACP 154

LAN 24

Laserstrahlen 64

Layer 2 Tunneling Protocol → L2TP

LC-Stecker 63

Leitungssuchgerätesatz 52

less 321

Lichtwellenleiter 54

Anspießen 62

Biegeradien 66

Bündelader 58

dauerhafte Glasfaserverbindungen 60

Eigenschaften 55

Ferrule 61

Glasfaser 54

Glasfaserkabel 58

Glasfaser-Steckverbindungen 61

Glaskern 66

Glasmantel 66

Gradientenindex 59–60

Hohlader 58

Kabel- und Leitungstester 67

Lichtwellenleiter (Forts.)
 Klebeteknik 62
 Kompaktader 58
 LC (LWL-Stecker) 63
 Monomode-Faser 58
 MTRJ (LWL-Stecker) 63
 Multimode-Faser 58
 Netzwerkstandards mit Glasfaserkabel
 56
 OM1 60
 OM2 60
 OM3 60
 OM4 60
 OS1 60
 Primärcoating 58
 Prüfen von LWL-Kabeln 67
 SC (LWL-Stecker) 63
 Schutz der Glasfasertechnik 66
 Schutzmaßnahmen bei LWL-Netzwerk-
 anlagen 65
 Schutzmaßnahmen vor Verletzungen
 durch Glasfaserteile 65
 Singlemode-Faser 58
 ST (LWL-Stecker) 62
 Stufenindex 59
 Stufenindexfasern 58
 Umgang mit LWL-Komponenten 64
 Vollader 58
 Vor- und Nachteile 55
 lighthttpd 238
 Link Aggregation 154
 Link Aggregation Control Layer → LACL
 Link Aggregation Control Protocols
 → LACP
 Link-local Unicast-Adressen 96
 Local Internet Registry 83
 local master 221
 Localhost 92, 130
 Logische Adressen 82
 Lokale Adressen 102
 Loopback-Adressen 92
 LSA 40
 LSA-Anlegewerkzeug 42
 LSA-Verbindung herstellen 43
 LTE 70
 LTE-Advanced 70
 LWL-Kabel
 Führung mit Stromleitungen 290
 LWL-Leitungstester 67

LWL-Multiplexer 292
 LWL-Nachteile 56
 LWL-Netzwerk-Anschlussdosen 292
 LWL-Patchfelder 292
 LWL-Vorteile 55
 lynx 239

M

MAC- und IP-Adresse 78
 MAC-Adressen 75, 109, 314
 Absender 77
 ändern 111
 arp 110
 ARP-Spoofing erkennen 112
 ifconfig 110
 ip neigh 110
 ipconfig 110
 MAC-Adresse ermitteln 109
 manuell setzen und ändern 112
 Setzen und Ändern von MAC-Adressen
 112
 Ziel 77
 Mail Transport Agent → MTA
 Mail User Agent → MUA
 Mail-Transport 241
 Content-Type-Eintrag 247
 CRAM-MD5 242
 EHLO 243
 E-Mail-Anhänge 246
 ESMTP-Protokoll 241
 exim 241
 Funktionsprüfung SMTP-Server 245
 HELO 243
 Kodierungen 247
 LOGIN 242
 MAIL FROM 243
 MIME 246
 MIME-Parts 247
 MS EXCHANGE 242
 MTA 241
 MUA 241
 multipart/mixed 248
 NTLM 242
 PLAIN 242
 postfix 241
 qmail 242
 QUIT 244

- Mail-Transport (Forts.)
 - RCPT TO* 244
 - RSET* 244
 - S/MIME* 246
 - SCRAM-SHA-1* 242
 - SMTP-Client* 243
 - SMTP-Protokoll* 241
 - SMTP-Relais* 245
 - SMTP-Server* 245
 - SSL* 242
 - Statuscodes* 244
 - text/html* 248
 - text/plain* 248
 - TLS* 242
- MAN 24
- Masterpasswort 241
- MAU 30
- MDI 38
- MDI-X 38
- Media Access Control 75
- Media Independend Interface → MII
- Medienkonverter 72, 292
- Medium Access Unit → MAU
- Metrik 169
- mgetty 302
- MII 72
- MIME 246
- MIME-Erweiterung 247
- Mobilfunknetze 70
- Modems für den Netzzugang
 - Beschaffung* 299
- Monomode-Faser 58
- Monomode-Glasfaser 58
- MS EXCHANGE 242
- MSTP 153
- MTA 241
- MTRJ-Stecker 63
- MUA 241
- Multicast-Adressen 96–97
- Multicast-Routing 176
- Multimode-Faser 58
- Multimode-Glasfasern 59
- Multiple Spanning Tree Protocol → MSTP
- NAPT 170
- NAS
 - Beschaffung* 299
- NAS-Box 120
- NAT 170, 209
- NAT/PAT 201
- NDP 80
- Neighbor Advertisement 81
- Neighbor Cache 82
- Neighbor Discovery Protocol → NDP
- Neighbor Solicitation 81
- net-Befehle für die Windows-Batch-
 - programmierung 229
- Netbios 217
- netbios name 221
- Netbios über TCP 217
- netstat 171, 200, 312
- Network Address Port Translation → NAPT
- Network Address Translation → NAT
- Network-File-System
 - /etc/defaults/nfs-common* 231
 - /etc/defaults/nfs-kernel-server* 231
 - /etc/exports* 231
 - /etc/fstab* 231, 234
 - /etc/hosts.allow* 232
 - /etc/hosts.deny* 232
 - Konfiguration des NFS-Clients* 233
 - Konfiguration des NFS-Servers* 230
 - zentrale Benutzerverwaltung* 230
- Network-File-System → NFS
- Netz- und Subnetzmaske 85
- Netzaktivitäten messen mit darkstat 319
- Netzlast erzeugen mit fping 321
- Netzlaufwerk verbinden (Windows 7)
 - 225
- Netzmaske 85
- Netzmaske berechnen 88
- Netzplanung 112
- Netzwerk-Anschlussdose 40
- Netzwerk-Anschlussdosens 288
- Netzwerkanteil 85
- Netzwerkanwendungen 259
 - authorized_keys* 266
 - cd* 262
 - Datenübertragung* 259
 - Fernsitzungen* 269
 - FTP* 259
 - FTP- und SFTP-Sitzungen* 261

N

named.conf 134, 140
 Name-Server-Abfragen 145

Netzwerkanwendungen (Forts.)

FTP-Client 260
get 262
id_rsa.pub 266
lpwd 262
ls 262
mget 262
mput 262
NX 275
nxclient 275
nxnode 275
nxserver 275
put 262
pwd 262
RDP 277
scp 263
SSH 265, 269, 271
SSHFS 264
ssh-keygen 266
SSH-Tunnel 267
VNC 272
vncserver 272
VNC-Sitzung 273

Netzwerkfestplatte

Beschaffung 299

Netzwerkgrenzen überschreiten 167

Netzwerkkarten 293

Netzwerkklassen 84

Netzwerkkonfiguration von PCs 114

Netzwerkplanung

Abhängigkeit von Kundendiensten 284
Anforderungen an Kabeltrassen und Installationskanäle 287
Ausfallsicherheiten vorsehen 283
Bausubstanz 282
Bedarf ermitteln 279
Berücksichtigung räumlicher und baulicher Verhältnisse 282
Bestandsnetz 287
Brandabschnitte 288
Brandmeldeanlage 282
Brandschott 288
CWDM 293
Denkmalschutz 282
Dosen und Patchfelder 288, 292
DWDM 293
Ermitteln des Ist-Zustandes 281
Funktionsausfall Switch 283
GBIC 292

Netzwerkplanung (Forts.)

Grundriss 282
Installationskanäle 287
Investitionssicherheit 282
Kabel (Cat. 5 und Cat. 7) 287
Kabelrinnen 287
Kabelschaden 283
Kabeltrasse 287
Kabeltrassen für LWL-Kabel 291
Klimatisierung 282–283
Leerrohre 283
LWL-Multiplexer 292
managbare Switches 285
Medienkonverter 292
minimale Biegeradien LWL 291
Netzwerke mit Glasfaserkabeln 290
Netzwerke mit Kupferkabeln 286
Neuinstallation 287
Potenzialunterschied 286
SFP 292
Spleißbox 291
Stromausfall 283
Stromversorgung 282
Switching, zentral oder verteilt 284
Telefonnetz 282
Trunking-Verbindungen 285
verteilte Unterbringung der Switches 284
VoIP 284
WWDM 293
XFP 292

Netzwerkprobleme 181

Netzwerkprotokollfamilie TCP/IP 20

Netzwerkschrank 40

Netzwerksegment 77

Netzwerksicherheit

Abschottung wichtiger Rechner 304
AES 308
allgemeine Maßnahmen 304
Arbeitsnetz 304
Betriebsvereinbarung 304
eigene Rechner 303
Firewall 304
Fremdes Wartungspersonal 303
Ignorieren von Firmware-Updates 303
Internetanwendungen 304
Internetanwendungsserver 305
IPSec 306
Kennwörter 303
L2TP 307

Netzwerksicherheit (Forts.)

- OpenVPN* 307
- PPTP* 307
- Proxyserver* 304
- Radius-Server* 308
- Schadsoftware* 303
- Sicherheitsprobleme* 303
- Sicherheitsregeln* 303
- Sicherheits-Updates* 303
- soziale Netzwerke* 303
- SSH-Tunnel mit Putty* 309
- SSL* 306
- Tunnel* 306
- Verteilen von Anwendungen* 305
- VPN* 306
- VPN-Router* 307
- Wartungsnetz* 305
- WLAN sicher konfigurieren* 308
- WLAN-Verschlüsselung* 308
- WPA2* 308
- Zugriffsregelungen* 304

Netzwerkspeicher

- Beschaffung* 299

Netzwerkstandards 27

- 10 Gigabit Ethernet* 33
- 1000Base-LX* 57
- 1000Base-SX* 57
- 1000Base-T* 33
- 100Base-FX* 56
- 100Base-SX* 56
- 100Base-TX* 33
- 10Base-2* 31
- 10BASE-5* 29
- 10Base-FL* 56
- 10Base-T* 33
- 10GBase-ER* 57
- 10GBase-LR* 57
- 10GBase-LX4* 57
- 10GBase-SR* 57
- 10GBase-T* 33
- AUI* 30
- Auto-MDI(X)* 38
- BNC* 31
- Cat. 1* 35
- Cat. 2* 35
- Cat. 3* 35
- Cat. 4* 35
- Cat. 5* 35
- Cat. 6* 35

Netzwerkstandards (Forts.)

- Cat. 7* 35
- CheaperNet* 31
- Crosskabel* 38
- Cross-over-Kabel* 39
- CSMA/CD* 31
- EIA/TIA-568B* 37
- Ethernet* 33
- Farbkennzeichnung/Adernfarbe* 37
- Fast Ethernet* 33
- Folienschirm* 34
- Geflecht- und Folienschirm* 34
- Geflechtschirm* 34
- Gigabit Ethernet* 33
- Glasfasernetzwerke* 56
- Halbduplex* 32
- IEEE-Standards* 28
- Kabelkategorien* 34
- Koaxialkabel* 29
- LSA-Verbindung herstellen* 43
- MAU* 30
- MDI* 38
- MDI-X* 38
- PoE* 54
- Quad Pair* 34
- RJ45* 32
- Thicknet* 29
- Thin Wire Ethernet* 30
- Transceiver* 30
- Twisted Pair* 34
- Twisted-Pair-Kabel* 32
- ungeschirmt* 34
- Verkabelungsbezeichnungen* 28
- Vollduplex* 32
- Western-Stecker* 32
- WLAN* 28
- Yellow Cable* 29

Netzwerktester 49

Netzzugangsschicht/Link Layer 24

Netzzugriff 211

Next Header 108

NFS 230

NFS-Client 233

NFS-Server 230

nmap 198, 213, 313

nmbd 219

Nomachine → NX

not alive 323

nslookup 145

Nutzdaten 78
 NX 275
 Free-Edition 275

O

OM1 (Faserkategorie) 60
 OM2 (Faserkategorie) 60
 OM3 (Faserkategorie) 60
 OM4 (Faserkategorie) 60
 Open Shortest Path First, OSPF 169
 OpenSSH 251
 OpenVPN 307
 Opera 239
 oping 324
 os level 221
 OS1 (Faserkategorie) 60
 OSI-Schichtenmodell 21
 Anwendungsschicht/Application 23
 Anwendungsschicht/Application Layer 23
 Darstellungsschicht/Presentation Layer 23
 Kommunikationsschicht/Session Layer 23
 physikalische Schicht/Physical Layer 22–23
 Sicherungsschicht/Data Link Layer 23
 Transportschicht/Transport Layer 23
 Vermittlungsschicht/Network Layer 23

P

Pad 78
 Padding 107
 Paketorientierung 18
 PAT 170, 209
 Patchfeld 39
 Patchfelder
 Netzplanung 288
 Patchkabel 39
 Payload Length 108
 personal Firewall 201
 Physikalische Adresse 75
 Physikalische Schicht/Physical Layer 23
 ping 143, 181, 323
 ping6 143, 323
 Plain SMB über TCP 217
 Planung von Netzwerken 279

Planungsfragen Netzwerk 279
 PLC 71
 PoE 54
 Point-to-Point Tunneling Protocol → PPTP
 Port and Address Translation → PAT
 Port Trunking 154
 Port-Nummern
 abweichende 212
 Übersicht 196
 Ports 194
 schließen 214
 Sicherheit 198
 Ports und Sockets 194
 /etc/services 196
 geschlossener Port 199
 netstat 199
 offener Port 199
 Port-Nummer 194
 Ports und Sicherheit 198
 Portscanner 198
 Port-Unreachable-Meldung 199
 registered Ports 196
 Schreibweise Sockets 196
 so wenig offene Ports wie möglich 200
 Standard-Port-Nummern 194
 Übersicht über die Port-Nummern 196
 UDP-Portscans 199
 well-known Ports 196
 Portscanner 198, 213
 Portscans
 Durchführung 213
 Port-Unreachable-Meldung 199
 postfix 241
 Potenzialunterschied 286
 Power over Ethernet → PoE
 Power-Line-Communication → PLC
 ppp 302
 PPTP 307
 Präambel 77
 Präfix 95
 Prefix List 82
 Primary Name-Server 133
 Printserver 120
 Beschaffung 297
 Private IPv4-Adressen 90
 Proxyserver 206, 304
 als eigenständiger Netzwerkteilnehmer 208
 Dedicated Proxyserver 207

Proxyserver (Forts.)
 generischer 207
 lokaler 208
 Reverse Proxyserver 207
 transparenter 207
 Prüf- und Diagnoseprogramme 312
 Prüfen LWL-Kabel 67
 Public-Key-Authentifizierung 251
 putty 251

Q

qmail 242
 Quarantäneverzeichnis 305

R

Radius-Server 308
 Rapid Spanning Tree Protocol → RSTP
 RARP 79
 Raumanbindung 283
 RDP 277
 Rechnernamen 129
 \$ORIGIN 137
 \$TTL 137
 /etc/host.conf 142
 /etc/hosts 130
 /etc/namedb/named.conf 135
 /etc/nsswitch.conf 142
 /etc/resolv.conf 136
 A 137
 AAAA 137
 autoritativ 133
 Caching-only-Name-Server 134
 CNAME 137
 DHCP-Server 141
 dig 146
 DNS 131
 Domain-Name 132
 Einstellungen beim Client 141
 FQDN 132
 host 145
 IN 137
 Konfigurationsdateien 132
 localhost 130
 MX 137
 Namensauflösung 129

Rechnernamen (Forts.)
 Name-Server-Abfragen 145
 NS 137
 nslookup 145
 ping 143
 ping6 143
 Primary Name-Server 133
 Prüfung Namensauflösung 143
 PTR 137
 resolv.conf 142
 Reverse-Zone 137
 Rückwärtsuche 138
 Secondary Name-Server 133
 Second-Level-Domain 132
 SOA-Record 136
 Subdomain 132
 tcpdump 147
 TLD 132
 Top-Level-Domain 132
 Vorwärtssuche 138
 Windows-Clients 141
 Rechtliche Hinweise 312
 Redirect Message 81
 Remote Desktop Protocol → RDP
 Repeater 72
 resolv.conf 142
 RESTful Webservices 235
 RFC-Dokumentenstatus 25
 RFCs 25
 Draft Standard 25
 Elective 25
 Experimental 25
 Informational 25
 Limited Use 26
 Not recommended 26
 Proposed Standard 25
 Recommended/Suggested 25
 Required 25
 Standard 25
 RG-58 31
 RJ45 32
 RJ-45-Stecker montieren 44
 Root-Bridge 153
 route 172
 Route löschen 175
 Route manuell hinzufügen 172
 Routenverfolgung 172
 Router
 Beschaffung 295

- Router Advertisement 81
- Router Solicitation 81
- Routing 167
 - Allgemeines* 168
 - autonomes System* 169
 - BGP* 169
 - Border Gateway Protocol* 169
 - dynamisches Routing* 168
 - Gemeinsame Nutzung einer IP-Adresse* 170
 - ICMP* 167
 - IGMP* 167
 - Intermediate System to Intermediate System Protocol* 169
 - IS-IS* 169
 - Metrik* 169
 - Multicast-Routing* 176
 - NAPT* 170
 - netstat* 171
 - Open Shortest Path First* 169
 - OSPF* 169
 - PAT* 170
 - RIP* 169
 - route* 172
 - Route löschen* 175
 - Route manuell hinzufügen* 172
 - Routenverfolgung mit traceroute* 172
 - Routing Information Protocol* 169
 - Routing-Tabelle abfragen* 171
 - Standard-Gateway* 169
 - Standard-Gateway festlegen* 170
 - Standard-Route* 169
 - Standard-Router* 169
 - statisches Routing* 168
- Routing Information Protocol, RIP 169
- Routing-Tabelle abfragen 171
- RSTP 153
- Rückwärtsuche 138

S

- S/MIME 246
- Safari 239
- Samba-Konfigurationsdatei 219
 - global* 219
 - homes* 219
 - interfaces* 220
 - local master* 220

- Samba-Konfigurationsdatei (Forts.)
 - nethbios name* 220
 - printers* 220
 - profiles* 220
 - security* 220
 - shares* 220
 - workgroup* 220
- Schadsoftware 303
- Schirmgeflecht 41
- Schleifen
 - Switch* 151
- Schleifstaub 65
- Schluckwiderstand 29
- Schneid-Klemmtechnik 40–41
- Schutz der Glasfasertechnik 66
- Scope-Feld 98
- scp 263, 265
- SC-Stecker 63
- Secondary Name-Server 133
- Second-Level-Domain 132
- Secure Copy → scp
- Secure Neighbor Discovery 101
- Secure Shell → SSH
- Server Message Block → SMB
- SFD 77
- SFTP 265
- Share 218
- Shell-Skript
 - fping* 321
- Sicherheitsprobleme 213, 303
- Sicherheitsregeln 303
- Sicherheits-Updates 303
- Sicherungsschicht/Data Link Layer 23
- Simple Mail Transport Protocol → SMTP
- Singlemode-Faser 58
- Site-local Unicast-Adressen 102
- Sitzung 217
- SMB 217
- smb.conf 219
- SMB/CIFS 217
 - Active Directory* 218
 - Arbeitsgruppen-Konfiguration* 218
 - Aufnehmen und Bearbeiten von Samba-Benutzern* 224
 - CIFS* 217
 - Client-Zugriffe unter Linux/FreeBSD* 226
 - Dateiattribute* 222
 - Domänen-Prinzip* 217
 - findsmb* 226

- SMB/CIFS (Forts.)
 - Freigaben von Verzeichnissen und Druckern unter Windows* 218
 - Grundlagen* 218
 - Linux/FreeBSD* 219
 - net-Befehle für Windows* 229
 - Netbios* 217
 - Netbios über TCP* 217
 - Netzlaufwerk verbinden (Windows 7)* 225
 - nmbd* 219
 - Plain SMB über TCP* 217
 - Samba-Konfigurationsdatei* 219
 - Share* 218
 - SMB* 217
 - smb.conf* 219
 - smbclient* 226
 - smbd* 219
 - smbpasswd* 224
 - smbstatus* 228
 - Starten, Stoppen und Neustart der Samba-Daemons* 224
 - Testen der Konfiguration* 223
 - testparm* 223
 - User* 218
 - Verbindungsaufbau in der GNOME-Oberfläche* 228
- smbclient 226
- SMB-Client-Zugriffe unter Linux/FreeBSD 226
- smbd 219
- smbpasswd 224
- smbstatus 228
- SMTP 241
- SMTP-Auth 242
- SMTP-Client 243
- SMTP-Server
 - Konfiguration* 245
- SOA-Record 136
- Sockets 194, 196
- Soziale Netzwerke 303
- Spanning Tree am Switch aktivieren 161
- Spanning Tree Protocol → STP
- Squid 209
- SSH 250, 265, 269
 - Anwendung* 251
 - Displayumleitung* 271
 - Fernsitzung* 269
 - Schlüssel erzeugen* 265
- SSHFS 264
- SSH-Key 251
- SSH-Tunnel 267
 - Aufbau* 267
- SSH-Tunnel mit Putty aufbauen 309
- SSL 251
- SSL Alert Protocol 252
- SSL Application Data Protocol 252
- SSL Change Cipher Specification Protocol 252
- SSL Handshake Protocol 252
- SSL Record Protocol 251
- Standard-Gateway 169
- Standard-Gateway festlegen 170
- Standard-Route 169
- Standard-Router 169
- Starten, Stoppen und Neustart der Samba-Daemons 224
- Stateful-Packet-Inspection 201
- Statisches Routing 168
- Statuscode 235
- Store and Forward-Bridging 149
- STP 152
 - Missbrauch* 157
- ST-Stecker 63
- Stufenindexfasern 58
- Subdomain 132
- Subnet-ID 95
- Subnetzmaske berechnen 113
- Switch 149
 - Angriffspunkte* 157
 - Anzeigen und Anschlüsse* 160
 - CFI* 157
 - dynamisches VLAN* 157
 - Ersatzverbindung* 153
 - Ersteinrichtung* 161
 - Funktionalität* 150
 - Geräteauswahl* 159
 - Kollisionsbereich* 150
 - Konfiguration* 161
 - LACL* 154
 - LACP* 154
 - Link Aggregation* 154
 - MSTP* 153
 - paketbasiertes VLAN* 155
 - Port Trunking* 154
 - portbasiertes VLAN* 155
 - Rechnerkonfiguration für tagged VLAN* 164

Switch (Forts.)
Root-Bridge 153
RSTP 153
Schleifen 151
Spanning Tree aktivieren 161
statisches VLAN 157
STP 152
tagged VLAN 155
TPID 157
Verbindungsabbrüche 153
VID 157
Virtuelle Netze 155
VLAN 155
VLAN-Konfiguration 162, 164–165, 167
zentrale Unterbringung 284
Switch, Beschaffung 296
Switches
verteilte Unterbringung 284

T

Tag Protocol Identifier 157
Tagged VLAN 155
Rechnerkonfiguration 164
TCP 187
TCP/IP-Referenzmodell 21
Anwendungsschicht/Application Layer 24
Internetschicht/Internet Layer 24
Netzzugangsschicht/Link Layer 24
Transportschicht/Transport Layer 24
TCP-Datagramm 187
tcpdump 147, 317
TCP-Paket
ACK 189
Aufbau 187
FIN 189
PSH 189
RST 189
SYN 189
URG 189
Window-Size 189
TCP-Pakete 187
TCP-Transportkontrolle 190
TCP-Verbindungssabbau 190, 192
Technische Anbindung 72
Teilsegmente 88
Teredo-Adressen 101
testparm 223

Thicknet 29
Thin Wire Ethernet 30
thttpd 238
TLD 132
TLS 251
Top-Level-Domain 132
Top-Level-Domain → TLD
TOS 106
TP-Netze
Crimpzange 45
Dosenkörper 41
Leitungssuchgeräte 53
LSA 40–41
LSA-Anlegewerkzeug 42
Netzwerk-Anschlussdose 40
Netzwerktester 49
PoE 54
Prüfen der Kabelverbindung 48
RJ45-Stecker montieren 44
Schneid-Klemmtechnik 40–41
traceroute 172
Traffic Class 107
Transaktionssicherung 20
Transceiver 30
Transmission Control Protocol → TCP
Transportschicht/Transport Layer 23–24
Trunking-Port, ungesicherter 157
Trunking-Verbindungen 285
TTL 106
Tunnel 201
Tunnel-Adressen 100
Twisted-Pair-Kabel
Aufbau 33
Typ 78

U

Überlauf
Switch 157
Überprüfung Namensauflösung von Hosts
143
Übertragungssicherung 20
UDP 193
UDP-Datagram-Header 193
UDP-Lite 194
UDP-Portscans 199
Umgang mit Glasfasertechnik 64
UMTS 70

Unicast-Adressen 96
 Unique-local Unicast-Adressen 102
 Unspezifizierte Adresse 99
 USB-WLAN-Stick 294
 User 218
 User Datagram Protocol → UDP

V

Verbinden von Netzwerkteilen 148
 Verbindungen anzeigen mit netstat 312
 Verbindungsaufbau
 zu einem Dienst mit geänderter
 Port-Nummer 212
 verbindungslos 19
 verbindungsorientiert 19
 Verbindungssteuerung 19
 Verkabelungsbezeichnungen 28
 Verkabelungstechnik 283
 Vermittlungsschicht/Network Layer 23
 Verschlüsselung von Datenübertragungen
 und Fernsitzungen
 Authentifizierung 251
 SSH 250
 SSH, praktische Anwendung 251
 SSH-Key 251
 SSL 251
 SSL Alert Protocol 252
 SSL Application Data Protocol 252
 SSL Change Cipher Specification Protocol
 252
 SSL Handshake Protocol 252
 SSL Record Protocol 251
 TLS 251
 Verschlüsselungsarten 251
 Version 106
 Virtual Network Computing → VNC
 Virtual Private Network → VPN
 Virtuelle Netze 155
 VLAN 77, 155
 dynamisches 157
 paketbasiert 155
 portbasiert 155
 statisches 157
 VLAN Identifier 157
 VLAN-Konfiguration
 FreeBSD 164
 Linux 165

VLAN-Konfiguration (Forts.)
 Windows 167
 VLAN-Konfiguration von Switches 162
 VLAN-Tag 77, 157
 VNC 272
 VNC-Desktop 274
 vncserver 272
 Vollader 58
 Vollduplex 32
 Vollduplex-Betrieb, Switch 150
 Vorwärtssuche 138
 VPN 306
 VPN-Router 307

W

w3m 239
 WAN 24
 Wartungsnetz 305
 Webbrowser und Sicherheit 240
 WebDAV 235
 Wechsel der Benutzerkennwörter 304
 Weitere reservierte IPv4. Adressen 93
 Western-Stecker 32
 wins support 221
 Wireshark 316
 WLAN 28, 68
 WLAN sicher konfigurieren 308
 WLAN-Router 294
 WLAN-Standards 69
 WLAN-Stick 294
 WLAN-Zugangsgerät 149
 workgroup 220–221
 WPA2-Verschlüsselung 308

Y

Yellow Cable 29

Z

Zentrale Datenhaltung 299
 Zeroconf 90, 129
 Zonendatei
 Recordtyp 137
 Zugdosen 283

Zugriff auf eine Freigabe unter GNOME 228
 Zugriffsregelungen 304
 Zugriffsverfahren 73
 6to4-Adressen 100
 Adresstypen des IPv6 96
 All-Zero-Adresse 99
 Anycast-Adressen 96
 ARP 78
 ARP-Broadcast 80
 ARP-Cache 79
 ARP-Spoofing 80
 Bestandteile von IPv6-Adressen 95
 Broadcast-Domänen 86
 Broadcast-MAC-Adresse 76
 Caches des NDP 81
 CGA 101
 CIDR 86
 Clear-to-Send-Signal 73
 CSMA/CA 73
 CSMA/CD 73
 Duplikate IP Address Detection 80
 Ethernet-Frames 77
 Ethernet-Pakete 77
 Globale Unicast-Adressen 96
 Group Identifier 98
 Herstellercode 75
 Host-Anteil 85
 hosts-Datei 129
 ICMPv6-Nachrichten 81
 Internetprotokoll 104
 IPv4 78
 IPv4-Adressen 84
 IPv4-Header 105
 IPv4-mapped IPv6-Adresse 99
 IPv6 80
 IPv6-Adressen 93
 IPv6-Header 107
 IPv6-Loopback-Adresse 98
 JAM-Signal 73
 Kenndaten des IPv6 94
 Knoten 80
 Kollisionserkennung 73

Zugriffsverfahren (Forts.)
 Kollisionsvermeidung 73
 kryptografisch erzeugte Adressen 101
 Link-local Unicast-Adressen 96
 Local Internet Registry 83
 Localhost 92
 logische Adressen 82
 Lokale Adressen 102
 Loopback-Adressen 92
 MTA 241
 Multicast-Adressen 97
 Nachrichtentypen des NDP 81
 NDP 80
 Neighbor Advertisement 80
 Neighbor Solicitation 80
 Neighbor Unreachability Detection 80
 Netzmaske 85
 Netzmaske berechnen 88
 Netzwerkanteil 85
 Netzwerkklasse 84
 Netzwerksegment 77
 Präfixe von IPv6-Adressen 102
 Private IPv4-Adressen 90
 RARP 79
 Regeln zur Adressbenutzung 103
 Request-to-send-Signal 73
 reservierte IPv4- Adressen 93
 RIPE NCC 83
 Schreibweisen von IPv6-Adressen 94
 Scope-Feld 98
 Secure Neighbor Discovery 101
 Site-local Unicast-Adressen 102
 Subnetzmaske 84
 Teredo-Adressen 101
 Tunnel-Adressen 100
 Unicast-Adressen 96
 Unique-local Unicast-Adressen 102
 unspezifizierte Adresse 99
 Unterteilung von Netzen 85
 virtuelle Netzwerke 77
 VLAN 77
 VLAN-Tag 77
 Zeroconf 90